Question #1 *Topic 1*

Your company has a Microsoft 365 ES subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment.
You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
✑ Identify unused personal data and empower users to make smart data handling decisions.
✑ Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
✑ Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?

A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

Suggested Answer: *C*
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:
Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.
Incorrect:
Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the day for uninterrupted, individual work.
Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export content that's responsive to your organization's internal and external investigations.
Reference:
https://docs.microsoft.com/en-us/privacy/priva/risk-management

Community vote distribution
C (100%)

e72726b 2 weeks, 5 days ago
Selected Answer: C
Questions have been updated - recently took exam and around 80% of the questions on it are in here.
upvoted 3 times

nocenta 2 months, 1 week ago
The questions may be updated, based on the new developments that have emerged in the sector: the main sections of the exam, 4 in total, are the same, I checked the official study guide of the exam, but within each individual section there have been changes, as you can verify by reading the "change log" section published in the official study guide of the exam: https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/sc-100
upvoted 1 times

nocenta 2 months, 2 weeks ago
Selected Answer: C
Hello, 63 questions in total, 140 minutes of time, 5 questions from the case study and 3 questions from the series that concerns the same scenario; at least 5 questions outside of examtopics, but this collection is still valid. Keep in mind that from April 21st this exam will be updated
upvoted 2 times

hadilyounis 2 months, 1 week ago
update how?
upvoted 2 times

Exam2us 3 months, 1 week ago
Selected Answer: C
Admin please update the exam questions. 90% of them are outdated. I only saw 10% of given questions appear in my exam.

upvoted 3 times

424ede1 3 months, 1 week ago

Is that true? even with contributor access??

upvoted 2 times

vdnh00 3 months, 3 weeks ago

Selected Answer: C

Took the exam today, and since this is the first question in this dumb I am providing my feedback here.
For this exact question, this was in the exam, so this is not outdated. Generally this dumb is covering every topic, even the Global secure access, so if you read the questions, check the answers and you are familiar the Azure Well-Architected Framework, RaMP, MCRA and SAF you are good to go. In real word you need to check the documentation on a regular basis anyway

upvoted 1 times

Praker 5 months, 1 week ago

Selected Answer: C

Outdated questions. More than 70% of the exam questions are missing.

upvoted 3 times

subhasht1 5 months, 2 weeks ago

Selected Answer: C

there are many new questions, please prepare well ..

upvoted 1 times

bareeee 5 months, 2 weeks ago

Do the questions/answers vary a lot, or are they similar and by studying these can we deduce? :(

upvoted 1 times

Praker 5 months, 1 week ago

Around 30% questions are same.

upvoted 1 times

bareeee 6 months ago

Selected Answer: C

In December 2024, have the questions changed a lot, or is this questionnaire up to date?

upvoted 1 times

d401c0d 9 months ago

Are these questions valid still?

upvoted 1 times

awsace 8 months, 1 week ago

I got quite a few new questions. I strongly recommend you to go through Microsoft's free test exam as well and make sure that you really understand the questions and answers.

upvoted 2 times

TheMCT 9 months, 1 week ago

Selected Answer: C

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:

Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.

upvoted 4 times

zellck 9 months, 1 week ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/privacy/priva/risk-management
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:
- Detect overexposed personal data so that users can secure it.

- Spot and limit transfers of personal data across departments or regional borders.
- Help users identify and reduce the amount of unused personal data that you store.

upvoted 2 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/privacy/priva/risk-management-policy-data-minimization
Data minimization policies focus on the age of your content and how long it has been since it was last modified. Monitoring for personal data that's still being retained in older, unused content can help you better manage your stored data and reduce risks.

Privacy Risk Management allows you to create policies to monitor data that hasn't been modified within a timeframe that you select. When a policy match is detected, you can send users email notifications with remediation options include marking items for deletion, notifying content owners, or tagging items for further review.

upvoted 1 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/privacy/priva/risk-management-notifications
Sending notifications to users can be an important component in helping your organization meet its privacy goals. The notifications are designed to:
- Bring immediate awareness to users when their actions could expose personal data to privacy risks.
- Provide remediation methods directly within the emails, so that users can take swift action to protect data at risk.
- Direct users to your organization's privacy guidelines and best practices.

Informing users of potential issues in the moment, and empowering them to remediate issues and refresh their skills, can be powerful tools for building sound data handling practices across your organization.

upvoted 1 times

AJ2021 9 months, 1 week ago

Selected Answer: C

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:

Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.

https://learn.microsoft.com/en-us/privacy/priva/risk-management

upvoted 4 times

fchahin 2 years, 2 months ago

Correct answer is C

upvoted 1 times

Einstein2 2 years, 3 months ago

Microsoft Priva is the correct answer

upvoted 1 times

rmafnc 2 years, 4 months ago

Microsoft Viva Insights is a solution that can enhance privacy management in a Microsoft 365 environment. Viva Insights provides employees with insights and guidance on how they are using collaboration tools, such as Microsoft Teams, to handle personal data. This can help employees make smart data handling decisions and minimize privacy risks. Viva Insights can also provide notifications and guidance when personal data is sent in Teams, helping to ensure compliance with privacy regulations. Additionally, Viva Insights can provide recommendations for mitigating privacy risks, further enhancing privacy management within the working environment.

upvoted 1 times

God2029 2 years, 5 months ago

Require (Enterprise Mobility + Security E3, Office E3, or Microsoft 365 E3 or E5 license) to purchase any compliance and data governance solutions.

Difference between Priva and Purview

Key features of Microsoft Priva Privacy Risk Management is to Assess your organization's privacy posture.
how much personal data exists in the environment, where it's located, how it moves, and the privacy risks detected.

Microsoft Purview automates data discovery by providing data scanning and classification for assets across your data estate. Metadata and descriptions of discovered data assets are integrated into a holistic map of your data estate.

upvoted 1 times

⊟ **TJ001** 2 years, 6 months ago

Correct Answer

upvoted 1 times

Question #2 *Topic 1*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort.
What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Event Hubs

C. Azure Functions apps

D. Azure Logics Apps

Suggested Answer: *D*
The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.
Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.
Incorrect:
Not C: Using Azure Functions apps would require more effort.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Community vote distribution
D (100%)

zellck Highly Voted 👍 9 months, 1 week ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

This feature can trigger consumption logic apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs. You'll also learn how to create logic apps using Azure Logic Apps.
upvoted 7 times

AJ2021 Most Recent 9 months, 1 week ago
Selected Answer: D
Workflow automation feature of Microsoft Defender for Cloud can trigger consumption Logic Apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs. To do this you would create a Logic App using Azure Logic Apps.
upvoted 2 times

fchahin 2 years, 2 months ago
S is the correct answer
upvoted 1 times

awssecuritynewbie 2 years, 4 months ago
It says logics app ... i know what it means but come one Microsoft
upvoted 1 times

TJ001 2 years, 6 months ago

Workflow Automation/Playbook (both in Sentinel and Defender for Cloud) requires Logic App

Answer D

upvoted 1 times

Aerocertif 2 years, 7 months ago

D is correct

upvoted 1 times

Just2a 2 years, 7 months ago

D is correct

upvoted 1 times

simonseztech 2 years, 9 months ago

Selected Answer: D

Correct

upvoted 3 times

tester18128075 2 years, 9 months ago

d - logic apps

upvoted 3 times

InformationOverload 2 years, 9 months ago

Selected Answer: D

Correct.

upvoted 1 times

HardcodedCloud 2 years, 9 months ago

Correct. Logic app is required for Workflow automation creation

upvoted 3 times

prabhjot 2 years, 10 months ago

yes logic app

upvoted 2 times

PlumpyTumbler 2 years, 10 months ago

Selected Answer: D

Yes. Logic Apps.

upvoted 3 times

Question #3 *Topic 1*

Your company is moving a big data solution to Azure.
The company plans to use the following storage workloads:
✑ Azure Storage blob containers
✑ Azure Data Lake Storage Gen2

Azure Storage file shares -
▪
✑ Azure Disk Storage
Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Storage file shares

B. Azure Disk Storage

C. Azure Storage blob containers

D. Azure Data Lake Storage Gen2

Suggested Answer: *CD*
C: Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.
You can scope access to Azure blob resources at the following levels, beginning with the narrowest scope:
* An individual container. At this scope, a role assignment applies to all of the blobs in the container, as well as container properties and metadata.
* The storage account.
* The resource group.
* The subscription.
* A management group.
D: You can securely access data in an Azure Data Lake Storage Gen2 (ADLS Gen2) account using OAuth 2.0 with an Azure Active Directory (Azure AD) application service principal for authentication. Using a service principal for authentication provides two options for accessing data in your storage account:
A mount point to a specific file or path

Direct access to data -
Incorrect:
Not A: To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS and then set the required domain properties on the storage account. To register your storage account with AD DS, create an account representing it in your AD DS.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

Community vote distribution
CD (75%) AD (25%)

WRITER00347 Highly Voted 9 months, 1 week ago
The two storage workloads that support authentication by using Azure Active Directory (Azure AD) are:

A. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Explanation:

Azure Storage file shares and Azure Data Lake Storage Gen2 both support authentication using Azure AD. Azure Disk Storage and Azure Storage blob containers do not currently support Azure AD authentication.

upvoted 12 times

syedaquib77 Highly Voted 9 months, 1 week ago

Selected Answer: CD

Azure Files supports identity-based authentication for Windows file shares over SMB using three methods.

On-premises AD DS authentication:

Azure AD DS authentication:

Azure AD Kerberos for hybrid identities:

Which means the answer C & D is correct.

upvoted 5 times

samsam5136431 Most Recent 1 week, 1 day ago

Selected Answer: AC

The answer is ACD

upvoted 1 times

Gagi79 2 months ago

Selected Answer: CD

Azure File Shares do support authentication by using Azure Active Directory (Azure AD) Domain Services. This allows you to mount a file share on-premises or in the cloud with the SMB protocol using Azure AD credentials. However, it's important to note that this feature is currently only supported with Azure AD Domain Services and not with Azure AD alone

upvoted 1 times

Jawa 5 months, 2 weeks ago

Selected Answer: CD

C. Azure Storage blob containers

D. Azure Data Lake Storage Gen2

upvoted 1 times

dsatizabal 5 months, 3 weeks ago

Selected Answer: CD

In 2025 the options may have changed, according to this:

https://learn.microsoft.com/en-us/azure/storage/common/authorize-data-access?tabs=files-rest

Files support EntraID not only with AD DS, there's a REST option that allows MI with EntraID, Also, this article:

https://docs.azure.cn/en-us/virtual-machines/managed-disks-overview

shows that Azure MANAGED disks (not sure if the managed may make any difference) supports RBAC, so I feel all options are valid and this question is pointless today.

upvoted 1 times

> **AWSPro24** 5 months, 1 week ago
>
> It does not say this. It specifically says the opposite. "Microsoft Entra ID Supported with Microsoft Entra Domain Services for cloud-only, or Microsoft Entra Kerberos for hybrid identities. "
>
> upvoted 1 times

dc864d4 8 months, 1 week ago

Blob Storage, File Shares, and Data Lake Storage Gen2 all support Entra ID authentication, this question is deprecated. Thank you.

upvoted 3 times

> **grimrodd** 7 months, 2 weeks ago
>
> I agree. To authenticate to Azure file shares you can enable Entra ID Domain Services.
>
> upvoted 1 times

Dan91 8 months, 1 week ago

Selected Answer: CD

Both Blob and Azure Data Lake storage support Azure RBAC for authorisation, therefore I would go with C and D

https://learn.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction#:~:text=The%20Azure%20Data%20Lake%20Storage%20access%20control%20model%20supports%20both%20Azure%20role%2Dbased%20acces

https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory#:~:text=Authorize%20access%20to%20blobs%20using%20M

upvoted 1 times

danb67 1 year, 1 month ago

C&D. I have literally just done this in production. I provided access for a service principal to access an azure storage blob container. Azure Data Lake Storage Gen2 is built on top of Azure Blob storage and extends its capabilities and also supports AD authentication.

upvoted 1 times

HCL 1 year, 2 months ago

Selected Answer: CD

Files support Azure AD Domain Services and not Azure AD

upvoted 2 times

SJHCI 1 year, 2 months ago

Selected Answer: AD

The correct answers are Azure Storage File Shares and Azure Data Lake Storage Gen2. Azure Disk Storage and Azure Storage Blob Containers don't support Azure AD authentication.

upvoted 1 times

sehlohomoletsane 1 year, 4 months ago

Selected Answer: AD

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable

upvoted 1 times

Tony416 9 months, 1 week ago

The question doesn't mention AD AD (AKA AD On-prem) but Entra ID. So, the correct answer is CD. I just wanted to let you know that you provided a link to an article related to AD DS.

upvoted 1 times

Murtuza 1 year, 5 months ago

Selected Answer: CD

C and D are the correct choice

upvoted 1 times

deposros 2 years, 2 months ago

i think c and d should be assumed to be correct

upvoted 3 times

fchahin 2 years, 2 months ago

C and D is the correct answer, I agree

upvoted 1 times

loverboz 2 years, 3 months ago

Selected Answer: AD

he two storage workloads that support authentication by using Azure Active Directory (Azure AD) in the given scenario are:

A. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Both Azure Storage file shares and Azure Data Lake Storage Gen2 support authentication through Azure AD. Azure Storage blob containers and Azure Disk Storage do not natively support authentication through Azure AD. However, Azure Disk Storage can be integrated with Azure AD using Managed Service Identity (MSI) to authenticate to other Azure services that support Azure AD.

Therefore, the correct answers are Azure Storage file shares and Azure Data Lake Storage Gen2.

upvoted 3 times

OCHT 2 years, 3 months ago

Selected Answer: AD

To summarize, the correct answers to the original question are A) Azure Storage file shares and D) Azure Data Lake Storage Gen2. Both Azure Storage file shares and Azure Data Lake Storage Gen2 support authentication using Azure Active Directory (Azure AD).

Azure Storage blob containers also support authentication using Azure AD, as pointed out in one of your previous messages. Therefore, the correct answers could be A) Azure Storage file shares and C) Azure Storage blob containers, or A) Azure Storage file shares and D) Azure Data Lake Storage Gen2.

The statement "To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS" is incorrect.

To enable Azure Active Directory Domain Services (AD DS) authentication over SMB for Azure file shares, you need to create an AD DS domain, and then join your Azure file shares to the AD DS domain. After you have completed these steps, you can use Azure AD DS to manage and authenticate users and groups for access to the Azure file shares.

upvoted 2 times

Holii 2 years ago

Azure AD DS =/= Azure AD.

It's impossible to sync a computer account directly to an Azure AD identity (without the placement of an AD DS or Azure AD DS to recognize the machine). Therefore, Azure Storage file shares cannot be authenticated strictly through Azure AD.

upvoted 5 times

Question #4 *Topic 1*

HOTSPOT -

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII).

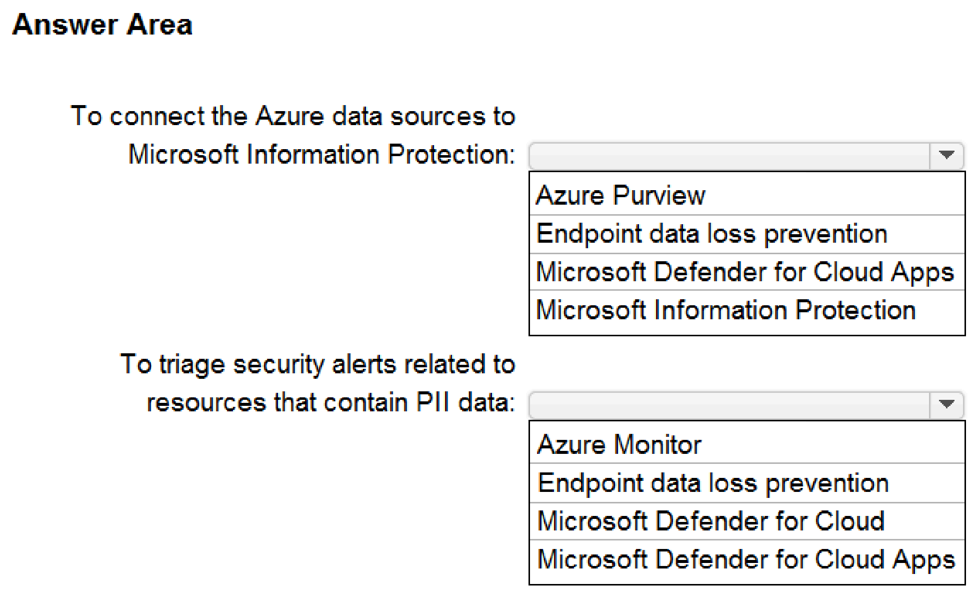
The company plans to use Microsoft Information Protection for the PII data store in Azure.

You need to recommend a solution to discover PII data at risk in the Azure resources.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

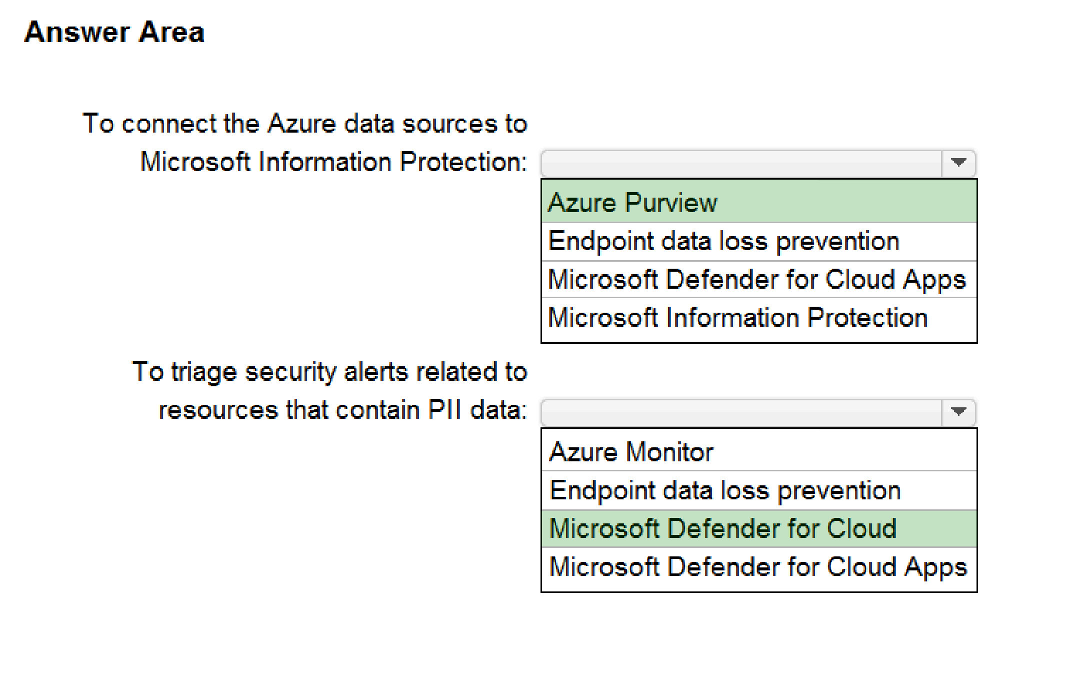
To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Suggested Answer:



Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- [✓ Azure Purview]
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- [✓ Microsoft Defender for Cloud]
- Microsoft Defender for Cloud Apps

Box 1: Azure Purview -

Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data.

Microsoft Purview allows you to:

Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

Enable data curators to manage and secure your data estate.

Empower data consumers to find valuable, trustworthy data.

Box 2: Microsoft Defender for Cloud

Microsoft Purview provides rich insights into the sensitivity of your data. This makes it valuable to security teams using Microsoft Defender for

Cloud to manage the organization's security posture and protect against threats to their workloads. Data resources remain a popular target for malicious actors, making it crucial for security teams to identify, prioritize, and secure sensitive data resources across their cloud environments. The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.
References:
https://docs.microsoft.com/en-us/azure/purview/overview
https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

tester18128075 Highly Voted 👍 2 years, 9 months ago
Purview and Defender for cloud
upvoted 21 times

ServerBrain Highly Voted 👍 1 year, 10 months ago
The answer is correct, but it's the first time I know about Azure Purview, I thought it should be Microsoft Purview,
upvoted 9 times

Gurulee Most Recent ⏲ 9 months, 1 week ago
Purview and Defender for Cloud; "The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.

Classifications and labels applied to data resources in Microsoft Purview are ingested into Microsoft Defender for Cloud, which provides valuable context for protecting resources. Microsoft Defender for Cloud uses the resource classifications and labels to identify potential attack paths and security risks related to sensitive data. The resources in the Defender for Cloud's Inventory and Alerts pages are also enriched with the classifications and labels discovered by Microsoft Purview, so your security teams can filter and focus to prioritize protecting your most sensitive assets."
upvoted 3 times

zellck 9 months, 1 week ago
1. Azure Purview
2. Microsoft Defender for Cloud

https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide
Defender for Cloud collects, analyzes, and integrates log data from your Azure, hybrid, and multicloud resources, the network, and connected partner solutions, such as firewalls and endpoint agents. Defender for Cloud uses the log data to detect real threats and reduce false positives. A list of prioritized security alerts is shown in Defender for Cloud along with the information you need to quickly investigate the problem and the steps to take to remediate an attack.
upvoted 5 times

orrery 9 months, 1 week ago
□Purview
□Microsoft Defender for Cloud Apps

The reason for choosing Microsoft Defender for Cloud Apps is the need for features that visualize cloud application usage and protect data to triage security alerts related to resources containing PII data. Defender for Cloud Apps enhances cloud application security and provides data loss prevention (DLP), shadow IT detection, and compliance evaluation.

Defender for Cloud focuses on managing the security of the entire Azure environment, Defender for Cloud Apps specializes in the security and data protection of cloud applications.
upvoted 4 times

> **Tony416** 9 months, 1 week ago
> Agreed.
> https://learn.microsoft.com/en-us/purview/information-protection?view=o365-worldwide#protect-your-data
> upvoted 1 times

Gagi79 1 year, 2 months ago
This is trick question due to integration with Defender for Cloud and PII data in Azure environment. So: Azure Purview and Microsoft Defender for Cloud
upvoted 1 times

⊟ **AJ2021** 2 years, 3 months ago

Correct:
Azure Purview
Defender for Cloud

Note the new name change as of April 2022:
Microsoft Purview—a comprehensive set of solutions from Microsoft to help you govern, protect, and manage your entire data estate. By bringing together the former Azure Purview and the former Microsoft 365 Compliance portfolio under one brand and over time, a more unified platform, Microsoft Purview can help you understand and govern the data across your estate, safeguard that data wherever it lives, and improve your risk and compliance posture in a much simpler way than traditional solutions on the market today.

upvoted 3 times

⊟ **janesb** 2 years, 5 months ago

as per my knowledge, it should be Purview and for alerting it should be Azure Monitor, Because Purview is integrated with Azure Monitor for Alerting.

upvoted 4 times

⊟ **TJ001** 2 years, 6 months ago

correct answers , Microsoft Purview is the new name for Azure Purview
https://learn.microsoft.com/en-us/azure/defender-for-cloud/information-protection

upvoted 2 times

⊟ **Just2a** 2 years, 7 months ago

There is nothing called Azure Purview. Correct name if Microsoft Purview and MDC is correct

upvoted 2 times

⊟ **techtest848** 2 years, 7 months ago

Azure Purview and Defender for Cloud are the correct answers.
https://learn.microsoft.com/en-us/azure/purview/register-scan-azure-multiple-sources
https://learn.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

upvoted 2 times

⊟ **Xyz_40** 2 years, 7 months ago

File policy integration with MIP in Microsoft Defender for Cloud App for sensitivity labels. In this case alerts are created when match is encountered.
The alert is also found in the MDCA
Ans: Azure/Microsoft Purview & Microsoft Defender for Cloud Apps

upvoted 1 times

⊟ **prabhjot** 2 years, 10 months ago

Azure Preview is changed to Microsoft Purview (the ans is Correct)

upvoted 5 times

Question #5 *Topic 1*

You have a Microsoft 365 E5 subscription and an Azure subscription.
You are designing a Microsoft deployment.
You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.
What should you recommend using in Microsoft Sentinel?

A. notebooks

B. playbooks

C. workbooks

D. threat intelligence

Suggested Answer: *C*
After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what's happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/get-visibility

Community vote distribution
C (100%)

zellck Highly Voted 2 years, 1 month ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data
Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.
upvoted 6 times

Exam2us Most Recent 3 months, 1 week ago
Selected Answer: C
Admin please update the exam questions. 90% of them are outdated. I only saw 10% of given questions appear in my exam.
upvoted 1 times

junglejoy 12 months ago
Selected Answer: C
the answer is C
upvoted 1 times

junglejoy 12 months ago
C is the answer
upvoted 1 times

Gurulee 2 years, 2 months ago
Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries.
upvoted 1 times

AJ2021 2 years, 3 months ago
Selected Answer: C
Correct
upvoted 2 times

adamsca 2 years, 4 months ago

Selected Answer: C

Correct

upvoted 1 times

TheMCT 2 years, 9 months ago

Selected Answer: C

Correct

upvoted 3 times

Emmuyah 2 years, 9 months ago

Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal.

WorkBook is the correct Answer

upvoted 3 times

BillyB2022 2 years, 10 months ago

Selected Answer: C

Workbooks

https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

upvoted 4 times

prabhjot 2 years, 10 months ago

work book is correct (as it has dash board too)

upvoted 4 times

Question #6 *Topic 1*

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity.
You are informed about incidents that relate to compromised identities.
You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered.
Which Defender for Identity feature should you include in the recommendation?

A. sensitivity labels

B. custom user tags

C. standalone sensors

D. honeytoken entity tags

Suggested Answer: *D*
Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.
Incorrect:

Not B: custom user tags -
After you apply system tags or custom tags to users, you can use those tags as filters in alerts, reports, and investigation.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-identity/entity-tags

Community vote distribution

D (100%)

⊟ **PlumpyTumbler** Highly Voted 👍 2 years, 10 months ago

Selected Answer: D

https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity

upvoted 11 times

⊟ **prabhjot** Highly Voted 👍 2 years, 10 months ago

Ans is correct as The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

upvoted 8 times

⊟ **zellck** Most Recent 🕘 9 months, 1 week ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/defender-for-identity/entity-tags#honeytoken-tags
Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.

upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 3 times

⊟ **AJ2021** 9 months, 1 week ago

Selected Answer: D

In MDI you can set three types of Defender for Identity entity tags: Sensitive tags, Honeytoken tags, and Exchange server tags.
For this question, D is correct: Honeytoken tags

upvoted 1 times

⊟ **SilNilanjan** 11 months, 2 weeks ago

Pretty similarly worded question in exam on 16072024, passed with 895

upvoted 1 times

⊟ **JG56** 1 year, 7 months ago

Selected answer: D,

upvoted 2 times

BillyB2022 2 years, 10 months ago

Selected Answer: D

D. honeytoken entity tags

upvoted 2 times

Question #7 *Topic 1*

Your company is moving all on-premises workloads to Azure and Microsoft 365.
You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:
✑ Minimizes manual intervention by security operation analysts
✑ Supports triaging alerts within Microsoft Teams channels
What should you include in the strategy?

A. KQL

B. playbooks

C. data connectors

D. workbooks

Suggested Answer: *B*
Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.
A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.
Incorrect:
Not A: Kusto Query Language is a powerful tool to explore your data and discover patterns, identify anomalies and outliers, create statistical modeling, and more.
The query uses schema entities that are organized in a hierarchy similar to SQL's: databases, tables, and columns.
Not D: Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive experiences.
Workbooks allow users to visualize the active alerts related to their resources.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

Community vote distribution

B (90%) 10%

prabhjot Highly Voted 2 years, 10 months ago
sentinel soar= playbook (logic app), so correct ans
upvoted 14 times

PlumpyTumbler Highly Voted 2 years, 10 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC
upvoted 8 times

Gagi79 Most Recent 2 months ago
Selected Answer: B
To design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that minimizes manual intervention by security operation analysts and supports triaging alerts within Microsoft Teams channels, you should include:
B. playbooks
Playbooks in Microsoft Sentinel allow you to automate responses to alerts and incidents, significantly reducing the need for manual intervention by security analysts. Additionally, playbooks can be configured to send alerts and notifications to Microsoft Teams channels, facilitating effective communication and triaging among team members.
While KQL (A) is essential for querying data, data connectors (C) are used for integrating various data sources, and workbooks (D) provide visualizations and reporting, none of these options specifically address automation and alert triaging in the context of your requirements as effectively as playbooks do.
upvoted 1 times

AJ2021 9 months, 1 week ago
Selected Answer: B

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription to which it belongs, but the Playbooks display shows you all the playbooks available across any selected subscriptions.

upvoted 2 times

zellck 9 months, 1 week ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents#what-are-automation-rules-and-playbooks
Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

upvoted 2 times

JG56 1 year, 7 months ago

Selected answer: B,

upvoted 3 times

Gurulee 2 years, 2 months ago

Selected Answer: B

"Minimizes manual intervention", this requires Playbooks

upvoted 2 times

fchahin 2 years, 2 months ago

Selected Answer: B

Answer is B

upvoted 3 times

OCHT 2 years, 3 months ago

Selected Answer: C

Data connecter

upvoted 1 times

adamsca 2 years, 4 months ago

Selected Answer: C

Correct

upvoted 1 times

Learing 2 years, 8 months ago

Selected Answer: B

correct

upvoted 2 times

TJ001 2 years, 9 months ago

correct answer

upvoted 2 times

Question #8 *Topic 1*

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.
All resources are backed up multiple times a day by using Azure Backup.
You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Enable soft delete for backups.

B. Require PINs for critical operations.

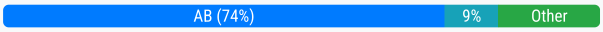
C. Encrypt backups by using customer-managed keys (CMKs).

D. Perform offline backups to Azure Data Box.

E. Use Azure Monitor notifications when backup configurations change.

Suggested Answer: *BE*
Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication.
As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.
Your backups need to be protected from sophisticated bot and malware attacks. Permanent loss of data can have significant cost and time implications to your business. To help protect against this, Azure Backup guards against malicious attacks through deeper security, faster notifications, and extended recoverability.
For deeper security, only users with valid Azure credentials will receive a security PIN generated by the Azure portal to allow them to backup data. If a critical backup operation is authorized, such as ג€delete backup data,ג€ a notification is immediately sent so you can engage and minimize the impact to your business. If a hacker does delete backup data, Azure Backup will store the deleted backup data for up to 14 days after deletion.
E: Key benefits of Azure Monitor alerts include:
Monitor alerts at-scale via Backup center: In addition to enabling you to manage the alerts from Azure Monitor dashboard, Azure Backup also provides an alert management experience tailored to backups via Backup center. This allows you to filter alerts by backup specific properties, such as workload type, vault location, and so on, and a way to get quick visibility into the active backup security alerts that need attention.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
https://www.microsoft.com/security/blog/2017/01/05/azure-backup-protects-against-ransomware/ https://docs.microsoft.com/en-us/azure/backup/move-to-azure-monitor-alerts

Community vote distribution



⊟ **malone0001** Highly Voted 9 months, 1 week ago
Selected Answer: AB
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
upvoted 34 times

⊟ **ChaBum** 2 years, 3 months ago
B E
https://learn.microsoft.com/en-us/azure/backup/security-overview
upvoted 3 times

⊟ **simonseztech** Highly Voted 2 years, 9 months ago
Selected Answer: AB
Keyword are CONTROLS and ENSURE. So A & B both are the answer. https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
upvoted 21 times

⊟ **svpulver** Most Recent 9 months, 1 week ago

I think the correct answer is BC. The question states clearly "in the event of a successful ransomware attack". The ransomware attack does not delete backups and does not modify backup schedules. The attack purpose is to encrypt. That said by using option C (C. Encrypt backups by using customer-managed keys (CMKs)) you will guarantee that an additional encryption attempt made by Ransomware will not be successful as at that point the backups will be already encrypted.

upvoted 2 times

alessag 5 months, 2 weeks ago

I don't think the C is correct because this feature doesn't support backup of virtual machines (VMs); look at https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk?tabs=portal#considerations (third bullet)

upvoted 1 times

d3an 9 months, 1 week ago

Selected Answer: AB

'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.'

Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

Answers are therefore A and B.

upvoted 6 times

ChaBum 2 years, 3 months ago

agreed, E would help detecting the attack, but has nothing to do to "ensure that Azure Backup can be used..."

upvoted 2 times

nited 9 months, 1 week ago

Selected Answer: AB

Soft delete protection, even if a malicious actor deletes a backup (or backup data is accidentally deleted). Backup data is retained for 14 additional days, allowing the recovery of a backup item with no data loss.
As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

upvoted 2 times

Gurulee 9 months, 1 week ago

Selected Answer: AB

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.
Soft delete protection, even if a malicious actor deletes a backup (or backup data is accidentally deleted). Backup data is retained for 14 additional days, allowing the recovery of a backup item with no data loss

upvoted 2 times

zellck 9 months, 1 week ago

Selected Answer: AB

AB is the answer.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature-cloud
Concerns about security issues, like malware, ransomware, and intrusion, are increasing. These security issues can be costly, in terms of both money and data. To guard against such attacks, Azure Backup now provides security features to help protect backup data even after deletion.

One such feature is soft delete. With soft delete, even if a malicious actor deletes a backup (or backup data is accidentally deleted), the backup data is retained for 14 additional days, allowing the recovery of that backup item with no data loss. The additional 14 days of retention for backup data in the "soft delete" state don't incur any cost to you.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature#authentication-to-perform-critical-operations

upvoted 7 times

gujjudesi420 9 months, 1 week ago

Options B (Require PINs for critical operations), D (Perform offline backups to Azure Data Box), and E (Use Azure Monitor notifications when backup configurations change) are not directly related to ensuring the availability and restore capabilities of Azure Backup in the event of a ransomware attack.

Therefore, the recommended controls to include in the strategy for protecting against ransomware attacks and ensuring the usability of Azure Backup for resource restoration are:
A. Enable soft delete for backups
C. Encrypt backups by using customer-managed keys (CMKs)
upvoted 7 times

alessag 5 months, 2 weeks ago
I don't think the C is correct because this feature doesn't support backup of virtual machines (VMs); look at https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk?tabs=portal#considerations (third bullet)
upvoted 1 times

Jonny_Cage 9 months, 1 week ago
A. Enable Soft Delete for Backups: Soft delete adds an additional layer of protection for your backup data. Even if a backup is deleted (whether accidentally or maliciously), it is retained for an additional period (14 days by default for Azure VMs and 30 days for Azure Blob Storage). During this retention period, the backup data can be recovered, ensuring that you can restore from these backups even if they are targeted in a ransomware attack.

B. Require PINs for Critical Operations: This control adds an extra layer of security by requiring a PIN for critical operations, such as deleting backup data or changing backup configurations. This can prevent malicious actors from easily performing destructive actions, even if they have compromised your environment. It's a form of multi-factor authentication that ensures only authorized users can perform sensitive operations on your backups.
upvoted 3 times

Ruttoh 9 months, 1 week ago
To ensure that Azure Backup can be used to restore resources in the event of a successful ransomware attack, you should include the following controls:

A. Enable soft delete for backups: This feature protects your backup data from accidental or malicious deletion by retaining deleted backup data for 14 additional days, allowing you to recover it before it's permanently lost1.

B. Require PINs for critical operations: This adds an extra layer of security by requiring a security PIN for critical operations, ensuring that only authorized users can perform such actions
upvoted 1 times

bxlin 1 year, 1 month ago
Agreed with B and E

A - enable soft delete on a resource, e.g storage account. not on backup
C - does not help.
D - "Store backups in offline or off-site storage" would be a perfect choice. but using Azure Data Box is incorrect, which is a data transfer device to move data from on-prem to Azure cloud. it is not a long-term data storage solution.
upvoted 1 times

alessag 5 months, 2 weeks ago
I don't think E is correct because when you receive a notification is too late because question require CONTROL (preliminary check) to ENSURE you can do remediation tasks (for instance recovery deleted backup).
upvoted 1 times

Bett 1 year, 3 months ago
Currently the solutions published by Microsoft are BD:
-Store backups in offline or off-site storage and/or immutable storage.
-Require out of band steps (such as MFA or a security PIN) before permitting an online backup to be modified or erased.

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#steps-to-take-before-an-attack
About Offline Backup -> https://learn.microsoft.com/en-us/azure/backup/offline-backup-overview
upvoted 2 times

masby661 1 year, 3 months ago
Selected Answer: AC
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq
upvoted 2 times

SFAY 1 year, 4 months ago

Selected Answer: BD

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

Please refer to the section 'Steps to take before an attack'.
Some of the steps mentioned are:
1. Store backups in offline or off-site storage - (Option B)
2. Require out of band steps such as MFA or a security PIN (Option D)

Option A - does not seem to be a valid choice as Soft Delete is enabled by default
Option C - Not mentioned in the MS link above
Option E- Not mentioned in the MS link above

Therefore, B & D are the correct choices as per MS article and not what the votes indicate.

upvoted 3 times

ubiquituz 1 year, 4 months ago

AB...there is no where in the steps to guard against ransomware did they say perform offline backups to azure data box...but soft delete protection and PIN/MFA use is advised

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

upvoted 1 times

Charly80 1 year, 5 months ago

"Soft Delete" doesn't works with Storage Account : https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature-cloud?tabs=azure-portal

upvoted 1 times

TomasValtor 1 year, 7 months ago

Answer: BD

Check this link (slide 20). https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F7%2F5%2F1%2F751682ca-5aae-405b-afa0-e4832138e436%2FRansomwareRecommendations.pptx&wdOrigin=BROWSELINK

upvoted 2 times

itmaster 1 year, 9 months ago

A, C, and E are best practices for ransomware attack:
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq
The right answer is A, soft delete, and C, enabling CMK, to be able to restore after successful attack. If the attack deletes the data, enabled soft delete will restore it. If the attack encrypts the data, the backups that are encrypted by CMK cannot be tampered with and can be decrypted and restored.

upvoted 6 times

Question #9 Topic 1

HOTSPOT -

You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:

✑ Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.

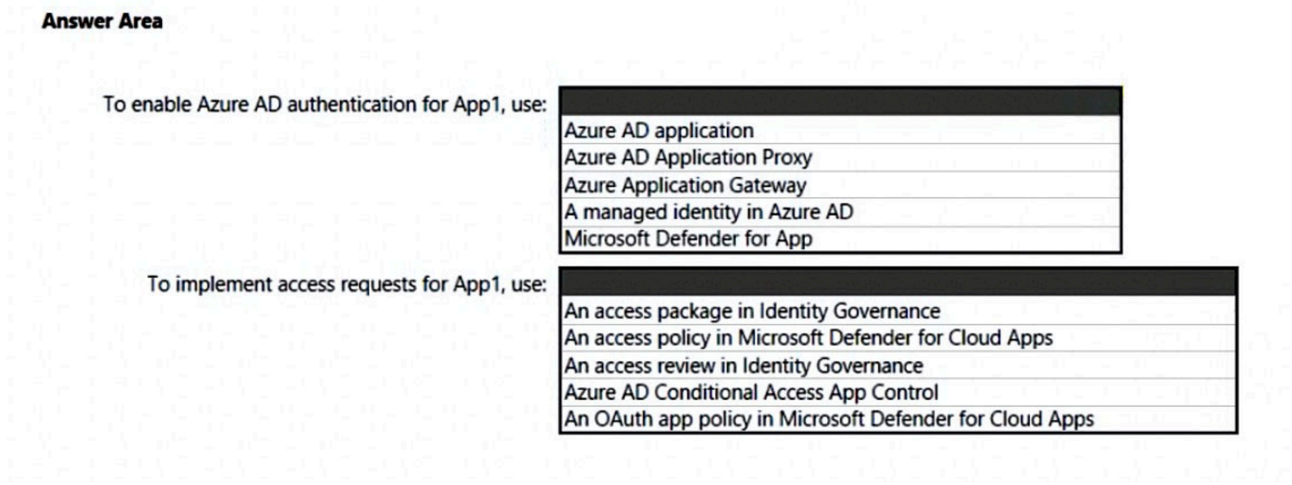
✑ Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

You need to recommend an access security architecture for App1.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

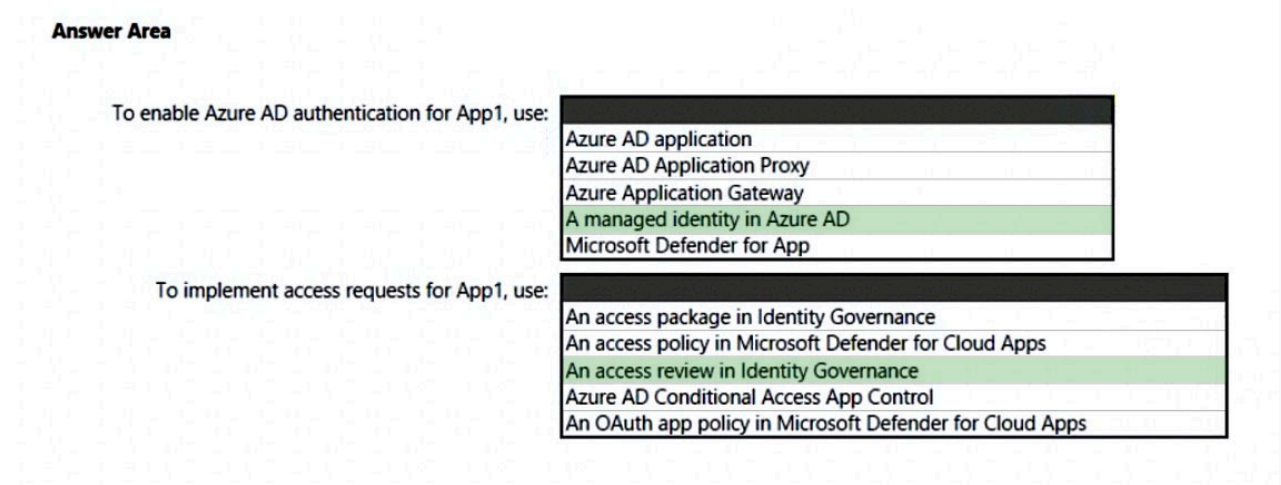
To enable Azure AD authentication for App1, use:

- Azure AD application
- Azure AD Application Proxy
- Azure Application Gateway
- A managed identity in Azure AD
- Microsoft Defender for App

To implement access requests for App1, use:

- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- An access review in Identity Governance
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

Suggested Answer:



Answer Area

To enable Azure AD authentication for App1, use:

- Azure AD application
- Azure AD Application Proxy
- Azure Application Gateway
- [✓ A managed identity in Azure AD]
- Microsoft Defender for App

To implement access requests for App1, use:

- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- [✓ An access review in Identity Governance]
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

Box 1: A managed identity in Azure AD

Use a managed identity. You use Azure AD as the identity provider.

Box 2: An access review in Identity Governance

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Jasper666 Highly Voted 2 years, 10 months ago

I would go for:

a) Azure AD application (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)

b) An access package in identity governance (https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create)

upvoted 124 times

prabhjot 2 years, 10 months ago

agree - How do I create an Azure AD application?
Register an application with Azure AD and create a service principal
Sign in to your Azure Account through the Azure portal.
Select Azure Active Directory.
Select App registrations.
Select New registration.
Name the application. Select a supported account type, which determines who can use the application.
upvoted 4 times

⊟ **JohnBentass** 2 years, 5 months ago
Agreed with this one, answer is A, A
upvoted 5 times

⊟ **Curious76** 2 years, 9 months ago
AGREE with this one
upvoted 1 times

⊟ **sunilkms** 2 years, 6 months ago
The requirement is pretty clear: "Enable Azure AD authentication for App1" hence A
upvoted 4 times

⊟ **BillyB2022** Highly Voted 2 years, 10 months ago
Answer is incorrect

Box 1 is the Azure AD Application

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Box 2 is Access Package in Identity Governance

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create
upvoted 27 times

⊟ **Dirkonormalo** Most Recent 7 months, 3 weeks ago
Yes, Box 2 is Access Package for me too. I was wondering about Access Review.
Access Reviews are used to re-view: Stale account or Periodic requests
Access Pagackes are used for requesting access and grouping packages for roles and partners. The Package can be based used with a workflow to contain stages for approval.
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-create
In Identity Governance, start the process to create an access package.

Select the catalog where you want to put the access package and ensure that it has the necessary resources.

Add resource roles from resources in the catalog to your access package.

Specify an initial policy for users who can request access.

Specify approval settings and lifecycle settings in that policy.
upvoted 2 times

⊟ **Navya6784** 1 year, 1 month ago
Azure AD Application Registration & An access package
upvoted 3 times

⊟ **Baz10** 1 year, 2 months ago
On Exam 8 Apr. 2024 scored 764
Answered Azure AD application Registration (updated answer) and Access package in Identity governance
upvoted 6 times

⊟ **JG56** 1 year, 7 months ago
Selected answer: Azure AD application REGISTRATION and Access package in Identity governance, In exam Nov 23
upvoted 7 times

mscloudguru24 1 year, 5 months ago

Correct, in the exam, it's now Application Registration.

upvoted 3 times

TomasValtor 1 year, 7 months ago

a) Azure AD application (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)

b) An access package in identity governance (https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create)

upvoted 1 times

smanzana 1 year, 8 months ago

Box1: Azure AD application

Box2: An access review in Identity Governance

upvoted 2 times

cyber_sa 1 year, 8 months ago

got this in exam 6oct23. passed with 896 marks. I answered

AZURE AD APP REGISTRATION

AN ACCESS PACKAGE IN IDENTITY GOVERNANCE

upvoted 10 times

haifaalse 5 months, 3 weeks ago

Dear,

From where you studied?

upvoted 1 times

slobav 1 year, 9 months ago

Box1: Azure AD application

Box2: An access review in Identity Governance

You can find explanation here:

https://www.youtube.com/playlist?list=PLQ2ktTy9rklhzzkSEZvDZT4QSIVUQZD-Y

upvoted 2 times

sbnpj 1 year, 11 months ago

Agree ans is AA

upvoted 2 times

ChrisBues 1 year, 11 months ago

Azure AD Application and Access Package in Identity Governance are the correct answers.

upvoted 2 times

zellck 2 years, 1 month ago

1. Azure AD application

2. Access package in Identity Governance

https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-aad

https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview#what-are-access-packages-and-what-resources-can-i-manage-with-them

Entitlement management introduces the concept of an access package. An access package is a bundle of all the resources with the access a user needs to work on a project or perform their task. Access packages are used to govern access for your internal employees, and also users outside your organization.

upvoted 3 times

Gurulee 2 years, 2 months ago

Box one is self explanatory with AAD App, and box two is Access Package in Identity Governance. The giveaway was "Users will request access to App1 through the My Apps portal"

https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-scenarios#access-package-manager-allow-employees-in-your-organization-to-request-access-to-resources

upvoted 2 times

loverboz 2 years, 3 months ago

To enable Azure AD authentication for App1, use Azure AD application

To implement access requests for App1, use an access package in identity governance

To enable Azure AD authentication for App1 and provide access security, the recommended solution is to use an Azure AD application. You should create an Azure AD application, configure the necessary permissions, and assign users and groups to the application.

An access package in identity governance should be used to implement access requests for App1. Identity Governance provides access packages that allow users to request access to specific applications, groups, or roles. The request is routed to the appropriate approver, who can either approve or reject the request. Access packages can be created, managed, and assigned in the Azure portal, and can be customized to include specific access policies and permissions. This provides a streamlined and secure way to manage access to App1, ensuring that only authorized users can access sensitive data or resources.

upvoted 3 times

⊟ **PeteNZ** 2 years, 4 months ago

If you really delve deep, its a sneaky question. As it states your app is running in the Azure App Service, and if you read about it, you can configure AAD as the identity provider here inside the resource group: https://learn.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service-as-user

So you don't need to touch 'Azure AD application' settings at all. The app gets registered by default when following the steps above.

upvoted 2 times

⊟ **nieprotetkniteeetr** 2 years, 5 months ago

Azure AD Application https://learn.microsoft.com/en-us/azure/active-directory/develop/authentication-flows-app-scenarios
An access package in Identity Governance https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create#requests

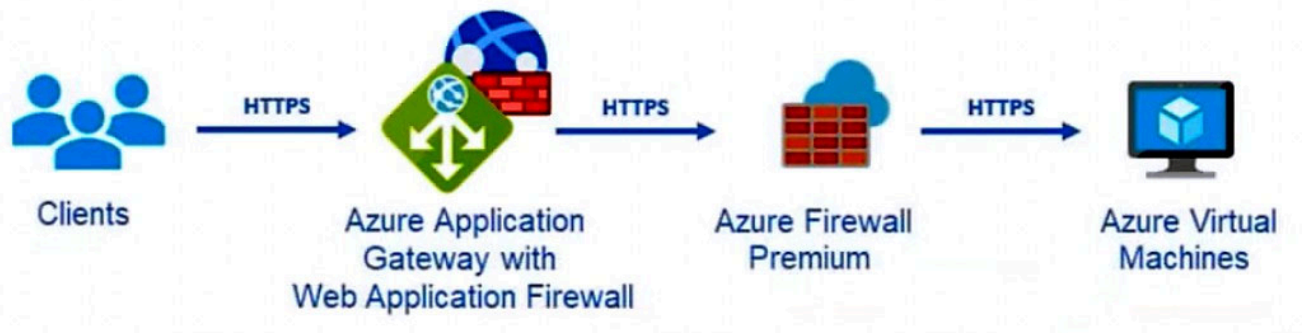
upvoted 1 times

Question #10 *Topic 1*

HOTSPOT -

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel.

The company is designing an application that will have the architecture shown in the following exhibit.



You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements:

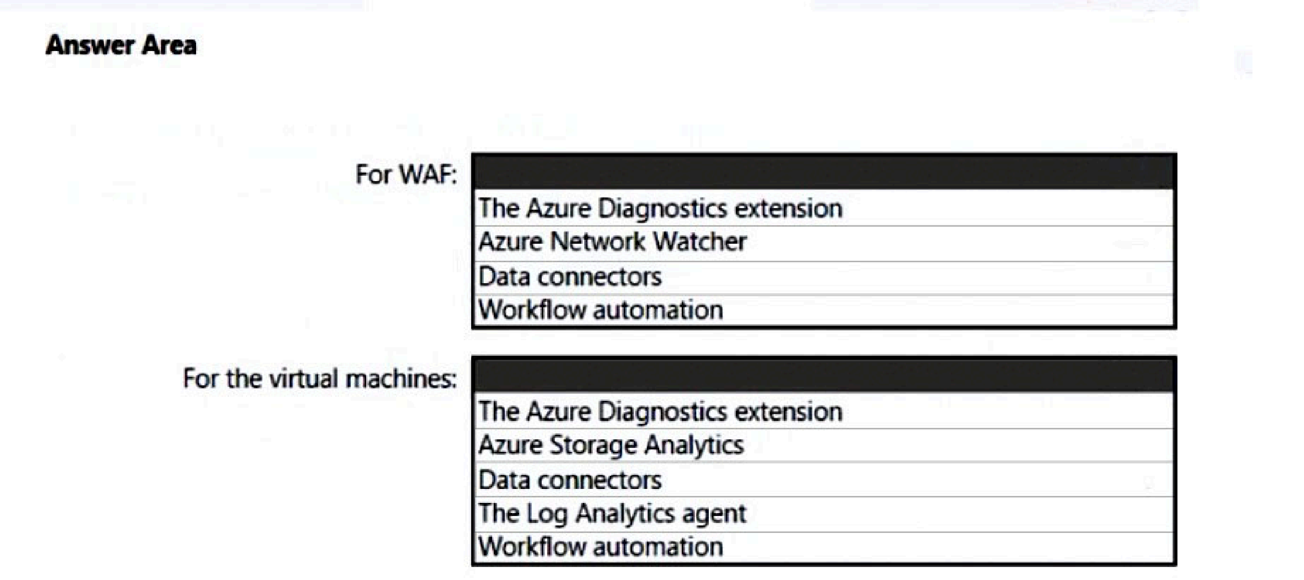
✑ Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.

✑ Use Defender for Cloud to review alerts from the virtual machines.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

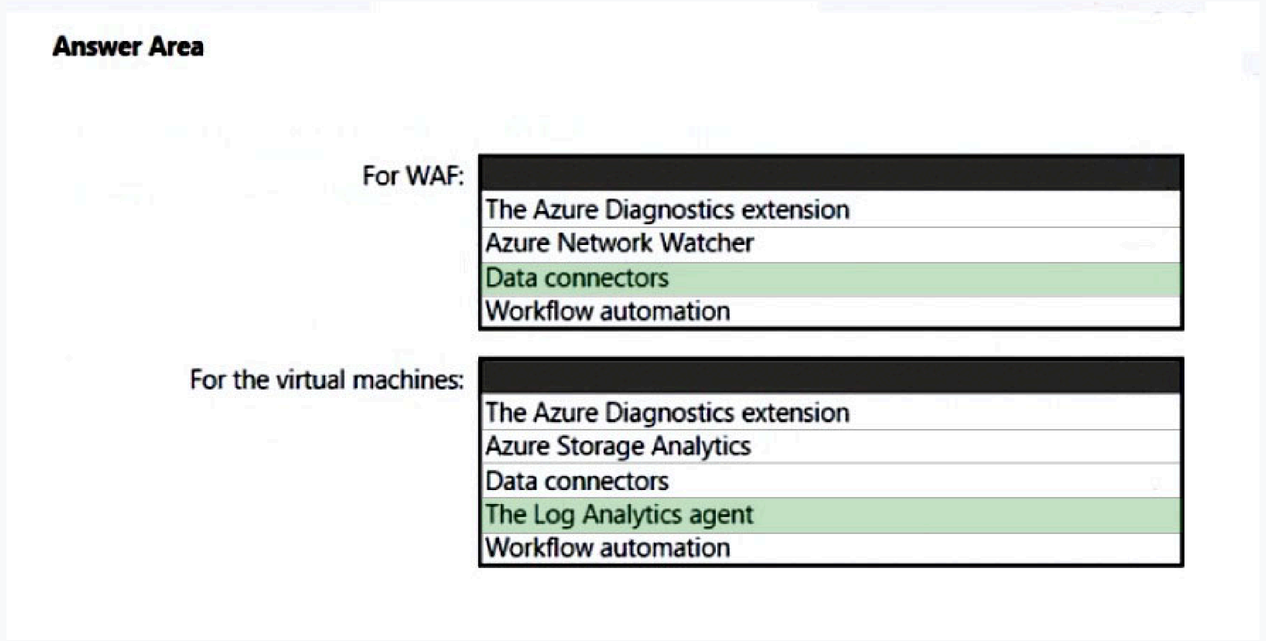


Answer Area

For WAF:
- The Azure Diagnostics extension
- Azure Network Watcher
- Data connectors
- Workflow automation

For the virtual machines:
- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- The Log Analytics agent
- Workflow automation

Suggested Answer:



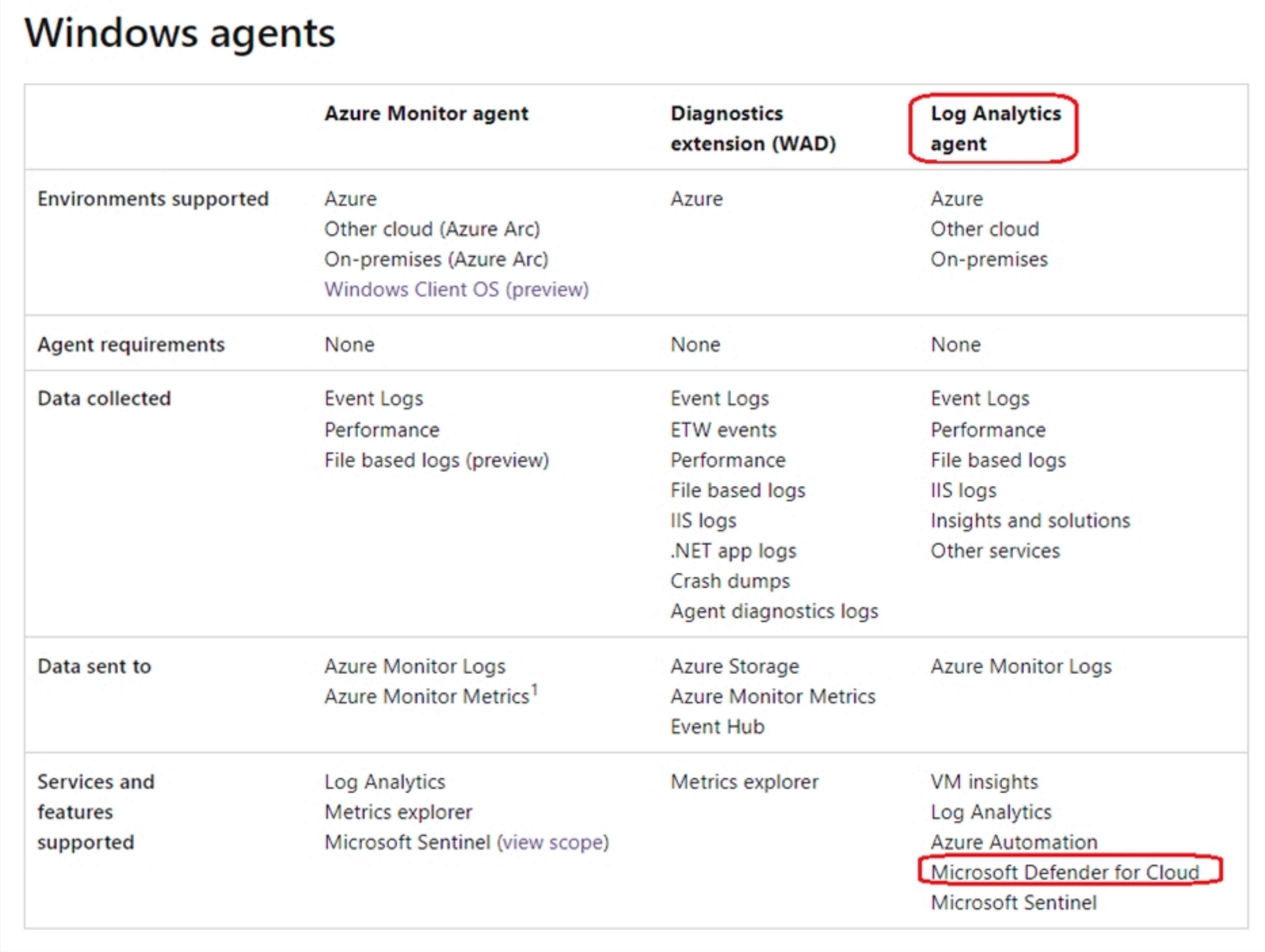
Answer Area

For WAF:
- The Azure Diagnostics extension
- Azure Network Watcher
- [✓ Data connectors]
- Workflow automation

For the virtual machines:
- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- [✓ The Log Analytics agent]
- Workflow automation

Box 1: Data connectors -
Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel.
Launch a WAF workbook (see step 7 below)
The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource.
To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:
1. Select Diagnostic settings.
2. Select + Add diagnostic setting.
3. In the Diagnostic setting page (details skipped)
4. On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.
5. Select an already active workspace or create a new workspace.
6. On the left side panel under Configuration select Data Connectors.
7. Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.
8. Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven't done so previously.
9. Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent -
Use the Log Analytics agent to integrate with Microsoft Defender for cloud.



Windows agents

	Azure Monitor agent	Diagnostics extension (WAD)	Log Analytics agent
Environments supported	Azure Other cloud (Azure Arc) On-premises (Azure Arc) Windows Client OS (preview)	Azure	Azure Other cloud On-premises
Agent requirements	None	None	None
Data collected	Event Logs Performance File based logs (preview)	Event Logs ETW events Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs Performance File based logs IIS logs Insights and solutions Other services
Data sent to	Azure Monitor Logs Azure Monitor Metrics[1]	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs
Services and features supported	Log Analytics Metrics explorer Microsoft Sentinel (view scope)	Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel

The Log Analytics agent is required for solutions, VM insights, and other services such as Microsoft Defender for Cloud.
Note: The Log Analytics agent in Azure Monitor can also be used to collect monitoring data from the guest operating system of virtual machines. You may choose to use either or both depending on your requirements.

Azure Log Analytics agent -
Use Defender for Cloud to review alerts from the virtual machines.
The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System
Center Operations Manager and sends collected data to your Log Analytics workspace in Azure Monitor.
Incorrect:
The Azure Diagnostics extension does not integrate with Microsoft Defender for Cloud.
Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

HardcodedCloud Highly Voted 2 years, 3 months ago

Correct Answer

upvoted 24 times

prabhjot Highly Voted 2 years, 4 months ago

For WAF - in Sentinel we have Data Conenctor

For the VM - we have to install the Log analytics agent in teh VM in the cloud or on premises

The ans is correct

upvoted 20 times

Abengbeng Most Recent 5 months ago

Taken exam Jan 2025 - Log Analytics Agent was not in the options anymore. Only 4 options remaining what could be the ans?

upvoted 2 times

> **Ali96** 4 months, 1 week ago
>
> Azure Monitor Agent
>
> upvoted 2 times

Strive_for_greatness_kc 9 months, 2 weeks ago

Now we can also use data connectors on VM which automatically install Azure Monitor Agent

upvoted 5 times

> **Henk1982** 8 months, 3 weeks ago
>
> Correct, LAA is being deprecated
>
> upvoted 2 times

JG56 1 year, 1 month ago

in Exam Nov 2023 1. Data Connectors 2. Log analytics agent

upvoted 4 times

smanzana 1 year, 2 months ago

1. Data connectors

2. Log Analytics agent

upvoted 2 times

Ario 1 year, 6 months ago

correct answer

upvoted 2 times

Holii 1 year, 6 months ago

I hate it when questions mention Azure Diagnostics extension...

(As an example) Setup the Diagnostic Settings in Azure AD to stream data to a Log Analytics workspace that hosts Sentinel, you will notice that the Azure AD connector becomes enabled.

I know this would make more sense to just say 'enable the connector', but it's technically correct as well if you stream it to LA; it works the same as if it was a data connector to Sentinel.

upvoted 3 times

zellck 1 year, 7 months ago

1. Data connectors

2. Log Analytics agent (but should use Azure Monitor Agent now)

https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/azure-web-application-firewall-waf

https://learn.microsoft.com/en-us/azure/sentinel/ama-migrate

upvoted 5 times

> **zellck** 1 year, 7 months ago
>
> https://learn.microsoft.com/en-us/azure/defender-for-cloud/working-with-log-analytics-agent
> https://learn.microsoft.com/en-us/azure/defender-for-cloud/auto-deploy-azure-monitoring-agent

upvoted 1 times

fchahin 1 year, 9 months ago

I agree with the answers

upvoted 1 times

TJ001 2 years ago

Correct Answers

New name for Log Analytics Agent - Azure Monitoring Agent

upvoted 8 times

EM1234 1 year, 8 months ago

No. It is not just a new name. Those are two completely different monitoring agents that in some cases can and need to both be installed. They can do similar things though.

upvoted 2 times

panoz 2 years ago

Nobody will comment that the azure firewall (premium) should be BEFORE the application gateway?

upvoted 1 times

erjosito 3 months, 2 weeks ago

Incorrect (although not relevant for the question): if you put AzFW premium before AppGW, you will not be able to inspect TLS traffic, unless you find a way to install your own private CA in every one of your app client devices so that they trust the self-signed certificates that AzFW generates on the fly to decrypt TLS.

upvoted 1 times

TJ001 2 years ago

It depends (premium SKU has application level filtering properties but not WAF).Both pattern works it depends where the public exposure is agreed in the APP GW or FW. Have seen more patterns to keep the APP GW behind FW; in which case only the private listener of APP GW is activated and public one even if reachable will just drop any connection requests.

upvoted 2 times

acert976 2 years ago

it depends on the requirement, please refer here for reference https://learn.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway#application-gateway-before-firewall

upvoted 1 times

tester18128075 2 years, 3 months ago

waf - Data connector

VM - LA Agent

upvoted 7 times

Alex_Burlachenko 2 years, 4 months ago

both are correct

upvoted 4 times

Question #11 *Topic 1*

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel.
You plan to integrate Microsoft Sentinel with Splunk.
You need to recommend a solution to send security events from Microsoft Sentinel to Splunk.
What should you include in the recommendation?

A. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

Suggested Answer: *A*
Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP
Data Collector API.
Reference:
https://splunkbase.splunk.com/app/5312/

Community vote distribution

B (86%) 14%

BPQ Highly Voted 2 years, 10 months ago
if data need to go to splunk then event hub.
https://www.splunk.com/en_us/blog/platform/splunking-azure-event-hubs.html
upvoted 46 times

prabhjot 2 years, 10 months ago
agree as i donot see any Splunk data connector in Sentinel and also no Azure Http PI connector in Sentinel
upvoted 6 times

xping85 1 year, 11 months ago
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029
upvoted 3 times

yaza85 Highly Voted 2 years, 5 months ago
Selected Answer: B
B. Data connectors are for receiving data not to send data
upvoted 11 times

nils241 1 year, 5 months ago
Thats the point .Read the Question

"...send security events FROM Microsoft Sentinel TO Splunk."

So it cant be an data connector
upvoted 1 times

Dev21 Most Recent 11 months, 1 week ago
Azure Event Hub is the correct answer.
upvoted 1 times

hondo1997 1 year ago
hub de eventos do azure
upvoted 1 times

DivG 1 year, 4 months ago
Azure Event Hub is the correct answer.
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029
upvoted 2 times

RickySmith 1 year, 5 months ago

Selected Answer: B

Azure Event Hubs.
"to send security events from Microsoft Sentinel to Splunk"
https://www.splunk.com/en_us/blog/platform/splunking-azure-event-hubs.html - Event Hubs can process data or telemetry produced from your Azure environment. They also provide us a scalable method to get your valuable Azure data into Splunk!
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029 - Another option would be to implement a Side-by-Side architecture with Azure Event Hub.
Not a Microsoft Sentinel data connector - Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs 'from' Splunk platform using the Azure HTTP

upvoted 1 times

TomasValtor 1 year, 7 months ago

Answer B
Preparation : The following tasks describe the necessary preparation and configurations steps.

Onboard Azure Sentinel
Register an application in Azure AD
Create an Azure Event Hub Namespace
Prepare Azure Sentinel to forward Incidents to Event Hub
Configure Splunk to consume Azure Sentinel Incidents from Azure Event Hub
Using Azure Sentinel Incidents in Splunk

upvoted 1 times

XtraWest 1 year, 7 months ago

Selected Answer: B

B. Events Hubs | Azure Event Hubs can be used to buffer and route events between Microsoft Sentinel and Splunk. This option provides scalability and reliability in handling high volumes of security events.

upvoted 1 times

ConanBarb 1 year, 9 months ago

Selected Answer: B

I must say that I do think it's strange and unusual for a Microsoft exam to have a scenario where data is going from their own product to a third party's. It's to my experience always the other way.

Therefor I suspect that it could be a typo saying "from Sentinel to Splunk".
It's more likely to be "to Sentinel from Splunk". I.e. Sentinel Data connectors

If appearing on a test make sure to read carefully...

upvoted 2 times

sherifhamed 1 year, 9 months ago

Selected Answer: A

To send security events from Microsoft Sentinel to Splunk, you should use a Microsoft Sentinel data connector. Data connectors in Microsoft Sentinel are used to export security events and logs to external systems, and Splunk is a supported destination for these connectors.

So, the correct recommendation is:

A. a Microsoft Sentinel data connector

upvoted 5 times

ServerBrain 1 year, 10 months ago

Rule of thumb - always go with most votes!!

upvoted 2 times

WRITER00347 1 year, 11 months ago

To send security events from Microsoft Sentinel to Splunk, you would typically use Azure Event Hubs as the messaging service that can integrate with both solutions. Azure Event Hubs can be used to collect and stream event data into various services, and it's suitable for integration with third-party SIEM solutions like Splunk.

So, the correct answer to include in the recommendation would be:

B. Azure Event Hubs.

upvoted 1 times

⊟ **MaciekMT** 1 year, 11 months ago

Selected Answer: B

my 2 cents:

given the options to chose from - I would go for event hub.

I would imagine the best solution in this case would be Microsoft Graph Security API Add-On for Splunk

https://splunkbase.splunk.com/app/4564

upvoted 1 times

⊟ **ariania** 2 years, 1 month ago

Selected Answer: B

Indeed B

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029

upvoted 1 times

⊟ **Jay_G** 2 years, 2 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/export-to-siem#stream-alerts-to-qradar-and-splunk

upvoted 1 times

⊟ **Hashamkhan** 2 years, 2 months ago

There is a distinction between data connectors for receiving (<a href="https://reminiapk.org/">ai</a>) data and data connectors for sending data

upvoted 1 times

Question #12 Topic 1

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.
The customer discovers that several endpoints are infected with malware.
The customer suspends access attempts from the infected endpoints.
The malware is removed from the endpoints.
Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The client access tokens are refreshed.

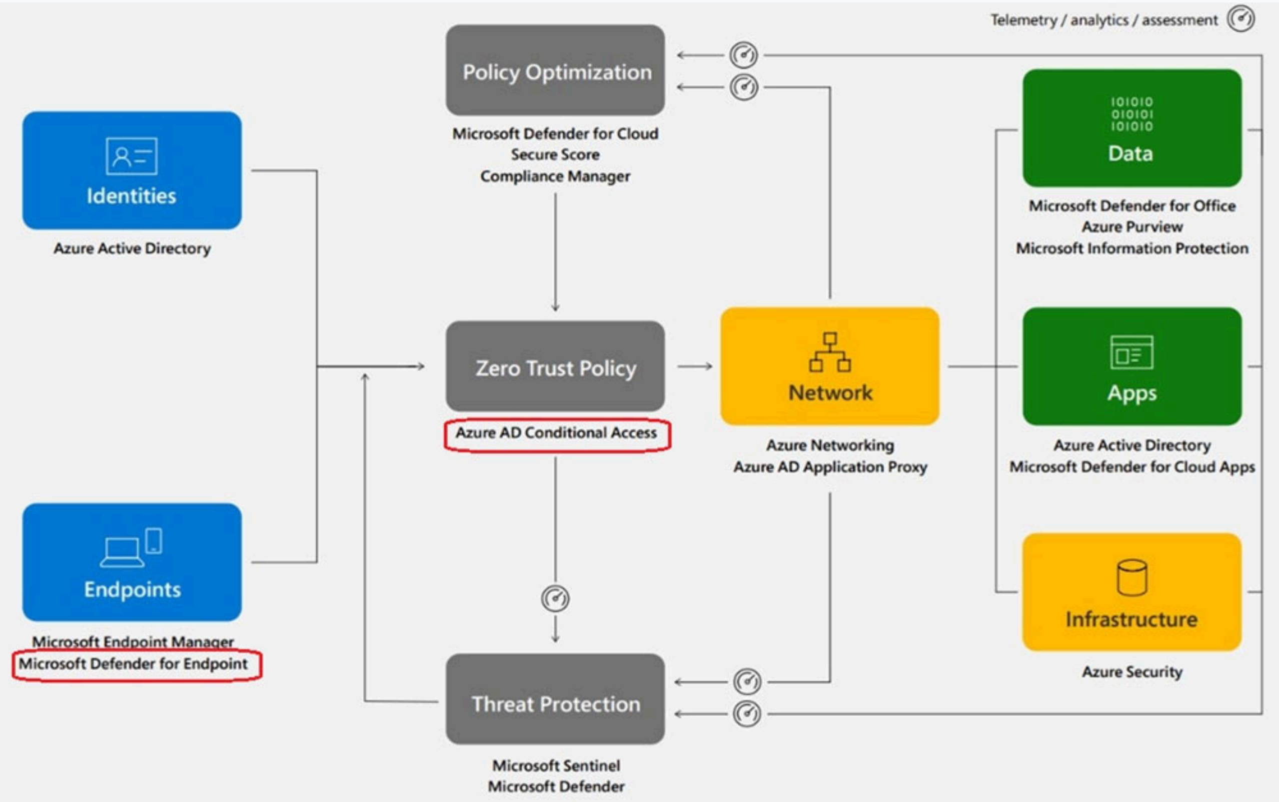
B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. Microsoft Defender for Endpoint reports the endpoints as compliant.

Suggested Answer: *AC*
A: When a client acquires an access token to access a protected resource, the client also receives a refresh token. The refresh token is used to obtain new access/refresh token pairs when the current access token expires. Refresh tokens are also used to acquire extra access tokens for other resources.

Refresh token expiration -
Refresh tokens can be revoked at any time, because of timeouts and revocations.
C: Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. It uses a combination of endpoint behavioral sensors, cloud security analytics, and threat intelligence.
The interviewees said that ג€by implementing Zero Trust architecture, their organizations improved employee experience (EX) and increased productivity.ג€ They also noted, ג€increased device performance and stability by managing all of their endpoints with Microsoft Endpoint Manager.ג€ This had a bonus effect of reducing the number of agents installed on a user's device, thereby increasing device stability and performance. ג€For some organizations, this can reduce boot times from
30 minutes to less than a minute,ג€ the study states. Moreover, shifting to Zero Trust moved the burden of security away from users.
Implementing single sign-on
(SSO), multifactor authentication (MFA), leveraging passwordless authentication, and eliminating VPN clients all further reduced friction and improved user productivity.


Telemetry / analytics / assessment
Policy Optimization
Microsoft Defender for Cloud
Secure Score
Compliance Manager
Identities
Azure Active Directory
Data
Microsoft Defender for Office
Azure Purview
Microsoft Information Protection
Zero Trust Policy
Azure AD Conditional Access
Network
Azure Networking
Azure AD Application Proxy
Apps
Azure Active Directory
Microsoft Defender for Cloud Apps
Endpoints
Microsoft Endpoint Manager
Microsoft Defender for Endpoint
Infrastructure
Azure Security
Threat Protection
Microsoft Sentinel
Microsoft Defender

Note: Azure AD at the heart of your Zero Trust strategy
Azure AD provides critical functionality for your Zero Trust strategy. It enables strong authentication, a point of integration for device security,

and the core of your user-centric policies to guarantee least-privileged access. Azure AD's Conditional Access capabilities are the policy decision point for access to resource
Reference:
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/
https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

Community vote distribution

AB (47%) BD (29%) 13% 8%

⊟ **Gar23** Highly Voted 👍 2 years, 9 months ago

Selected Answer: AB

AB looks correct to me

upvoted 40 times

⊟ **424ede1** 2 months, 4 weeks ago

Documents say otherwise!
https://learn.microsoft.com/en-us/azure/security/fundamentals/recover-from-identity-compromise#remediate-user-and-service-account-access

upvoted 2 times

⊟ **Gagi79** 1 month, 3 weeks ago

Wrong. Defender for Endpoint alone does not directly mark a device as "compliant" in Conditional Access. Instead, it assesses the device's security state and shares that with Intune, which then determines compliance based on its policies. So the integration between Defender for Endpoint and Intune is critical to the compliance process. Microsoft Defender for Endpoint (MDE) integrates with Microsoft Intune through a compliance connector. This integration allows MDE to share device risk level data with Intune. Intune is the authority that determines and reports device compliance based on Defender for Endpoint's input. It's a trick question.

upvoted 1 times

⊟ **BillyB2022** Highly Voted 👍 2 years, 10 months ago

I don't think this is correct.

Zero Trust its reffering to Conditional Access, so would be

Microsoft Intune reports the endpoints as compliant.
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

and I assume

The client access tokens are refreshed.

upvoted 15 times

⊟ **prabhjot** 2 years, 10 months ago

In Identity to achieve zero trust (we have to use Conditional access policy stating a condition as that the resource is compliant) so i guess ans is correct (whereas Intune is for configuring the compliance policy via MDM and MAM)

upvoted 2 times

⊟ **prabhjot** 2 years, 10 months ago

A second thought (why NEW conditional access policy??) so the ans seems wrong and the correct one looks like Microsoft intune reports the endpoints as compliant and The client access token are refreshed

upvoted 11 times

⊟ **jgvh** 2 years, 9 months ago

Maybe the Conditional access already in place since he follow zero trust ? so i feel like it should be AB ?

upvoted 5 times

⊟ **TJ001** 2 years, 6 months ago

how the current malware is detected should have been mentioned in the question. only clue given is currently Zero Trust is implemented and each access attempt is inspected which means a conditional access policy would have been in place already to detect sign in risk (fed from Azure Identity Protection) ..

upvoted 1 times

⊟ **ChaBum** 2 years, 3 months ago

You're assuming endpoints are enrolled in Intune, and assuming is never a good idea in Microsoft exams.
The question says "The customer discovers ..." and "The customer suspends ...", there is nothing about Intune.

upvoted 5 times

jasscomp 1 year, 9 months ago

Conditional Access reaches out to Intune to check if a device is seen as compliant or not.
Intune will receive the risk score from Defender for Endpoint.
Devices have to be managed by Intune in order for Conditional Access to get the compliance check.

upvoted 3 times

Gagi79 Most Recent 1 month, 3 weeks ago

Selected Answer: AB

A. The client access tokens are refreshed. Once access is suspended (e.g., via Conditional Access), any existing tokens may still be valid. After remediation, refreshing the tokens ensures that the new compliant state is recognized and access can be restored.

B. Microsoft Intune reports the endpoints as compliant. Intune is the authority that determines and reports device compliance based on Defender for Endpoint's input. Defender for Endpoint alone does not directly mark a device as "compliant" in Conditional Access. Instead, it assesses the device's security state and shares that with Intune, which then determines compliance based on its policies. So the integration between Defender for Endpoint and Intune is critical to the compliance process.

upvoted 1 times

sborrone 2 months ago

Selected Answer: AD

Devices must be marked as compliant before Intune policies will allow them to access the network

upvoted 1 times

424ede1 2 months, 4 weeks ago

Selected Answer: AC

• Enforce conditional access based on trusted devices. We recommend that you enforce location-based conditional access to suit your organizational requirements.
• Reset passwords after eviction for any user accounts that may have been compromised.
• Revoke refresh tokens immediately after rotating your credentials.

https://learn.microsoft.com/en-us/azure/security/fundamentals/recover-from-identity-compromise#remediate-user-and-service-account-access

upvoted 1 times

olsookie 3 months, 1 week ago

Selected Answer: BD

B. Microsoft Intune reports the endpoints as compliant: Intune ensures that the endpoints meet the organization's compliance policies, verifying that they are secure and properly configured.
https://learn.microsoft.com/en-us/security/zero-trust/deploy/endpoints

D. Microsoft Defender for Endpoint reports the endpoints as compliant: Defender for Endpoint provides advanced threat protection and ensures that the endpoints are free from malware and other security threats.
https://learn.microsoft.com/en-us/defender-endpoint/zero-trust-with-microsoft-defender-endpoint

These conditions help maintain the integrity of the Zero Trust model by ensuring that only secure and compliant endpoints can access corporate applications.

upvoted 2 times

olsookie 3 months, 1 week ago

after further investigation, A and B are correct because MDE does not directly report endpoints as compliant in the same way that Microsoft Intune does. MDE provides detailed reports on device health, antivirus status, and threat protection, but compliance reporting is typically managed through Intune. Therefore A + B = Correct!

upvoted 1 times

Reevs 3 months, 3 weeks ago

Selected Answer: BD

B. Microsoft Intune reports the endpoints as compliant: In a Zero Trust model, compliance is verified before granting access. Intune is used to manage device compliance policies, and the endpoints need to be reported as compliant to ensure they are safe for accessing corporate applications again.

D. Microsoft Defender for Endpoint reports the endpoints as compliant: Defender for Endpoint provides security management for endpoints. After the malware is removed, Defender must report that the endpoints are secure and compliant, ensuring that they are safe for access.

upvoted 1 times

⊟ **Ali96** 4 months, 1 week ago

Selected Answer: AB

A. The client access tokens are refreshed

B. Microsoft Intune reports the endpoints as compliant

upvoted 2 times

⊟ **oscarpopi** 5 months, 1 week ago

Selected Answer: AB

Agree with the given answer

upvoted 1 times

⊟ **jim85** 4 months, 3 weeks ago

Agree, as per the links below, MS says:

n Intune, a device compliance policy is used with Microsoft Entra Conditional Access to block access to applications. In parallel, an automated investigation and remediation process is launched.

A user can still use the device while the automated investigation and remediation is taking place, but access to enterprise data is blocked until the threat is fully remediated.

To resolve the risk found on a device, you need to return the device to a compliant state. A device returns to a compliant state when there's no risk seen on it.

upvoted 1 times

⊟ **Dirkonormalo** 7 months, 3 weeks ago

Tokens need to be refreshed, when a device is marked as incompliant. The access is revoked due to the incomliance state. Answer A

In Intune you configure the compliance policy. Within the compliance policy you configure the risk level for defender. Intune reports the compliance state as compliant, if the defender risk level is equal to or lower than the configured value. Answer B.

Answer C: Is wrong

Answer D is incorrect, because Defender does not report compliance. It reports the client risk level.

upvoted 3 times

⊟ **Dan91** 8 months, 1 week ago

Selected Answer: BD

Questions asks "which 2 conditions must be met". The answer is:

D: Defender must report the risk as being mitigated to Intune

B: Intune reports the device as compliant

upvoted 3 times

⊟ **Lapatiser** 8 months, 1 week ago

Answer should be B and C from the below key points in the question and the reference conditional access link:

The customer discovers that several endpoints are infected with malware. - This comes under Microsoft intune compliance reporting.

The customer suspends access attempts from the infected endpoints. - Conditional access kicks in "when a threat is seen on a device, access to sensitive content is blocked until the threat is remediated."

The malware is removed from the endpoints. - "an automated investigation and remediation process is launched."

https://learn.microsoft.com/en-us/defender-endpoint/conditional-access?view=o365-worldwide

<<Understand the Conditional Access flow>>

upvoted 2 times

⊟ **Ruttoh** 9 months, 1 week ago

To ensure that endpoint users can access the corporate applications again after malware removal, the following two conditions must be met:

B. Microsoft Intune reports the endpoints as compliant: This ensures that the devices meet the organization’s compliance policies and are considered secure1.

D. Microsoft Defender for Endpoint reports the endpoints as compliant: This confirms that the endpoints are free from threats and meet the security requirements1.

upvoted 2 times

⊟ **Savitho** 9 months, 1 week ago

B and D is correct answer

upvoted 2 times

⊟ **orrery** 11 months, 3 weeks ago

Selected Answer: BD

Answer: B. Microsoft Intune reports the endpoint as compliant. D. Microsoft Defender for Endpoint reports the endpoint as compliant.

Reason: In a Zero Trust model, it is necessary to verify the security and compliance status of endpoints before they access corporate applications. Microsoft Intune and Microsoft Defender for Endpoint report the compliance status of endpoints and ensure that the endpoints are secure.

Reasons why other answers are different:

A. Client access tokens are refreshed: While refreshing tokens is important, it is not directly related to verifying the security status of endpoints.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is applied: Conditional access policies help with access control but are not directly related to verifying the compliance status of endpoints.

upvoted 4 times

⊟ **crutester** 12 months ago

Answer is BD

Source: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/conditional-access?view=o365-worldwide

upvoted 2 times

⊟ **Tony416** 9 months, 1 week ago

According to this article, the answer should be BC and not BD.

upvoted 1 times

⊟ **emartiy** 1 year ago

Selected Answer: AD

Today, I read more about this question and eliminated given options based on the question scenario.. So, company uses zero trust model.. It already performed what needs to be done.. So, if some endpoints are malware infected and suspended to access company applications.. For re-access to applications (it says corporate applications not Microsoft 365 apps etc.) User's token needs to be refreshed and also Microsoft Defender for Endpoint also mark device healthy after scan etc.. So Options are;

A and D.

upvoted 3 times

Question #13 Topic 1

HOTSPOT -

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender,

Defender for Cloud, and Azure.

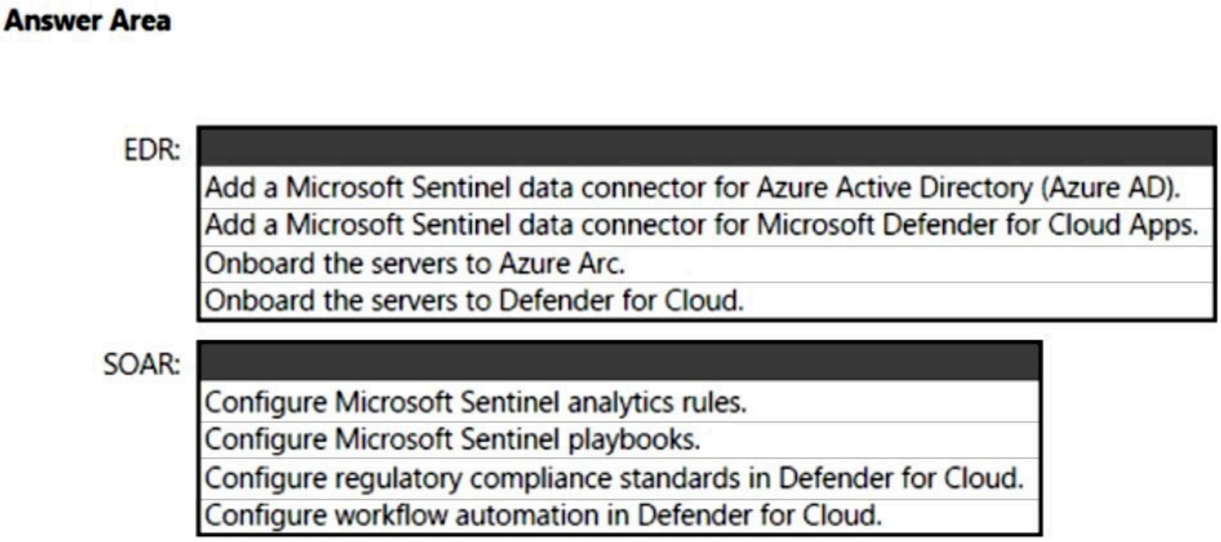
You plan to deploy Azure virtual machines that will run Windows Server.

You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

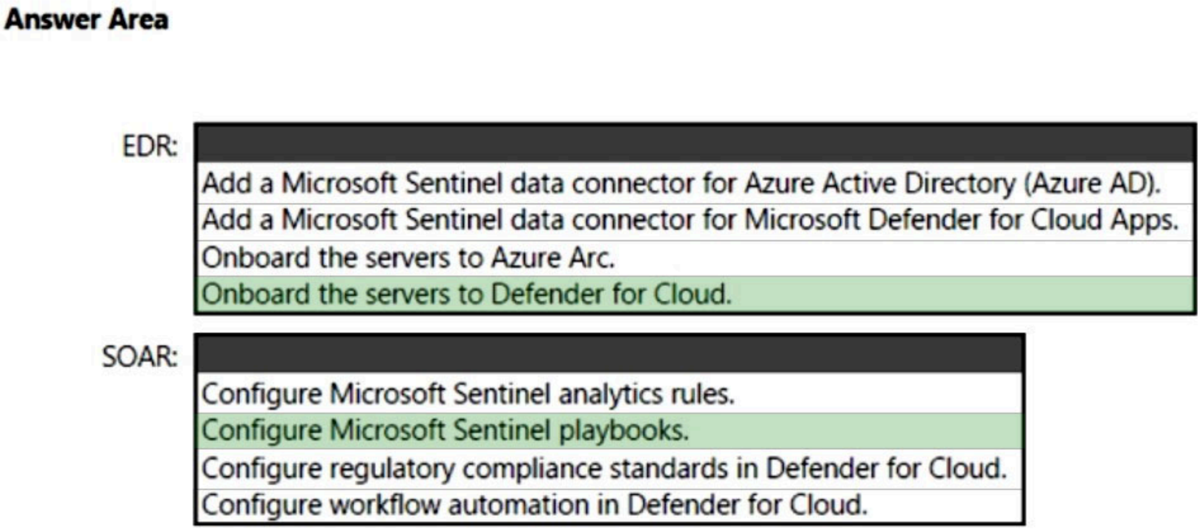


Answer Area

EDR:
- Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD).
- Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps.
- Onboard the servers to Azure Arc.
- Onboard the servers to Defender for Cloud.

SOAR:
- Configure Microsoft Sentinel analytics rules.
- Configure Microsoft Sentinel playbooks.
- Configure regulatory compliance standards in Defender for Cloud.
- Configure workflow automation in Defender for Cloud.

Suggested Answer:



Answer Area

EDR:
- Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD).
- Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps.
- Onboard the servers to Azure Arc.
- [✓ Onboard the servers to Defender for Cloud.]

SOAR:
- Configure Microsoft Sentinel analytics rules.
- [✓ Configure Microsoft Sentinel playbooks.]
- Configure regulatory compliance standards in Defender for Cloud.
- Configure workflow automation in Defender for Cloud.

Box 1: Onboard the servers to Defender for Cloud.

Extended detection and response (XDR) is a new approach defined by industry analysts that are designed to deliver intelligent, automated, and integrated security across domains to help defenders connect seemingly disparate alerts and get ahead of attackers.

As part of this announcement, we are unifying all XDR technologies under the Microsoft Defender brand. The new Microsoft Defender is the most comprehensive

XDR in the market today and prevents, detects, and responds to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

Box 2: Configure Microsoft Sentinel playbooks.
As a SOAR platform, its primary purposes are to automate any recurring and predictable enrichment, response and remediation tasks that are the responsibility of
Security Operations Centers (SOC/SecOps). Leveraging SOAR frees up time and resources for more in-depth investigation of and hunting for advanced threats.
Automation takes a few different forms in Microsoft Sentinel, from automation rules that centrally manage the automation of incident handling and response to playbooks that run predetermined sequences of actions to provide robust and flexible advanced automation to your threat response tasks.
Reference:
https://www.microsoft.com/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-automation-ninja/ba-p/3563377

PlumpyTumbler Highly Voted 2 years, 4 months ago
I agree with the answer but the explanation and links are not very good. For SOAR read this https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of Microsoft Defender.
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide
upvoted 27 times

JG56 Highly Voted 1 year, 1 month ago
Given answer is correct, in exam Nov 23
upvoted 5 times

kazaki Most Recent 10 months ago
Vms will use agent less to onboard to defender the connector needed for sentinel before automation
upvoted 2 times

Ario 1 year, 6 months ago
Given answer is correct
upvoted 4 times

Itu2022 1 year, 6 months ago
was on exam 15/06/23
upvoted 2 times

zellck 1 year, 7 months ago
1. Onboard the servers to Defender for Cloud
2. Configure Microsoft Sentinel playbooks

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers

https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually on-demand on entities (in preview - see below) and alerts, or set to run automatically in response to specific alerts or incidents, when triggered by an automation rule.
upvoted 3 times

> **zellck** 1 year, 7 months ago
> Gotten this in May 2023 exam.
> upvoted 4 times

AJ2021 1 year, 9 months ago
Correct Answers
upvoted 2 times

crypticdeed 1 year, 11 months ago
correct answers provided
upvoted 2 times

omarrob 2 years, 1 month ago
answer is correct:
https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

https://learn.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows

upvoted 1 times

Akintade 2 years, 2 months ago

Agree to the answer provided.

upvoted 4 times

SAMSH 2 years, 3 months ago

was in 20Sep2020 exam

upvoted 4 times

tester18128075 2 years, 3 months ago

correct

upvoted 1 times

HardcodedCloud 2 years, 3 months ago

Correct. But the acronym for extended detection and response is (XDR) not (EDR) which refers to Endpoint detection and response.

upvoted 3 times

prabhjot 2 years, 4 months ago

yes seems to be correct

upvoted 2 times

Alex_Burlachenko 2 years, 4 months ago

correct from my side

upvoted 3 times

Question #14 *Topic 1*

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD).
The customer plans to obtain an Azure subscription and provision several Azure resources.
You need to evaluate the customer's security environment.
What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

A. Azure AD Privileged Identity Management (PIM)

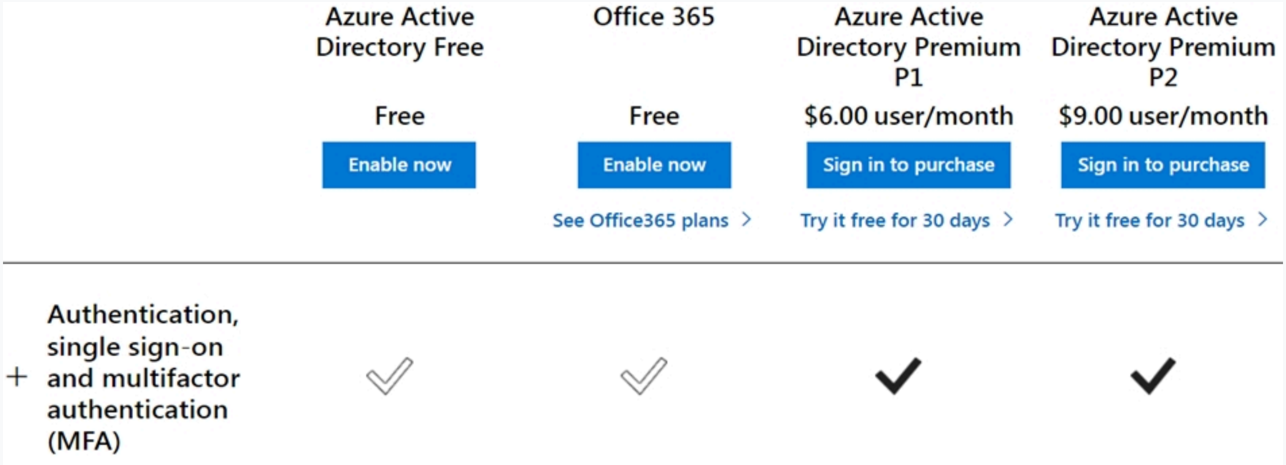
B. role-based authorization

C. resource-based authorization

D. Azure AD Multi-Factor Authentication

Suggested Answer: *D*

Multifactor authentication (MFA), an important component of the Zero Trust Model, is missing in Azure AD Free edition.



	Azure Active Directory Free	Office 365	Azure Active Directory Premium P1	Azure Active Directory Premium P2
	Free	Free	$6.00 user/month	$9.00 user/month
	Enable now	Enable now	Sign in to purchase	Sign in to purchase
		See Office365 plans >	Try it free for 30 days >	Try it free for 30 days >
+ Authentication, single sign-on and multifactor authentication (MFA)	✓	✓	✓	✓

Reference:

https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing

Community vote distribution

A (92%) 8%

d3an Highly Voted 2 years, 9 months ago

Selected Answer: A

PIM is correct. MFA can be enable on AAD Free using Security Defaults.

upvoted 45 times

xping85 1 year, 11 months ago

I agree.

The picture in the answer shows the whole package. If we look at the detailed view, we can see that MFA is already available in Azure Free.

https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing

upvoted 4 times

jasscomp 1 year, 9 months ago

Correct PIM is a P1/P2 feature and also on EMS E5 (not on EMS E3)

upvoted 1 times

Pereiraman Highly Voted 2 years, 9 months ago

Selected Answer: A

PIM is the correct.

upvoted 25 times

svpulver Most Recent 9 months, 1 week ago

The answer should be B. The MFA now is enforced across all Entra ID tenant types, the PIM is an option of Entra ID P2 feature

upvoted 1 times

emartiy 1 year ago

Selected Answer: A

PIM is correct. When security defaults are enabled. MFA section is automatically enabled so it is used in Free edition too. fyi

upvoted 1 times

b9e98e8 1 year, 1 month ago

MFA is activated partially only for all users (all user model or per user model) using security default of Free AAD. However, MFA with conditions that is necessary to evaluate compliance is not achieved by this. We need conditional access policy for such set up. Hence we need AAD P1.

upvoted 1 times

bxlin 1 year, 1 month ago

Selected Answer: D

I would agree with D to ensure full MFA and Conditional Access first, which require Entra ID P1 license. PIM required P2 license.

upvoted 1 times

zul_n 1 year, 3 months ago

Selected Answer: A

the answer is PIM

https://techcommunity.microsoft.com/t5/microsoft-entra/pim-license-requirement/m-p/3950269

upvoted 3 times

kazaki 1 year, 3 months ago

Selected Answer: D

Both A and D are correct

upvoted 1 times

> **Mnguyen0503** 1 year, 2 months ago
>
> Not correct. Entra Free tier gives you Security Defaults, which comes with MFA feature, just no options to customize the security controls around it. So answer is A - PIM.
>
> upvoted 1 times

DivG 1 year, 4 months ago

Azure PIM is the correct answer.

upvoted 1 times

Aedefix 1 year, 5 months ago

Selected Answer: A

https://www.microsoft.com/en-ca/security/business/microsoft-entra-pricing?ef_id=_k_fbefaf89b2b81fcf43d9ca1f56389099_k_&OCID=AIDcmm4bo1g8yk_SEM__k_fbefaf89b2b81fcf43d9ca1f56389099_k_&msclkid=fbefaf89b2b81fcf43

upvoted 1 times

Edgecrusher77 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

casualbork 1 year, 9 months ago

Selected Answer: A

PIM is correct. It's a P2 Feature

upvoted 2 times

HappyMahaseth 1 year, 10 months ago

PIM cis the correct one

upvoted 1 times

Datta2023 1 year, 10 months ago

PIM is correct. Check https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing -> Identity Governance -> PIM

upvoted 1 times

ChrisBues 1 year, 11 months ago

Selected Answer: A

PIM is correct. MFA is free.

upvoted 1 times

ehsanhabib 2 years ago

PIM is correct answer

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#license-requirements
Using this feature requires Azure AD Premium P2 licenses.

upvoted 1 times

Question #15 *Topic 1*

You are designing the security standards for a new Azure environment.
You need to design a privileged identity strategy based on the Zero Trust model.
Which framework should you follow to create the design?

A. Microsoft Security Development Lifecycle (SDL)

B. Enhanced Security Admin Environment (ESAE)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)

Suggested Answer: *C*
RaMP initiatives for Zero Trust.
To rapidly adopt Zero Trust in your organization, RaMP offers technical deployment guidance organized in these initiatives.
In particular, meet these deployment objectives to protect your privileged identities with Zero Trust.
1. Deploy secured privileged access to protect administrative user accounts.
2. Deploy Azure AD Privileged Identity Management (PIM) for a time-bound, just-in-time approval process for the use of privileged user accounts.
Note 1: RaMP guidance takes a project management and checklist approach:
* User access and productivity
1. Explicitly validate trust for all access requests

Identities -
Endpoints (devices)

Apps -

Network -
* Data, compliance, and governance
2. Ransomware recovery readiness
3. Data
* Modernize security operations
4. Streamline response
5. Unify visibility
6. Reduce manual effort
Note 2: As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and gives you a set of deployment paths to more quickly implement key layers of protection.
By providing a suggested mapping of key stakeholders, implementers, and their accountabilities, you can more quickly organize an internal project and define the tasks and owners to drive them to conclusion.
By providing a checklist of deployment objectives and implementation steps, you can see the bigger picture of infrastructure requirements and track your progress.
Incorrect:
Not B: Enhanced Security Admin Environment (ESAE)
The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is an approach to provide a secure environment for Windows Server Active Directory (AD) administrators.
Microsoft's recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP) guidance as the default recommended approach for securing privileged users. The ESAE hardened administrative forest pattern (on-prem or cloud-based) is now considered a custom configuration suitable only for exception cases listed below.
What are the valid ESAE use cases?
While not a mainstream recommendation, this architectural pattern is valid in a limited set of scenarios.
In these exception cases, the organization must accept the increased technical complexity and operational costs of the solution. The organization must have a sophisticated security program to measure risk, monitor risk, and apply consistent operational rigor to the usage and maintenance of the ESAE implementation.
Example scenarios include:
Isolated on-premises environments - where cloud services are unavailable such as offline research laboratories, critical infrastructure or

utilities, disconnected operational technology (OT) environments such as Supervisory control and data acquisition (SCADA) / Industrial Control Systems (ICS), and public sector customers that are fully reliant on on-premises technology.
Highly regulated environments ג€" industry or government regulation may specifically require an administrative forest configuration.
High level security assurance is mandated - organizations with low risk tolerance that are willing to accept the increased complexity and operational cost of the solution.
Reference:
https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview https://docs.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities https://docs.microsoft.com/en-us/security/compass/esae-retirement

Community vote distribution

C (85%) B (15%)

BillyB2022 Highly Voted 2 years, 4 months ago

Answer is correct.

https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan
This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

upvoted 17 times

blopfr 2 years, 2 months ago

agree with the answer but this link provide the zero trust view on it (not the admin access only)
https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 2 times

Baz10 Highly Voted 8 months, 3 weeks ago

Selected Answer: C

On Exam 8 Apr 2024 - scored 764

upvoted 10 times

casualbork Most Recent 1 year, 3 months ago

Selected Answer: C

as pointed out multiple times, C (RaMP) is the correct answer.

upvoted 4 times

Ario 1 year, 6 months ago

B is correct

upvoted 2 times

Ario 1 year, 6 months ago

Sorry guys , Answer C is correct based on Microsoft new recommendation :Microsoft's recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP)

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview
As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and gives you a set of deployment paths to more quickly implement key layers of protection.

upvoted 1 times

OCHT 1 year, 9 months ago

Selected Answer: B

I think B. RaMP is not a recognized security framework or model

upvoted 5 times

Gurulee 1 year, 8 months ago

Thinking of RaMP and the definition of a framework may help: "a framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful."

upvoted 1 times

AJ2021 1 year, 9 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 3 times

MichaelMu 1 year, 10 months ago

C

Rapid Modernization Plan (RaMP) is a framework developed by Microsoft to help organizations quickly implement key layers of protection based on Zero Trust principles. Unlike traditional deployment guidance, RaMP guidance takes a project management and checklist approach to provide a set of deployment paths and a checklist of deployment objectives and implementation steps. The framework provides a suggested mapping of key stakeholders, implementers, and their accountabilities to help organizations organize internal projects and define tasks and owners to drive them to completion. RaMP guidance helps organizations see the bigger picture of infrastructure requirements and track progress.

upvoted 2 times

Sec_Arch_Chn 2 years, 1 month ago

Selected Answer: C

Rapid Modernization Plan (RaMP) checklist helps you establish a security perimeter for cloud applications and mobile devices that uses identity as the control plane and explicitly validates trust for user accounts and devices before allowing access, for both public and private networks - Source: https://learn.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities

upvoted 2 times

tester18128075 2 years, 3 months ago

RaMP is correct

upvoted 2 times

HardcodedCloud 2 years, 3 months ago

Selected Answer: C

Rapid Modernization Plan (RaMP)

upvoted 3 times

prabhjot 2 years, 4 months ago

Rapid Modernization Plan (RaMP) is coorect ans - (as per MCRA) RaMP helps to achieve ZERO Trust

upvoted 2 times

Alex_Burlachenko 2 years, 4 months ago

correct

upvoted 1 times

PlumpyTumbler 2 years, 4 months ago

Selected Answer: C

C, BillyB provides a great link. SDL and OSA are SDLC related. ESAE has been retired and replaced by RAMP.

upvoted 5 times

Question #16 *Topic 1*

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All on-premises servers in the perimeter network are prevented from connecting directly to the internet.
The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend solutions to meet the following requirements:
✑ Ensure that the security operations team can access the security logs and the operation logs.
✑ Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two solutions should you include in the recommendation? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a custom collector that uses the Log Analytics agent

B. the Azure Monitor agent

C. resource-based role-based access control (RBAC)

D. Azure Active Directory (Azure AD) Conditional Access policies

Suggested Answer: *BC*
A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.
Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.
You can connect your data sources to Microsoft Sentinel using custom log formats.
C: Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.
Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel. The different roles give you fine-grained control over what Microsoft Sentinel users can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel inherits.
Incorrect:
A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.
Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.
You can connect your data sources to Microsoft Sentinel using custom log formats.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview https://docs.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG https://docs.microsoft.com/en-us/azure/sentinel/roles

Community vote distribution
BC (76%) AC (24%)

PlumpyTumbler Highly Voted 👍 2 years, 4 months ago
These answer options have been abridged. Other dumps say:
A. Create a custom collector that uses the Log Analytics agent.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Configure Azure Active Directory (Azure AD) Conditional Access policies.
upvoted 23 times

PlumpyTumbler 2 years, 4 months ago
Given the expanded answers B and C are the clear best choices.
B - this use case is spelled out in exact detail. This is must be the exact wording that the question was created from
https://docs.microsoft.com/en-us/azure/sentinel/best-practices-data#on-premises-windows-log-collection
C - https://docs.microsoft.com/en-us/azure/sentinel/resource-context-rbac#scenarios-for-resource-context-rbac
upvoted 19 times

JakeCallham 2 years, 2 months ago
The link for B also states this Servers do not connect to the internet, Use the Log Analytics gateway Configuring a proxy to your agent requires extra firewall rules to allow the Gateway to work.

upvoted 3 times

Gurulee 1 year, 8 months ago

"The Log Analytics gateway supports: Windows computers on which either the Azure Monitor Agent or the legacy Microsoft Monitoring Agent is directly connected to a Log Analytics workspace in Azure Monitor. Both the source and the gateway server must be running the same agent. You can't stream events from a server running Azure Monitor agent through a server running the gateway with the Log Analytics agent."

upvoted 2 times

Sorrynotsorry Highly Voted 👍 2 years, 4 months ago

Selected Answer: BC

I agree with B & C after the expaned version of the answers

upvoted 16 times

AleFerrillo Most Recent 🕘 3 months, 2 weeks ago

Selected Answer: BC

Custom collector when sources are API/3rd parties/Apps -> no A

upvoted 1 times

JAGUDERO 8 months, 3 weeks ago

To meet the specified requirements for the customer's hybrid cloud infrastructure, the two solutions that should be included in the recommendation are:

A. Custom Collector with Log Analytics Agent: This solution can collect security and operation logs from on-premises servers and send them to Microsoft Sentinel. The custom collector can be configured to ensure that the security operations team has access to both security and operation logs.

C. Resource-Based RBAC: This allows for fine-grained access control. By implementing RBAC, you can ensure that the security operations team has access to security logs and operation logs, while the IT operations team has access only to the operation logs.

Solutions B and D are not complete solutions for the requirements stated. The Azure Monitor agent (B) is primarily for data collection and doesn't provide access control, while Azure AD Conditional Access policies (D) are used for managing access based on conditions and do not directly control log access.

upvoted 3 times

JHJ44 8 months, 3 weeks ago

A/C

Custom Collector with Log Analytics Agent:

Deploy a custom collector that utilizes the Log Analytics agent.

This agent allows you to collect security logs and operation logs from various sources, including on-premises servers.

By configuring custom collectors, the security operations team can access both security logs and operation logs.

Points: 1

Resource-Based Role-Based Access Control (RBAC):

Utilize Azure RBAC to create and assign roles within your security operations team.

Assign appropriate roles to grant access to Microsoft Sentinel resources.

For the IT operations team, assign roles that provide access only to operation logs (such as event logs from servers in the perimeter network).

By fine-tuning RBAC, you ensure that each team has the necessary access without compromising security.

upvoted 1 times

Murtuza 12 months ago

Requires splitting operation and security logs Use the Microsoft Monitor Agent or Azure Monitor Agent multi-home functionality

upvoted 2 times

Azerty1313 1 year ago

Really don't get the point of B. Why?

It all depends on how you read the question.

There is a need for 2 different teams to see the logs. -> RBAC

Second part is only from the perimeter. I read this as the operation people need to be at a certain place before they can read it -> conditional access

So I would go for C & D.

upvoted 1 times

Azerty1313 1 year ago

reading it again it will probably be the servers in the perimeter network

upvoted 1 times

BlackZeros 1 year, 5 months ago

the actual multiple-choice answers did not make much sense until Plumpy pointed out the full wording.

upvoted 4 times

Ario 1 year, 6 months ago

A and B

upvoted 1 times

Ario 1 year, 5 months ago

Was A TYPO A AND C

upvoted 1 times

imsidrai 1 year, 6 months ago

what is Resource Based Access control??

Its Role based Access control,

upvoted 1 times

Avanade2023 1 year, 6 months ago

I am sorry, maybe my understand is wrong. why B is the answer like C as a complete solution? the Question condition is "Each correct answer presents a complete solution". I think that Azure Monitor agent is needed of cause, but it is for collecting the log data, doesn't meet the solution's requirements to control access. If the question condition is "Each correct answer presents part of the solution", I will agree with B & C.

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources#custom-logs

For some data sources, you can collect logs as files on Windows or Linux computers using the Log Analytics custom log collection agent.

https://learn.microsoft.com/en-us/azure/sentinel/resource-context-rbac

Typically, users who have access to a Microsoft Sentinel workspace also have access to all the workspace data, including security content. Administrators can use Azure roles to configure access to specific features in Microsoft Sentinel, depending on the access requirements in their team.

upvoted 2 times

AJ2021 1 year, 9 months ago

Selected Answer: BC

B: Tricky one, no internet on on-premise servers, you need to use the Log Analytics gateway in Azure Monitor.

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/gateway

C: RBAC

upvoted 3 times

God2029 1 year, 10 months ago

The legacy Log Analytics agent will be deprecated by August 2024, Microsoft recommends to migrate/use Azure Monitor Agent. So if both Log analytics agent and Azure monitor Agents are there in the answer choose the latter.

upvoted 6 times

rmafnc 1 year, 11 months ago

A. a custom collector that uses the Log Analytics agent

C. resource-based role-based access control (RBAC)

upvoted 2 times

awssecuritynewbie 1 year, 11 months ago

I agree With the answers, but the explanation is very poor. I would really improve on that.

upvoted 1 times

hpl1908 1 year, 11 months ago

Selected Answer: AC

A & C is the right answer

upvoted 2 times

hpl1908 1 year, 11 months ago

To meet the requirements of ensuring that the security operations team can access the security logs and the operation logs, and ensuring that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network, you can recommend the following solutions:

A. A custom collector that uses the Log Analytics agent - this will allow you to collect security logs and operation logs from on-premises servers and Microsoft 365, and send the logs to Microsoft Sentinel.

C. Resource-based role-based access control (RBAC) - this will allow you to assign specific access permissions to different teams based on the resources they need to access. For example, you can assign the security operations team access to both the security logs and the operation logs, and assign the IT operations team access only to the operation logs, including the event logs of the servers in the perimeter network.

upvoted 1 times

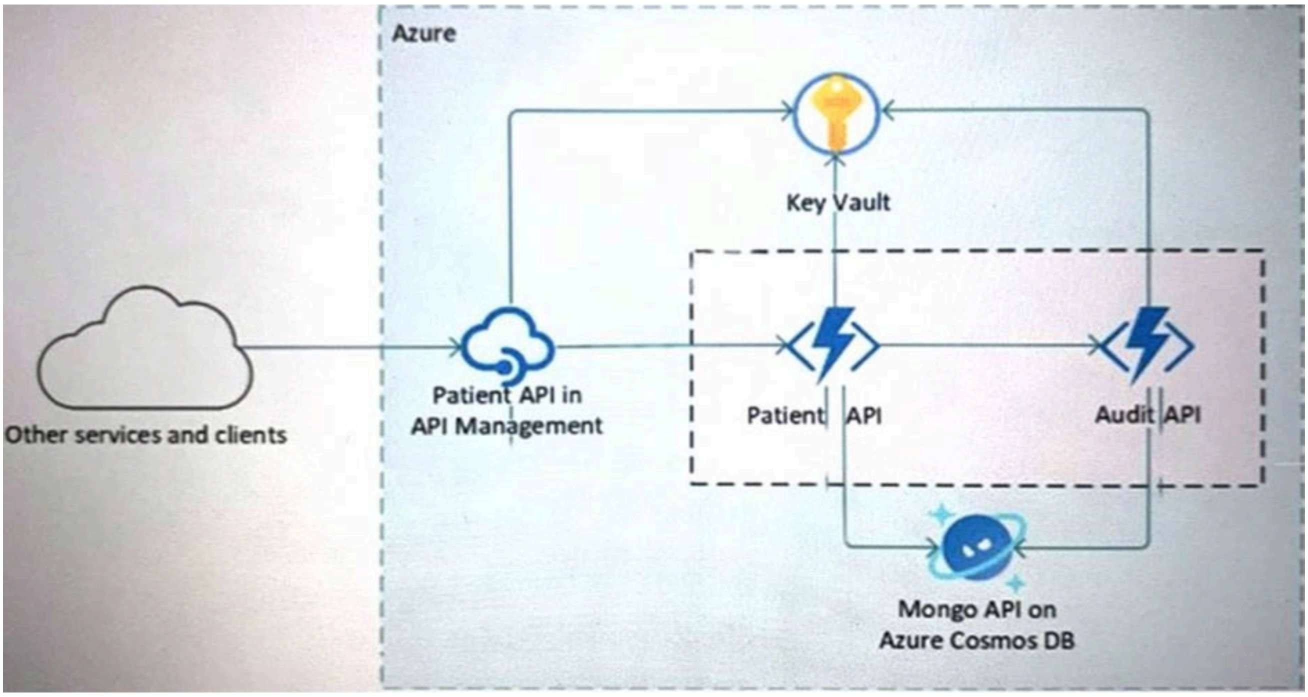
⊟ **Fal991l** 1 year, 9 months ago

That's from ChatGPT.

upvoted 2 times

Question #17 Topic 1

Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.


Azure
Key Vault
Other services and clients
Patient API in API Management
Patient API
Audit API
Mongo API on Azure Cosmos DB

You need to recommend a solution to isolate the compute components on an Azure virtual network.

What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications

B. an Azure App Service Environment (ASE)

C. Azure service endpoints

D. an Azure Active Directory (Azure AD) application proxy

Suggested Answer: *B*

The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale. This capability can host your:

Windows web apps -

Linux web apps -

Docker containers -

Mobile apps -

Functions -

App Service environments (ASEs) are appropriate for application workloads that require:

Very high scale.

Isolation and secure network access.

High memory utilization.

Customers can create multiple ASEs within a single Azure region or across multiple Azure regions. This flexibility makes ASEs ideal for horizontally scaling stateless application tiers in support of high requests per second (RPS) workloads.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/environment/intro

Community vote distribution

B (93%) 7%

InformationOverload Highly Voted 2 years, 3 months ago

Selected Answer: B

Answer is correct.
https://docs.microsoft.com/en-us/azure/app-service/environment/overview

upvoted 10 times

Murtuza Most Recent 1 year ago

The exhibit shows function apps so ASE can support it

upvoted 2 times

JG56 1 year, 1 month ago

Given answer is correct, in exam Nov 23

upvoted 2 times

Ario 1 year, 6 months ago

B is correct

upvoted 1 times

Itu2022 1 year, 6 months ago

was on exam 15/06/23

upvoted 3 times

edurakhan 1 year, 7 months ago

On exam 5/25/2023

upvoted 3 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/environment/intro#overview
The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale.

upvoted 2 times

zellck 1 year, 7 months ago

Gotten this in May 2023 exam.

upvoted 3 times

Cock 1 year, 7 months ago

Thank you Zelleck. I took AZ-500 and SC-100 shortly after you. You helped me a lot. I know you wouldn't see this message, but I really appreciate your effort

upvoted 4 times

zellck 1 year, 7 months ago

Glad that my comments are useful! =)

upvoted 4 times

OCHT 1 year, 9 months ago

Selected Answer: C

Azure service endpoints provide secure and direct connections to Azure services over an Azure virtual network. By using service endpoints, traffic between the virtual network and the Azure service does not traverse the public internet, which enhances security and network performance. Service endpoints can also be used to restrict access to specific Azure services to only specific subnets within a virtual network. Therefore, including Azure service endpoints in the recommendation can help isolate the compute components on an Azure virtual network.

Azure Active Directory (Azure AD) enterprise applications, an Azure App Service Environment (ASE), and an Azure Active Directory (Azure AD) application proxy are all valid solutions for different scenarios, but they do not address the specific requirement of isolating compute components on an Azure virtual network.

upvoted 1 times

init2winit 1 year, 9 months ago

In the above exhibit; it references APIs not hosts, so not endpoints so App Service Environment is the correct answer

upvoted 2 times

KrisDeb 1 year, 10 months ago

App Service Environment v2 will be retired on 31 August 2024. There's a new version of App Service Environment that is easier to use and runs on more powerful infrastructure.

https://learn.microsoft.com/en-us/azure/app-service/environment/overview

upvoted 2 times

⊟ **itbrpl** 1 year, 10 months ago

who cares about that. we are in 2023

upvoted 2 times

⊟ **Ajdlfasudfo0** 1 year, 10 months ago

only an idiot would start building on outdated components

upvoted 4 times

⊟ **Sec_Arch_Chn** 2 years, 1 month ago

Correct Answer. App Service environments are appropriate for application workloads that require 'Isolation and secure network access.'

Source: https://docs.microsoft.com/en-us/azure/app-service/environment/intro

upvoted 2 times

⊟ **tester18128075** 2 years, 3 months ago

ASE is correct, webapps on this are hosted in your VNET in a dedicated subnet.

upvoted 4 times

⊟ **TheMCT** 2 years, 3 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/archive/msdn-magazine/2017/april/azure-the-new-azure-app-service-environment

The Azure App Service Environment (ASE) is a Premium feature offering of the Azure App Service. It gives a single-tenant instance of the Azure App Service that runs right in your own Azure virtual network (VNet), providing network isolation and improved scaling capabilities.

upvoted 3 times

⊟ **Alex_Burlachenko** 2 years, 4 months ago

correct, agree

upvoted 2 times

⊟ **prabhjot** 2 years, 4 months ago

App Service environments (ASEs) are appropriate for application workloads that require:

Very high scale,Isolation and secure network access,High memory utilization.This capability can host your:

Windows web apps,Linux web apps

Docker containers,Mobile apps

Functions

upvoted 4 times

Question #18 Topic 1

HOTSPOT

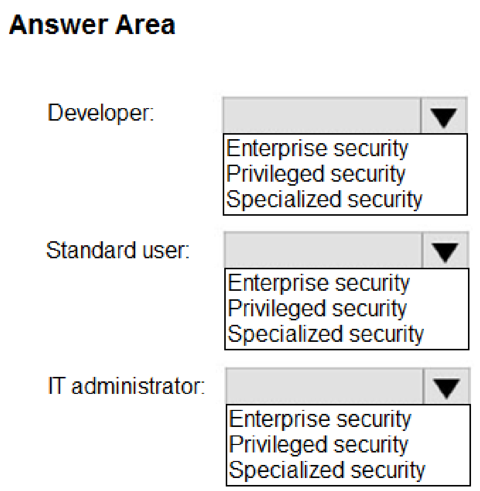
-

You are planning the security levels for a security access strategy.

You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security level should you configure for each job role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



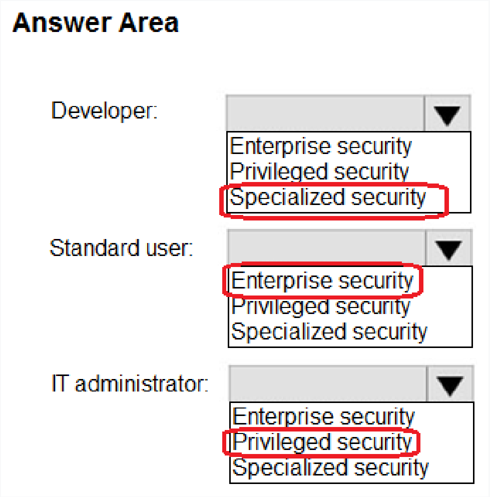
Answer Area

Developer: ▼
Enterprise security
Privileged security
Specialized security

Standard user: ▼
Enterprise security
Privileged security
Specialized security

IT administrator: ▼
Enterprise security
Privileged security
Specialized security

Suggested Answer:



Answer Area

Developer: ▼
Enterprise security
Privileged security
[✓ Specialized security]

Standard user: ▼
[✓ Enterprise security]
Privileged security
Specialized security

IT administrator: ▼
Enterprise security
[✓ Privileged security]
Specialized security

Jacquesvz Highly Voted 1 year, 11 months ago

Correct Answer: reference = https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra (check page 59 of the MCRA powerpoint deck)

upvoted 17 times

lt9898 11 months, 2 weeks ago

Now on slide 84 as of the Dec 2023 update

upvoted 4 times

billo79152718 10 months, 1 week ago

Correct. Thanks.

upvoted 1 times

TomasValtor 1 year, 1 month ago

check page 60 of the MCRA powerpoint deck

upvoted 2 times

⊟ **TomasValtor** 1 year, 1 month ago

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

upvoted 1 times

⊟ **zellck** Highly Voted 1 year, 7 months ago

1. Specialised security
2. Enterprise security
3. Privileged security

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#specialized
Specialized security provides increased security controls for roles with an elevated business impact (if compromised by an attacker or malicious insider).
Specialized roles typically include:
- Developers of business critical systems.

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#enterprise
Enterprise security is suitable for all enterprise users and productivity scenarios. In the progression of the rapid modernization plan, enterprise also serves as the starting point for specialized and privileged access as they progressively build on the security controls in enterprise security.

upvoted 6 times

⊟ **zellck** 1 year, 7 months ago

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#privileged
Privileged security is the highest level of security designed for roles that could easily cause a major incident and potential material damage to the organization in the hands of an attacker or malicious insider. This level typically includes technical roles with administrative permissions on most or all enterprise systems (and sometimes includes a select few business critical roles)

upvoted 2 times

⊟ **dsatizabal** Most Recent 5 months, 2 weeks ago

The only problem with slide 84 of MCRA PPT is that devs and admins show both on specialized and privileged accounts

upvoted 1 times

⊟ **[Removed]** 1 year, 9 months ago

This mentioned above reference architecture is really a hardcore.

upvoted 1 times

⊟ **God2029** 1 year, 10 months ago

An Easy pick, based on the insider threat logic

upvoted 1 times

Question #19 *Topic 1*

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment.

You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Suggested Answer: *ACE*

Community vote distribution

ACE (89%) | 11%

Stubentiger Highly Voted 2 years, 5 months ago

Selected Answer: ACE

answers ok.

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 20 times

Pinpin42 Most Recent 8 months ago

ACE

https://learn.microsoft.com/en-us/training/modules/introduction-zero-trust-best-practice-frameworks/3-zero-trust-initiatives?source=learn

upvoted 1 times

KRISTINMERIEANN 1 year, 2 months ago

Selected Answer: ACE

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 2 times

Naqsh27 1 year, 5 months ago

Selected Answer: BCE

As of the Dec 2023 Slides it should be

Secure Identities and Access

Modern SecOps

Infrastructure and Development Security

upvoted 1 times

Ramye 1 year, 5 months ago

Based on the given answers, answer B is not a Zero Trust principle but answer A is.

upvoted 1 times

TomasValtor 1 year, 7 months ago

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

upvoted 1 times

TomasValtor 1 year, 7 months ago

check page 22 of the MCRA powerpoint deck

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: ACE

ACE is the answer.

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview#ramp-initiatives-for-zero-trust
Top priority
- User access and productivity
- Data, compliance, and governance
- Modernize security operations

upvoted 3 times

⊟ **alifrancos** 2 years, 2 months ago

Selected Answer: ACE

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview
User access and productivity
Data, compliance, and governance
Modernize security operations

As needed:
OT and Industrial IoT
Datacenter & DevOps Security

upvoted 3 times

⊟ **alifrancos** 2 years, 2 months ago

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 1 times

⊟ **MichaelMu** 2 years, 2 months ago

To rapidly adopt Zero Trust in your organization, RaMP(Rapid Modernization Plan) offers technical development guidance organized in these initiatives.
The top priority initiatives are
1. User access and productivity
2 Data, compliance and governance
3 Modernize security operations.

As needed initiatives are
1. OT and industrial IoT
2 Datacenter and DevOps Security

upvoted 1 times

⊟ **Fal991l** 2 years, 3 months ago

Selected Answer: BCE

ChatGTP: Based on the Zero Trust Rapid Modernization Plan (RaMP), the top three modernization areas to prioritize are:

B. Infrastructure and development, to ensure a secure foundation for the IT environment.
C. User access and productivity, to ensure secure and efficient access to resources for users.
E. Modern security operations, to detect and respond to security incidents and threats in real-time.

Therefore, options B, C, and E are the correct answers.

upvoted 3 times

⊟ **technocorgi** 2 years, 2 months ago

while chatGPT also gave me the same answer, https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview lists ACE as the correct answer

upvoted 1 times

⊟ **AJ2021** 2 years, 3 months ago

Selected Answer: ACE

Correct, just a slight rewording on E: Modernize security operations

upvoted 2 times

⊟ **rmafnc** 2 years, 4 months ago

B. infrastructure and development
C. user access and productivity

E. modern security operations

upvoted 3 times

⊟ **Discuss4certi** 2 years, 5 months ago

Selected Answer: ACE

Correct,

link below lists all three as top priorities:

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

in order:

1. user access and productivity: explicitly verify trust for identities, devices, apps and networks
2. data, complaince and governance: ransomware readiness and data policies
3. modern security operations: streamline response, unify visibility, reduce manual effort.

upvoted 4 times

⊟ **smosmo** 2 years, 5 months ago

Selected Answer: ACE

Correct following RAMP

upvoted 2 times

Question #20 *Topic 1*

HOTSPOT

-

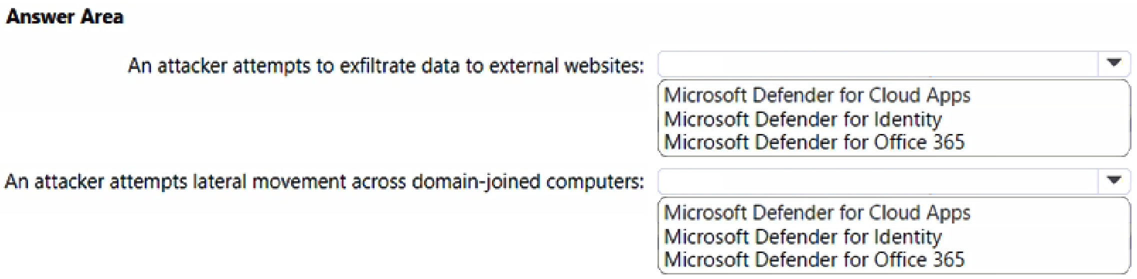
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to protect against the following external threats of an attack chain:

• An attacker attempts to exfiltrate data to external websites.
• An attacker attempts lateral movement across domain-joined computers.

What should you include in the recommendation for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

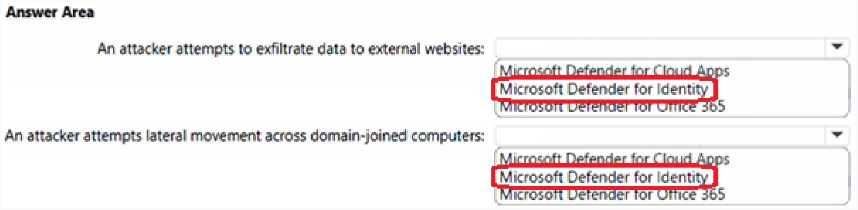
An attacker attempts to exfiltrate data to external websites:

Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers:

Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

Suggested Answer:



Answer Area

An attacker attempts to exfiltrate data to external websites:

Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers:

Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

Sam_Gutterson Highly Voted 2 years, 5 months ago

Exfiltration of data - Defender for Cloud Apps

Data across domains - Defender for Identity

Reference: MCRA Slide 15

upvoted 84 times

plantbased 8 months ago

Correct.

https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls

upvoted 1 times

SFAY 1 year, 4 months ago

Correct, however MCRA(2023) slide number is 67

upvoted 6 times

cyber_sa Highly Voted 1 year, 8 months ago

got this in exam 6oct23. passed with 896 marks. I answered

MD FOR CLOUD APPS

MD FOR IDENTITY

upvoted 16 times

allinict_111 1 year, 5 months ago

that's not mean that's the answer, we must know if that's the answer to this question if not please say nothing then.

upvoted 2 times

Ramye 1 year, 5 months ago

Be thankful that s/he's sharing this and the fact s/he's got high score, most likely this is correct.

upvoted 8 times

Ali96 Most Recent 4 months, 1 week ago

An attacker attempts to exfiltrate data to external websites: Microsoft Defender for Cloud Apps

An attacker attempts lateral movement across domain-joined computers: Microsoft Defender for Identity

upvoted 4 times

Pinpin42 8 months ago

https://learn.microsoft.com/en-us/training/modules/case-study-design-solutions-security-best-practices-priorities/3-case-study-answers

To prevent a ransomware attacker from copying files outside of the Microsoft 365 tenant, customers can use Microsoft Purview Data Loss Prevention (DLP) policies, which detect, warn, and block risky, inadvertent, or inappropriate sharing of data containing personal data and confidential organization information based on sensitivity labels. This can be supplemented by Microsoft Defender for Cloud Apps, which supports session monitoring as part of Conditional Access App Control. The monitoring applies to the flow of data between users and managed applications and can be used to block transfers of business sensitive content.

upvoted 1 times

Pinpin42 8 months ago

Exfiltration of data - Defender for Cloud Apps

Data across domains - Defender for Identity

Reference: MCRA Slide 67 and https://learn.microsoft.com/en-us/training/modules/design-resiliency-strategy-common-cyberthreats-like-ransomware/1-common-cyberthreats-attack-patterns

upvoted 1 times

Ruttoh 9 months, 1 week ago

To protect against the specified external threats in a Microsoft cloud environment based on the Microsoft Cybersecurity Reference Architectures (MCRA), you should include the following recommendations:

For an attacker attempting to exfiltrate data to external websites:

Microsoft Defender for Cloud Apps: This solution provides comprehensive visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all your cloud services1.

For an attacker attempting lateral movement across domain-joined computers:

Microsoft Defender for Identity: This tool helps detect and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization

https://learn.microsoft.com/en-us/security/adoption/mcra

upvoted 1 times

b9e98e8 1 year, 1 month ago

I dont know correct answer but here is though:

MDO - Email forwarding rule

Defender For Cloud - Suspicious Network behavior + user anomaly behavior + Suspicious File Activity Alert

MDCA - Cloud Anomaly detection (supply chain attack) , This policy will be depreciated

Sentinel - UBEA , custom KQL based alerts (for data weight based transaction , number of transaction) + Single browser session + DNS sinkhole alerts from custom Firewall Data sources

ALL of above are indicators of Data Exfiltration.

upvoted 1 times

Navya6784 1 year, 1 month ago

Exfiltration of data - MS Defender for Cloud Apps

Data across domains - Defender for Identity

upvoted 1 times

TamZei 1 year, 2 months ago

Preventing Data Exfiltration is by Microsoft Defender for Cloud Apps

https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls#:~:text=against%20replay%20attacks.-,Microsoft%20Defender%20for%20Cloud%20Apps,-Actions%20that%20would

upvoted 1 times

⊟ **Murtuza** 1 year, 5 months ago

Actions that would compromise the security of customer data must be detected and prevented. For example, employees may be using an unapproved cloud application for storing sensitive corporate data or downloading a vast number of sensitive files for exfiltration. These actions can be prevented by Microsoft Defender for Cloud Apps.

upvoted 3 times

⊟ **UberTech_1888** 1 year, 11 months ago

the keyword is "Attacker" = "Identity"

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

1. Microsoft Defender for Cloud Apps
2. Microsoft Defender for Identity

https://learn.microsoft.com/en-us/defender-for-identity/what-is
Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

upvoted 3 times

⊟ **Fal991l** 2 years, 3 months ago

An attacker attempts to exfiltrate data to external websites:
Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers:
Microsoft Defender for Identity

upvoted 3 times

⊟ **Fal991l** 2 years, 3 months ago

To protect against an attacker attempting to exfiltrate data to external websites, the best solution would be to use Microsoft Defender for Office 365, which can help detect and prevent data exfiltration attempts. It provides data loss prevention (DLP) policies that can identify and protect sensitive information, and advanced threat protection (ATP) that can detect and block suspicious activities.

To protect against an attacker attempting lateral movement across domain-joined computers, the best solution would be to use Microsoft Defender for Identity. It provides continuous monitoring of user activities, behavior analytics, and machine learning-based detection capabilities to identify and block suspicious activities. It can also help identify and remediate weak passwords, and enforce multi-factor authentication (MFA) policies to prevent unauthorized access. Microsoft Defender for Identity can also integrate with other security solutions, such as Azure Sentinel, to provide a comprehensive security solution.

upvoted 1 times

⊟ **Fal991l** 2 years, 3 months ago

While Microsoft Defender for Cloud Apps can help protect against data exfiltration attempts, it is primarily focused on protecting against threats to cloud applications, such as Microsoft 365, Dynamics 365, and more. It can monitor user activity, detect suspicious behavior, and help enforce policies to prevent data exfiltration.

However, if an attacker is attempting to exfiltrate data from a device or a network that is not connected to a cloud application, Microsoft Defender for Cloud Apps may not be effective. In this case, Microsoft Defender for Office 365, which provides advanced threat protection and data loss prevention policies, would be a better solution.

So, for protecting against an attacker attempting to exfiltrate data to external websites, the best solution would be to use Microsoft Defender for Office 365, which is specifically designed for this purpose.

upvoted 1 times

⊟ **Holii** 2 years ago

Defender for O365 is designed for SharePoint, Exchange and phishing/spam attempts for data transferred via email. It is not designed to handle data being exfiltrated to websites.

Also, I am not even sure if Microsoft Defender for O365 can do DLP anymore, I believe that functionality has been shifted to Microsoft Purview.

MDCA is designed for data exfiltration/tracking for websites, and CAN still perform DLP through its action portal (it has separate functionality from Purview) on a variety of policy-types.

upvoted 3 times

⊟ **OCHT** 2 years, 3 months ago

For Box 1:

The recommendation should be MS Defender for Cloud Apps as it can protect the cloud application and its data from unauthorized access, and it has the capability to detect and prevent data exfiltration attempts.

For Box 2:

The recommendation should be MS Defender for Identity, as it can protect against lateral movement by detecting and blocking suspicious activities across domain-joined computers. It can also identify and remediate misconfigurations and vulnerabilities in the identity infrastructure that attackers could exploit to move laterally.

upvoted 7 times

⊟ **AJ2021** 2 years, 3 months ago

First answer incorrect.
Should be:
MDCA
MDI

upvoted 1 times

⊟ **Gurulee** 2 years, 4 months ago

"Employees may be using an unapproved cloud application for storing sensitive corporate data or downloading a vast number of sensitive files for exfiltration. These actions can be prevented by Microsoft Defender for Cloud Apps."

upvoted 3 times

⊟ **buguinha** 2 years, 4 months ago

Defender Cloud Apps to the first and MDI to the second

upvoted 1 times

Question #21 *Topic 1*

For an Azure deployment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

You need to recommend a best practice for implementing service accounts for Azure API management.

What should you include in the recommendation?

A. application registrations in Azure AD

B. managed identities in Azure

C. Azure service principals with usernames and passwords

D. device registrations in Azure AD

E. Azure service principals with certificate credentials

Suggested Answer: *B*

Community vote distribution

B (70%) A (26%) 4%

mynk29 Highly Voted 2 years, 5 months ago

Selected Answer: A

It depends on what is "Service account" in the question. Microsoft benchmark recommends https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline to use OAuth 2.0 "Configure your Azure API Management instance to protect your APIs by using the OAuth 2.0 protocol with Azure AD." --> App registration

AND
managed identity for the "to allow your API Management instance to easily and securely access other Azure AD-protected resources, such as Azure Key Vault instead of using service principals." --> Managed Identity

Its poorly worded question but I would choose A since key consideration for an API gateway in general is authentication of developers which warrants app registration.

upvoted 15 times

Gurulee 2 years, 4 months ago

Agreed

upvoted 2 times

kalyankrishna1 1 year, 8 months ago

app reg, SPs with certs, managed Identities all eventually end up as service principals anyways and the most secure type of SP is a managed Identity, so B is the correct answer

upvoted 3 times

maku067 2 years, 5 months ago

At the begining I pointed to rather B but now I choose rather A.
https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-aad#manually-enable-azure-ad-application-and-identity-provider
Step 6

upvoted 4 times

smosmo 2 years, 5 months ago

I still think it is B: https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline in context with SERVICE PRINCIPALS in section IM3

upvoted 11 times

Rocko1 Highly Voted 2 years, 3 months ago

Selected Answer: B

managed identities in Azure recommended solution for service accounts

upvoted 13 times

MarcoHurry Most Recent 5 months, 2 weeks ago

Selected Answer: B

I agree on B because in https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline
at IM-3: Manage application identities securely and automatically
we can read "use a Managed Service Identity generated by Azure Active Directory (Azure AD) to allow your API Management instance to easily and securely access etc..."

upvoted 1 times

Tony416 9 months, 1 week ago

Selected Answer: B

Considering the following statement, I chose B because it mentions best practices for implementing service accounts. But it's tricky :S
Statement:
"You need to recommend a best practice for implementing service accounts for Azure API management."

upvoted 2 times

Ramye 1 year, 5 months ago

The keyword in the questions is “Implementing Service Accounts” and for the Managed Identity is the answer

upvoted 5 times

sherifhamed 1 year, 9 months ago

Selected Answer: B

B. Managed identities in Azure: Managed identities provide a way to automatically manage the credentials used by applications and services. Using managed identities is a best practice for securing access to Azure resources without the need for storing and managing credentials. It aligns with the principle of least privilege and reduces the risk associated with credential exposure.

upvoted 3 times

BlackZeros 1 year, 11 months ago

Selected Answer: B

Option B seems like the most secure option.
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline#im-3-manage-application-identities-securely-and-automatically

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: E

Azure service principals with certificate credentials

upvoted 3 times

> **Ario** 1 year, 11 months ago
>
> B is the correct answer
>
> upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-use-managed-service-identity
A managed identity generated by Azure Active Directory (Azure AD) allows your API Management instance to easily and securely access other Azure AD-protected resources, such as Azure Key Vault. Azure manages this identity, so you don't have to provision or rotate any secrets.

upvoted 3 times

Tictactoe 2 years, 1 month ago

B right

upvoted 1 times

alifrancos 2 years, 2 months ago

Selected Answer: B

it is Managed Identity,
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline
IM-3

upvoted 6 times

shahnawazkhot 2 years, 2 months ago

I think the answer should be between Service Principal options and managed identity option... And in these options, managed identity option is preferred here considering better security and convenience. Therefore, the correct answer appears to be option "B".

upvoted 1 times

⊟ **etblue** 2 years, 3 months ago

Refer to https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline IM-3 Manage application identities securely and automatically, selected answer should be B. There is nothing listed in API management security baseline regards to app registration. I do think by using managed identity would meant require earlier app registration as pre-requisite. Hence, answer B is more comprehensive.

upvoted 4 times

⊟ **AJ2021** 2 years, 3 months ago

Selected Answer: B

Configuration Guidance: Use a Managed Service Identity generated by Azure Active Directory (Azure AD) to allow your API Management instance to easily and securely access other Azure AD-protected resources, such as Azure Key Vault instead of using service principals. Managed identity credentials are fully managed, rotated, and protected by the platform, avoiding hard-coded credentials in source code or configuration files.
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline

upvoted 4 times

⊟ **Fal991l** 2 years, 3 months ago

Selected Answer: B

ChatGPT:The Microsoft Cloud Security Benchmark recommends using managed identities in Azure as a best practice for implementing service accounts for Azure API management. Managed identities are a secure and automated way to provide applications running on Azure services with an automatically managed identity in Azure Active Directory (Azure AD). By using managed identities, you can avoid storing credentials in your code or configuration files, which reduces the risk of exposing sensitive information.

Therefore, the correct answer is B. Managed identities in Azure.

upvoted 3 times

⊟ **PeteNZ** 2 years, 3 months ago

B - managed identities because: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-introduction-azure

upvoted 1 times

⊟ **PeteNZ** 2 years, 4 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline

upvoted 2 times

Question #22 *Topic 1*

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators groups on the Windows computers.

You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised.

What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

Suggested Answer: *A*

Community vote distribution

A (93%) 3%

zellck Highly Voted 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
Windows Local Administrator Password Solution (Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Azure Active Directory-joined or Windows Server Active Directory-joined devices. You also can use Windows LAPS to automatically manage and back up the Directory Services Restore Mode (DSRM) account password on your Windows Server Active Directory domain controllers. An authorized administrator can retrieve the DSRM password and use it.

upvoted 8 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 2 times

yarvis Highly Voted 2 years, 4 months ago

Selected Answer: A

LAPS - https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

upvoted 5 times

P1mp Most Recent 7 months, 1 week ago

Selected Answer: A

Implement LAPS to securely manage and randomize local administrator passwords. This ensures administrative access is provided securely and minimizes the risk of lateral movement in the event of an account compromise.

upvoted 1 times

Dirkonormalo 7 months, 3 weeks ago

Selected Answer: C

I configured that with pim too. We decided against laps, because we wanted personalized accounts in central audit with justification. Ites confusing me

upvoted 2 times

keithtemplin 10 months, 1 week ago

Selected Answer: C

You add an empty domain group to the local admins group. You use Azure PIM to provide JITA membership to that group.
https://techcommunity.microsoft.com/t5/intune-customer-success/configuring-microsoft-intune-just-in-time-admin-access-with/ba-p/3843972

upvoted 2 times

besoaus 1 year ago

I'm confused, Why not "C"? PIM will allow us to apply the same, and we can give also "Just in time" Access. And it will eliminate Lateral movement

upvoted 3 times

[Removed] 1 year, 3 months ago

Selected Answer: D

PAWs are specifically designed to minimize the risk of lateral movement by segregating administrative tasks to dedicated workstations. Admins use these workstations solely for privileged activities, reducing the chances of exposing credentials in less secure environments. This strategy helps to contain and limit the impact of compromised administrator accounts on regular workstations.

upvoted 1 times

Zabulon777 1 year, 3 months ago

Wrong as you are not going to deploy PAW machines to every employee in the company. It specifies changing the administrator account on all machines which LAPS does. Answers is A

upvoted 1 times

Ramye 1 year, 5 months ago

The more I read about LAPS the more confusing it is.
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-scenarios-azure-active-directory

upvoted 2 times

JG56 1 year, 7 months ago

LAPS is the answer, in exam Nov 23

upvoted 3 times

Kvoth3 1 year, 10 months ago

What about D.
To provide users with administrative access to the Windows computers only when access is required, you can use Privileged Access Workstations (PAWs). PAWs are dedicated operating systems for sensitive tasks that are protected from Internet attacks and threat vectors. They separate these sensitive tasks and accounts from the daily use workstations and devices, providing strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket 1.

PAWs can be used to minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised. PAWs provide a secure environment for administrative tasks that require elevated privileges. They are designed to protect against advanced persistent threats (APTs) and other sophisticated attacks.

upvoted 4 times

nExoR 1 year, 6 months ago

PAWs are administration workstations. concept from totally different area. the question asks about users having access on their regular workstations - e.g. to install app. not some specialized, isolated workstation

upvoted 1 times

Ario 1 year, 12 months ago

for those check discussions don't be fool by most rated answers .

upvoted 4 times

Baz10 1 year, 3 months ago

Hahah leaving a riddle and then dipping smh

upvoted 2 times

Bondaexam 1 year, 6 months ago

what should be the final judgement when multiple answers are chosen by multiple people . Dont tell us to go back and look into the documentation, we all know that . What should be the final judgement???

upvoted 1 times

Itu2022 2 years ago

was on exam 15/06/23

upvoted 2 times

edurakhan 2 years, 1 month ago

On exam 5/25/2023

upvoted 2 times

init2winit 2 years, 2 months ago

Selected Answer: A

Agree with A, as Yarvis pointed out in the link.

For endpoint administrative management, use the local administrative password solution (LAPS).

upvoted 2 times

Bouncy 2 years, 4 months ago

Selected Answer: A

A, but only because the others don't make sense.

If you ever need to remove admins from PCs in real life, do not use LAPS. Use Microsoft Intune Endpoint Privilege Management instead. It lets you decide precisely for which action users may receive an elevation, whereas LAPS will give users full local admin access until the password changes - which can take days or even weeks in reality...

upvoted 4 times

ARYMBS 1 year, 9 months ago

This does not work on Hybrid AzureAD Joined....

upvoted 1 times

jasscomp 1 year, 9 months ago

Incorrect - it does work on HAADJ devices - worked for me

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview#understand-device-join-state-restrictions

upvoted 1 times

mynk29 2 years, 5 months ago

Selected Answer: A

Granting users access to their PC is not the typical use case for LAPS- admins use it for troubleshooting/as a break glass account.

But PIM is explicitly not meant to do it. see https://www.reddit.com/r/Intune/comments/yqdiyf/azure_ad_joined_device_local_admin_via_pim/

PAW and Identity protection are not relevant so will reluctantly go with A.

upvoted 3 times

Jacquesvz 2 years, 5 months ago

Selected Answer: A

Agree with A, check this link for reason - https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-guide-how-to-configure-microsoft-local/ba-p/2806185

upvoted 5 times

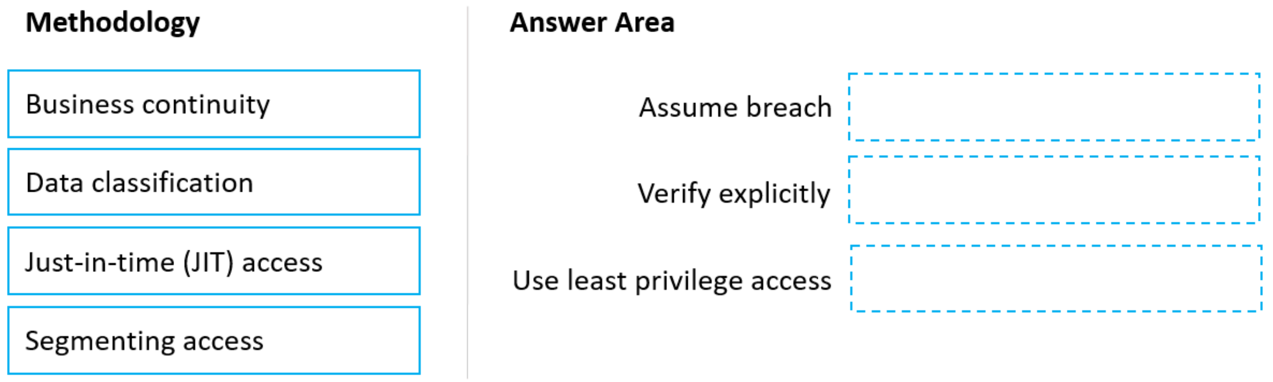
Question #23 *Topic 1*

29 DRAG DROP

For a Microsoft cloud environment, you need to recommend a security architecture that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security methodologies should you include in the recommendation? To answer, drag the appropriate methodologies to the correct principles. Each methodology may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Methodology

- Business continuity
- Data classification
- Just-in-time (JIT) access
- Segmenting access

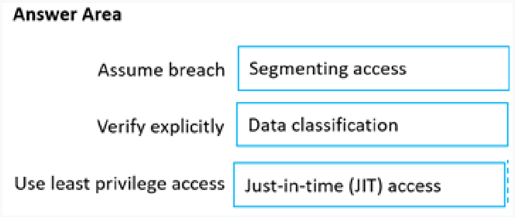
Answer Area

Assume breach

Verify explicitly

Use least privilege access

Suggested Answer:



Answer Area

Assume breach	Segmenting access
Verify explicitly	Data classification
Use least privilege access	Just-in-time (JIT) access

zellck Highly Voted 2 years, 1 month ago

1. Segmenting access
2. Data classification
3. JIT access

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust

- Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

- Verify explicitly

Always authenticate and authorize based on all available data points.

- Use least privilege access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

upvoted 21 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 4 times

Baz10 Highly Voted 1 year, 2 months ago

On Exam 8 Apr 2024 scored 764

1. Segmenting access
2. Data classification
3. JIT access

upvoted 6 times

Er_01 Most Recent 4 months, 2 weeks ago

1 - segment access - assume breach means contain attacker

2- JIT - slide 31 JIT / JEA under explicit and least privileged.

The issue is they left out JEA as an option but per slide 31 it infers both.

Misleading question that requires more clarity and accuracy for such a fundamental concept.

upvoted 1 times

Lapatiser 8 months, 1 week ago

From page 31 of MCRA, correct answer is:

Business continuity

Segmenting Access

Just-in-time (JIT)

upvoted 2 times

alessag 5 months, 2 weeks ago

I don't think it is correct because slide #31 doesn't mention Business continuity, but business enablement. It is a bit different. Question is: please help me to understand why do you think behind enablement = business continuity?

upvoted 1 times

emartiy 1 year ago

I have checked MCRA presentation (Pages 31-32) Source: aka.ms/MCRA(Download presentation file from link bottom of page on the link aka)

1-Business continuity - Assume breach

2 -Segmenting - Verify explicitly

3 -Just-intime (JIT) - Use least privilege access

upvoted 1 times

alessag 5 months, 2 weeks ago

I don't think it is correct because slide #31 doesn't mention Business continuity, but business enablement. It is a bit different. Question is: please help me to understand why do you think behind enablement = business continuity?

upvoted 2 times

cris_exam 1 year, 4 months ago

Answer seems correct. Slide 31 of the MCRA.

https://github.com/MicrosoftDocs/security/blob/main/Downloads/mcra-december-2023.pptx?raw=true

upvoted 2 times

Ario 1 year, 12 months ago

Segmenting access is an important methodology for implementing a least privileged access approach within a Zero Trust architecture

upvoted 2 times

edurakhan 2 years, 1 month ago

Exam question 5/25/2023

upvoted 4 times

PrettyFlyWifi 2 years, 2 months ago

Slide 20 of the MCRA, answer looks correct!

upvoted 3 times

God2029 2 years, 4 months ago

Segmentation will contain the breach with the specific instance - This will help to isolate the breach. Enforcing Principle 1 : Assume Breach

Data Classification helps to determine the most sentive data and labeling them, enforcing RBAC based access control on the data will help to enforce the Principle 2 Verify Explicitly.

Finally JIT is providing access based on time period, Enforcing the 3rd in the list, Principles of Least Previlage

upvoted 4 times

Ceuse 2 years, 4 months ago

Answer Looks Good :

https://www.microsoft.com/en-us/security/business/zero-trust

Zero Trust principles

Verify explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least-privilege access
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

upvoted 3 times

⊟ **Jame** 2 years, 4 months ago

I think Answer is correct.

https://www.microsoft.com/en-us/security/business/zero-trust

Zero Trust principles

Verify explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least-privilege access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

upvoted 4 times

Question #24 *Topic 1*

You have legacy operational technology (OT) devices and IoT devices.

You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures (MCRA). The solution must minimize the risk of disrupting business operations.

Which two security methodologies should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. active scanning

B. threat monitoring

C. software patching

D. passive traffic monitoring

Suggested Answer: *BC*

Community vote distribution

BD (84%) BC (16%)

El_m_o Highly Voted 👍 2 years, 4 months ago

Selected Answer: BD

From MCRA slide 17 (OT): "Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, so they can only be selectively applied (or have a limited security effect). Basic security hygiene for OT starts with network isolation (including good maintenance/**monitoring** of that isolation boundaries), **threat monitoring**, and carefully managing vendor access risk."

upvoted 22 times

dsatizabal 5 months, 2 weeks ago

As per Jan 2025 this is slide 61 of MCRA, observe that the information is in the slide's notes, not on the slides canvas contents.

upvoted 1 times

Ajdlfasudfo0 Highly Voted 👍 2 years, 4 months ago

Selected Answer: BC

In some legacy environments where modern authentication protocols are unavailable such as operational technology (OT), network controls may be used exclusively. - Slide 61, MCRA

Slide 17 -
OT - Safety/Integrity/Availability
Hardware Age: 50-100 years (mechanical + electronic overlay)
Warranty length: up to 30-50 years
Protocols: Industry Specific (often bridged to IP networks)
Security Hygiene: Isolation, threat monitoring, managing vendor access risk, (patching rarely)

upvoted 9 times

danb67 Most Recent 🕒 1 year ago

Answer correct based on slide 60 of the MCRA passive collection) – provides data gathering with passive traffic monitoring to avoid disruption of OT and IIoT operations. This passive approach is critical because active scanning can slow or disrupt business operations (potentially altering sensitive physical operation timing or potentially crashing older OT computer systems).

Security Hygiene - threat monitoring

upvoted 2 times

emartiy 1 year ago

Selected Answer: BD

I continue with this options based on MCRA slides... A is someting performance reducing progress so option D is more reliable and option B since question says "which security methodolgy"

upvoted 1 times

Baz10 1 year, 2 months ago

Selected Answer: BD

On Exam 8 Apr 2024 scored 764

upvoted 4 times

[Removed] 1 year, 3 months ago

Selected Answer: BD

D. Passive Traffic Monitoring:

Passive traffic monitoring involves observing network traffic without actively scanning or disrupting devices. This approach aligns with Zero Trust principles by allowing you to gain insights into the behavior of devices without introducing potential risks associated with active scanning. It helps in understanding the normal traffic patterns and identifying anomalies or suspicious activities without impacting the operation of OT and IoT devices.
B. Threat Monitoring:

Threat monitoring is essential for actively monitoring and analyzing security events to detect and respond to potential threats. Implementing threat monitoring aligns with Zero Trust principles by continuously assessing the security posture of OT and IoT devices. This proactive approach enables the identification of security incidents and allows for timely responses to mitigate risks, all while minimizing disruptions to business operations.

upvoted 3 times

Charly80 1 year, 5 months ago

MCRA Slide 65 "Apply zero trust principles to securing OT and industrial IoT environments" : Security Hygiene: Multi-factor authentication (MFA), patching, threat monitoring, antimalware

upvoted 2 times

Funkydave 1 year, 9 months ago

"The solution must minimize the risk of disrupting business operations."

patching is absolutely not non-disruptive

upvoted 4 times

POOJI123 1 year, 10 months ago

what is mcra slide mentioned in comments how do i find it

upvoted 1 times

theplaceholder 1 year, 10 months ago

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

upvoted 1 times

Ario 1 year, 12 months ago

BD is correct

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: BD

BD is the answer.

OT Security hygiene is different because these systems frequently weren't built with modern threats and protocols in mind (and often rely on 'end of life' software). Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, so they can only be selectively applied (or have a limited security effect). Basic security hygiene for OT starts with network isolation (including good maintenance/monitoring of that isolation boundaries), threat monitoring, and carefully managing vendor access risk.

upvoted 4 times

Tictactoe 2 years, 1 month ago

BD right

upvoted 1 times

PrettyFlyWifi 2 years, 2 months ago

Selected Answer: BD

B and D seem most suitable here, both are mentioned on slide 17 of MCRA.
It doesn't look like C - Software patching is a valid answer. Look at slide 17 of MCRA it states "Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, so they can only be selectively applied (or have a limited security effect). ", so this confirms it isn't practical, so it can't be "best practice".

upvoted 4 times

edurakhan 2 years, 2 months ago

Selected Answer: BC

I would go with threat monitoring and patching (rarely, according to MCRA, but there is nothing about passive traffic monitoring)

upvoted 1 times

zellck 2 years, 1 month ago

Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, so they can only be selectively applied (or have a limited security effect).

upvoted 2 times

GeVanDerBe 2 years, 2 months ago

Read the notes in slide 17 --> Microsoft's approach to threat monitoring is focused on bringing modern security approaches that also deeply respects the constraints and sensitivity of these systems. The approach is based on technology developed by CyberX (recently acquired and integrated into Microsoft).

The solution consists of

Network TAP/SPAN (passive collection) – provides data gathering with passive traffic monitoring to avoid disruption of OT and IIoT operations.

upvoted 3 times

Fal991l 2 years, 3 months ago

Selected Answer: BD

ChatGTP: The two security methodologies that should be included in the recommendation for applying Zero Trust principles to OT and IoT devices based on the MCRA while minimizing the risk of disrupting business operations are:

B. Threat monitoring: Continuous monitoring and analysis of network traffic, system logs, and other data sources can help detect and respond to threats and attacks targeting OT and IoT devices. Threat monitoring can help identify indicators of compromise (IoCs) and provide early warning of potential security incidents.

D. Passive traffic monitoring: Passive traffic monitoring involves monitoring network traffic without actively sending packets or generating traffic. This approach can help minimize the risk of disrupting business operations while still providing visibility into network activity and potential security incidents. Passive traffic monitoring can also help identify anomalies and suspicious activity that may indicate a security threat.

upvoted 4 times

Fal991l 2 years, 3 months ago

Option A, active scanning, and option C, software patching, are not necessarily the best practices for applying Zero Trust principles to OT and IoT devices, as they can potentially disrupt business operations and cause compatibility issues with legacy devices. While software patching can help mitigate vulnerabilities, it should be done in a controlled and tested manner to avoid introducing new issues or downtime.

upvoted 3 times

aks_exam 1 year, 4 months ago

ChatGPT may lead you to the right answer, but please don't comment on what it explains.

upvoted 1 times

AJ2021 2 years, 3 months ago

Selected Answer: BD

Adapt processes to Operational Technology (OT) - Adjust your tools and processes to the constraints of OT environments as you integrate them. These environments prioritize safety and often have older systems which don't have patches available and may crash from an active scan. Focusing on approaches like passive network detections for threats and isolation of systems is often the best approach.

https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/3-recommend-for-protecting-from-insider-external-attacks

upvoted 5 times

Question #25 *Topic 1*

You have an on-premises network and a Microsoft 365 subscription.

You are designing a Zero Trust security strategy.

Which two security controls should you include as part of the Zero Trust solution? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Always allow connections from the on-premises network.

B. Disable passwordless sign-in for sensitive accounts.

C. Block sign-in attempts from unknown locations.

D. Block sign-in attempts from noncompliant devices.

Suggested Answer: *CD*

Community vote distribution

CD (89%) 11%

⊟ **bmulvIT** Highly Voted 👍 1 year, 7 months ago

Selected Answer: CD

MRCA slide 15 recommmends using passwordless so B is wrong.. "The top priority is to require strong multi-factor authentication (MFA), (and preferably Passwordless authentication). Attackers have easy availability to compromised username/passwords and commonly used passwords, so organizations must prioritize moving beyond password-only authentication as their first step. "

upvoted 5 times

⊟ **JG56** Highly Voted 👍 1 year, 1 month ago

C,D is right answer, in exam Nov 23

upvoted 5 times

⊟ **cris_exam** Most Recent ⏱ 10 months, 2 weeks ago

Selected Answer: CD

Slide 14 from MCRA: "Require separate accounts for Admins and enforce MFA/passwordless"

This rules out B so I go with C & D.

upvoted 2 times

⊟ **BlackZeros** 1 year, 5 months ago

Selected Answer: BC

B seems to be the most obvious answer, since MFA on all Admin accounts is the very basic best practice.

C is most likely the case since company doesnt want to have the access given to anyone outside of onprem network.

D is irrelevant in this case because the devices are part of the onprem network, which is not a big threat since option C will enforce the connectivity to be from internal network only.

upvoted 1 times

⊟ **jasscomp** 1 year, 3 months ago

Zero Trust is about always assuming breach. MFA should ideally be enabled for everyone not just sensitive accounts.

upvoted 2 times

⊟ **hw121693** 1 year, 5 months ago

According to microsoft passwordless is the best way to protect account, better than MFA

upvoted 3 times

⊟ **zellck** 1 year, 7 months ago

Selected Answer: CD

CD is the answer.

https://learn.microsoft.com/en-us/security/zero-trust/deploy/identity#v-user-device-location-and-behavior-is-analyzed-in-real-time-to-determine-risk-and-deliver-ongoing-protection

upvoted 4 times

Tictactoe 1 year, 7 months ago

BC IS CORRECT

upvoted 1 times

CatoFong 1 year, 7 months ago

Selected Answer: CD

CD makes the most sense to me

upvoted 3 times

Hanley1999 1 year, 8 months ago

Disable passwordless sign-in - as in go back to passwords? Doesn't sound like ZT to me

upvoted 2 times

deposros 1 year, 8 months ago

still confused, what should be the answer?

upvoted 1 times

edurakhan 1 year, 8 months ago

Selected Answer: CD

I don’t think A and B make any sense here

upvoted 4 times

shinda 1 year, 8 months ago

Selected Answer: BC

C speaks for itself but B is biometric or FIDO2 only. If they include biometric plus a password aka MFA then it would be okay

upvoted 1 times

Question #26 *Topic 1*

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

Suggested Answer: *B*

Community vote distribution

E (82%) Other

WRITER00347 Highly Voted 👍 1 year, 11 months ago

The primary goal here is to minimize the risk of ransomware encrypting local user files. A feature designed to protect against unauthorized access to critical system files and user data, particularly from ransomware, is protected folders.
Option E, "protected folders," should be included in the recommendation.

In Windows, the Controlled Folder Access feature protects files in key system folders and user-defined folders by only allowing authorized apps to make changes. This can prevent ransomware from encrypting files in those folders.
While some of the other options listed, such as B. Microsoft Defender for Endpoint, may provide broader protection against malware, option E specifically targets the requirement to protect local user files against ransomware encryption. Therefore, the correct answer is:
E. protected folders.

upvoted 31 times

hovlund 1 year, 8 months ago

I Agree!

upvoted 2 times

jasscomp 1 year, 9 months ago

Well explained - thanks

upvoted 2 times

sbnpj Highly Voted 👍 1 year, 11 months ago

Selected Answer: E

Protected folders

upvoted 8 times

sweetykaur Most Recent 🕓 4 months, 3 weeks ago

Selected Answer: E

Protected folders, a feature of Microsoft Defender for Endpoint, can help safeguard your critical data by preventing unauthorized applications, including ransomware, from accessing and encrypting local user files.

upvoted 1 times

emartiy 1 year ago

Selected Answer: E

Protected Folders feature is designed for this scenario. Read about it..

upvoted 1 times

emadmf76 1 year, 1 month ago

Selected Answer: D

the request Includes Encryption, Controlled folder does not include Encryption, only controlling access

upvoted 1 times

zul_n 1 year, 3 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/built-in-protection?view=o365-worldwide

Microsoft Defender for Endpoint helps prevent, detect, investigate, and respond to advanced threats, such as ransomware attacks.

upvoted 4 times

[Removed] 1 year, 3 months ago

Selected Answer: E

Protected Folders is a feature provided by Microsoft Defender Antivirus that helps safeguard specific folders from unauthorized changes. It is designed to protect user files, documents, and data from being encrypted by ransomware. This feature allows you to specify certain folders that are considered sensitive, and any attempt to make changes to files within those folders is closely monitored for suspicious activity.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders?view=o365-worldwide

upvoted 4 times

kazaki 1 year, 3 months ago

Selected Answer: E

Joining to endpoint alone is useless until you start configuring based on your needs

upvoted 2 times

masby661 1 year, 5 months ago

Controlled Folder Access is a feature of Microsoft Defender for Endpoint that helps protect your valuable data from malicious apps and threats, such as ransomware.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders?view=o365-worldwide

upvoted 2 times

JG56 1 year, 7 months ago

in exam Nov 23

upvoted 4 times

Ramye 1 year, 5 months ago

What was your answer?

upvoted 1 times

Lonlystar 1 year, 7 months ago

How can I help keep my PC secure?
Make sure your PC is up to date with the latest version of Windows and all the latest patches. Learn more about Windows Update.

Be sure Windows Security is turned on to help protect you from viruses and malware (or Windows Defender Security Center in previous versions of Windows 10).

In Windows 10 or 11 turn on Controlled Folder Access to protect your important local folders from unauthorized programs like ransomware or other malware.
Link: https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3

upvoted 3 times

snowfresh 1 year, 8 months ago

"Controlled folder access is especially useful in helping to protect your documents and information from ransomware"
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

upvoted 2 times

rahulnair 1 year, 8 months ago

B is correct answer - Controlled folder access works best with Microsoft Defender for Endpoint, which gives you detailed reporting into controlled folder access events and blocks as part of the usual alert investigation scenarios.

upvoted 2 times

ZZNZ 1 year, 10 months ago

E is correct

upvoted 1 times

Socgen1 1 year, 10 months ago

option E
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

upvoted 3 times

⊟ **Darkren4eveR** 1 year, 11 months ago

D

https://learn.microsoft.com/es-mx/azure/security/fundamentals/data-encryption-best-practices

upvoted 1 times

Question #27 *Topic 1*

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

D. an Azure AD user account that has a password stored in Azure Key Vault

Suggested Answer: *D*

Community vote distribution

A (64%) D (36%)

⊟ **WRITER00347** Highly Voted 1 year, 11 months ago

In the context of deploying applications using CI/CD pipelines in Azure and following DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure, using managed identities is often recommended. Managed identities provide an identity for applications to use when connecting to resources that support Azure AD authentication, without needing to manage credentials like usernames and passwords.

A managed identity in Azure is automatically managed by Azure and does not require you to provision or rotate secrets. This aligns with the principles of DevSecOps, where security is integrated into the development process, and the management of secrets and credentials is handled securely and automatically.

So, the correct recommendation for this scenario would be:
A. a managed identity in Azure.

upvoted 16 times

⊟ **ayadmawla** Highly Voted 1 year, 4 months ago

Selected Answer: D

Its both but it depends where the resources needed for CI/CD are stored and who authenticates/authorises access to them. According to the link below: Key Vault makes it possible for your client application to use a secret to access resources not secured by Microsoft Entra ID. Managed identities are automatically managed by Azure.

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

upvoted 5 times

⊟ **ayadmawla** 1 year, 4 months ago

although my concern is for the wording of D : "an Azure AD user account that has a password stored in Azure Key Vault" If it is an Azure account, then it would not be used for external resources. So "A" could be a better answer.

upvoted 2 times

⊟ **Ali96** Most Recent 4 months, 1 week ago

Selected Answer: A

A. A managed identity in Azure is the most appropriate solution because it is secure, doesn't require managing credentials, and integrates seamlessly with Azure services, making it the ideal choice for automated deployments in a CI/CD pipeline

upvoted 1 times

⊟ **Dirkonormalo** 7 months, 3 weeks ago

Selected Answer: A

as writer writes, added for wrote count

upvoted 1 times

Dirkonormalo 7 months, 3 weeks ago

Selected Answer: A

as writer writes, added for wrote count

upvoted 1 times

jayek 1 year ago

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops

upvoted 2 times

Jonada1773 1 year, 2 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

upvoted 1 times

alan9999 1 year, 4 months ago

D as per the link below and key words from the question:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops#azure-key-vault

upvoted 2 times

Jony_2 1 year, 4 months ago

Selected Answer: D

Pipelines and code repositories should not include hard-coded credentials and secrets. Credentials and secrets should be stored elsewhere and use CI vendor features for security.
A.- Is not correct if the CI vendor has internal users/credentials
Check the indicated https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops where indicates "If your CI platform supports it, consider storing credentials in a dedicated secret store, for example Azure Key Vault. Credentials are fetched at runtime by the build agent and your attack surface is reduced."

upvoted 2 times

epomatti 1 year, 4 months ago

Selected Answer: A

Long and behold, Azure DevOps now supports managed identities.

https://devblogs.microsoft.com/devops/introducing-service-principal-and-managed-identity-support-on-azure-devops/

https://learn.microsoft.com/en-us/azure/devops/integrate/get-started/authentication/service-principal-managed-identity?view=azure-devops#create-a-managed-identity

upvoted 5 times

tocane 1 year, 5 months ago

Selected Answer: D

azure devops cannot connect to azure using managed identities (You need to recommend which types of identities to use for the deployment credentials of the service connection.)

upvoted 1 times

> **epomatti** 1 year, 4 months ago
>
> Try practicing and studying a bit before answering nonsense.
>
> https://devblogs.microsoft.com/devops/introducing-service-principal-and-managed-identity-support-on-azure-devops/
>
> https://learn.microsoft.com/en-us/azure/devops/integrate/get-started/authentication/service-principal-managed-identity?view=azure-devops#create-a-managed-identity
>
> upvoted 2 times

rahulnair 1 year, 8 months ago

A - since D says user account

upvoted 3 times

sherifhamed 1 year, 9 months ago

Selected Answer: A

For an Azure DevOps solution that follows DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure, the recommended choice for deployment credentials in a service connection is a managed identity in Azure (Option A).

Here's why this is the recommended choice:

A. Managed identity in Azure: Managed identities provide a secure way to authenticate and authorize services or applications in Azure without the need for explicit credentials such as passwords or secrets. Using a managed identity ensures that your CI/CD pipelines can securely access Azure resources without exposing credentials. It also aligns with best practices for security and eliminates the need to manage and rotate passwords or secrets.

upvoted 4 times

⊟ **ZZNZ** 1 year, 10 months ago

A. a managed identity in Azure
https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

upvoted 1 times

⊟ **theplaceholder** 1 year, 10 months ago

Selected Answer: A

Managed Identities, nobody knows the password, not accessible to anyone except the identity itself.

upvoted 4 times

⊟ **celomomo** 1 year, 10 months ago

Selected Answer: A

A. A managed identity in Azure

Using a managed identity aligns with DevSecOps best practices, as it provides a secure and automated way to manage credentials for your CI/CD pipelines. This approach reduces the risk of exposing sensitive information and follows the principle of least privilege

upvoted 1 times

⊟ **ServerBrain** 1 year, 10 months ago

Selected Answer: A

A, 100%

upvoted 1 times

Question #28 *Topic 1*

You have an Azure Kubernetes Service (AKS) cluster that hosts Linux nodes.

You need to recommend a solution to ensure that deployed worker nodes have the latest kernel updates. The solution must minimize administrative effort.

What should you recommend?

A. The nodes must restart after the updates are applied.

B. The updates must first be applied to the image used to provision the nodes.

C. The AKS cluster version must be upgraded.

Suggested Answer: *B*

Community vote distribution

B (81%) A (19%)

SFAY Highly Voted 10 months, 1 week ago

Selected Answer: B

B is the correct answer.

Microsoft creates a new node image for AKS nodes approximately once per week. A node image contains up-to-date OS security patches, OS kernel updates, Kubernetes security updates, updated versions of binaries like kubelet, and component version updates that are listed in the release notes.

When a node image is updated, a cordon and drain action is triggered on the target node pool's nodes:

A node with the updated image is added to the node pool. The number of nodes added at a time is governed by the surge value.
One of the existing nodes is cordoned and drained. Cordoning ensures that the node doesn't schedule pods. Draining removes its pods and schedules them to other nodes.
After the node is fully drained, it's removed from the node pool. The updated node added by the surge replaces it.
This process is repeated for each node that needs to be updated in the node pool.

A similar process occurs during a cluster upgrade.

Source: https://learn.microsoft.com/en-us/azure/architecture/operator-guides/aks/aks-upgrade-practices
upvoted 7 times

lt9898 10 months, 1 week ago

I now agree with SFAY that it seems like the ideal solution (least admin overhead) would be to leverage 'cordon and drain' via the automated NodeImage update channel and configure an aksManagedNodeosUpgradeSchedule maintenance window. Thanks for sharing the link.

A - No, although this functionality is still supported by the 'unmanaged' update channel, there is now a better solution to minimise admin overhead than leveraging Kured to faciliate an in-place update
B - Yes, we need to ensure the image used to provision the node had been updated (despite it being automatic now). However, agree with SFAY that i'd probably pick this if forced as it's closest.
C - No, the cluster version never needs updating for this

Seems there's no way to update my previous answer below...
upvoted 2 times

Alex1405 Most Recent 1 week, 3 days ago

Selected Answer: C

The AKS cluster version must be upgraded.
In Azure Kubernetes Service (AKS), kernel updates and other OS-level patches (including security updates) for the worker nodes are tied to the AKS cluster version. When you upgrade the AKS cluster, Azure ensures that:
The node image used includes the latest Linux kernel updates and patches.

You automatically get updated base images with minimal manual effort.
Security patches and system updates are applied in a controlled and tested way.

upvoted 1 times

PierreTang 10 months, 1 week ago

Selected Answer: A

Lt9898

upvoted 1 times

lt9898 10 months, 2 weeks ago

Selected Answer: A

Hang on, why is everybody favouring selecting the image before provision of the node? That was my original choice without reading then I found the page below published 20/4/2023.
https://learn.microsoft.com/en-us/azure/aks/node-updates-kured

"To protect your clusters, security updates are automatically applied to Linux nodes in AKS. These updates include OS security fixes or kernel updates. Some of these updates require a node reboot to complete the process. AKS doesn't automatically reboot these Linux nodes to complete the update process.
...
This article shows you how to use the open-source kured (KUbernetes REboot Daemon) to watch for Linux nodes that require a reboot, then automatically handle the rescheduling of running pods and node reboot process"

upvoted 2 times

lt9898 10 months, 1 week ago

Switching to B although I can't edit my initial vote. SFAY shared the more recently updated page that outlines the automated update process via the weekly image updates published by MS.

If the requirements said that we need to stay up to date to the day, then i'd consider Kured to apply the nightly updates available via the 'Unmanaged' update channel

upvoted 1 times

cris_exam 10 months, 2 weeks ago

I tend to be convinced by your finding and also add this extra bit from the same page.

"Some security updates, such as kernel updates, require a node reboot to finalize the process."
"You can use your own workflows and processes to handle node reboots, or use kured to orchestrate the process."

So, reboot seems to be required but these could be configured to happen orchestrated to minimize admin effort.

https://learn.microsoft.com/en-us/azure/aks/node-updates-kured#understand-the-aks-node-update-experience

upvoted 1 times

sbnpj 1 year, 4 months ago

Selected Answer: B

agree wtih the answer

upvoted 2 times

Elvoo 1 year, 4 months ago

Selected Answer: B

Correct

upvoted 2 times

Victory007 1 year, 4 months ago

Selected Answer: B

Answer is Correct.

upvoted 2 times

Question #29 *Topic 1*

You have the following on-premises servers that run Windows Server:

- Two domain controllers in an Active Directory Domain Services (AD DS) domain
- Two application servers named Server1 and Server2 that run ASP.NET web apps
- A VPN server named Served that authenticates by using RADIUS and AD DS

End users use a VPN to access the web apps over the internet.

You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

What should you include in the recommendation?

A. Publish the web apps by using Azure AD Application Proxy.

B. Configure the VPN to use Azure AD authentication.

C. Configure connectors and rules in Microsoft Defender for Cloud Apps.

D. Configure web protection in Microsoft Defender for Endpoint.

Suggested Answer: *A*

Community vote distribution

A (100%)

WRITER00347 Highly Voted 👍 1 year, 4 months ago

The Zero Trust model emphasizes never trusting and always verifying, regardless of whether something is inside or outside the corporate network. It minimizes reliance on traditional network security boundaries and instead focuses on identities, endpoints, and resources.In the given scenario, the main goal is to increase the security of connections to the web apps, aligning with the Zero Trust principles.Option A would align well with these requirements. Azure AD Application Proxy provides secure remote access to your on-premises applications. It allows users to access their apps from anywhere without having to connect to the VPN and enables additional security features like Conditional Access and MFA.
This solution minimizes the attack surface by eliminating the need to expose the web applications directly to the internet and follows the Zero Trust principles of MCRA, making it the appropriate recommendation.So the correct answer is: A

upvoted 12 times

cris_exam 10 months, 2 weeks ago

You must be in love with GPT

upvoted 9 times

JG56 Most Recent 🕒 1 year, 1 month ago

A , in exam Nov 23

upvoted 3 times

Myguard 1 year, 1 month ago

Selected Answer: A

Correct Answer

upvoted 2 times

Victory007 1 year, 4 months ago

Selected Answer: A

Correct Answer

upvoted 2 times

Question #30 *Topic 1*

HOTSPOT

-

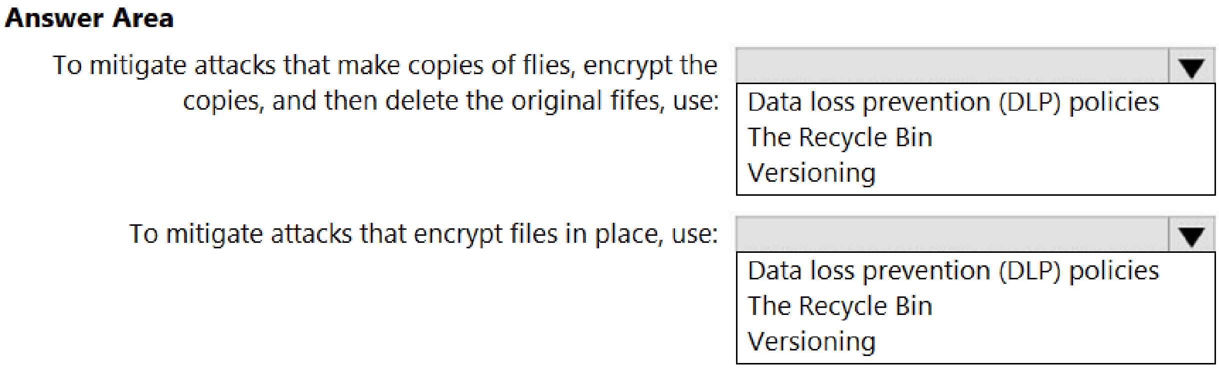
You have a Microsoft 365 E5 subscription that uses Microsoft Purview, SharePoint Online, and OneDrive for Business.

You need to recommend a ransomware protection solution that meets the following requirements:

- Mitigates attacks that make copies of files, encrypt the copies, and then delete the original files
- Mitigates attacks that encrypt files in place
- Minimizes administrative effort

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

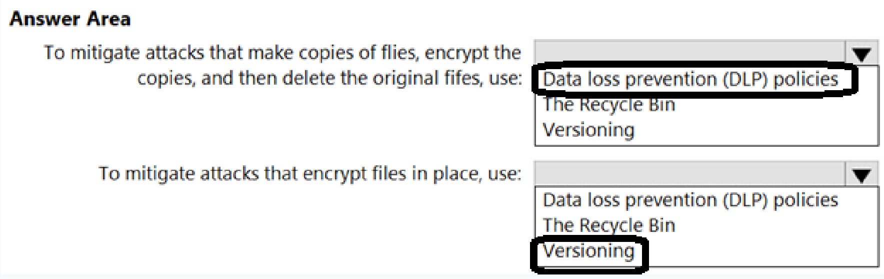
To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use:

- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use:

- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

Suggested Answer:



Answer Area

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use:

- [✓ Data loss prevention (DLP) policies]
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use:

- Data loss prevention (DLP) policies
- The Recycle Bin
- [✓ Versioning]

jasscomp Highly Voted 1 year, 9 months ago

Recycle Bin and Versioning after reading : https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#deleting-files-or-email

upvoted 23 times

SFAY 1 year, 4 months ago

As per MS article titled: Deploy ransomware protection for your Microsoft 365 tenant

Deleting files or email

Files in SharePoint and OneDrive for Business are protected by:

> Versioning:

Microsoft 365 retains a minimum of 500 versions of a file by default and can be configured to retain more.

To minimize the burden on your security and helpdesk staff, train your users on how to restore previous versions of files.

> Recycle bin:

If the ransomware creates a new encrypted copy of the file and deletes the old file, customers have 93 days to restore it from the recycle bin. After 93 days, there is a 14-day window where Microsoft can still recover the data.

Encrypting files in place

As previously described, files in SharePoint and OneDrive for Business are protected from malicious encryption with:

> Versioning
> Recycle bin
> Preservation Hold library

Source: https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#encrypting-files-in-place

upvoted 5 times

sbnpj Highly Voted 1 year, 10 months ago

correct answers are Recycle Bin and Versioning

https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#deleting-files-or-email

upvoted 10 times

ServerBrain 1 year, 10 months ago

No. what do you do with an encrypted file that is in the Recycle bin???

upvoted 6 times

LJWBA 1 year, 9 months ago

It's the original file that would be deleted, so the file in the recycle bin wouldn't be encrypted. I agree with sbnpj

upvoted 6 times

Mendel 1 year, 4 months ago

The Recycle Bin is a useful feature for recovering deleted files, but it's not specifically designed to mitigate ransomware attacks. Ransomware often involves encrypting files and deleting the original copies, which can bypass the Recycle Bin since it typically deals with files that are intentionally deleted by users.

upvoted 3 times

Onimole Most Recent 9 months, 1 week ago

Keywork that everyone seems to have forgotten ------> Minimizes administrative effort

DLP requires some admin effort but versioning and recycle bin are inbuilt and require minimal effort

upvoted 2 times

orrery 11 months, 3 weeks ago

Answer:

To mitigate attacks where a copy of a file is created, encrypted, and then the original file is deleted, use “version control.” To mitigate attacks where a file is encrypted on the spot, use “Data Loss Prevention (DLP) policies.”

Reason:

Version control is effective against attacks where a copy is encrypted and deleted because it saves previous versions of files, allowing recovery even if the original file is deleted.

Data Loss Prevention (DLP) policies are effective against attacks where a file is encrypted on the spot because they prevent unauthorized access and sharing of sensitive information.

Why other answers are different:

The Recycle Bin temporarily stores deleted files but cannot restore encrypted copies.

Version control saves previous versions of files but is not a direct defense against on-the-spot encryption attacks.

upvoted 1 times

damasie 1 year ago

The answer is correct for me. Recycle bin or Versioning do not prevent to make copies of the files.

Therefore:

- Data loss prevention
- Versioning

upvoted 1 times

JAGUDERO 1 year, 2 months ago

Copilot Response

To recommend a ransomware protection solution that meets the specified requirements, you should include the following:

Versioning: This feature in SharePoint Online and OneDrive for Business keeps a history of changes made to files. It can help mitigate attacks that make copies of files, encrypt the copies, and then delete the original files by allowing you to restore previous versions of the files.

Versioning: Similarly, for attacks that encrypt files in place, versioning allows you to revert to an unencrypted state of the file, effectively mitigating the attack.

These features are part of Microsoft 365 E5's capabilities and can significantly reduce the risk of ransomware damage with minimal administrative effort, as they are built into the service and do not require extensive setup or maintenance. Remember to configure versioning settings according to your organization's needs to ensure optimal protection.

upvoted 4 times

cris_exam 1 year, 4 months ago

ah... tricky question this one.

If it would have NOT mentioned Purview, I would have gone without hesitation to Recycle Bin and Versioning... buuut, since we see it mentioned, Purview with its DLP capabilities, offering a way to configure a policy against copying files outside the org, I tend to go with DLP and Versioning, still not 100% convinced.

You never know what they were thinking when they wrote this question....

upvoted 1 times

Mendel 1 year, 4 months ago

Answer is correct:

Data loss prevention: This helps prevent unauthorized access to sensitive data and can be configured to detect and prevent ransomware attacks by monitoring and controlling the movement of files.

Versioning: SharePoint Online and OneDrive for Business support versioning, which allows you to store, track, and restore previous versions of files. This can help mitigate ransomware attacks that involve encrypting files by providing the ability to revert to unaffected versions.

upvoted 4 times

smanzana 1 year, 8 months ago

1-Recycle Bin

2-Versioning

upvoted 5 times

sbnpj 1 year, 10 months ago

Correct Answers are Recycle Bin and DLP

https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#deleting-files-or-email

upvoted 2 times

DavidSapery 1 year, 10 months ago

Answers are Recycle Bin and Versioning.

https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

upvoted 4 times

Victory007 1 year, 10 months ago

Answer Wrong. 1. Versioning - Versioning allows developers (who use it) to keep tracks of the files. This can help you recover your data if it is encrypted or deleted by an attack. 2. DLP Policies: DLP policies help prevent the unauthorized sharing, transfer, or use of sensitive data. They can help you monitor and protect your data across on-premises systems, cloud-based locations, and endpoint devices.

upvoted 1 times

Question #31 *Topic 1*

You are designing a security operations strategy based on the Zero Trust framework.

You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts.

What should you do?

A. Enable built-in compliance policies in Azure Policy.

B. Enable self-healing in Microsoft 365 Defender.

C. Automate data classification.

D. Create hunting queries in Microsoft 365 Defender.

Suggested Answer: *A*

Community vote distribution

B (100%)

⊟ **WRITER00347** Highly Voted 1 year, 4 months ago

Among the options provided, B. Enable self-healing in Microsoft 365 Defender is the one that aligns most closely with this goal.

Self-healing capabilities in Microsoft 365 Defender can automatically detect, investigate, and remediate security threats, which would otherwise require manual intervention by SOC analysts. By automating these processes, you can minimize the operational load on Tier 1 analysts and allow them to focus on more complex security issues.

Options A, C, and D are relevant to various aspects of security and compliance but don't specifically target the operational load on Tier 1 SOC analysts in the same way that option B does. Therefore, the correct answer is:
B. Enable self-healing in Microsoft 365 Defender.

upvoted 19 times

⊟ **cyber_sa** Highly Voted 1 year, 2 months ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 8 times

⊟ **Arockia** Most Recent 12 months ago

To minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts while designing a security operations strategy based on the Zero Trust framework, the recommended action is:

B. Enable self-healing in Microsoft 365 Defender: Enabling self-healing capabilities in Microsoft 365 Defender can significantly reduce the operational load on Tier 1 SOC analysts. Self-healing features automate the detection and remediation of common security issues and threats, allowing for faster response times and reducing the need for manual intervention. By automating the remediation process, Tier 1 analysts can focus on more complex and critical security incidents, improving efficiency and productivity.

upvoted 1 times

⊟ **sherifhamed** 1 year, 3 months ago

Selected Answer: B

To minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts as part of a Zero Trust security operations strategy, you should recommend enabling self-healing in Microsoft 365 Defender (Option B).

Here's why this recommendation is appropriate:

A. Enable built-in compliance policies in Azure Policy: While compliance policies are essential for maintaining security and compliance, they do not directly address minimizing the operational load on SOC analysts. These policies help in ensuring that resources are compliant with organizational standards but may require SOC analysts to review and remediate non-compliant resources.

upvoted 4 times

⊟ **bronyrafon** 1 year, 3 months ago

ChatGPT says option C...

upvoted 1 times

ThePrinceJozef 1 year, 4 months ago

Selected Answer: B

BBBBBBBBBBBBB

upvoted 3 times

ServerBrain 1 year, 4 months ago

Selected Answer: B

B is the correct answer

upvoted 3 times

Lippes 1 year, 4 months ago

Selected Answer: B

Would go for B

upvoted 4 times

Victory007 1 year, 4 months ago

Selected Answer: B

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527.

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527

upvoted 4 times

Question #32 *Topic 1*

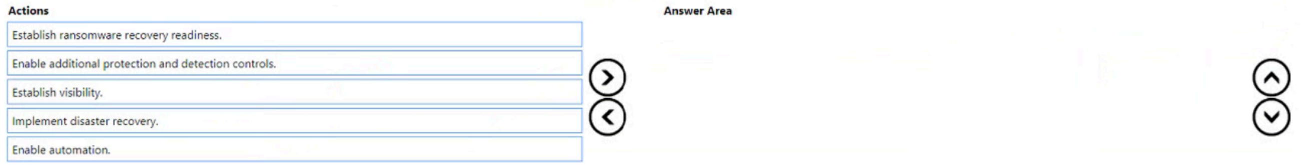
DRAG DROP

-

You are designing a security operations strategy based on the Zero Trust framework.

You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).

Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.

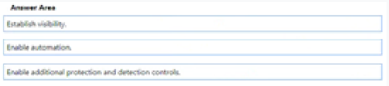


Actions

- Establish ransomware recovery readiness.
- Enable additional protection and detection controls.
- Establish visibility.
- Implement disaster recovery.
- Enable automation.

Answer Area

Suggested Answer:



Answer Area

- Establish visibility.
- Enable automation.
- Enable additional protection and detection controls.

hcmonteiro Highly Voted 1 year, 8 months ago

The answer is for blind people. But seems correct.

upvoted 43 times

ok22 1 year, 5 months ago

your comment cracked me up! haha

Nice to see some humor once in a while during a study session.

upvoted 17 times

emartiy Highly Voted 1 year ago

Answer Area:

Establish Visibility

Enable Automation

Enable additional protection and detection controls

first chars. of last words "V-A-C"

upvoted 9 times

424ede1 3 months, 1 week ago

OR can remove the ones that contain "recovery" :)

upvoted 1 times

Baz10 Most Recent 1 year, 2 months ago

On Exam 8 Apr 2024 scored 764

Visibility

Automation

Additional protection

upvoted 4 times

poesklap 1 year, 4 months ago

Looks like we're going in blind with this one boys.

upvoted 2 times

poesklap 1 year, 4 months ago

I like how the first answer is visibility yet we can't see it.

upvoted 8 times

RickySmith 1 year, 5 months ago

Correct.

https://learn.microsoft.com/en-us/security/zero-trust/deploy/visibility-automation-orchestration#visibility-automation-and-orchestration-zero-trust-deployment-objectives

upvoted 5 times

⊟ **shanti0091** 1 year, 8 months ago

Answer is correct. The focus here is to increase SOC efficiency.

upvoted 3 times

Question #33 Topic 1

HOTSPOT

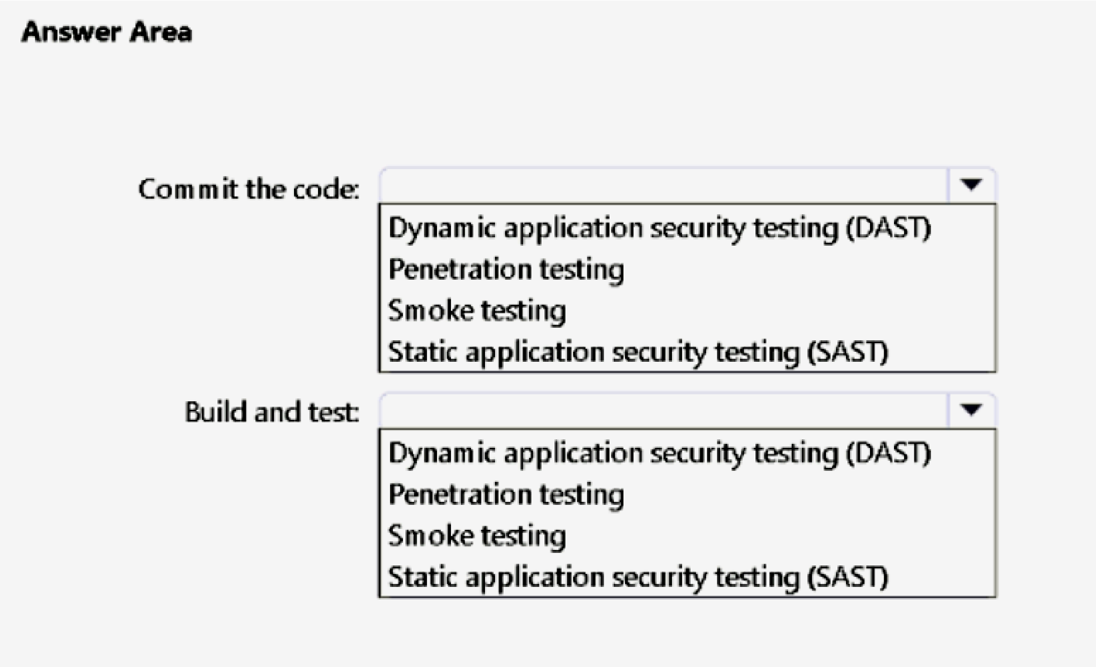
-

You have an Azure subscription that contains multiple apps. The apps are managed by using continuous integration and continuous deployment (CCD) pipelines in Azure DevOps.

You need to recommend DevSecOps controls for the Commit the code and the Build and test CI/CD process stages based on the Microsoft Cloud Adoption Framework for Azure.

Which testing method should you recommend for each stage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

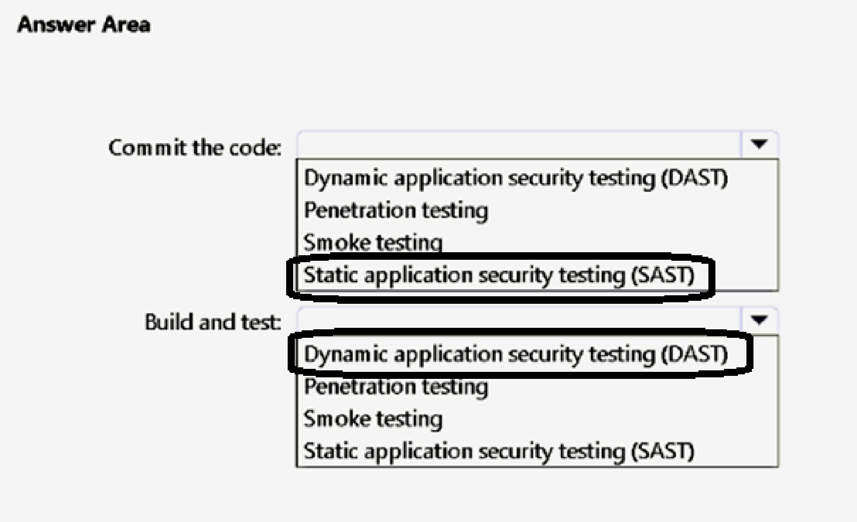


Answer Area

Commit the code: ▼
- Dynamic application security testing (DAST)
- Penetration testing
- Smoke testing
- Static application security testing (SAST)

Build and test: ▼
- Dynamic application security testing (DAST)
- Penetration testing
- Smoke testing
- Static application security testing (SAST)

Suggested Answer:



Answer Area

Commit the code: ▼
- Dynamic application security testing (DAST)
- Penetration testing
- Smoke testing
- [✓ Static application security testing (SAST)]

Build and test: ▼
- [✓ Dynamic application security testing (DAST)]
- Penetration testing
- Smoke testing
- Static application security testing (SAST)

⊟ **676ae1a** 5 months ago

Commit the code:SAST.Build and test:DAST

upvoted 2 times

⊟ **676ae1a** 5 months ago

La respuesta parece correcta.

upvoted 1 times

Question #34 *Topic 1*

You have a Microsoft Entra tenant that contains 10 Windows 11 devices and two groups named Group1 and Group2. The Windows 11 devices are joined to the Microsoft Entra tenant and are managed by using Microsoft Intune.

You are designing a privileged access strategy based on the rapid modernization plan (RaMP). The strategy will include the following configurations:

• Each user in Group1 will be assigned a Windows 11 device that will be configured as a privileged access device.
• The Security Administrator role will be mapped to the privileged access security level.
• The users in Group1 will be assigned the Security Administrator role.
• The users in Group2 will manage the privileged access devices.

You need to configure the local Administrators group for each privileged access device. The solution must follow the principle of least privilege.

What should you include in the solution?

A. Only add Group2 to the local Administrators group.

B. Configure Windows Local Administrator Password Solution (Windows LAPS) in legacy Microsoft LAPS emulation mode.

C. Add Group2 to the local Administrators group. Add the user that is assigned the Security Administrator role to the local Administrators group of the user's assigned privileged access device.

Suggested Answer: *C*

Community vote distribution

C (100%)

francescoc 1 month, 2 weeks ago

Selected Answer: C

The correct answer is C, not A. Because A doesn't allow Group1 users to perform their privileged duties on their own devices. Violates usability.

upvoted 3 times

francescoc 2 months, 1 week ago

Selected Answer: C

Answare is C, not A. Group1 users need local admin rights on their assigned device to perform privileged operations. This option would block them

upvoted 1 times

424ede1 2 months, 4 weeks ago

Selected Answer: A

Under the RaMP guidelines, you want to enforce the principle of least privilege. To minimize the risk of lateral movement or compromise, these privileged access devices should not grant local administrator rights to the security administrators.

upvoted 1 times

olsookie 3 months, 1 week ago

Selected Answer: A

To follow the principle of least privilege, you should include Option A: Only add Group2 to the local Administrators group in your solution. This ensures that only the users responsible for managing the privileged access devices have administrative rights, minimizing the risk of unnecessary access.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices
https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin

upvoted 3 times

devop23 4 months ago

Selected Answer: A

Answer is A:
https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment

Remove local admin rights
This method requires that users of the VIP, DevOps, and Privileged workstations have no administrator rights on their machines.

Group2 users will manage these devices so they should have local admin access anyway. So option C is eliminated. Option B doesn't make sense here.

upvoted 3 times

⊟ **Er_01** 5 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment

It says not to add anyone to admin on privileged wa. So A and C are against best practice.
B will not work as legacy laps not be used on cloud joined was.
So the best answer would be C because it allows for different group to manage and only 1 person to use.
Bad question.

upvoted 2 times

⊟ **jim85** 4 months, 3 weeks ago

I think, the 2nd half of the answer would be D and in that case C gets its meaning

upvoted 1 times

⊟ **676ae1a** 5 months ago

Selected Answer: C

Respuesta correcta

upvoted 1 times

HOTSPOT

-

Case Study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

-

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment

-

Litware has a Microsoft Entra tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to 20 Azure subscriptions. Microsoft Entra Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Microsoft Entra tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes

-

Litware plans to implement the following changes:

- Create a management group hierarchy for each Microsoft Entra tenant.
- Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

- Implement Microsoft Entra Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

- Minimize any additional on-premises infrastructure.
- Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

- Enable the management of on-premises resources from Azure, including the following:

o Use Azure Policy for enforcement and compliance evaluation.
o Provide change tracking and asset inventory.
o Implement patch management.

- Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

- Detect brute force attacks that directly target AD DS user accounts.
- Implement leaked credential detection in the Microsoft Entra tenant of Litware.
- Prevent AD DS user accounts from being locked out by brute force attacks that target Microsoft Entra user accounts.
- Implement delegated management of users and groups in the Microsoft Entra tenant of Litware, including support for:

o The management of group properties, membership, and licensing
o The management of user properties, passwords, and licensing
o The delegation of user management based on business units

Requirements. Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

- Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
- Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
- Use the principle of least privilege.

Requirements. Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

- Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
- Provide a secure score scoped to the landing zone.
- Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
- Minimize the possibility of data exfiltration.
- Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

- Be created in a dedicated subscription.
- Use a DNS namespace of litware.com.

Requirements. Application Security Requirements

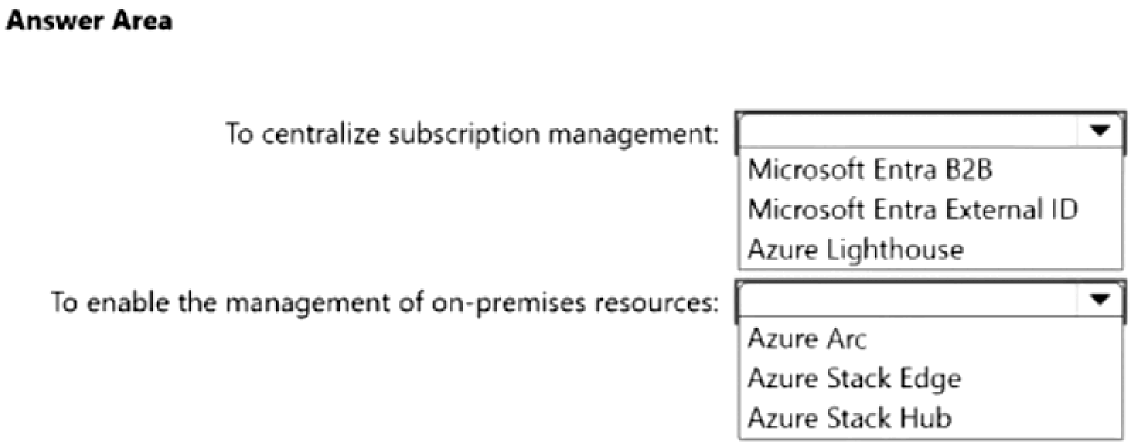
Litware identifies the following application security requirements:

- Identify internal applications that will support single sign-on (SSO) by using Microsoft Entra Application Proxy.
- Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

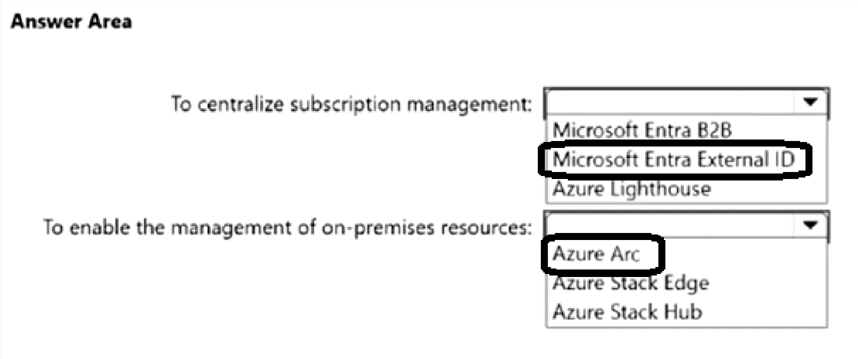


Answer Area

To centralize subscription management:
- Microsoft Entra B2B
- Microsoft Entra External ID
- Azure Lighthouse

To enable the management of on-premises resources:
- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

Suggested Answer:



Answer Area

To centralize subscription management:
- Microsoft Entra B2B
- [✓ Microsoft Entra External ID]
- Azure Lighthouse

To enable the management of on-premises resources:
- [✓ Azure Arc]
- Azure Stack Edge
- Azure Stack Hub

AlbertE1nstein Highly Voted 5 months ago

1. Azure Lighthouse
2. Azure Arc

upvoted 12 times

6c0ca3d Most Recent 1 month, 2 weeks ago

1. Azure Lighthouse
2. Azure Arc

external id required guest users

upvoted 1 times

StevenBeWeavin 2 months, 3 weeks ago

1. Azure Lighthouse (I have deployed this many times)
2. Azure Arc

upvoted 1 times

⊟ **Cyko** 4 months, 3 weeks ago

Without the use of guest accounts, will leave us one option-Azure lighthouse

upvoted 1 times

⊟ **676ae1a** 5 months ago

1.Lighthouse. Azure Lighthouse permite a Litware gestionar recursos de varios inquilinos sin necesidad de crear cuentas de invitados, minimizando la sobrecarga administrativa.Microsoft Entra External ID puede ser una solución complementaria para gestionar identidades externas, como socios comerciales y clientes, pero no es la solución principal para centralizar la gestión de suscripciones y recursos en un entorno híbrido y de múltiples inquilinos

upvoted 1 times

Question #36 *Topic 1*

You have an Azure subscription.

You plan to deploy enterprise-scale landing zones based on the Microsoft Cloud Adoption Framework for Azure. The deployment will include a single-platform landing zone for all shared services and three application landing zones that will each host a different Azure application.

You need to recommend which resource to deploy to each landing zone. The solution must meet the Cloud Adoption Framework best-practice recommendations for enterprise-scale landing zones.

What should you recommend?

A. an Azure firewall

B. an Azure virtual network gateway

C. an Azure Private DNS zone

D. an Azure key vault

Suggested Answer: *C*

Community vote distribution

A (50%) D (50%)

⊟ **424ede1** 2 months, 4 weeks ago

Selected Answer: D

Landing Zone Subscription --> Azure Key Vault
Connectivity Subscription --> Azure Firewall

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/define-an-azure-network-topology#virtual-wan-network-topology

upvoted 2 times

⊟ **424ede1** 3 months, 1 week ago

Selected Answer: D

Based on the provided picture and the conceptual architecture of the landing zone, both landing zone subscriptions include KeyVault.
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/#azure-landing-zone-architecture

upvoted 1 times

⊟ **Er_01** 4 months, 3 weeks ago

Selected Answer: D

The question related to ent scale application landing zones from the document only shows Azure Key Vault in each one. Also, in the access section it states to “separate key vaults for each application environment in each region”. Pg 419

upvoted 4 times

⊟ **sweetykaur** 4 months, 3 weeks ago

Selected Answer: A

The best recommendation to meet the Cloud Adoption Framework best-practice recommendations for enterprise-scale landing zones is A. an Azure firewall.

Deploying an Azure firewall in each landing zone provides centralized protection against network threats and supports security and compliance requirements. This aligns with the Cloud Adoption Framework's best-practices for securing your environment and ensuring consistent security controls across all landing zones.

upvoted 1 times

⊟ **jim85** 4 months, 3 weeks ago

Selected Answer: A

should be A for app landing zone and D for single-platform landing zone

upvoted 1 times

⊟ **Ali96** 5 months ago

Selected Answer: C

an Azure Private DNS zone

upvoted 1 times

tuyi2 5 months ago

Selected Answer: D

From Chat GPT: The Microsoft Cloud Adoption Framework for Azure recommends deploying an Azure Key Vault in each landing zone to securely manage and store secrets, keys, and certificates for the applications and resources hosted in the landing zone. This approach ensures that sensitive information is isolated and secured within each application landing zone.

upvoted 1 times

676ae1a 5 months ago

Selected Answer: D

Azure key vault es uno de los recursos que debe tener una zona de aterrizaje en relación a seguridad y cumplimiento y por lo tanto sería la opción más óptima pese a que se recomiende un Azure firewall relativo a redes y conectividad

upvoted 1 times

676ae1a 5 months ago

Selected Answer: A

Azure firewall es uno de los recursos que debe tener la zona de aterrizaje

upvoted 1 times

Question #37 *Topic 1*

HOTSPOT

-

You have 1,000 on-premises servers that run Windows Server 2022 and 500 on-premises servers that run Linux.

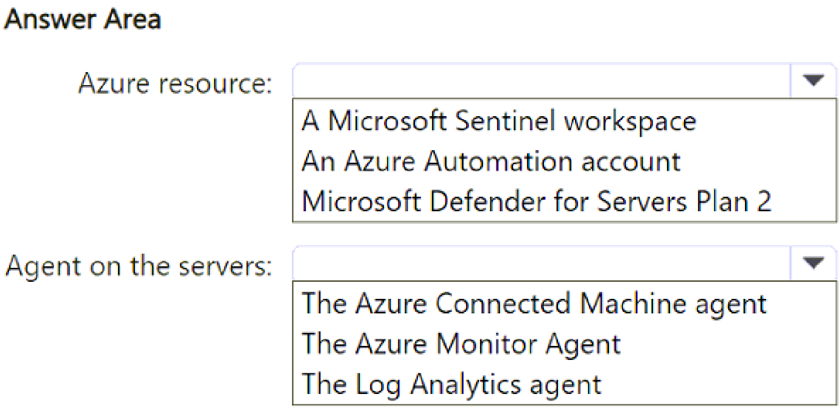
You have an Azure subscription that contains the following resources:

• A Log Analytics workspace
• A Microsoft Defender Cloud Security Posture Management (CSPM) plan

You need to deploy Update Management for the servers.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

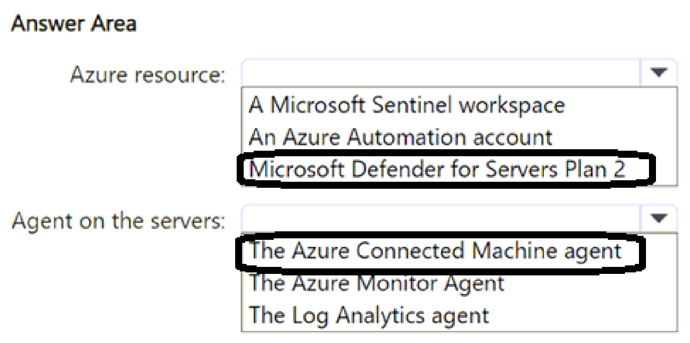


Answer Area

Azure resource: ▾
- A Microsoft Sentinel workspace
- An Azure Automation account
- Microsoft Defender for Servers Plan 2

Agent on the servers: ▾
- The Azure Connected Machine agent
- The Azure Monitor Agent
- The Log Analytics agent

Suggested Answer:



Answer Area

Azure resource: ▾
- A Microsoft Sentinel workspace
- An Azure Automation account
- [✓ Microsoft Defender for Servers Plan 2]

Agent on the servers: ▾
- [✓ The Azure Connected Machine agent]
- The Azure Monitor Agent
- The Log Analytics agent

⊟ **676ae1a** Highly Voted 5 months ago

1.Azure automation account 2.Log analytics agent

upvoted 7 times

⊟ **Gagi79** Most Recent 1 month, 3 weeks ago

I don't see how Defender for Servers Plan 2 have anything with Azure Update Manager - https://learn.microsoft.com/en-us/azure/update-manager/prerequisites

upvoted 1 times

⊟ **ada1ba2** 2 months, 4 weeks ago

Connect hybrid machines to Azure from Automation Update Management

Automation account - This method requires that you are a member of the Automation Job Operator role or higher so you can create runbook jobs in the Automation account.

You can enable Azure Arc-enabled servers for one or more of your Windows or Linux virtual machines or physical servers hosted on-premises or other cloud environment that are managed with Azure Automation Update Management. This onboarding process automates the download and installation of the Connected Machine agent.

https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-update-management-machines

upvoted 2 times

⊟ **424ede1** 3 months, 1 week ago

1. Defender for Servers Plan 2

2. Log Analytics agent

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers#deployment-steps
https://learn.microsoft.com/en-us/azure/defender-for-cloud/monitoring-components#log-analytics-agent

upvoted 1 times

⊟ **reyreyg** 4 months, 2 weeks ago

"Automation Update Management has retired on 31 August 2024 and we recommend that you use Azure Update Manager. Follow the guidelines for migration from Automation Update Management to Azure Update Manager."

upvoted 2 times

⊟ **zpack** 4 months, 4 weeks ago

DfS has nothing to do with update management. Needs automation account as pre-req for AUM and ARC to bring on-prem to azure.

upvoted 1 times

⊟ **jim85** 4 months, 4 weeks ago

2: Azure connected machine agent as per https://techcommunity.microsoft.com/blog/azuregovernanceandmanagementblog/generally-available-azure-update-manager/3928878

upvoted 1 times

⊟ **reyreyg** 5 months ago

Defender for servers plan 2

Azure connected machine agent - azure arc

upvoted 3 times

⊟ **reyreyg** 4 months, 3 weeks ago

I take that back, i believe it is Sentinel possibly

upvoted 1 times

⊟ **AlbertE1nstein** 5 months ago

1. A Microsoft Sentinel Workspace

2, The Log Analytics agent

upvoted 1 times

Question #38 *Topic 1*

HOTSPOT

-

You have an Active Directory Domain Services (AD DS) domain that contains a virtual desktop infrastructure (VDI). The VDI uses non-persistent images and cloned virtual machine templates. VDI devices are members of the domain.

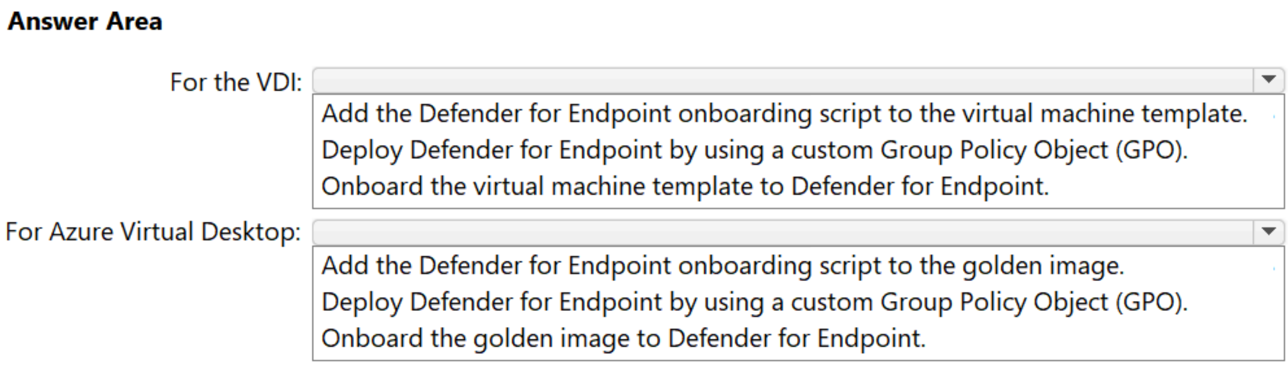
You have an Azure subscription that contains an Azure Virtual Desktop environment. The environment contains host pools that use a custom golden image. All the Azure Virtual Desktop deployments are members of a single Microsoft Entra Domain Services domain.

You need to recommend a solution to deploy Microsoft Defender for Endpoint to the hosts. The solution must meet the following requirements:

- Ensure that the hosts are onboarded to Defender for Endpoint during the first startup sequence.
- Ensure that the Microsoft Defender portal contains a single entry for each deployed VDI host.
- Minimize administrative effort.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

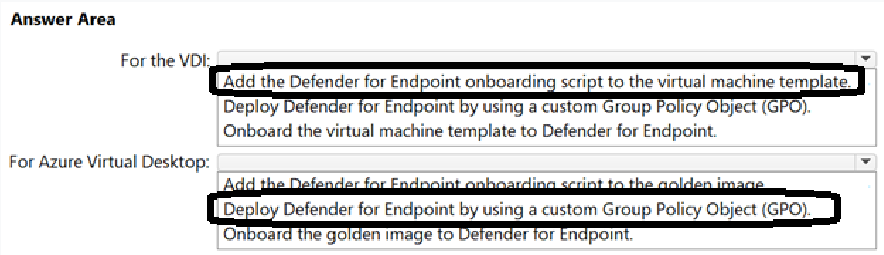


Answer Area

For the VDI:
- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.

For Azure Virtual Desktop:
- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.

Suggested Answer:



Answer Area

For the VDI:
- [✓ Add the Defender for Endpoint onboarding script to the virtual machine template.]
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.

For Azure Virtual Desktop:
- Add the Defender for Endpoint onboarding script to the golden image.
- [✓ Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).]
- Onboard the golden image to Defender for Endpoint.

424ede1 Highly Voted 3 months, 1 week ago

1. For VDI: Add the Defender for Endpoint onboarding script to the virtual machine template.
https://learn.microsoft.com/en-us/defender-endpoint/configure-endpoints-vdi

2. Add the Defender for Endpoint onboarding script to the golden image.
https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-multi-session-device

upvoted 8 times

Naqsh27 1 month ago

correct

upvoted 1 times

cl1984 Most Recent 3 months, 1 week ago

For the VDI - Deploy MDE using GPO - https://learn.microsoft.com/en-us/defender-endpoint/configure-endpoints-vdi#onboarding-steps
For AVD - Add MDE using onboarding script - https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-multi-session-device#before-you-begin

upvoted 1 times

Question #39 *Topic 1*

You have 10 Azure subscriptions that contain 100 role-based access control (RBAC) role assignments.

You plan to consolidate the role assignments.

You need to recommend a solution to identify which role assignments were NOT used during the last 90 days. The solution must minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Defender for Cloud

B. Microsoft Entra access reviews

C. Microsoft Entra Privileged Identity Management (PIM)

D. Microsoft Entra Permissions Management

Suggested Answer: *D*

Community vote distribution

B (100%)

424ede1 3 months, 1 week ago

Selected Answer: D

Microsoft Entra Permissions Management

The answer is obvious in following Microsoft diagrams

https://learn.microsoft.com/en-us/entra/architecture/permissions-manage-ops-guide-three

upvoted 1 times

AleFerrillo 3 months, 2 weeks ago

Selected Answer: D

EPM can tell you if an identity has not used a permission in the last 90 days

upvoted 1 times

Lrrr_FromOmicronPersei8 3 months, 4 weeks ago

Selected Answer: D

Entra Permissions Management

upvoted 1 times

Sundaycorn 4 months, 1 week ago

Selected Answer: B

Access reviews cover rbac roles which this question is asking. Microsoft Entrance Permissions Management covers users, groups, sites etc.

upvoted 2 times

lam_15 4 months, 2 weeks ago

Selected Answer: D

Microsoft Entra Permissions Management:

https://learn.microsoft.com/en-us/entra/permissions-management/overview

upvoted 1 times

RabbitB 4 months, 2 weeks ago

Selected Answer: D

Entra Permissions Management.

This explains everything. https://www.youtube.com/watch?v=-S-z3qx79YQ

upvoted 1 times

oscarpopi 4 months, 3 weeks ago

Selected Answer: D

Right answer is EPM -> 100 subscriptions and minimal effort.

upvoted 1 times

Er_01 4 months, 3 weeks ago

Selected Answer: C

The best answer is C as it can create a review every quarter to verify membership or self review access, which would give you a list. The question is incomplete as it leaves out the taking action part to remove stale access.

upvoted 1 times

> **Er_01** 4 months, 3 weeks ago
>
> I think I selected the wrong letter as access reviews are B.
>
> upvoted 1 times

zpack 4 months, 4 weeks ago

Selected Answer: D

Wrong answer, correct is D. Access review is to see if users should still belong to groups, not to see if a role wasn't used in 90 days.

upvoted 2 times

Ali96 5 months ago

Selected Answer: B

Entra access reviews

upvoted 1 times

reyreyg 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

upvoted 1 times

676ae1a 5 months ago

Selected Answer: B

B.Reseñas de acceso a Microsoft Entra: Esta herramienta permite auditar y revisar el uso de roles y permisos en Azure, facilitando la identificación de asignaciones de roles que no se han utilizado. Puedes generar informes detallados y filtrar las asignaciones de roles según el período de tiempo especificado

upvoted 1 times

AlbertE1nstein 5 months ago

Selected Answer: B

B. Microsoft Entra access reviews

upvoted 1 times

Question #40 *Topic 1*

You have a Microsoft Entra tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised local administrator account cannot be used to stop scheduled backups.

What should you do?

A. From Azure Backup, configure multi-user authorization by using Resource Guard.

B. From Microsoft Entra Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.

D. From a Recovery Services vault, generate a security PIN for critical operations.

Suggested Answer: *A*

Community vote distribution

A (100%)

SMHcalicut Highly Voted 3 months, 2 weeks ago

Selected Answer: A

Ransomware Protection and Multi-User Authorization
Microsoft recommends enabling multi-user authorization (MUA) to protect backup configurations from unauthorized changes. Resource Guard allows you to enforce MUA for critical backup operations, ensuring that a compromised administrator account alone cannot modify or disable backups without additional authorization.

upvoted 5 times

Alagong Most Recent 2 months, 1 week ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/backup/guidance-best-practices#ransomware-protection

upvoted 2 times

424ede1 3 months, 1 week ago

Selected Answer: D

From a Recovery Services vault, generate a security PIN for critical operations

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature#authentication-to-perform-critical-operations

upvoted 1 times

lam_15 4 months, 2 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization-concept?tabs=recovery-services-vault

upvoted 4 times

676ae1a 5 months ago

Selected Answer: A

Esta configuración agrega una capa adicional de protección a las operaciones críticas en los almacenes de Recovery Services, asegurando que solo las personas autorizadas puedan realizar ciertas acciones.

upvoted 1 times

Question #41 *Topic 1*

HOTSPOT

-

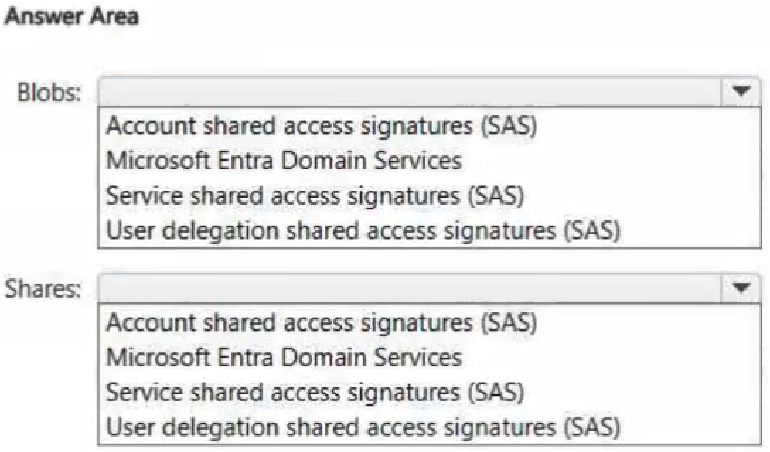
You have an Azure subscription that contains multiple Azure Storage blobs and Azure Files shares.

You need to recommend a security solution for authorizing access to the blobs and shares. The solution must meet the following requirements:

• Support access to the shares by using the SMB protocol.
• Limit access to the blobs to specific periods of time.
• Include authentication support when possible.

What should you recommend for each resource? To answer, select the options in the answer area.

NOTE: Each correct selection is worth one point.

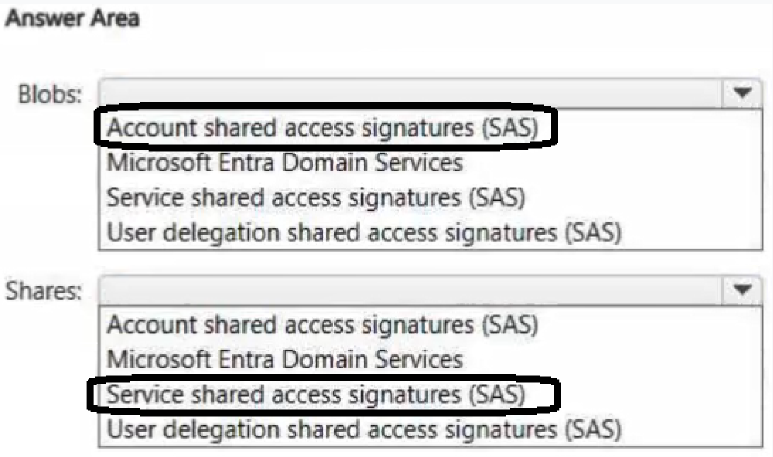


Answer Area

Blobs:
- Account shared access signatures (SAS)
- Microsoft Entra Domain Services
- Service shared access signatures (SAS)
- User delegation shared access signatures (SAS)

Shares:
- Account shared access signatures (SAS)
- Microsoft Entra Domain Services
- Service shared access signatures (SAS)
- User delegation shared access signatures (SAS)

Suggested Answer:



Answer Area

Blobs:
- [✓ Account shared access signatures (SAS)]
- Microsoft Entra Domain Services
- Service shared access signatures (SAS)
- User delegation shared access signatures (SAS)

Shares:
- Account shared access signatures (SAS)
- Microsoft Entra Domain Services
- [✓ Service shared access signatures (SAS)]
- User delegation shared access signatures (SAS)

6c0ca3d 1 month, 3 weeks ago

blobs sas
shares entra ADDS

sas not support smb

upvoted 1 times

424ede1 3 months, 1 week ago

Blob: User delegation shared access signatures (SAS)
Share: Microsoft Entra Domain Services

When SAS authorization is necessary (access for limited time), Microsoft recommends using user delegation SAS for limited delegated access to blob resources.

https://learn.microsoft.com/en-us/azure/storage/common/authorize-data-access?tabs=blobs#authorization-for-data-operations

upvoted 2 times

olsookie 3 months, 1 week ago

Azure Files Share would be Entra Domain Services

Blobs would be User Delegation SA

upvoted 2 times

cl1984 3 months, 1 week ago

Blobs are User SAS - https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json#user-delegation-sas

Shares are Entra Domain Services - https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-domain-services-enable?tabs=azure-portal

upvoted 1 times

Lrrr_FromOmicronPersei8 3 months, 3 weeks ago

Blobs: User Delegation SAS

Shares: Entra Domain Services

upvoted 3 times

Ali96 4 months, 1 week ago

Blobs : User delegation shared access signatures (SAS) – Car cette solution permet de limiter l'accès à des utilisateurs spécifiques et prend en charge l'authentification avec Azure AD.

Shares : Microsoft Entra Domain Services – Pour permettre l'accès via SMB avec une authentification basée sur Active Directory, ce qui est nécessaire pour les partages de fichiers.

upvoted 1 times

Cyko 4 months, 3 weeks ago

Blobs-service SAS

Shares- Microsoft Entra DOmain service

upvoted 1 times

676ae1a 5 months ago

Blobs:User delegación SAS.shared:Entra Domain service

upvoted 2 times

AlbertE1nstein 5 months ago

1.Shared Access Signatures (SAS)

2. Microsoft Entra Domain Services

upvoted 1 times

Question #42 *Topic 1*

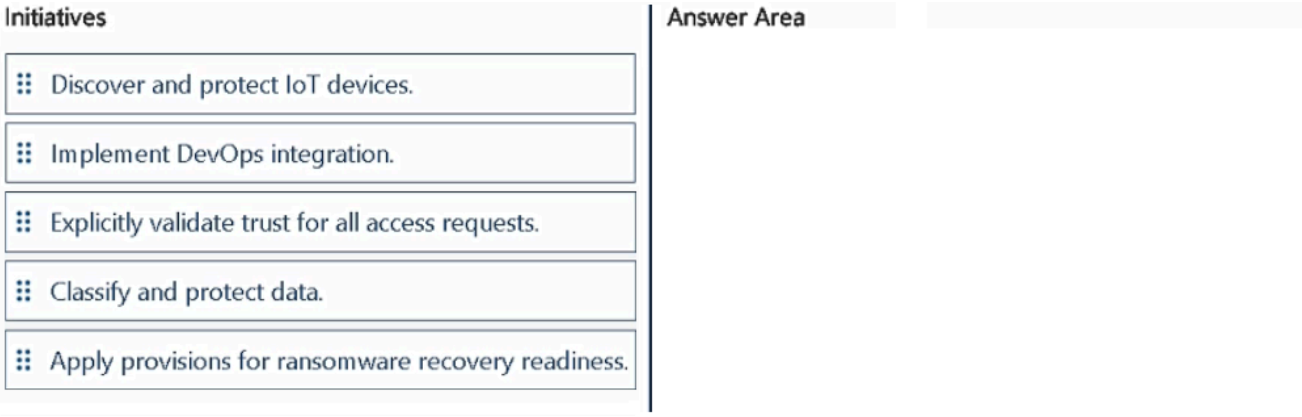
DRAG DROP

-

You need to design a solution to accelerate a Zero Trust security implementation. The solution must be based on the Zero Trust Rapid Modernization Plan (RaMP).

Which three initiatives should you include in the solution, and in which order should you implement the initiatives? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

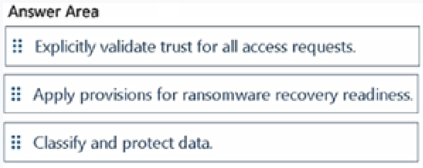


Initiatives

- Discover and protect IoT devices.
- Implement DevOps integration.
- Explicitly validate trust for all access requests.
- Classify and protect data.
- Apply provisions for ransomware recovery readiness.

Answer Area

Suggested Answer:



Answer Area

- Explicitly validate trust for all access requests.
- Apply provisions for ransomware recovery readiness.
- Classify and protect data.

Ruphus 3 months ago

Answer is correct:

https://learn.microsoft.com/en-us/training/modules/introduction-zero-trust-best-practice-frameworks/3-zero-trust-initiatives

upvoted 1 times

jim85 4 months, 4 weeks ago

given answer is correct, as per https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 4 times

676ae1a 5 months ago

Explicitly validate trust for all access requests

Discover and protect IoT devices

Classify and protect data

upvoted 2 times

Question #1 *Topic 2*

You are evaluating an Azure environment for compliance.
You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.
Which effect should you use in Azure Policy?

A. Deny

B. Modify

C. Append

D. Disabled

Suggested Answer: *D*
This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disable a single assignment instead of disabling all of that policy's assignments.
An alternative to the Disabled effect is enforcementMode, which is set on the policy assignment. When enforcementMode is Disabled, resources are still evaluated.
Incorrect:
Not A: Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
Not B: Modify evaluates before the request gets processed by a Resource Provider during the creation or updating of a resource. The Modify operations are applied to the request content when the if condition of the policy rule is met. Each Modify operation can specify a condition that determines when it's applied.
Operations with conditions that are evaluated to false are skipped.
Not C: Append is used to add additional fields to the requested resource during creation or update.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

Community vote distribution
D (77%) A (23%)

[Removed] Highly Voted 2 years, 6 months ago
The question is misleadingly worded. The question asks which effect can be used to report on compliance without changing anything. The Azure Policy "effect" used to do this is "Audit", which is not one of the provided options. There isn't an "effect" setting in the choices that matches the criteria.

However, "Disabled" and "Enabled" are the two Azure Policy "enforcement" setting options. If an Azure Policy's "enforcement" is set to "Disabled", any "effect" set on this Azure Policy will report but will not make changes.
"Disabled" is the best answer available, although technically incorrect because "Disabled" isn't an Azure Policy "effect".
upvoted 29 times

AWSPro24 5 months, 1 week ago
This is the correct answer. If you set enforcementMode to disabled resources are still evaluated but log activity isn't created. audit works as well.
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-disabled
upvoted 1 times

Fal991l 2 years, 3 months ago
I am on your side
upvoted 2 times

epomatti 1 year, 4 months ago
1. You're confused between "effect" and an "enforcement mode".
2. Policy definitions that use the Disabled effect have the default compliance state Compliant after assignment.

The only possible answer is A - Deny.
upvoted 3 times

Joanale 1 year, 6 months ago
100% correct, please guys report this question if still no see the option "audit".
upvoted 1 times

Gar23 Highly Voted 👍 2 years, 9 months ago

Selected Answer: D

It has to be disabled since deny will send the compliance report as non-complaint.

upvoted 27 times

BlackZeros 1 year, 11 months ago

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deny-evaluation

upvoted 2 times

sweetykaur Most Recent ⊙ 4 months, 3 weeks ago

Selected Answer: D

The correct effect to use in Azure Policy for evaluating compliance without changing any resources is D. Disabled.

When a policy is set to the "Disabled" effect, it will not enforce any changes but can still be used to evaluate and report on the compliance state of the resources. This allows you to monitor compliance without making any modifications to the resources.

upvoted 1 times

Dan91 8 months, 1 week ago

Selected Answer: A

A: Deny makes the most sense. The questions states you need to evaluate compliance. D: Disabled has a default compliance state of "compliant". From an auditing perspective this wouldn't make sense.

upvoted 4 times

Brainrot 8 months, 1 week ago

Key word without changing resources. I think it has to be Append because of this. append effect in Azure Policy can be used to evaluate compliance. When a policy definition using the append, effect is evaluated, it doesn't modify existing resources. Instead, it marks any resource that meets the specified conditions as non-compliant. This allows you to identify resources that do not meet your policy requirements without making immediate changes to them.

upvoted 1 times

ariania 9 months, 3 weeks ago

Deny marks resources as non-compliant during evaluation but does not make changes to existing resources. It enforces compliance by preventing the creation or modification of non-compliant resources but can be used for evaluation purposes as well, without altering existing resources.

Modify changes the resource, so it's not applicable when you don't want to make any changes.

Append adds fields to the resource during creation or update, but its main function is to enforce certain configurations, and it's not solely for compliance evaluation.

Disabled doesn't evaluate compliance at all and marks everything as compliant by default, which doesn't fulfill the goal of evaluating compliance.

Thus, Deny is the best option for evaluating compliance without modifying any resource

upvoted 1 times

ariania 9 months, 3 weeks ago

Disabled (effect): Completely stops policy evaluation and marks everything as compliant.
enforcementMode (assignment setting): Keeps the policy evaluating compliance but doesn't enforce any action, logging, or modification to resources.

To go back to your original question, the Disabled effect would mark everything as compliant and wouldn't evaluate compliance at all. The enforcementMode (disabled) is a different setting entirely, used to evaluate compliance without enforcement, which seems closer to what you're looking for in some situations but isn't one of the options in your question.

Since enforcementMode isn't an effect, in the context of your question, A. Deny remains the correct answer, as it evaluates compliance and marks non-compliant resources without changing existing ones.

upvoted 2 times

oreoale 1 year, 3 months ago

Answer is D - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#disabled

upvoted 1 times

kazaki 1 year, 3 months ago

It is not disabled it isn't deny it is audit

upvoted 2 times

⊟ **PierreTang** 1 year, 4 months ago

Selected Answer: A

Deny. "During evaluation of existing resources, resources that match a deny policy definition are marked as non-compliant."
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deny-evaluation

upvoted 1 times

⊟ **cris_exam** 1 year, 4 months ago

Selected Answer: A

The key words from this question are "evaluating compliance".

This can be done with DENY, because it doesn't allow any resource change but blocks it before happening with a 403 error and logs the block for a later review to see the non-compliant activity.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deny-evaluation

MS words it like below, fulfilling the requirements of the given question while checking if an Azure environment IS or NOT compliant.

"During evaluation of existing resources, resources that match a deny policy definition are marked as non-compliant."

upvoted 2 times

⊟ **epomatti** 1 year, 4 months ago

Selected Answer: A

You guys are hallucinating.

The question clearly asks which EFFECT (not an enforcement mode) should be used to evaluate resources without changing them.

The only option available is DENY.

The effect "Disabled" will always show as compliant:
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#disabled

The questions is NOT asking for enforcement mode:
"Policy definitions that use the Disabled effect have the default compliance state Compliant after assignment."

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#enforcement-mode

upvoted 2 times

⊟ **Arockia** 1 year, 5 months ago

"Disabled" effect ensures that the policy is applied for evaluation purposes but does not enforce any specific actions or modifications on the resources themselves. This allows you to gather compliance data and assess the configuration of resources in your Azure environment without impacting their current state.

upvoted 2 times

⊟ **UberTech_1888** 1 year, 11 months ago

Keyword = "Evaluating"

upvoted 1 times

⊟ **Ario** 1 year, 12 months ago

D is Correct , Using the "Disabled" effect in Azure Policy is particularly useful for scenarios where you want to assess compliance and gather information without making any immediate changes or disruptions to the resources

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#disabled
This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disable a single assignment instead of disabling all of that policy's assignments.

upvoted 1 times

NinjaSchoolProfessor 1 year, 11 months ago

D as you stated is correct. What the question is missing is a reference to the enforcement mode. You can use the enforcement mode Disabled (DoNotEnforce) on your policy assignment to prevent the effect from triggering or activity log entries from being created.

This step gives you a chance to evaluate the compliance results of the new policy on existing resources without impacting work flow.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/evaluate-impact#audit-existing-resources

upvoted 1 times

alifrancos 2 years, 2 months ago

Selected Answer: D

the Deny effect, prevent ressources from creation if that not match the policy, but if it match it will be created or modified, i think that'is clear

upvoted 1 times

Fal991l 2 years, 3 months ago

Selected Answer: A

ChatGPT: If you have to choose only one between Disabled and Deny, and the question does not provide any further details or constraints, then the best answer would be Deny.

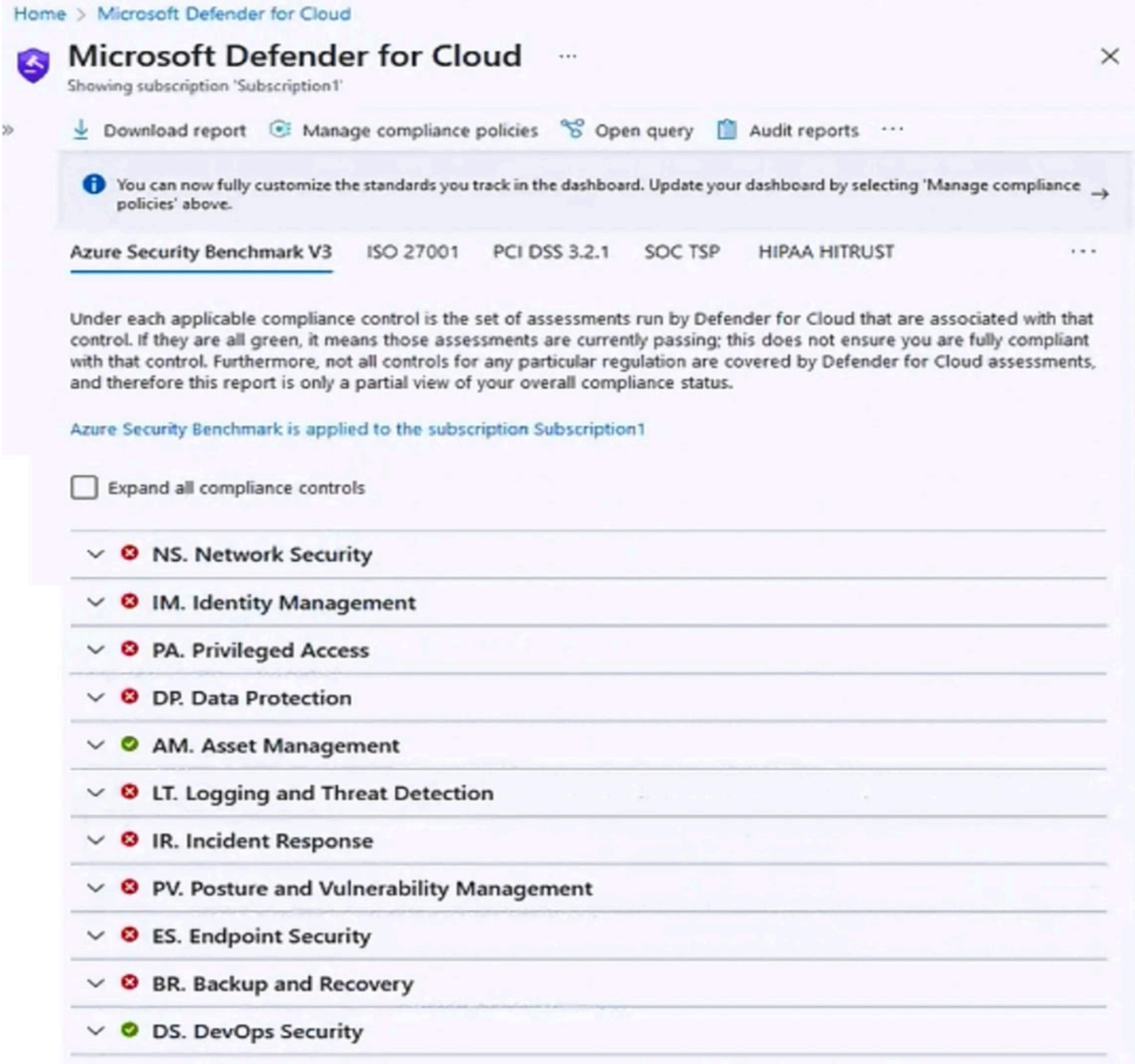
The Deny effect is a more appropriate and specific choice for evaluating compliance without changing any resources in an Azure environment, as it explicitly blocks non-compliant resources from being created or modified while not modifying any existing resources. This can help ensure that the environment remains in compliance and does not drift away from the desired state.

upvoted 2 times

Question #2 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.


Home > Microsoft Defender for Cloud
Download report
Manage compliance policies
Open query
Audit reports
Azure Security Benchmark V3
ISO 27001
PCI DSS 3.2.1
SOC TSP
HIPAA HITRUST

Microsoft Defender for Cloud

Showing subscription 'Subscription1'

ⓘ You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription Subscription1

□ Expand all compliance controls

- ⊗ NS. Network Security
- ⊗ IM. Identity Management
- ⊗ PA. Privileged Access
- ⊗ DP. Data Protection
- ✓ AM. Asset Management
- ⊗ LT. Logging and Threat Detection
- ⊗ IR. Incident Response
- ⊗ PV. Posture and Vulnerability Management
- ⊗ ES. Endpoint Security
- ⊗ BR. Backup and Recovery
- ✓ DS. DevOps Security

You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows.

Which compliance control should you evaluate?

A. Asset Management

B. Posture and Vulnerability Management

C. Data Protection

D. Endpoint Security

E. Incident Response

Suggested Answer: *D*

Microsoft Defender for servers compliance control installed on Windows

Defender for clout "Endpoint Security" azure security benchmark v3

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.

Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.

Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.

Incorrect:

Not A: Asset Management covers controls to ensure security visibility and governance over Azure resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for services and resources (inventory, track, and correct).

Not B: Posture and Vulnerability Management focuses on controls for assessing and improving Azure security posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting, and correction in Azure resources.

Not C: Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key and certificate management in Azure.

Not E: Incident Response covers controls in incident response life cycle - preparation, detection and analysis, containment, and post-incident activities, including using Azure services such as Microsoft Defender for Cloud and Sentinel to automate the incident response process.

Reference:

https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

Community vote distribution

D (100%)

PlumpyTumbler Highly Voted 1 year, 10 months ago

Selected Answer: D

No grey area. Endpoint security is the option that meets the goal.

upvoted 22 times

tester18128075 Highly Voted 1 year, 9 months ago

D is correct

upvoted 6 times

zpack Most Recent 4 months, 4 weeks ago

Selected Answer: D

Correct D. But Defender for Servers is not installed in the machine, is used to deploy MDE.

upvoted 1 times

Ario 12 months ago

D is correct

upvoted 1 times

Itu2022 1 year ago

was on exam 15/06/23

upvoted 2 times

edurakhan 1 year, 1 month ago

Exam question 5/23/2023

upvoted 2 times

zellck 1 year, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

upvoted 1 times

zellck 1 year, 1 month ago

Gotten this in May 2023 exam.

upvoted 3 times

D3D1997 1 year, 4 months ago

Selected Answer: D

by definition

upvoted 3 times

TJ001 1 year, 6 months ago

Correct answer

upvoted 2 times

⊟ **TJ001** 1 year, 6 months ago

Defender for Endpoint is available with Defender for Servers Plan1 and 2 .

upvoted 1 times

⊟ **prabhjot** 1 year, 10 months ago

correct D is fine

upvoted 5 times

⊟ **TheMCT** 1 year, 10 months ago

The given answer D, is correct.

upvoted 4 times

⊟ **Alex_Burlachenko** 1 year, 10 months ago

great, and yes correct

upvoted 4 times

Question #3 Topic 2

HOTSPOT -

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to evaluate the existing environment to increase the overall security posture for the following components:

✑ Windows 11 devices managed by Microsoft Intune

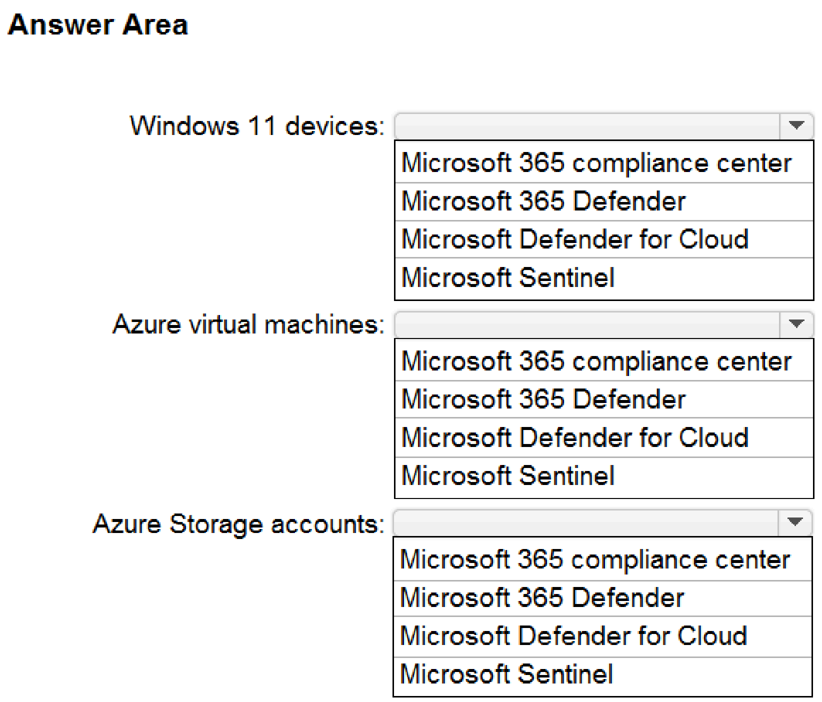
✑ Azure Storage accounts

✑ Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



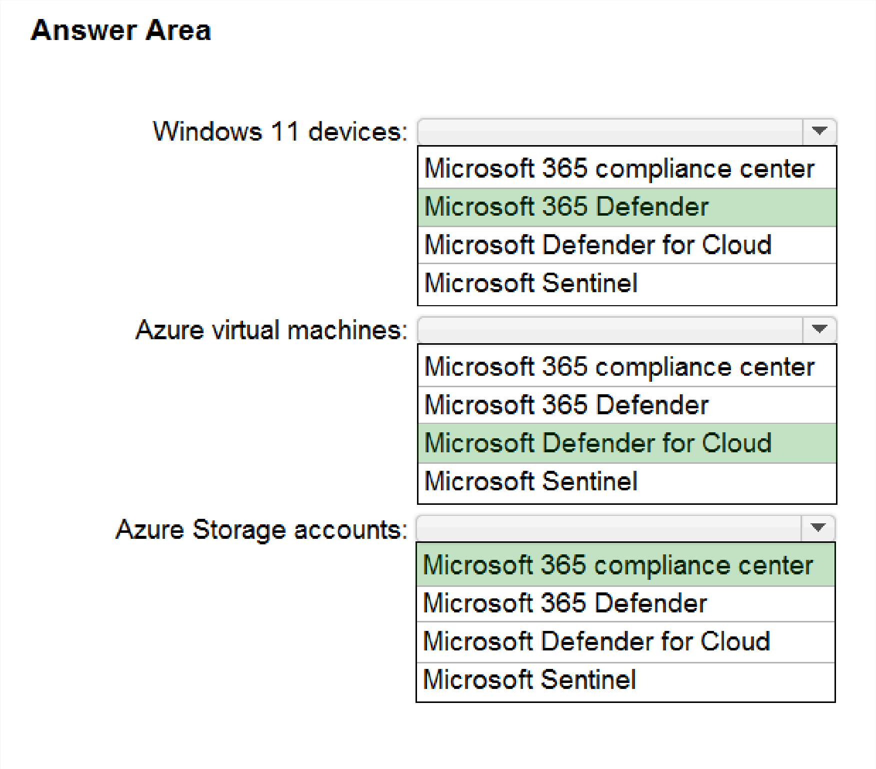
Answer Area

Windows 11 devices:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure virtual machines:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure Storage accounts:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Suggested Answer:



Answer Area

Windows 11 devices:
- Microsoft 365 compliance center
- [✓ Microsoft 365 Defender]
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure virtual machines:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- [✓ Microsoft Defender for Cloud]
- Microsoft Sentinel

Azure Storage accounts:
- [✓ Microsoft 365 compliance center]
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Box 1: Microsoft 365 Defender -

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes

Microsoft Defender for Endpoint.
Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.
Microsoft Defender for Endpoint works with devices that run:

Android -
iOS/iPadOS

Windows 10 -

Windows 11 -
Box 2: Microsoft Defender for Cloud
Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed Instance and Azure Virtual Machines.
Box 3: Microsoft 365 Compliance Center
Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.
Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.
Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender
?
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

HardcodedCloud Highly Voted 2 years, 3 months ago
Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it).
Selection 2: Microsoft Defender for Cloud.
Selection 3: Microsoft Defender for Cloud.
upvoted 136 times

Azzzurrre 1 year, 12 months ago
Microsoft 365 Defender includes both of those and quite a bit else.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide
"Here's a list of the different Microsoft 365 Defender products and solutions:
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Microsoft Defender Vulnerability Management
Azure Active Directory Identity Protection
Microsoft Data Loss Prevention
App Governance
Microsoft Defender for Cloud"
upvoted 2 times

chicaa 5 months, 4 weeks ago
correct, but i think they call it microsoft defender XDR now.
upvoted 1 times

bsakabato 1 year, 3 months ago
The correct wording in the website is :
Here's a list of the different Microsoft 365 Defender products and solutions that Microsoft 365 Defender coordinates with : .....
So Microsoft 365 Defender don't include all theses products, the full list is further down in the documentation and unrelated to the second and third questions.

upvoted 2 times

Ramye 11 months, 3 weeks ago

It's confusing the way Microsoft is describing this products bundle. For clarity, they should say that Microsoft 365 Defender is a product suite that has these (the ones named above) products and it integrates / coordinates with other solutions.

upvoted 1 times

M20200713 2 years, 3 months ago

agreed x2

upvoted 1 times

InformationOverload 2 years, 3 months ago

agreed.

upvoted 4 times

PlumpyTumbler Highly Voted 👍 2 years, 4 months ago

Defender for cloud on VMs & Storage

Read "Security posture management for storage" in this learning module:

https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-security-requirements-for-storage-workloads

upvoted 12 times

Ali96 Most Recent 4 months, 1 week ago

Windows 11 devices : Microsoft 365 Defender

Azure virtual machines : Microsoft Defender for Cloud

Azure Storage accounts : Microsoft Defender for Cloud

upvoted 2 times

zpack 4 months, 4 weeks ago

MDC has Defender for Storage plan to cover this.

upvoted 1 times

Arockia 12 months ago

By using Microsoft 365 Defender, you can evaluate the security posture of Windows 11 devices managed by Microsoft Intune. This solution provides advanced threat protection, detection, and response capabilities for endpoints within the Microsoft 365 environment.

For the evaluation of Azure Storage accounts and Azure virtual machines, you should utilize Microsoft Defender for Cloud (formerly known as Azure Defender). It offers comprehensive threat protection and security monitoring for various Azure services, including Azure Storage accounts and Azure virtual machines. This will help you assess their security configurations, detect vulnerabilities, and receive security recommendations.

upvoted 4 times

Bondaexam 1 year ago

Always look for documentation using the keyword instead of wearing multiple biased hats - Lol - https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction

upvoted 2 times

Bondaexam 1 year ago

Microsoft Defender for Cloud

upvoted 1 times

smanzana 1 year, 2 months ago

1. Microsoft 365 Defender
2. Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud

upvoted 3 times

rahulnair 1 year, 2 months ago

Additional context for 3 - Defender for Storage which is part of Defender for cloud

upvoted 1 times

cyber_sa 1 year, 2 months ago

got this in exam 6oct23. passed with 896 marks. I answered

1. Microsoft 365 Defender
2. Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud

upvoted 8 times

⊟ **Itu2022** 1 year, 6 months ago

was on exam 15/06/23

upvoted 3 times

⊟ **zellck** 1 year, 7 months ago

1. Microsoft 365 Defender
2. Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud

https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide#microsoft-365-defender-protection
Microsoft 365 Defender services protect:
- Endpoints with Defender for Endpoint - Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.

upvoted 1 times

⊟ **zellck** 1 year, 7 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers
Microsoft Defender for Servers extends protection to your Windows and Linux machines that run in Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), and on-premises. Defender for Servers integrates with Microsoft Defender for Endpoint to provide endpoint detection and response (EDR) and other threat protection features.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction
Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential threats to your storage accounts.
It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption.

upvoted 1 times

⊟ **kazaki** 1 year, 7 months ago

Ms 365 defender is post preach defend system so it is not a choice
Section 1 defender for endpoint or compliance center
Section 2 and 3 defender for cloud

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

upvoted 1 times

⊟ **Fal991l** 1 year, 9 months ago

ChatGTP:
Windows 11 Devices: Microsoft 365 Defender
Azure Virtual Machines: Microsoft Sentinel/MS Defender for Cloud
Azure Storage Accounts: Microsoft Defender for Cloud

upvoted 2 times

⊟ **AJ2021** 1 year, 9 months ago

Your first two are correct, last one is incorrect.
Should be:
MS 365 Defender
MDC
MDC

upvoted 1 times

⊟ **[Removed]** 2 years, 1 month ago

For storage accounts protection it's "Defender for Clouds" hands down. No other choices :)

upvoted 1 times

⊟ **SAMSH** 2 years, 3 months ago

was in 20Sep2020 exam

upvoted 2 times

⊟ **tester18128075** 2 years, 3 months ago

Windows client - MS 365 Defender
Server and Storage - MS Defender for cloud

upvoted 4 times

Question #4 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Suggested Answer: *A*
The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in NIST SP 800-53 Rev. 5.
The following mappings are to the NIST SP 800-53 Rev. 5 controls. Use the navigation on the right to jump directly to a specific compliance domain. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open Policy in the Azure portal and select the
Definitions page. Then, find and select the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

Community vote distribution
A (100%)

PlumpyTumbler Highly Voted 👍 1 year, 10 months ago
Selected Answer: A
The given answer is probably the closest. In real life I'd add a regulatory compliance standard in Defender for Cloud. This question might be seen written another way where that is the answer.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-are-available-in-defender-for-cloud
upvoted 21 times

NinjaSchoolProfessor 11 months, 2 weeks ago
A - I agree that I'd probably use Defender for Cloud as the UI is much better, however this service simply doesn't do the work, rather it invokes the Azure Policy initiative which is then reported back to Defender for Cloud.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/policy-reference
upvoted 3 times

zpack Most Recent 🕘 4 months, 4 weeks ago
Selected Answer: C
You need to do it via DfC, using policy blade to check policies assigned from DfC is not a good experience as policies are applied many times with different parameters. Plus the NIST controls will only be mapped under DfC.
upvoted 1 times

Itu2022 1 year ago
was on exam 15/06/23
upvoted 4 times

zellck 1 year, 1 month ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5
upvoted 3 times

AJ2021 1 year, 3 months ago
Selected Answer: A
A is correct

upvoted 2 times

⊟ **Nappy123** 1 year, 4 months ago

One keyword in the question is "review". Answer A would "assign" the policy initiative - not "review". Given that the company has Defender for Cloud, Answer C would be my choice.

upvoted 4 times

⊟ **Toschu** 1 year, 3 months ago

I thought the same, but it says for "the current subscription". Assigning an initiative directly to the mentioned subscription might be easier if there are several.

upvoted 1 times

⊟ **TJ001** 1 year, 6 months ago

Correct Answer.. It is policy initiative assignment .. can be done directly from Policy Blade or Insider Defender for Cloud..end of the day it is an Azure policy .. Correct Answer A

upvoted 2 times

⊟ **Zstefanovic** 1 year, 9 months ago

Selected Answer: A

A, built in policy to comply with that regulation

upvoted 2 times

⊟ **tester18128075** 1 year, 9 months ago

A is correct

upvoted 2 times

⊟ **prabhjot** 1 year, 10 months ago

ans seems correct (azure policy) as in another option - Defender for Cloud, review the Azure security baseline for audit report. (review it is mentioned not creating from custom policy)

upvoted 2 times

Question #5 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have an Amazon Web Services (AWS) implementation.
You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc.
Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Containers

B. Microsoft Defender for servers

C. Azure Active Directory (Azure AD) Conditional Access

D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

E. Azure Policy

Suggested Answer: *ACE*
Environment settings page (in preview) (recommended) - This preview page provides a greatly improved, simpler, onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud's enhanced security features to your AWS resources:
*(A) Microsoft Defender for Containers brings threat detection and advanced defenses to your Amazon EKS clusters. This plan includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control recommendations and more.
* Microsoft Defender for Servers, though it requires Arc.
C: AWS installations can benefit from Conditional Access. Defender for Cloud Apps integrates with Azure AD Conditional Access to enforce additional restrictions, and monitors and protects sessions after sign-in. Defender for Cloud Apps uses user behavior analytics (UBA) and other AWS APIs to monitor sessions and users and to support information protection.
E: Kubernetes data plane hardening.
For a bundle of recommendations to protect the workloads of your Kubernetes containers, install the Azure Policy for Kubernetes. You can also auto deploy this component as explained in enable auto provisioning of agents and extensions.
With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure to enforce the best practices and mandate them for future workloads.
Incorrect:
Not B: To enable the Defender for Servers plan you need Azure Arc for servers installed on your EC2 instances.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-security-solutions

Community vote distribution
ACD (45%) ACE (43%) 6%

zts Highly Voted 2 years, 9 months ago
Selected Answer: ACE
I would go for ACE. That being said, this link covers Azure Policy Extension in hardening Kubernetes data plane. https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=aws-eks
upvoted 23 times

[Removed] 2 years, 9 months ago
Not B (servers require Arc). Not D: PIM is more of the kind nice-to-have.
upvoted 2 times

Fal991l 2 years, 3 months ago
No, Microsoft Defender for servers does not require Azure Arc to extend protection to hybrid cloud workloads, including servers running on AWS.

Azure Arc is a separate Azure service that enables you to manage servers, Kubernetes clusters, and applications on-premises, at the edge, and in multi-cloud environments from a single control plane. It provides a centralized management experience and enables you to apply policies, update servers, and deploy applications across your hybrid cloud environment.

However, if you want to use Azure Arc to manage your servers running on AWS, you can do so by using the Azure Arc enabled servers feature.

This feature allows you to onboard your AWS instances to Azure Arc and manage them through the Azure portal or Azure APIs. In this case, you can also use Microsoft Defender for servers to extend protection to those AWS instances.

upvoted 3 times

Gagi79 1 month, 3 weeks ago

Not true. Here are prerequisites for using Defender to p[protect VMs on AWS - https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws#defender-for-servers

upvoted 1 times

wsrudmen 1 year, 4 months ago

False, it's required:
https://learn.microsoft.com/fr-fr/azure/defender-for-cloud/plan-defender-for-servers

upvoted 4 times

mynk29 2 years, 5 months ago

PIM is privilege identity management.. I wouldn't say its nice to have..its a must

upvoted 3 times

Raven84 1 year, 6 months ago

its only a security feature if you use 4-eyes principle. JIT access is no security feature if u can give roles by urself

upvoted 1 times

jasscomp 1 year, 9 months ago

Yes, it's a must for protecting identity but not the answer for this requirement.

upvoted 2 times

Jajee Highly Voted 2 years, 5 months ago

E can not be an answer, because in-order to apply Azure Policy on AWS based resources, you must need to use Azure Arc, which can not be the case based on requirements.

So, ACD can be the possible answers.

upvoted 17 times

424ede1 Most Recent 3 months ago

Selected Answer: ACD

DFC supports containers and servers for AWS, but Defender for Servers requires Arc
Conditional access and PIM are supported as part of IAM for the authentication process.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws

upvoted 2 times

Ali96 4 months, 1 week ago

Selected Answer: ACE

A. Microsoft Defender for Containers
C. Azure Active Directory (Azure AD) Conditional Access
E. Azure Policy

upvoted 1 times

lam_15 4 months, 2 weeks ago

Selected Answer: ABE

A. Microsoft Defender for Containers
B. Microsoft Defender for servers
E. Azure Policy

upvoted 3 times

sweetykaur 4 months, 3 weeks ago

Selected Answer: ABE

To provide security for the AWS resources while extending your Azure security strategy, you can use the following three services:

A. Microsoft Defender for Containers: Provides security monitoring for containerized environments, including those hosted on AWS.

B. Microsoft Defender for servers: Provides advanced threat protection for servers, whether they are hosted on Azure, AWS, or on-premises.

E. Azure Policy: Helps manage and enforce compliance by creating and applying policies across your resources, including those in AWS.

These services ensure a comprehensive security approach that extends to your AWS implementation.

upvoted 3 times

zpack 4 months, 4 weeks ago

Selected Answer: ACD

DfS can be onboarded using MDE, there's a feature called direct onboarding, although experience will be limited.

Will go to ACD as don't think the question is with feature in mind.

upvoted 1 times

Jawa 5 months, 2 weeks ago

Selected Answer: ACD

ACD is the answer

upvoted 2 times

jvallespin 11 months ago

Selected Answer: ACD

ACD - Without Arc, you cannot onboard VMs from AWS to Defender for cloud for servers so you cannot use it for increase security. Without Arc, you cannot apply Azure Policies to any AWS resources (With Arc only to EC2 Instances). PIM and Conditional Access are linked, if you assume that you can use one (because of AWS SSO integration), the other one as well. Defender for containers can be used without Arc to onboard the EKS Clusters.

upvoted 2 times

crutester 11 months, 3 weeks ago

Selected Answer: ACD

from ChatGPT

No, Azure Policy cannot directly manage or enforce policies on AWS resources without Azure Arc. Azure Policy is designed to work natively within the Azure ecosystem, and to extend its governance capabilities to other cloud environments like AWS, Azure Arc is required.

How Azure Policy Works with Azure Arc:

Azure Arc for Servers: By connecting your AWS virtual machines to Azure Arc, they become Azure resources. You can then apply Azure Policy to these AWS VMs as if they were native Azure VMs.

Azure Arc for Kubernetes: Similarly, you can connect your Kubernetes clusters running on AWS to Azure Arc. This allows you to apply Azure Policy to manage and enforce compliance on these Kubernetes clusters.

Azure Arc for Data Services: This allows managing SQL Servers and other data services running on AWS using Azure Policy through Azure Arc.

upvoted 2 times

bxlin 1 year, 1 month ago

Selected Answer: ACD

Microsoft Defender for Server: requires Arc in AWS

Azure Policy for Kubernetes: requires Arc in AWS

upvoted 4 times

JHJ44 1 year, 2 months ago

Selected Answer: ABC

Microsoft Defender for Containers (Option A):

This service provides runtime protection for containers, including threat detection, vulnerability assessment, and security recommendations.

It helps secure containerized workloads running in AWS by identifying and mitigating risks.

Microsoft Defender for Servers (Option B):

This service offers endpoint protection for servers, including real-time threat detection, behavioral analysis, and automated response.

By deploying it to your AWS instances, you can monitor and protect against malicious activities.

Azure Active Directory (Azure AD) Conditional Access (Option C):

Azure AD Conditional Access allows you to define policies that control access to your AWS resources based on conditions such as user location, device health, and risk level.

You can enforce multi-factor authentication (MFA) or restr

upvoted 3 times

PierreTang 1 year, 4 months ago

Selected Answer: ACD

E Kubernetes data plane hardening, but based on doc, "To deploy the Azure Policy for Kubernetes to specified clusters:

From the recommendations page, search for the relevant recommendation:

....

AWS and On-premises - "Azure Arc-enabled Kubernetes clusters should have the Azure policy extension for Kubernetes extension installed"."
https://learn.microsoft.com/en-us/azure/defender-for-cloud/kubernetes-workload-protections#deploy-azure-policy-for-kubernetes-on-existing-clusters

upvoted 2 times

Jonny_Cage 1 year, 5 months ago

For designing security for Azure landing zones and looking to implement preventive controls to increase the secure score, the two options that would be most relevant are:

A. Azure Web Application Firewall (WAF) - It provides centralized protection of your web applications from common exploits and vulnerabilities.

B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) - It manages, controls, and monitors access within Azure AD, Azure, and other Microsoft Online Services.

upvoted 1 times

Jonny_Cage 1 year, 5 months ago

For extending Azure security strategies to AWS resources without using Azure Arc, the three services you can use are:

B. Microsoft Defender for servers
C. Azure Active Directory (Azure AD) Conditional Access
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

upvoted 2 times

Jonny_Cage 1 year, 5 months ago

These services can provide security for AWS resources by offering protection for servers (Defender), managing access based on conditions (Conditional Access), and controlling and monitoring privileged access (PIM).

upvoted 2 times

Cleggs 1 year, 5 months ago

Selected Answer: ACD

MDS and Azure Policy both require arc.

upvoted 2 times

joshuactz 1 year, 4 months ago

No, Defender for Servers can work by just installing the Log analytics Agent - Azure Arc is not necessary. So imo the answer is BCD.

upvoted 2 times

ayadmawla 1 year, 5 months ago

Selected Answer: ACE

ACE seems right as per the following: https://learn.microsoft.com/en-us/defender-cloud-apps/protect-aws

Policy / Sign-in / containers

upvoted 2 times

Question #6 *Topic 2*

Your company has on-premises network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency for developers.
Which three actions should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.

B. Deploy a Remote Desktop server to an Azure region located in France.

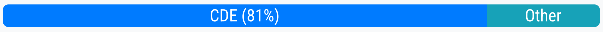
C. Migrate from the Remote Desktop server to Azure Virtual Desktop.

D. Implement Azure Firewall to restrict host pool outbound access.

E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

Suggested Answer: *CDE*
E: Organizations can use this location for common tasks like:
Requiring multi-factor authentication for users accessing a service when they're off the corporate network.
Blocking access for users accessing a service from specific countries or regions.
The location is determined by the public IP address a client provides to Azure Active Directory or GPS coordinates provided by the Microsoft Authenticator app.
Conditional Access policies by default apply to all IPv4 and IPv6 addresses.
CD: Use Azure Firewall to protect Azure Virtual Desktop deployments.
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
Reference:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

Community vote distribution



zellck Highly Voted 1 year, 7 months ago
Selected Answer: CDE
CDE is the answer.

https://learn.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop?tabs=azure
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
upvoted 10 times

zellck 1 year, 7 months ago
https://learn.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa
Users can sign into Azure Virtual Desktop from anywhere using different devices and clients. However, there are certain measures you should take to help keep yourself and your users safe. Using Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) with Azure Virtual Desktop prompts users during the sign-in process for another form of identification in addition to their username and password. You can enforce MFA for Azure Virtual Desktop using Conditional Access, and can also configure whether it applies to the web client, mobile apps, desktop clients, or all clients.

upvoted 5 times

Ramye Highly Voted 11 months, 3 weeks ago

Why D over A? A seems to be better choice but most choosing D. Can someone explain pls?

upvoted 5 times

RabbitB Most Recent 4 months, 2 weeks ago

Selected Answer: CDE

Because A, B does not make sense at all.

upvoted 1 times

Jacek_ 11 months, 1 week ago

I'm wondering Azure Active directory is now Entra ID on exam we see old naming convention or new one ?

upvoted 1 times

Ario 1 year, 6 months ago

ACE are correct answers here

upvoted 2 times

Holii 1 year, 6 months ago

This question is terrible.

B could work to solve the latency issue...and MFA is explicitly stated as a requirement to migrate their existing firewall, but in the context of Zero Trust > latency I would go with E over B.

CDE.

upvoted 1 times

Holii 1 year, 6 months ago

is not stated as a requirement to migrate their existing firewall*

upvoted 1 times

uffman 1 year, 8 months ago

Selected Answer: CDE

Correct.

upvoted 2 times

Gurulee 1 year, 8 months ago

Selected Answer: CDE

This is a tricky one… Based on zero trust, minimizing latency, and keeping the existing firewall requirement in place; I'd go with C,D,E

upvoted 4 times

Holii 1 year, 6 months ago

How exactly does CDE do anything to minimizing latency?

upvoted 2 times

Fal991l 1 year, 9 months ago

Selected Answer: ABE

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges: This action will restrict access to the on-premises network and the Azure subscription to only specific logical groupings of IP address ranges. This helps ensure that only authorized traffic is allowed to access the resources.

B. Deploy a Remote Desktop server to an Azure region located in France: This action will help reduce latency for developers by ensuring that they have a closer connection to the Remote Desktop server. This can be achieved by deploying the Remote Desktop server in an Azure region located in France.

E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations: This action will help ensure that only authorized users are allowed to access the resources. Azure AD Conditional Access can be used to enforce MFA and restrict access based on named locations. This helps ensure that only authorized users are accessing the resources.

upvoted 4 times

Fal991l 1 year, 9 months ago

Selected Answer: BCE

AI: To implement a modern security solution based on the Zero Trust model and minimize latency for developers, the following actions should be recommended:

Migrate from the Remote Desktop server to Azure Virtual Desktop: Azure Virtual Desktop is a modern solution that allows users to securely access their virtual desktops and applications from any device, anywhere. By migrating from the on-premises Remote Desktop server to Azure Virtual Desktop, you can provide secure remote access to the virtual machines hosted in Azure without compromising on security.

upvoted 1 times

Fal991l 1 year, 9 months ago

ChatGPT:

I apologize for the confusion. My previous response was incorrect. The recommended actions for a modern security solution based on the Zero Trust model that minimizes latency for developers and allows access to Azure virtual machines hosted in the Azure subscription by a third-party development firm from France are:

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Deploy a Remote Desktop server to an Azure region located in France.
E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

I hope this clears up any confusion.

upvoted 1 times

jasscomp 1 year, 3 months ago

ChatGPT isn't always right and you need to feed it more info to for more contect.

option B isn't a modern 'security' feature

upvoted 3 times

Rowanomaly 8 months, 1 week ago

All you need to do to change ChatGPTs mind is to drop a paragraph from one of the other option. Then it'll apologize again and change it to the answer you "suggested"

upvoted 1 times

Fal991l 1 year, 9 months ago

Deploy a Remote Desktop server to an Azure region located in France: To minimize latency for developers, you can deploy a Remote Desktop server in an Azure region located in France. This will ensure that developers can access the resources they need quickly and efficiently.

upvoted 1 times

Fal991l 1 year, 9 months ago

Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations: Azure AD Conditional Access allows you to control access to resources based on user identity, device health, and location. By configuring Azure AD Conditional Access with MFA and named locations, you can ensure that only authorized users are able to access the resources they need, from trusted locations.

upvoted 1 times

Fal991l 1 year, 9 months ago

Therefore, the correct answers are C. Migrate from the Remote Desktop server to Azure Virtual Desktop, B. Deploy a Remote Desktop server to an Azure region located in France, and E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

upvoted 2 times

jasscomp 1 year, 3 months ago

Don't use ChatGPT for answers to Microsoft exam questions - I tested it on my renewal exam and it got 50% wrong!

upvoted 1 times

TJ001 2 years ago

CDE is perfect

upvoted 4 times

Bill831231 2 years, 2 months ago

why there is no option for bastion host?

upvoted 2 times

mistralst 2 years ago

Because: "by using custom administrative tools installed on the Remote Desktop server."

upvoted 2 times

PeteNZ 1 year, 10 months ago

The real reason is that they are replacing an RDS environment, so the Azure version of this is AVD. Bastion doesn't support connections to AVD, so it wouldn't be useful in this respect.

upvoted 2 times

nicknamedude 2 years ago

Bastion for OBM

upvoted 2 times

JCkD4Ni3L 2 years, 3 months ago

Selected Answer: CDE

CDE is appropriate

upvoted 2 times

tester18128075 2 years, 3 months ago

CDE IS CORRECT

upvoted 3 times

InformationOverload 2 years, 3 months ago

Selected Answer: CDE

CDE looks fine to me

upvoted 3 times

zts 2 years, 3 months ago

Selected Answer: CDE

same here.

upvoted 2 times

HardcodedCloud 2 years, 3 months ago

Selected Answer: CDE

Correct answer

upvoted 2 times

Question #7 Topic 2

HOTSPOT -

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation.

You need to recommend a security posture management solution for the following components:

➾ Azure IoT Edge devices

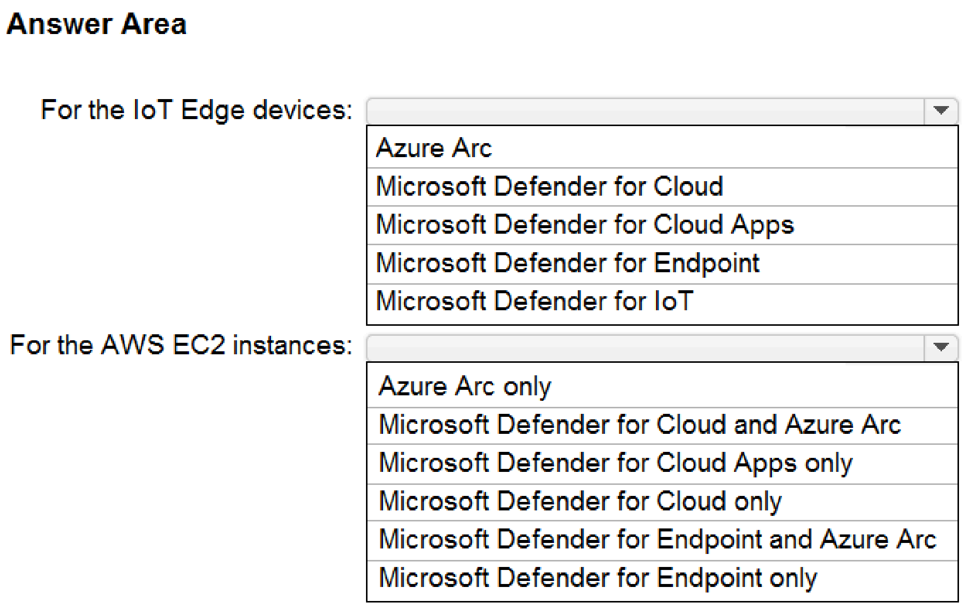
AWS EC2 instances -

▪

Which services should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

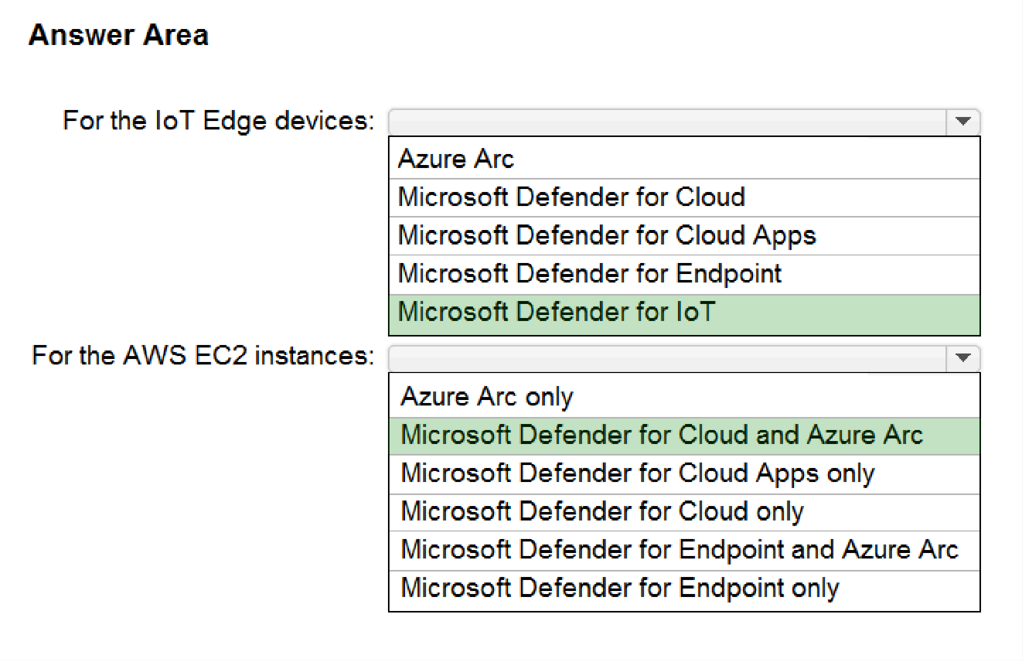
For the IoT Edge devices:

- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:

- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Suggested Answer:



Answer Area

For the IoT Edge devices:

- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- [✓ Microsoft Defender for IoT]

For the AWS EC2 instances:

- Azure Arc only
- [✓ Microsoft Defender for Cloud and Azure Arc]
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Box 1: Microsoft Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Azure IoT Edge provides powerful capabilities to manage and perform business workflows at the edge. The key part that IoT Edge plays in IoT environments make it particularly attractive for malicious actors.

Defender for IoT azureiotsecurity provides a comprehensive security solution for your IoT Edge devices. Defender for IoT module collects, aggregates and analyzes raw security data from your Operating System and container system into actionable security recommendations and

alerts.
Box 2: Microsoft Defender for Cloud and Azure Arc
Microsoft Defender for Cloud provides the following features in the CSPM (Cloud Security Posture Management) category in the multi-cloud scenario for AWS.
Take into account that some of them require Defender plan to be enabled (such as Regulatory Compliance):
* Detection of security misconfigurations
* Single view showing Security Center recommendations and AWS Security Hub findings
* Incorporation of AWS resources into Security Center's secure score calculations
* Regulatory compliance assessments of AWS resources
Security Center uses Azure Arc to deploy the Log Analytics agent to AWS instances.
Incorrect:
AWS EC2 Microsoft Defender for Cloud Apps
Amazon Web Services is an IaaS provider that enables your organization to host and manage their entire workloads in the cloud. Along with the benefits of leveraging infrastructure in the cloud, your organization's most critical assets may be exposed to threats. Exposed assets include storage instances with potentially sensitive information, compute resources that operate some of your most critical applications, ports, and virtual private networks that enable access to your organization.
Connecting AWS to Defender for Cloud Apps helps you secure your assets and detect potential threats by monitoring administrative and sign-in activities, notifying on possible brute force attacks, malicious use of a privileged user account, unusual deletions of VMs, and publicly exposed storage buckets.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/security-edge-architecture
https://samilamppu.com/2021/11/04/multi-cloud-security-posture-management-in-microsoft-defender-for-cloud/

PlumpyTumbler Highly Voted 👍 2 years, 4 months ago
Good answer, bad references
Defender for IoT
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture

EC2 instances need Defender for Cloud by way of Arc
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings
https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations
upvoted 24 times

zts 2 years, 3 months ago
We should still be thankful with examtopic researchers for their efforts, and least such examples makes us to validate our review and correct those mistakes :D)
upvoted 20 times

AWSPro24 5 months, 1 week ago
This is the way to study hands down. Trying to memorize the right answers just plain sucks. I actually end up learning more drilling these questions and digging in to figure out the right answer than I would just trying to memorize a ton of content.
upvoted 1 times

hb0011 2 years, 3 months ago
So this means the answer has to be Defender for IoT and Azure Arc only.
upvoted 2 times

Baz10 Highly Voted 👍 8 months, 3 weeks ago
On Exam 8 Apr 2024 scored 764
answered as solution.
upvoted 7 times

ayadmawla Most Recent ⏲ 12 months ago
AWS accounts should have Azure Arc auto provisioning enabled For full visibility of the security content from Microsoft Defender for servers, EC2 instances should be connected to Azure Arc. To ensure that all eligible EC2 instances automatically receive Azure Arc, enable auto-provisioning from Defender for Cloud at the AWS account level.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws
upvoted 1 times

Arockia 12 months ago

For Question 1: Azure IoT Edge devices, the recommended security posture management solution is:

e. Microsoft Defender for IoT: Microsoft Defender for IoT is designed specifically for securing IoT devices and provides advanced threat protection, vulnerability management, and continuous monitoring for IoT environments. It helps protect Azure IoT Edge devices by detecting and responding to security threats.

For Question 2: AWS EC2 instances, the recommended security posture management solution is:

f. Microsoft Defender for Endpoint only: Microsoft Defender for Endpoint (formerly known as Microsoft Defender ATP) is a comprehensive endpoint security solution that provides protection against various threats, including malware, advanced attacks, and vulnerabilities. While Azure Arc can be used to manage and monitor AWS resources, Microsoft Defender for Endpoint is the appropriate choice for securing the EC2 instances.
upvoted 2 times

⊟ **AWSPro24** 5 months, 1 week ago
The question says security posture management. It's good to get into your head that Defender for Endpoint is basically AV / Anti-Malware. If you check it out you'll see it doesn't do "posture management" it does detect and respond. https://learn.microsoft.com/en-us/defender-endpoint/
upvoted 1 times

⊟ **Ramye** 12 months ago
Any idea, why Microsoft XDR references don't include Defender for IoT/OT. Below is what I see mostly

The component services that are part of the Microsoft Defender XDR stack are:
Microsoft Defender for Identity
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
upvoted 1 times

⊟ **Murtuza** 1 year ago
1. Microsoft Defender for IoT
2. Microsoft Defender for Cloud and Azure Arc
upvoted 1 times

⊟ **zellck** 1 year, 7 months ago
1. Microsoft Defender for IoT
2. Microsoft Defender for Cloud and Azure Arc

https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/overview
Microsoft Defender for IoT is a unified security solution built specifically to identify IoT and OT devices, vulnerabilities, and threats. Use Defender for IoT to secure your entire IoT/OT environment, including existing devices that may not have built-in security agents.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings
With cloud workloads commonly spanning multiple cloud platforms, cloud security services must do the same. Microsoft Defender for Cloud protects workloads in Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), GitHub and Azure DevOps (ADO).

To enable the Defender for Servers plan, you'll need:
- Azure Arc for servers installed on your EC2 instances.
upvoted 6 times

⊟ **calotta1** 1 year, 4 months ago
You are right about Azure Arc, but once the AWS connector is configured on MDC, and auto-provisioning enabled, Azure Arc will install on the EC2 instances.

"We recommend that you use the auto-provisioning process to install Azure Arc on all of your existing and future EC2 instances"
upvoted 1 times

⊟ **GeVanDerBe** 1 year, 8 months ago
You need to recommend a security posture management solution. with that for AWS EC2 MDC only. https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings. --> Provide an agentless connection.
upvoted 1 times

⊟ **GeVanDerBe** 1 year, 8 months ago

wrong response. Forget my comment above!

upvoted 1 times

AJ2021 1 year, 9 months ago

correct

upvoted 1 times

SAMSH 2 years, 3 months ago

was in 20Sep2020 exam

upvoted 5 times

AzureJobsTillRetire 1 year, 10 months ago

I think he meant that he took the exam on 20 Sept 2022. Thank him for taking the time to verify that this question was in exam. Not many people do that. I was one of those lazy people as well. sorry for those see this comment...

upvoted 6 times

PeteNZ 1 year, 10 months ago

This exam wasn't even out then. Dude posts this everywhere.

upvoted 2 times

Pete_4779 2 years, 2 months ago

Did you get it right? What was your score?

upvoted 1 times

JakeCallham 2 years, 3 months ago

Dude stop this nonsense

upvoted 30 times

tester18128075 2 years, 3 months ago

correct

upvoted 3 times

JMuller 2 years, 3 months ago

correct

upvoted 1 times

Alex_Burlachenko 2 years, 4 months ago

correct

upvoted 3 times

Question #8 *Topic 2*

Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company's on-premises network.
The company's secutity policy prevents the use of personal devices for accessing company data and applications.
You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.
What should you include in the recommendation?

A. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

B. Redesign the VPN infrastructure by adopting a split tunnel configuration.

C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.

D. Migrate the on-premises applications to cloud-based applications.

Suggested Answer: *A*
You can connect an Azure Virtual Desktop to an on-premises network using a virtual private network (VPN), or use Azure ExpressRoute to extend the on- premises network into the Azure cloud over a private connection.
* Azure AD: Azure Virtual Desktop uses Azure AD for identity and access management. Azure AD integration applies Azure AD security features like conditional access, multi-factor authentication, and the Intelligent Security Graph, and helps maintain app compatibility in domain-joined VMs.
* Azure Virtual Desktop, enable Microsoft Defender for Cloud.
We recommend enabling Microsoft Defender for Cloud's enhanced security features to:
Manage vulnerabilities.
Assess compliance with common frameworks like PCI.
* Microsoft Defender for Cloud Apps, formerly known as Microsoft Cloud App Security, is a comprehensive solution for security and compliance teams enabling users in the organization, local and remote, to safely adopt business applications without compromising productivity.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cloud-apps/ba-p/2835842

Community vote distribution
A (100%)

Ramkid Highly Voted 1 year, 12 months ago
it is really nice to see that everyone says the same answer
upvoted 15 times

Ramye Most Recent 11 months, 2 weeks ago
Answer is A.
But curious why it included Defender for Cloud Apps and not Defender for Cloud? These VDIs are Azure resources so Defender for Cloud should have been better option, no?
upvoted 4 times

zellck 1 year, 7 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/virtual-desktop/overview

https://learn.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa
Users can sign into Azure Virtual Desktop from anywhere using different devices and clients. However, there are certain measures you should take to help keep yourself and your users safe. Using Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) with Azure Virtual Desktop prompts users during the sign-in process for another form of identification in addition to their username and password. You can enforce MFA for Azure Virtual Desktop using Conditional Access, and can also configure whether it applies to the web client, mobile apps, desktop clients, or all clients.

upvoted 3 times

⊟ **zellck** 1 year, 7 months ago

Gotten this in May 2023 exam.

upvoted 3 times

⊟ **uffman** 1 year, 8 months ago

Selected Answer: A

Correct, use AVD.

upvoted 1 times

⊟ **Xax** 1 year, 9 months ago

I recommend deploying Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access to provide temporary employees with access to company resources. This solution can scale on demand and is secure as it allows you to control access to your applications and data based on conditions such as user location, device compliance, and real-time risk.

This solution also provides a single console for managing devices and applications across all platforms including Windows, Android, iOS, and macOS.

upvoted 1 times

⊟ **TJ001** 2 years ago

indeed no brainer

upvoted 2 times

⊟ **googler015** 2 years, 1 month ago

No brainer - The answer is A

upvoted 1 times

⊟ **IXone** 2 years, 1 month ago

A is correct

upvoted 1 times

⊟ **theOldSoldier** 2 years, 3 months ago

I would go with A

upvoted 2 times

⊟ **tester18128075** 2 years, 3 months ago

vdi is correct

upvoted 1 times

⊟ **InformationOverload** 2 years, 3 months ago

Selected Answer: A

Very logical. Nobrainer.

upvoted 1 times

⊟ **PlumpyTumbler** 2 years, 4 months ago

Selected Answer: A

That is the only way.

upvoted 4 times

⊟ **Alex_Burlachenko** 2 years, 4 months ago

A is correct

upvoted 1 times

Question #9 *Topic 2*

Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Web Application Firewall (WAF)

B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

Suggested Answer: *BC*
B: Azure identity and access for landing zones, Privileged Identity Management (PIM)
Use Azure AD Privileged Identity Management (PIM) to establish zero-trust and least privilege access. Map your organization's roles to the minimum access levels needed. Azure AD PIM can use Azure native tools, extend current tools and processes, or use both current and native tools as needed.
Azure identity and access for landing zones, Design recommendations include:
* (B) Use Azure AD managed identities for Azure resources to avoid credential-based authentication. Many security breaches of public cloud resources originate with credential theft embedded in code or other text. Enforcing managed identities for programmatic access greatly reduces the risk of credential theft.
* Etc.
C: Improve landing zone security, onboard Microsoft Sentinel
You can enable Microsoft Sentinel, and then set up data connectors to monitor and protect your environment. After you connect your data sources using data connectors, you choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.
Note: Landing zone security best practices
The following list of reference architectures and best practices provides examples of ways to improve landing zone security:
Microsoft Defender for Cloud: Onboard a subscription to Defender for Cloud.
Microsoft Sentinel: Onboard to Microsoft Sentinel to provide a security information event management (SIEM) and security orchestration automated response
(SOAR) solution.
Secure network architecture: Reference architecture for implementing a perimeter network and secure network architecture.
Identity management and access control: Series of best practices for implementing identity and access to secure a landing zone in Azure.
Network security practices: Provides additional best practices for securing the network.
Operational security provides best practices for increasing operational security in Azure.
The Security Baseline discipline: Example of developing a governance-driven security baseline to enforce security requirements.
Incorrect:
Not E: Implementing alerts is not a preventive measure.
Reference:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones
https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

Community vote distribution

AD (82%) Other

⊟ **PlumpyTumbler** Highly Voted 2 years, 10 months ago

Selected Answer: AD

This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secure score. Sentinel & PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

Which leads me to believe that only firewalls fit the bill.

upvoted 51 times

grimrodd 7 months, 2 weeks ago

The below article also confirms the answers being A and D

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

upvoted 3 times

jarihd1 2 years, 8 months ago

What if - there is no application gateway / traffic manager / CDN etc configured - how you will configure WAF ? CAF needs basic things for the security readiness! Do not confuse people.

upvoted 4 times

mikenyga 2 years, 9 months ago

Why defender for cloud? Question about landing zone, (CAF) answer correct.
Onboard Microsoft Sentinel.
Azure Identity Management and access control security best practices.
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/landing-zone-security

upvoted 2 times

alpars 2 years, 9 months ago

Sentinel does not increase security score and it is used widely for detection and correlation.

upvoted 7 times

PeteNZ 2 years, 4 months ago

Well, disagree. This is about landing zones and if you scroll down here, I'd say PIM would definitely be an answer.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security

upvoted 7 times

NinjaSchoolProfessor 1 year, 11 months ago

ABCD are correct. All items except "Defender for Cloud alerts" are tools that improve security and are available for use with Azure Landing Zone.

upvoted 3 times

Ramkid 2 years, 3 months ago

I agree with you.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones#privileged-identity-management-pim

upvoted 1 times

meelaran 1 year, 6 months ago

it does not increase security score

upvoted 1 times

HardcodedCloud Highly Voted 2 years, 9 months ago

Selected Answer: AD

Preventative controls are WAF & Firewall

upvoted 21 times

Ramye 1 year, 5 months ago

Certainly, but does it improve the security score? No. So these can't be score…

upvoted 1 times

Ramye 1 year, 5 months ago

Sorry meant to say these can't be answers

upvoted 1 times

dsatizabal Most Recent 5 months, 1 week ago

Selected Answer: BC

For me, being this about ALZ, I definitely go for BC, firewall and WAF are for applications, not for the zone where those lands, I mean, what if you have a private cluster with no public access? Besides, this article already shared:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security mentiones that:

"Make use of the recommendations, alerting, and remediation capabilities of Microsoft Defender for Cloud. Your security team can also integrate Microsoft Defender for Cloud into Microsoft Sentinel if they need a more robust, centrally managed hybrid and multicloud Security Information Event Management (SIEM)/Security Orchestration and Response (SOAR) solution."

So, sentinel definitely helps increasing the ALZ security.

upvoted 1 times

JuicyLinux 8 months, 2 weeks ago

Selected Answer: AD

A good reference from Microsoft Learn on how to improve the security score in Microsoft Defender for Cloud:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#improving-a-secure-score

upvoted 1 times

Tony416 9 months, 1 week ago

Selected Answer: BE

Tricky question. Reading the CAF, and based on the following TOPIC: "Design area overview," https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security#design-area-overview

However, I recommend everyone expand the research...

upvoted 1 times

JAGUDERO 1 year, 2 months ago

COPILOT RESPONSE

B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM): Este servicio ayuda a gestionar, controlar y supervisar el acceso a recursos importantes en la organización. Puede ayudar a reducir los riesgos asociados con los privilegios de acceso al proporcionar acceso justo a tiempo y acceso justo lo suficiente.

E. Microsoft Defender for Cloud alerts: Estas alertas proporcionan notificaciones en tiempo real sobre actividades sospechosas y violaciones de políticas en tu entorno de nube. Pueden ayudarte a detectar y responder rápidamente a amenazas de seguridad.

upvoted 1 times

Cleggs 1 year, 5 months ago

Selected Answer: AD

The only two that show up in the secure score metrics are A and D. PIM is mentioned to increase score but I cant find anything in MDC that shows that.

upvoted 2 times

ayadmawla 1 year, 5 months ago

Selected Answer: BC

Answers given are correct and are inline with the Security design component of an Azure landing zone: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security

upvoted 2 times

Azerty1313 1 year, 6 months ago

Here you find the list:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security

The question to answer which ones are preventative? According to me WAF, Firewall & PIM.
Next question which does improve the score? Not sure there.

upvoted 1 times

rahulnair 1 year, 8 months ago

Selected Answer: BC

Improve SS for landing zone explicitly calls out sentinel and PIM. WAF and FW are not classified as basic controls
"Azure native controls. Azure Firewall and Azure Web Application Firewall offer basic security advantages. Advantages are a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration."

upvoted 2 times

yyYPpp 1 year, 8 months ago

Selected Answer: AB

The two preventative controls that can be implemented to increase the secure score in Azure landing zones are:

A. Azure Web Application Firewall (WAF)
B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

while C. Microsoft Sentinel, D. Azure Firewall, and E. Microsoft Defender for Cloud alerts are all valuable tools for enhancing security in Azure, they are not specifically categorized as preventative controls for increasing the secure score.

upvoted 1 times

calotta1 1 year, 10 months ago

WAF is only required for specific scenario, so many ALZ do not have a requirement for WAF but will PIM is a must for any deployment. AFW is similar, must have on any secure ALZ.

upvoted 1 times

celomomo 1 year, 10 months ago

Selected Answer: AD

Both Azure WAF and Azure Firewall are preventative controls that enhance the security posture of your Azure environment by protecting against unauthorized access, threats, and attacks. These controls help in securing your applications and network traffic, contributing to an improved secure score.

upvoted 1 times

Ario 1 year, 12 months ago

A and D are correct

upvoted 1 times

rhylos 2 years ago

Selected Answer: AD

chatgpt:
A. Azure Web Application Firewall (WAF): Azure WAF helps protect your web applications from common exploits and vulnerabilities by providing centralized protection, monitoring, and logging for your web traffic. It can prevent attacks such as SQL injection, cross-site scripting (XSS), and other malicious activities targeted at web applications.
D. Azure Firewall: Azure Firewall is a managed, cloud-based network security service that provides network traffic filtering and protection for Azure resources. It acts as a preventive control by allowing you to define and enforce network and application-level policies to secure your Azure landing zones. Azure Firewall provides inbound and outbound traffic filtering, application-level inspection, and threat intelligence integration to protect against unauthorized access and threats.

Both Azure WAF and Azure Firewall help increase the secure score by providing essential security controls to protect your Azure landing zones.

upvoted 1 times

ltu2022 2 years ago

was on exam 15/06/23

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: AD

AD is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
- Restrict unauthorized network access
Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.
Use these recommendations to manage Defender for Cloud's adaptive network hardening settings, ensure you've configured Azure Private Link for all relevant PaaS services, enable Azure Firewall on your virtual networks, and more.

- Protect applications against DDoS attacks
Azure's advanced networking security solutions include Azure DDoS Protection, Azure Web Application Firewall, and the Azure Policy Add-on for Kubernetes. Use these recommendations to ensure your applications are protected with these tools and others.

upvoted 4 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 2 times

Question #10 *Topic 2*

You are designing security for an Azure landing zone.
Your company identifies the following compliance and privacy requirements:
✑ Encrypt cardholder data by using encryption keys managed by the company.
✑ Encrypt insurance claim files by using encryption keys hosted on-premises.
Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed keys.

B. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.

C. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM.

D. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.

Suggested Answer: *CD*
C: Azure Key Vault Managed HSM (Hardware Security Module) is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguard cryptographic keys for your cloud applications, using FIPS 140-2 Level 3 validated HSMs.
D: You can generate HSM-protected keys in your on-premise HSM and import them securely into Managed HSM.
Incorrect:
Not A: The company must manage the keys, not Microsoft.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

Community vote distribution
BC (67%) CD (32%)

Alex_Burlachenko Highly Voted 2 years, 10 months ago
I would like to select B & C
upvoted 40 times

maltns 1 year, 4 months ago
B: Customer provided keys (CPK) enables you to store and manage keys in on-premises or key stores other than Azure Key Vault to meet corporate, contractual, and regulatory compliance requirements for data security.
https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service-encryption/
upvoted 4 times

PlumpyTumbler Highly Voted 2 years, 9 months ago
Selected Answer: CD
Hardware Security Module takes the cake. Want to use your own keys? Great. You can still do that with BYOK.
upvoted 14 times

mynk29 2 years, 5 months ago
Azure Key Vault Managed HSM. are not hosted on pre. B and C are right answer
upvoted 7 times

Learing 2 years, 8 months ago
You can add a local key to an managed HSM, but with customer-provided (not customer-managed) keys they are not stored in any Azure Service
upvoted 3 times

tzg Most Recent 6 months ago
Selected Answer: BC
D does not meet the requirement of using encryption keys hosted on-premises, as Managed HSM is an Azure-hosted service.
upvoted 1 times

jvallespin 11 months, 1 week ago
Its C and D, customer managed keys for blob and files must be stored in key vault or Azure HSM.
https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview
https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption#about-encryption-key-management
upvoted 1 times

⊟ **jvallespin** 11 months ago

Correction to my answer, its B and C. Because you can use a customer-provided key (not customer-managed) to include into the cleint request for Blob Storage.

As is said in the link below: "Customer-provided keys can be stored in Azure Key Vault or in another key store" meanwhile the Customer-Managed keys for Storage must be stored in AKV or HSM but is not the case. Additionally the D answer does not mention the key, it just says encrypt using an HSM that cannot be because an HSM by itself does not encrypt.
https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-customer-provided-key

upvoted 2 times

⊟ **besoaus** 1 year ago

It is obvious for me B & C

upvoted 2 times

⊟ **emartiy** 1 year ago

Selected Answer: CD

C - everybody almost agree with this option. So, what is second for insurence claim files?

You can use on prem keys and store them on Azure Managed HSM

Import keys from your on-premises HSMs
Generate HSM-protected keys in your on-premises HSM and import them securely into Managed HSM.
https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview#import-keys-from-your-on-premises-hsms

upvoted 1 times

⊟ **ayadmawla** 1 year, 4 months ago

It is not D and for those choosing D, please refer to the diagram for Azure Storage here: https://rajanieshkaushikk.com/2023/04/08/azure-blob-storage-vs-file-storage-vs-disk-storage-which-is-right-for-you/

upvoted 1 times

⊟ **Mendel** 1 year, 4 months ago

Selected Answer: CD

Answer seems correct.
C. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM: This option aligns with the requirement to encrypt cardholder data using encryption keys managed by the company. Azure Key Vault Managed HSM provides FIPS 140-2 Level 3 validated HSMs, ensuring a high level of security for key management.

D. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM: This option allows you to generate HSM-protected keys on-premises and securely import them into Azure Key Vault Managed HSM. By encrypting insurance claim files with keys stored in Azure Key Vault Managed HSM, you can meet the requirement to encrypt insurance claim files using encryption keys hosted on-premises while leveraging the security and manageability of Azure Key Vault Managed HSM.

https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/hsm-protected-keys-byok

upvoted 1 times

⊟ **Arockia** 1 year, 5 months ago

Option A is incorrect because it uses Microsoft-managed keys, which does not meet the requirement for the company to manage the encryption keys for cardholder data.

Option D is incorrect because it uses Azure Key Vault Managed HSM, which is a cloud-based service. The requirement for insurance claim files is to use keys hosted on-premises.

upvoted 1 times

⊟ **Murtuza** 1 year, 6 months ago

Selected Answer: C

C is definitely one of the answers

upvoted 1 times

⊟ **sherifhamed** 1 year, 9 months ago

Selected Answer: CD

To meet the compliance and privacy requirements for encrypting cardholder data and insurance claim files, you should consider the following configurations:

✅ C. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM.

✅ D. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.

upvoted 1 times

calotta1 1 year, 10 months ago

C and D - surely you can't recommend storing cardholder data in a storage account.

upvoted 1 times

Ramye 1 year, 5 months ago

Of course you can as long as you can keep it safe, secure and encrypted .

upvoted 1 times

[Removed] 1 year, 11 months ago

CD

https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

upvoted 1 times

apyasir 1 year, 12 months ago

Currently, Azure Blob storage does not support customer-provided keys (BYOK) for encryption. Azure Blob storage utilizes Azure Storage Service Encryption (SSE) to automatically encrypt data at rest.

With SSE, Azure Blob storage encrypts your data using Microsoft-managed keys. These keys are managed and rotated by Azure behind the scenes, providing a high level of security for your data. You do not have direct control over the encryption keys used by Azure Blob storage.

so answer: C & D

upvoted 1 times

NinjaSchoolProfessor 1 year, 11 months ago

Incorrect, Data in Blob storage and Azure Files is always protected by customer-managed keys when customer-managed keys are configured for the storage account.

https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json#customer-managed-keys-for-queues-and-tables

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: BC

BC is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql

Azure SQL transparent data encryption (TDE) with customer-managed key (CMK) enables Bring Your Own Key (BYOK) scenario for data protection at rest, and allows organizations to implement separation of duties in the management of keys and data. With customer-managed TDE, the customer is responsible for and in a full control of a key lifecycle management (key creation, upload, rotation, deletion), key usage permissions, and auditing of operations on keys.

upvoted 6 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-customer-provided-keys

Clients making requests against Azure Blob storage can provide an AES-256 encryption key to encrypt that blob on a write operation. Subsequent requests to read or write to the blob must include the same key. Including the encryption key on the request provides granular control over encryption settings for Blob storage operations. Customer-provided keys can be stored in Azure Key Vault or in another key store.

upvoted 2 times

Zapman 2 years, 1 month ago

AB is correct in my opinion ,Explanation:

A. Storing cardholder data in an Azure SQL database encrypted with Microsoft-managed keys ensures that the data is encrypted. Microsoft-managed keys are suitable for encrypting cardholder data as per compliance requirements.

B. Storing insurance claim data in Azure Blob storage encrypted with customer-provided keys allows for encryption of the data. By using on-premises keys, the company maintains control over the encryption keys and meets the requirement for encrypting insurance claim files.

upvoted 1 times

Tictactoe 2 years, 1 month ago

AB is right

upvoted 1 times

Ramye 1 year, 5 months ago

A definitely not - requirements is not to use Microsoft keys

upvoted 2 times

Question #11 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You need to enforce ISO 27001:2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically.
What should you use?

A. Azure Policy

B. Azure Blueprints

C. the regulatory compliance dashboard in Defender for Cloud

D. Azure role-based access control (Azure RBAC)

Suggested Answer: *A*
Control mapping of the ISO 27001 Shared Services blueprint sample
The following mappings are to the ISO 27001:2013 controls. Use the navigation on the right to jump directly to a specific control mapping.
Many of the mapped controls are implemented with an Azure Policy initiative.
Open Policy in the Azure portal and select the Definitions page. Then, find and select the [Preview] Audit ISO 27001:2013 controls and deploy specific VM
Extensions to support audit requirements built-in policy initiative.
Note: Security Center can now auto provision the Azure Policy's Guest Configuration extension (in preview)
Azure Policy can audit settings inside a machine, both for machines running in Azure and Arc connected machines. The validation is performed by the Guest
Configuration extension and client.
With this update, you can now set Security Center to automatically provision this extension to all supported machines.
Enforcing a secure configuration, based on a specific recommendation, is offered in two modes:
Using the Deny effect of Azure Policy, you can stop unhealthy resources from being created
Using the Enforce option, you can take advantage of Azure Policy's DeployIfNotExist effect and automatically remediate non-compliant resources upon creation
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive https://docs.microsoft.com/en-us/azure/defender-for-cloud/prevent-misconfigurations

Community vote distribution
A (82%) B (18%)

HardcodedCloud Highly Voted 2 years, 9 months ago
Selected Answer: A
Azure policy
upvoted 13 times

crutester Highly Voted 11 months, 3 weeks ago
Selected Answer: A
Azure Blueprints is excellent for deploying a consistent set of resources, policies, and role assignments, but it does not continuously enforce compliance or provide automatic remediation on its own.
Azure Policy provides the ongoing enforcement and remediation capabilities needed to ensure that resources remain compliant with ISO 27001:2013 standards.
Therefore, while Azure Blueprints can be used to initially deploy the necessary compliance infrastructure, Azure Policy is the tool that ensures continuous compliance and automatic remediation.
upvoted 5 times

Noexperience Most Recent 9 months, 3 weeks ago
Selected Answer: B
You need to enforce and automatic remediation.
upvoted 1 times

ayadmawla 1 year, 4 months ago
Selected Answer: B

I would go with Blueprint because it contains Policies, and RBAC and customised configuration. Once Blueprint is used it maintains its link to configuration to ensure automated compliance.

See the table here: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-management-guide/operational-compliance?tabs=UpdateManagement%2CAzurePolicy%2CAzureBlueprints

See the differences here: https://k21academy.com/az-305/azure-rbac-vs-azure-policies-vs-azure-blueprints/

upvoted 2 times

macka2005 11 months, 3 weeks ago

You are going beyond the requirements, whilst policy and RBAC etc can be part of Blue prints. All that is needed here in the most simplistic form is Azure policy.

upvoted 2 times

sehlohomoletsane 1 year, 4 months ago

https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

upvoted 3 times

edurakhan 2 years, 1 month ago

Exam 5/25/2023

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 4 times

OCHT 2 years, 3 months ago

Selected Answer: B

Blueprint to enforce.

upvoted 1 times

Gurulee 2 years, 3 months ago

Selected Answer: A

Automatic remediation was the key requirement here for me and it aligns directly with Azure Policy

upvoted 3 times

KrishnaSK1 2 years, 4 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal

upvoted 1 times

Rocky83 2 years, 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/governance/blueprints/samples/iso-27001-2013

upvoted 1 times

GeVanDerBe 2 years, 2 months ago

In the same link the first explanation refers to Azure Policy --> The ISO 27001 blueprint sample provides governance guardrails using Azure Policy

upvoted 1 times

TJ001 2 years, 6 months ago

blueprint contains policy as a child item , I think key here automatic resolution which happens when deployifnotexists effect is added in the policy; so will go with policy to honor the details present in the question

upvoted 3 times

Sec_Arch_Chn 2 years, 7 months ago

deployifnotexist to be enabled in Azure Policy. Source: https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal

upvoted 1 times

techtest848 2 years, 7 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal

upvoted 1 times

SelloLed 2 years, 8 months ago

B

https://azure.microsoft.com/en-us/products/blueprints/#features

upvoted 1 times

Kamal_SriLanka 2 years, 8 months ago

B. Azure Blueprints 100% sure

upvoted 2 times

JCkD4Ni3L 2 years, 9 months ago

Selected Answer: A

Azure Policy, unfortunatly at the moment of this writting Blueprints are in preview and thus should not be used in production (this will change in the future as it is a good solution).

upvoted 4 times

Question #12 *Topic 2*

DRAG DROP -

You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

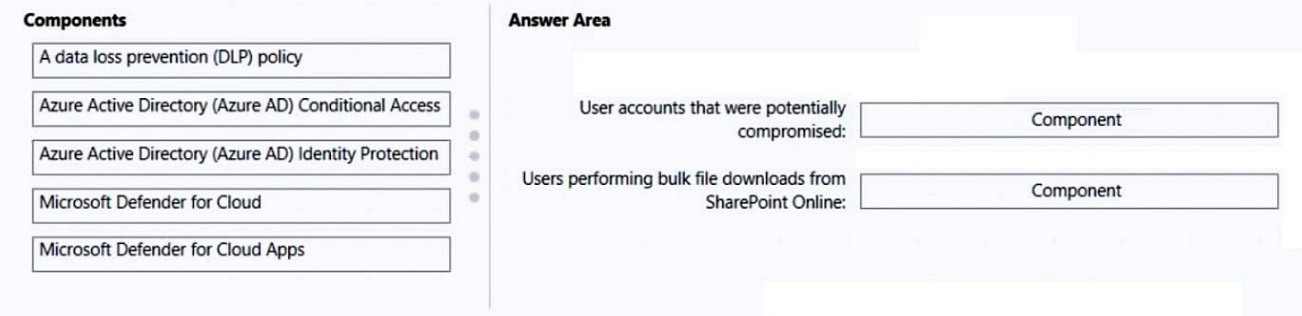
✑ User accounts that were potentially compromised

✑ Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Components

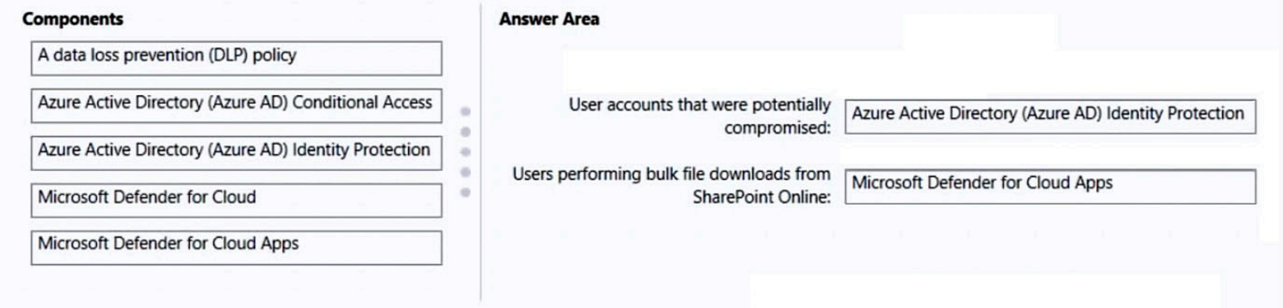
- A data loss prevention (DLP) policy
- Azure Active Directory (Azure AD) Conditional Access
- Azure Active Directory (Azure AD) Identity Protection
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer Area

User accounts that were potentially compromised: Component

Users performing bulk file downloads from SharePoint Online: Component

Suggested Answer:



Components

- A data loss prevention (DLP) policy
- Azure Active Directory (Azure AD) Conditional Access
- Azure Active Directory (Azure AD) Identity Protection
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer Area

User accounts that were potentially compromised: Azure Active Directory (Azure AD) Identity Protection

Users performing bulk file downloads from SharePoint Online: Microsoft Defender for Cloud Apps

Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

Premium sign-in risk detections include:

* Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.

* Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This detection may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.

* Etc.

Incorrect:

Not: Microsoft 365 Defender for Cloud

Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365

Defender portal from Incidents & alerts > incident > Users.

Box 2: Microsoft 365 Defender for App

Defender for Cloud apps detect mass download (data exfiltration) policy

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

TheMCT Highly Voted 👍 2 years, 10 months ago

The given answer is correct.

upvoted 25 times

zellck Highly Voted 👍 2 years, 1 month ago

1. Azure AD Identity Protection

2. Microsoft Defender for Cloud Apps

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#nonpremium-user-risk-detections

https://learn.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

upvoted 13 times

rekaro Most Recent 🕘 1 year ago

Correct

upvoted 3 times

besoaus 1 year ago

Answer is true

upvoted 1 times

calotta1 1 year, 10 months ago

Has anyone considered DLP as the better solution here since the question is about reporting?

REF: https://www.microsoft.com/en-gb/security/business/security-101/what-is-data-loss-prevention-dlp?ef_id=_k_Cj0KCQjw_5unBhCMARIsACZyzS11Eh7eQSTGLIRjq5TP3xT2cbyWnDkJaHSav13rcKytz0ZwytyaBugaAqq4EALw_wcB_k_&OCID=AIDcmmao55x8o7_SE

upvoted 4 times

> **Ramye** 1 year, 5 months ago
>
> DLP is for data loss prevention in terms of sensitive data, i.e., credit card, health info, social security card etc.,
>
> upvoted 1 times

TJ001 2 years, 6 months ago

The given answers are correct as it is for monitoring purpose

upvoted 2 times

examtopics_100 2 years, 6 months ago

Correct

upvoted 3 times

JCkD4Ni3L 2 years, 9 months ago

Answers are correct !

upvoted 2 times

tester18128075 2 years, 9 months ago

identity protection and cloud

upvoted 2 times

JMuller 2 years, 9 months ago

Correct

upvoted 3 times

prabhjot 2 years, 10 months ago

yes correct ans

upvoted 4 times

Alex_Burlachenko 2 years, 10 months ago

right, correct answer

upvoted 4 times

Question #13 *Topic 2*

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.
You receive the following recommendations in Defender for Cloud
✑ Access to storage accounts with firewall and virtual network configurations should be restricted.
✑ Storage accounts should restrict network access using virtual network rules.
✑ Storage account should use a private link connection.
✑ Storage account public access should be disallowed.
You need to recommend a service to mitigate identified risks that relate to the recommendations.
What should you recommend?

A. Azure Policy

B. Azure Network Watcher

C. Azure Storage Analytics

D. Microsoft Sentinel

Suggested Answer: *A*
An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled. Built in definitions include things like controlling what type of resources can be deployed or enforcing the use of tags on all resources. You can also create your own custom policy definitions.
Note: Azure security baseline for Azure Storage
This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Azure Storage. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Azure Security
Benchmark and the related guidance applicable to Azure Storage.
You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory
Compliance section of the Microsoft Defender for Cloud dashboard.
For example:
* 1.1: Protect Azure resources within virtual networks
Guidance: Configure your storage account's firewall by restricting access to clients from specific public IP address ranges, select virtual networks, or specific
Azure resources. You can also configure Private Endpoints so traffic to the storage service from your enterprise travels exclusively over private networks.
* 1.8: Minimize complexity and administrative overhead of network security rules
Guidance: For resource in Virtual Networks that need access to your Storage account, use Virtual Network Service tags for the configured Virtual Network to define network access controls on network security groups or Azure Firewall. You can use service tags in place of specific IP addresses when creating security rules.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

Community vote distribution
A (100%)

theOldSoldier Highly Voted 1 year, 9 months ago
Selected Answer: A
Only answer that meet the given conditions
upvoted 9 times

roman203 Most Recent 8 months, 3 weeks ago
Selected Answer: A
Agreed. A is the only answer that meet the given conditions
upvoted 2 times

ServerBrain 10 months, 2 weeks ago
Selected Answer: A

other suggested answers are about alerting..

upvoted 2 times

zellck 1 year, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 3 times

TJ001 1 year, 6 months ago

Policy however it needs to have the right effect set 'deployifnotexists' to remediate existing workloads..

upvoted 1 times

tester18128075 1 year, 9 months ago

Azure policy

upvoted 1 times

ele123 1 year, 9 months ago

Selected Answer: A

Azure Policy can "mitigate identified risks"

upvoted 4 times

JMuller 1 year, 9 months ago

Selected Answer: A

correct

upvoted 1 times

HardcodedCloud 1 year, 9 months ago

Selected Answer: A

Azure Policy for sure.

upvoted 3 times

PlumpyTumbler 1 year, 10 months ago

Selected Answer: A

Policy does that.

upvoted 3 times

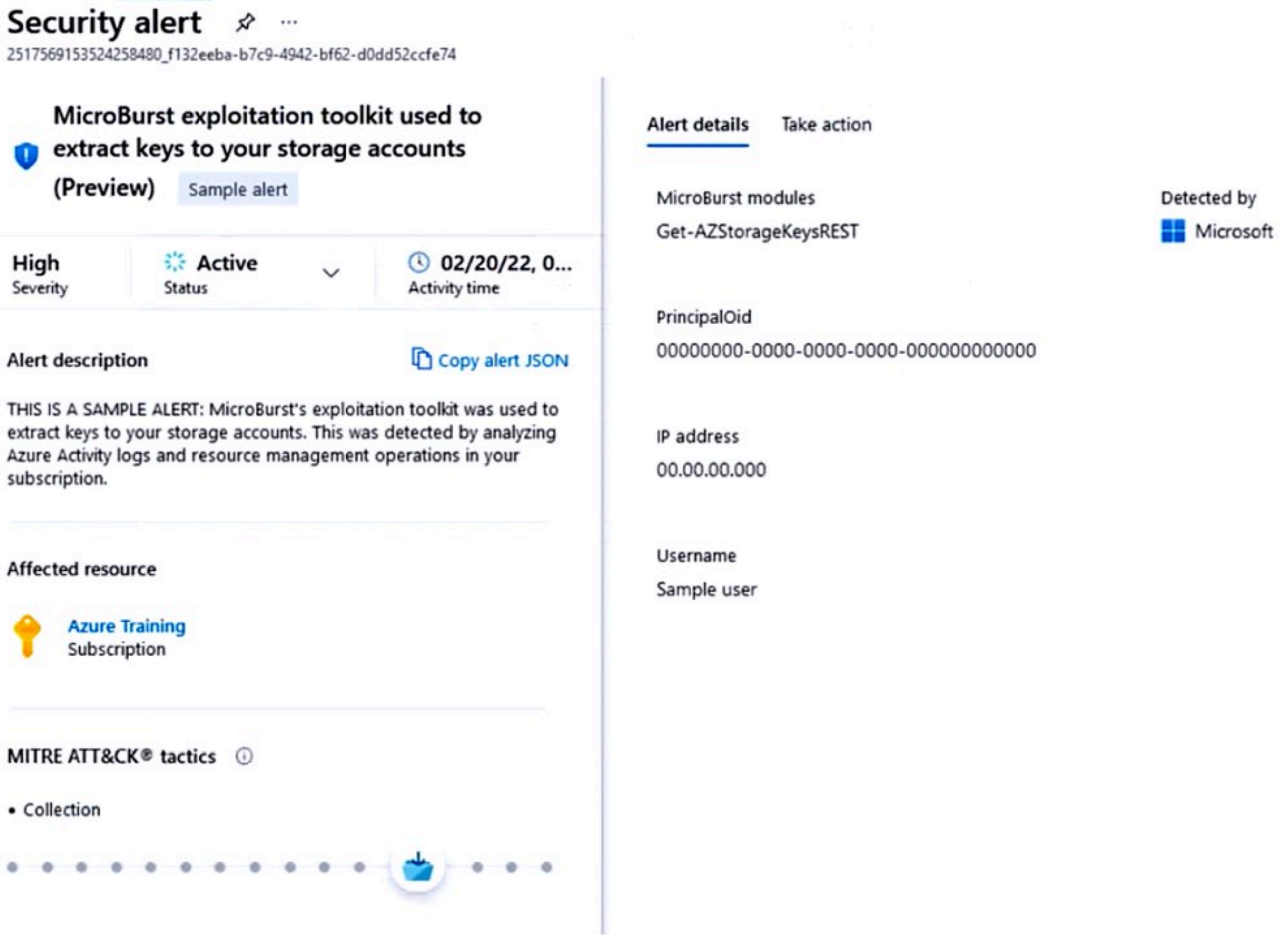
Alex_Burlachenko 1 year, 10 months ago

right and correct

upvoted 2 times

Question #14 *Topic 2*

You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



Security alert

2517569153524258480_f132eeba-b7c9-4942-bf62-d0dd52ccfe74

MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview) Sample alert

High Severity | Active Status | 02/20/22, 0... Activity time

Alert description

Copy alert JSON

THIS IS A SAMPLE ALERT: MicroBurst's exploitation toolkit was used to extract keys to your storage accounts. This was detected by analyzing Azure Activity logs and resource management operations in your subscription.

Affected resource

Azure Training
Subscription

MITRE ATT&CK® tactics

- Collection

Alert details | Take action

MicroBurst modules
Get-AZStorageKeysREST

Detected by
Microsoft

PrincipalOid
00000000-0000-0000-0000-000000000000

IP address
00.00.00.000

Username
Sample user

After remediating the threat, which policy definition should you assign to prevent the threat from reoccurring?

A. Storage account public access should be disallowed

B. Azure Key Vault Managed HSM should have purge protection enabled

C. Storage accounts should prevent shared key access

D. Storage account keys should not be expired

Suggested Answer: *A*

Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but may also present a security risk. It's important to manage anonymous access judiciously and to understand how to evaluate anonymous access to your data. Operational complexity, human error, or malicious attack against data that is publicly accessible can result in costly data breaches. Microsoft recommends that you enable anonymous access only when necessary for your application scenario.

Note: Attackers have been crawling for public containers using tools such as MicroBurst.

Exploiting Anonymous Blob Access

Now, there are thousands of articles explaining how this can be abused and how to search for insecure storage in Azure. One of the easiest way is to use

MicroBurst, provide the storage account name to search for, and it'll check if the containers exists based on a wordlist saved in the Misc/permutations.txt

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent https://hackingthe.cloud/azure/anonymous-blob-access/

Community vote distribution

C (75%) | A (25%)

walkaway Highly Voted 2 years, 5 months ago

Selected Answer: C

C is the correct answer. You should read Microburst toolkit - it is an open-source tool. Find Get-AZStorageKeysREST.ps1 it tries to enumerate all storage accounts then the respective storage keys. There is nothing to do with anonymous access here. Even if a storage account allows public acces you can't get the key without being authenticated and authorized.

The preventive control here is to manage Shared Key Authorization.

upvoted 32 times

Alex_Burlachenko Highly Voted 👍 2 years, 10 months ago

I would select "Storage accounts should prevent shared key access"

upvoted 17 times

purek77 2 years, 5 months ago

... by applying read-only lock.

upvoted 1 times

Onimole Most Recent 🕘 10 months ago

MicroBurst exploitation toolkit used to extract keys to your storage accounts
(ARM_MicroBurst.AZStorageKeysREST)

Description: A PowerShell script was run in your subscription and performed a suspicious pattern of extracting keys to Storage Account(s). Threat actors use automated scripts, like MicroBurst, to list keys and use them to access sensitive data in your Storage Account(s). This was detected by analyzing Azure Resource Manager operations in your subscription. This operation might indicate that an identity in your organization was breached, and that the threat actor is trying to compromise your environment for malicious intentions.

IF IT NEEDS TO BE BREACHED, THEN MAYBE SHARED KEY ACCESS WILL BE THE ANSWER

upvoted 1 times

Socgen1 11 months, 3 weeks ago

Option C - When you disallow Shared Key authorization for a storage account, Azure Storage rejects all subsequent requests to that account that are authorized with the account access keys. Only secured requests that are authorized with Microsoft Entra ID will succeed.

upvoted 1 times

Neverwinter 1 year, 2 months ago

Selected Answer: A

The Correct Answer is A. According to Microsoft Public storage accounts have a URL of a public endpoint (more information in the Background section), which means that it's possible to guess storage accounts names by performing DNS queries on the URL and examining the response. The way to prevent this is to remove Public access.

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/protect-your-storage-resources-against-blob-hunting/ba-p/3735238

upvoted 2 times

ayadmawla 1 year, 4 months ago

Selected Answer: A

Not sure why preventing shared key access would be better than blocking public access. After all there are far more hackers in the outer world that would rather push an open door than test shared keys. Just my own two pennies

upvoted 1 times

Ragdoll 1 year, 2 months ago

Remember that threats could come from inside, not just outside. That's why C is the right answer. If no key is available, there is nothing to steal.

upvoted 1 times

SFAY 1 year, 4 months ago

Selected Answer: A

Not sure how 80% voted for the wrong answer.

The correct answer is A.

https://hacknowledge.com/blog-post/azure-blob-storage-detect-and-prevent-public-accesses/

upvoted 3 times

sehlohomoletsane 1 year, 4 months ago

Selected Answer: C

After remediating the threat, to prevent it from reoccurring, you should assign the following policy definition:

C. Storage accounts should prevent shared key access

This policy ensures that shared keys are not used for access to storage accounts, which aligns with security best practices and helps prevent similar threats in the future .

upvoted 2 times

Arockia 1 year, 5 months ago

MicroBurst leverages the Get-AZStorageKeysREST.ps1 script to brute-force enumerate storage accounts and subsequently attempt to retrieve their keys using REST API calls. Public access isn't directly targeted by this script.
While disallowing public access (option A) is a generally good security practice, it wouldn't specifically prevent the MicroBurst exploitation technique that relies on shared key access. Even with public access blocked, the script could still enumerate accounts and try brute-forcing shared keys.
Preventing shared key access (option C) directly addresses the vulnerability exploited by the script. By disabling this access method, storage accounts become protected from unauthorized key retrieval attempts using Get-AZStorageKeysREST.ps1 or similar tools.

upvoted 4 times

Joe1126 1 year, 7 months ago

Selected Answer: C

is the right answer

upvoted 1 times

slobav 1 year, 9 months ago

Selected Answer: A
From the picture above you can see access from IP 0.0.0.0 that means from internet (public access).
SAS token allow limited access to storage.

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=portal
Every secure request to an Azure Storage account must be authorized. By default, requests can be authorized with either Azure Active Directory (Azure AD) credentials, or by using the account access key for Shared Key authorization. Of these two types of authorization, Azure AD provides superior security and ease of use over Shared Key, and is recommended by Microsoft. To require clients to use Azure AD to authorize requests, you can disallow requests to the storage account that are authorized with Shared Key.

upvoted 7 times

TomRoute66 9 months, 1 week ago

Adding more from the same page:
"When you disallow Shared Key authorization for a storage account, Azure Storage rejects all subsequent requests to that account that are authorized with the account access keys. Only secured requests that are authorized with Microsoft Entra ID will succeed. "

upvoted 1 times

valeriafarias 2 years, 2 months ago

The correct is C, see the docs: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference

upvoted 2 times

etblue 2 years, 3 months ago

My answer would be C.
Note that the question is asking "After remediating the threat, which policy definition should you assign to prevent the threat from reoccurring".
Answer A mitigate the attack by limiting exploit only thru private network links. However, to entirely prevent threat from re-occuring, simply stop using preShare key authorization.

upvoted 3 times

vins_vins_vins 2 years, 4 months ago

I vote for C.
Azure AD provides superior security and ease of use over Shared Key, and is recommended by Microsoft.

here the link: https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=portal

upvoted 1 times

KrisDeb 2 years, 4 months ago

I am torn between A and C, in my opinion it should be both that would make sense. I really don't know what to choose for the exam now - A or C.

upvoted 1 times

⊟ **Azzzurrre** 2 years, 6 months ago

"... By default, requests can be authorized with either Azure Active Directory credentials, or by using the account access key for Shared Key authorization. Of these two types of authorization, Azure AD provides superior security and ease of use over Shared Key, and is recommended by Microsoft."

https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Storage/StorageAccountAllowSharedKeyAccess_Audit.json

upvoted 3 times

⊟ **maku067** 2 years, 5 months ago

I agree. C is correct.

upvoted 2 times

Question #15 *Topic 2*

You have 50 Azure subscriptions.
You need to monitor the resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
What are two ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.

B. Assign a policy to each subscription.

C. Assign a policy to a management group.

D. Assign an initiative to each subscription.

E. Assign a blueprint to each subscription.

F. Assign a blueprint to a management group.

Suggested Answer: *AF*
An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions en masse.
If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions.
Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.
F: Blueprint definition locations
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have
Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.
A: Create and assign an initiative definition
With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.
Note: The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in ISO 27001:2013.
The Azure Policy control mapping provides details on policy definitions included within this blueprint and how these policy definitions map to the compliance domains and controls in ISO 27001. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions.
Incorrect:
Not B, D, E: If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001
https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

Community vote distribution
AF (75%) AC (20%) 5%

HardcodedCloud Highly Voted 2 years, 9 months ago
Selected Answer: AF
Initiative & Blueprint at the management group level
upvoted 20 times

InformationOverload Highly Voted 2 years, 9 months ago
Selected Answer: AF
Initiative; A group of related policies joined logically to accomplish a common goal. Better to use initiatives than a single policy in this case. Use it on management group level. Answer is correct.
upvoted 8 times

jvallespin Most Recent 11 months ago

Selected Answer: AC

Blueprint for monitoring? I would assign an initiative to mgmt group and later a policy to that initiative and im monitoring and minimizing the effort.

upvoted 1 times

> **jvallespin** 11 months ago
>
> My apologizes, it's A and F, blueprint could be used for monitoring adding an Azure Policy but because Blueprint have predefined blueprints for ISO 27001:2013, the administrative effort required to modify list of monitored policy definitions would be less.
>
> upvoted 1 times

rahulnair 1 year, 8 months ago

Selected Answer: AF

Initiative not required as Azure policy already covers ISO. If multiple standards would have been in scope, then inititaives would have made sense.

upvoted 1 times

calotta1 1 year, 10 months ago

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment - "Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription"

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: AF

AF is the answer.

https://learn.microsoft.com/en-us/azure/governance/blueprints/samples/iso-27001-2013
https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

upvoted 2 times

vitodobra 2 years, 3 months ago

Selected Answer: AC

To minimize the effort required to modify the list of monitored policy definitions for the subscriptions while monitoring resource compliance with the ISO 27001:2013 standards, you can assign policies to a management group or assign initiatives to a management group. This way, the policies or initiatives will apply to all the subscriptions within that management group, making it easier to manage and update policy definitions across multiple subscriptions at once.

Therefore, the correct answers are:

A. Assign an initiative to a management group.
C. Assign a policy to a management group.

upvoted 2 times

> **Toschu** 2 years, 3 months ago
>
> A policy doesn't include all the policy definitions needed, which means a big overhead in assigning them all and updating them in the future.
> They can be all assigned to one blueprint, and the blueprint to the management group.
> But it's important to use the initiative because it gets updated by Microsoft if new policy definitions are added! So always use the initiative.
>
> upvoted 3 times

KrishnaSK1 2 years, 4 months ago

Selected Answer: AF

https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

upvoted 1 times

sean2022 2 years, 6 months ago

why not c?

upvoted 2 times

Sec_Arch_Chn 2 years, 7 months ago

Question mentions 'minimize the effort required to modify the list of monitored policy definitions for the subscriptions'.

Initiative - collection of policy definitions that are tailored towards achieving a singular overarching goal
Blueprint - Enables the creation of fully governed environments in a repetitive manner using policies & initiatives.
A -> Ensures compliance of existing resources in the environment
F-> Ensures compliance for any resources getting created in the environment

upvoted 5 times

IHensch 2 years, 7 months ago

Selected Answer: AC

You can use Azure Policy or Initiative (a group of policies) to achieve this goal. The Blueprint does not make sense for this question. There are two possible solutions. In my opinion, they are exactly these.

upvoted 5 times

Jacquesvz 2 years, 5 months ago

I agree with IHensch. the question states: "You need to MONITOR the resource(s) in the subscriptions for compliance" You need to MONITOR, not ensure that all new and future deployments are compliant. Policies or Initiatives make sense. To minimize the effort, one would assign it at the Management group level, and not at each subscription. Just my 2 cents worth.

upvoted 2 times

dudus999 1 year, 10 months ago

I agree blue print not make sense

upvoted 3 times

omarrob 2 years, 7 months ago

AF are the correct answers

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

upvoted 1 times

blopfr 2 years, 8 months ago

Selected Answer: AD

Blueprint can't be assigned to management group can't be F

upvoted 2 times

jayek 1 year ago

A and D
The Definition Location is the place in the management group hierarchy where this blueprint definition will be stored. Once the definition is created, a blueprint assignment can be created at or below this location in the management group hierarchy. Management groups are groups that can contain subscriptions, or other management groups. You can learn more at:
aka.ms/BlueLocation

upvoted 1 times

Learing 2 years, 8 months ago

You can

upvoted 1 times

omarrob 2 years, 7 months ago

You can assign blueprint to managed group

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

upvoted 2 times

IHensch 2 years, 7 months ago

=> "Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription."

upvoted 1 times

EmmanuelDan 2 years, 7 months ago

yes you can I just finished watching Azure Fridays on Blueprint, and the architects for blueprints mentioned that you can assign blueprints to management groups

upvoted 4 times

tester18128075 2 years, 9 months ago

A and F

upvoted 2 times

Alex_Burlachenko 2 years, 10 months ago

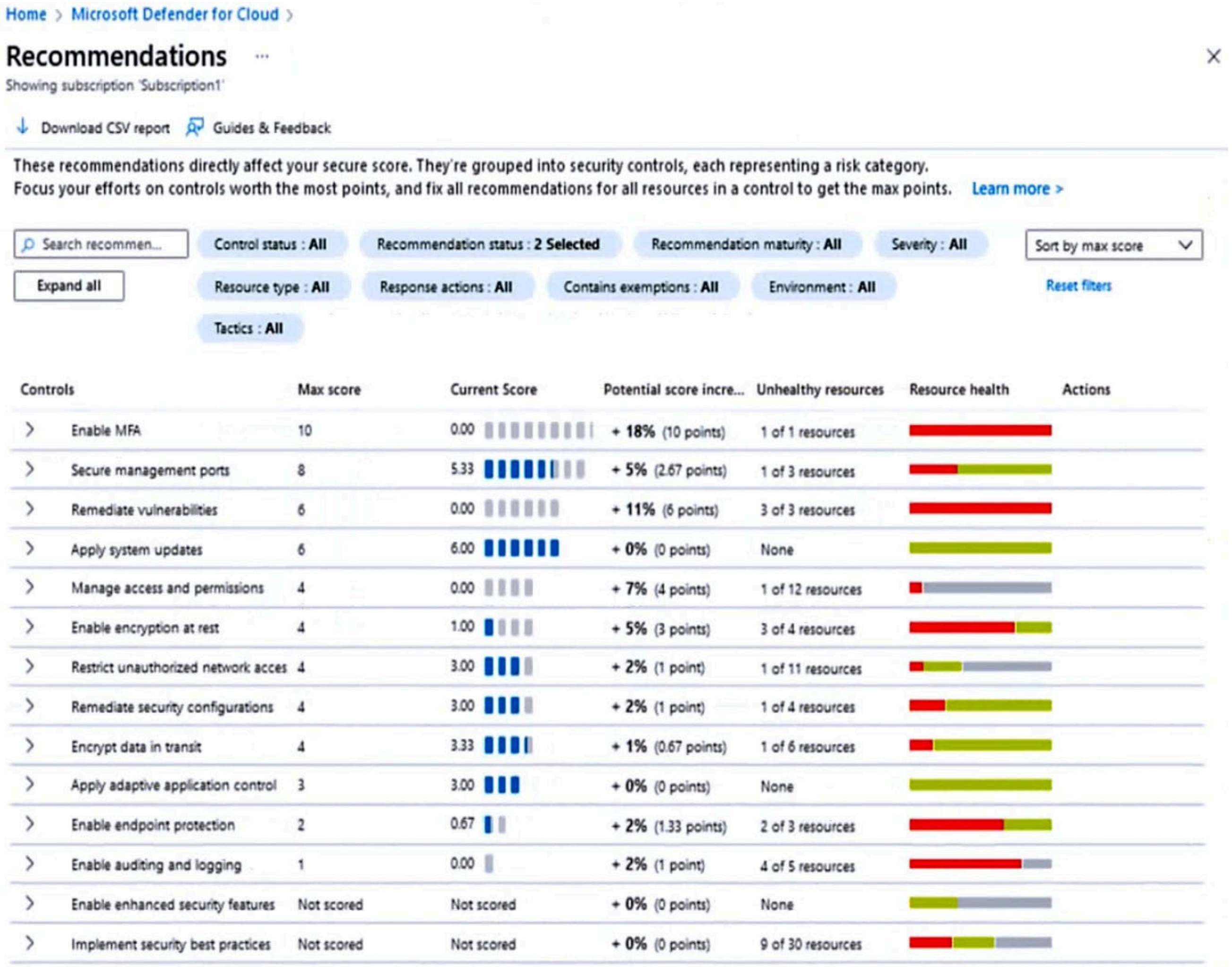
briliant, correct answer

upvoted 5 times

Question #16 *Topic 2*

HOTSPOT -

You open Microsoft Defender for Cloud as shown in the following exhibit.



Home > Microsoft Defender for Cloud >

Recommendations

Showing subscription 'Subscription1'

These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category.
Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points. Learn more >

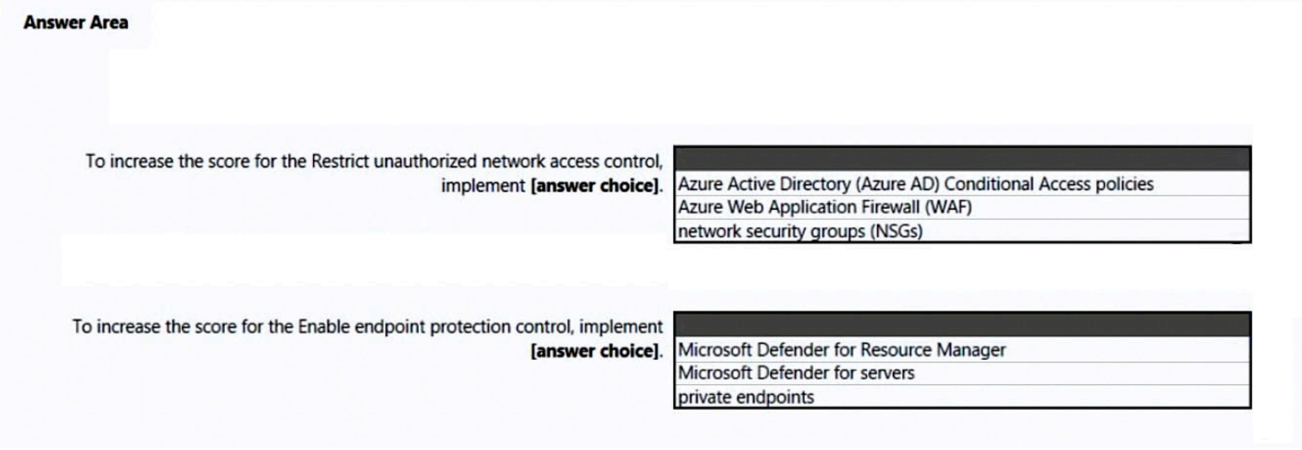
Control status : All | Recommendation status : 2 Selected | Recommendation maturity : All | Severity : All | Resource type : All | Response actions : All | Contains exemptions : All | Environment : All | Tactics : All

Controls	Max score	Current Score	Potential score incre...	Unhealthy resources	Resource health	Actions
Enable MFA	10	0.00	+ 18% (10 points)	1 of 1 resources	🟥	
Secure management ports	8	5.33	+ 5% (2.67 points)	1 of 3 resources	🟥🟩	
Remediate vulnerabilities	6	0.00	+ 11% (6 points)	3 of 3 resources	🟥	
Apply system updates	6	6.00	+ 0% (0 points)	None	🟩	
Manage access and permissions	4	0.00	+ 7% (4 points)	1 of 12 resources	🟥⬜	
Enable encryption at rest	4	1.00	+ 5% (3 points)	3 of 4 resources	🟥🟩	
Restrict unauthorized network acces	4	3.00	+ 2% (1 point)	1 of 11 resources	🟥🟩⬜	
Remediate security configurations	4	3.00	+ 2% (1 point)	1 of 4 resources	🟥🟩	
Encrypt data in transit	4	3.33	+ 1% (0.67 points)	1 of 6 resources	🟥🟩	
Apply adaptive application control	3	3.00	+ 0% (0 points)	None	🟩	
Enable endpoint protection	2	0.67	+ 2% (1.33 points)	2 of 3 resources	🟥🟩	
Enable auditing and logging	1	0.00	+ 2% (1 point)	4 of 5 resources	🟥⬜	
Enable enhanced security features	Not scored	Not scored	+ 0% (0 points)	None	🟩⬜	
Implement security best practices	Not scored	Not scored	+ 0% (0 points)	9 of 30 resources	🟥🟩⬜	

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

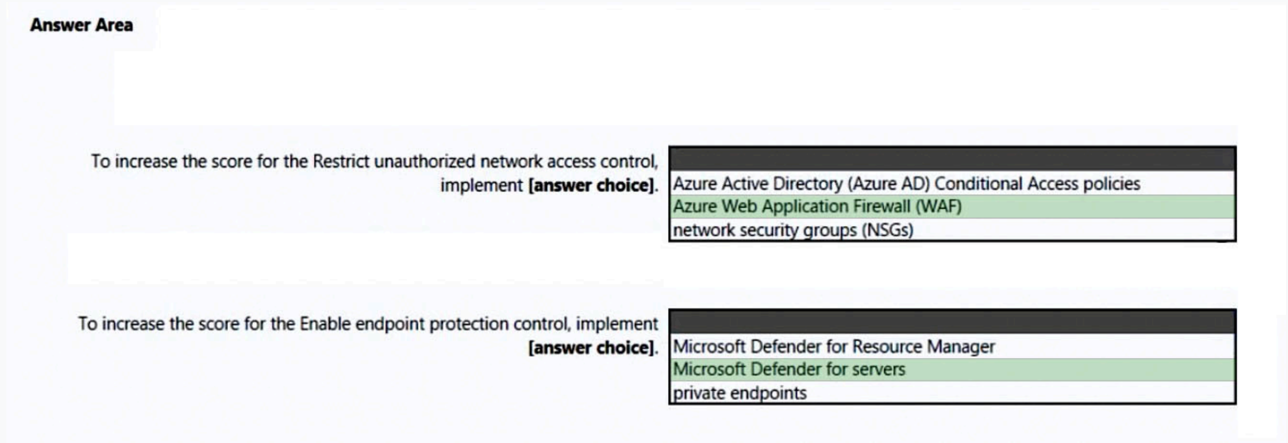
To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

- Azure Active Directory (Azure AD) Conditional Access policies
- Azure Web Application Firewall (WAF)
- network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

- Microsoft Defender for Resource Manager
- Microsoft Defender for servers
- private endpoints

Suggested Answer:



Answer Area

To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

Azure Active Directory (Azure AD) Conditional Access policies
[✓ Azure Web Application Firewall (WAF)]
network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

Microsoft Defender for Resource Manager
[✓ Microsoft Defender for servers]
private endpoints

Box 1: Azure Web Application Firewall (WAF)

Restrict unauthorized network access control: 1 resource out of 11 needs to be addresses.

Restrict unauthorized network access - Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.

Use these recommendations to manage Defender for Cloud's adaptive network hardening settings, ensure you've configured Azure Private Link for all relevant

PaaS services, enable Azure Firewall on your virtual networks, and more.

Note: Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway.

Azure WAF protects inbound traffic to the web workloads, and the Azure Firewall inspects inbound traffic for the other applications. The Azure Firewall will cover outbound flows from both workload types.

Incorrect:

Not network security groups (NSGs).

Box 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft

Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

HardcodedCloud Highly Voted 2 years, 9 months ago

Selection 1: NSG

Selection 2: Microsoft Defender for servers

upvoted 102 times

[Removed] Highly Voted 2 years, 10 months ago

NSGs: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833

upvoted 22 times

junglejoy Most Recent 12 months ago

Selection 1: NSG - https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833

Selection 2: Defender for servers

upvoted 3 times

ayadmawla 1 year, 4 months ago

For those choosing NSG, you should actually look at the options given in the recommendation under Network Security and you will see clearly that it DOES NOT EXIST. The recommendations are for a Firewall, WAF, etc but not NSG which is applicable at the level of a VNET and not a subscription which may or may not have any vnets.

upvoted 2 times

> **Mnguyen0503** 1 year, 2 months ago
>
> Incorrect. WAF is a layer-7 appliance. It doesn't care about network (layer 3), only application protocols (HTTP, HTTPS, etc).
>
> upvoted 1 times

> **wsrudmen** 1 year, 4 months ago
>
> No you're wrong
>
> Expand the menu and you can see:
> Internet-facing virtual machines should be protected with network security groups
> All network ports should be restricted on NSG associated to your VM
> etc.
>
> There's no WAF and CA item in the list...
>
> upvoted 4 times

harimurti20 1 year, 6 months ago

NSG:Unautorised Network access can be prevented by NSG
Microsoft Defender for Server

upvoted 2 times

smanzana 1 year, 8 months ago

Box1: NSG
Box2: Microsoft Defender for servers

upvoted 2 times

slobav 1 year, 9 months ago

Selection 1: NSG
Selection 2: Microsoft Defender for servers
Explanation: Question 85
https://www.youtube.com/watch?v=_DvisTemjGQ&list=PLQ2ktTy9rklhzzkSEZvDZT4QSIVUQZD-Y&index=6

upvoted 2 times

calotta1 1 year, 10 months ago

I'd have selected WAF but i can see it is under "Protect applications against DDoS attacks" recommendations. NSG is the right for 1st box and MDfS is correct.

REF: https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls?branch=main#security-controls-and-their-recommendations

upvoted 3 times

bmulvIT 2 years, 1 month ago

Question in the exam today 19/05/2023

upvoted 7 times

> **JpTheCloudGuy** 1 year, 11 months ago
>
> What were your selections?
>
> upvoted 1 times

> **allinict_111** 1 year, 5 months ago
>
> please if you dont have the right answers do not type anything.
>
> upvoted 1 times
>
> > **poesklap** 1 year, 4 months ago
> >
> > That was not very nice
> >
> > upvoted 4 times

zellck 2 years, 1 month ago

1. NSG
2. Microsoft Defender for servers

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 4 times

Ajdlfasudfo0 2 years, 4 months ago

NSG + MDfS

upvoted 1 times

steve_gatsby 2 years, 4 months ago

WAF is incorrect as it only affects level 7 layer of HTTP protocol

upvoted 4 times

ad77 2 years, 5 months ago

1. nsg - ref. 4, https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls?branch=main#how-your-secure-score-is-calculated

2.. defender for endpoint ref 2. https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls?branch=main#how-your-secure-score-is-calculated

upvoted 2 times

> **ad77** 2 years, 5 months ago
>
> 2.. defender for server
>
> upvoted 1 times

nieprotetkniteeetr 2 years, 5 months ago

NSG https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833

upvoted 3 times

Rocky83 2 years, 5 months ago

NSG and M$ Defender for Servers

upvoted 2 times

Hullstar 2 years, 5 months ago

1 and 2, just checked my live environment and NSG is at the top of the list

upvoted 1 times

> **Hullstar** 2 years, 5 months ago
>
> sorry: 1-NSG, 2:MDS
>
> upvoted 1 times

purek77 2 years, 5 months ago

Quick analysis of https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls tells us that

- Restrict unauthorized network access = Virtual networks should be protected by Azure Firewall

- Enable endpoint protection = Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as [list], [list] shows Defender for Servers and/or Defender for Containers.

Therefore answers are:

- Azure Web Application Firewall (WAF)
- Microsoft Defender for Servers

upvoted 1 times

> **purek77** 2 years, 5 months ago
>
> Well, after rethinking it should be NSG and MDfS
>
> upvoted 1 times

Question #17 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling the VMAccess extension on all virtual machines.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Note:
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution
B (100%)

PlumpyTumbler Highly Voted 1 year, 4 months ago
Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration
upvoted 12 times

[Removed] 1 year, 3 months ago
Adaptive Network Hardening does not increase the score of the Secure management ports controls (as far as I can tell). Use Microsoft Defender for Cloud Adaptive Network Hardening to recommend NSG hardening rules that further limit ports, protocols and source IPs based on threat intelligence and traffic analysis result.
upvoted 2 times

Learing 1 year, 2 months ago
Correct about instructions, but adaptive network hardening is in different category:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
upvoted 1 times

bmulvIT Most Recent 7 months, 1 week ago
Selected Answer: B
Question in the exam today 19/05/2023
upvoted 2 times

zellck 7 months, 2 weeks ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 1 times

ksksilva2022 1 year, 1 month ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 1 times

SAMSH 1 year, 3 months ago

was in 20Sep2020 exam

upvoted 1 times

Jasper666 1 year, 3 months ago

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls, half way under Secure management ports; NSG, JIT, not internet faced. None of those are met so B

upvoted 1 times

djayawar 1 year, 4 months ago

Correct

upvoted 2 times

BillyB2022 1 year, 4 months ago

Selected Answer: B

Correct

upvoted 3 times

Question #18 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling adaptive network hardening.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Note:
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution
B (79%) A (21%)

yf Highly Voted 2 years, 9 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls lists "Adaptive network hardening" for "Restrict unauthorized network access" and not for "Secure management ports"
upvoted 37 times

Jacquesvz 2 years, 5 months ago
Agreed: only 3 controls you can implement for Management Ports =
1.) Internet facing vm's should be protected with NSG's
2.) Management ports should be closed on your vm's
3.) Management ports on VM's should be protected with JIT
Logon to Defender for Cloud and have a look under "General/Recommendations".
upvoted 7 times

PlumpyTumbler Highly Voted 2 years, 10 months ago
Selected Answer: A
Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration
upvoted 10 times

Learing 2 years, 8 months ago

Correct about instructions, but adaptive network hardening is in different category:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 6 times

Jacquesvz 2 years, 5 months ago

100%. Adaptive network hardening is to address "Restrict Unauthorized Network Access", and not management ports.

upvoted 2 times

emartiy Most Recent 1 year ago

Selected Answer: B

To enhance the Secure management ports controls and increase your score, consider the following recommendations:

Enable Just-In-Time (JIT) VM Access:
JIT allows you to open management ports (like RDP and SSH) only when needed, reducing exposure.
When a request is made, JIT dynamically opens the port for a specified time window, then closes it afterward1.
Protect Internet-Facing Virtual Machines with Network Security Groups (NSGs):
Restrict access to VMs by configuring NSGs to allow only necessary traffic.
Avoid exposing VMs directly to the internet unless required (e.g., for specific use cases like development environments)1.
Close Management Ports on Virtual Machines:
Ensure that management ports (such as 3389 for RDP and 22 for SSH) are closed when not actively needed.
Open them only during maintenance or management tasks

upvoted 1 times

Murtuza 1 year, 5 months ago

Selected Answer: B

You recommend enabling just-in-time (JIT) VM access on all virtual machines.

upvoted 1 times

Arjanussie 1 year, 6 months ago

adaptive network hardening is part of Restrict unauthorized network access NOT part of secure management port - just logon in your tenant and you will see

upvoted 1 times

cyber_sa 1 year, 8 months ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 6 times

Ario 1 year, 12 months ago

this is very tricky question , Adaptive network hardening potentially can improve the security but require additional configuration and JIT is one of those , i would vote for B

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 2 times

WRITER00347 2 years, 1 month ago

B. No

Enabling adaptive network hardening in Microsoft Defender for Cloud can help improve the security posture of your network by providing recommendations for network security group (NSG) rules. However, it does not directly impact the score of the Secure management ports controls in the Azure Security Benchmark V3 report.

To increase the score for the Secure management ports controls, you should focus on implementing recommendations specific to securing management ports, such as restricting access to management ports, enabling just-in-time VM access, and using Azure Bastion for secure access to your virtual machines.

upvoted 1 times

Ajdlfasudfo0 2 years, 4 months ago

Selected Answer: B

No, https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

"Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups."

upvoted 1 times

ad77 2 years, 5 months ago

Selected Answer: B

Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.

upvoted 1 times

Hullstar 2 years, 5 months ago

In my live environment it does not list and Adaptive Network Hardening is not there.

upvoted 2 times

TJ001 2 years, 6 months ago

JIT make sense when we talk about management ports I will stick with B

upvoted 2 times

examtopics_100 2 years, 6 months ago

No: Applicable remediations:

Internet-facing virtual machines should be protected with network security groups

- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 4 times

sunilkms 2 years, 6 months ago

Selected Answer: B

The answer is clearly B the ask is to gain the potential 8 points which you will only get by doing the recommendation in the Secure management ports, whereas adaptive network hardening comes under "Restrict unauthorized network access" and potential max point you can gain is 4.

upvoted 3 times

hamshoo 2 years, 7 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

upvoted 1 times

dija123 2 years, 8 months ago

Selected Answer: B

Secure management ports :

- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 2 times

Question #19 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution
A (100%)

PlumpyTumbler Highly Voted 2 years, 10 months ago
Selected Answer: A
Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration
upvoted 12 times

TJ001 2 years, 6 months ago
JIT and NSG make sense under this recommendation category...
upvoted 2 times

JMuller Highly Voted 2 years, 9 months ago
Selected Answer: A
Plumpy is right, there are 2 correct answers in this set. JIT is only ONE of them.
upvoted 5 times

jayek Most Recent 1 year ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#:~:text=To%20get%20all,your%20secure%20score.
upvoted 1 times

cyber_sa 1 year, 8 months ago
Selected Answer: A
got this in exam 6oct23. passed with 896 marks. I answered A
upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 1 times

⊟ **TomHoff** 2 years, 3 months ago

Selected Answer: A

yes, correct

upvoted 1 times

⊟ **steve_gatsby** 2 years, 4 months ago

https://learn.microsoft.com/en-us/azure/governance/policy/samples/gov-azure-security-benchmark#avoid-standing-access-for-accounts-and-permissions

upvoted 1 times

⊟ **[Removed]** 2 years, 6 months ago

There are 3 recommendations, at this link. JIT is one of the 3.

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-secure-management-ports/ba-p/1505770

upvoted 2 times

⊟ **SAMSH** 2 years, 9 months ago

was in 20Sep2020 exam

upvoted 1 times

⊟ **Alex_Burlachenko** 2 years, 10 months ago

yep, correct

upvoted 4 times

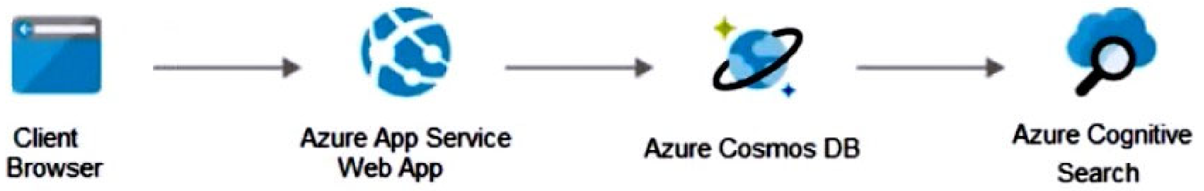
Question #20 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.

You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend creating private endpoints for the web app and the database layer.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS

Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.

They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service

Bus, or Azure Automations.

Reference:

https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

A (86%) 14%

⊟ **HardcodedCloud** Highly Voted 2 years, 3 months ago

Selected Answer: A

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

upvoted 13 times

⊟ **Ajdlfasudfo0** 1 year, 10 months ago

you need vnet integration in order to send traffic from app service to the cosmos db. Please read it up first.

upvoted 2 times

⊟ **JoeMel** Highly Voted 1 year, 12 months ago

"The solution must follow the Zero Trust model."

Isn't Zero Trust requires mutual authentication ?

The solution proposed is based on trusting the internal network which is not Zero-Trust.

upvoted 8 times

gsesh32 Most Recent 9 months, 3 weeks ago

This answer is only correct if the Web App is meant to be internal facing, thus the key question here is why would an 'eCommerce' website be made internal??? Do they intend for only internal stakeholders to access the web-app? If that's not the case then the best option would be B

upvoted 1 times

cris_exam 10 months, 2 weeks ago

The way the recommendation is worded, is awful.
YES, private endpoints (PE) could very well be a good idea, but not implementing PEs to both webapp and DB, but only to the DB and integrating the webapp to the VNET for outbound access - but NOT webapp PE.

Let me explain:
For this design to work well, the webapp should just be integrated with a VNET and then the DB configured with a PE, preferably in the same VNET for good performance and easier setup, then YES, this way would be more secure then leaving them publicly accessible.

But the way the recommendation is worded, lets to understand that both webapp and DB would have private endpoints configured, which would NOT work, as PE only receives traffic, it cannot initiate, hence the webapp would not be able to communicate using it's PE private IP to reach the PE of DB, but the webapp will initiate traffic from the public outbound IPs and this connection will fail because DB PE will not accept a public connection.

upvoted 3 times

cris_exam 10 months, 2 weeks ago

Though, I also don't find the Az Key Vault to be the solution as these questions stream go, the PE implementation would seem the closest best answer, if implemented as explained above.

upvoted 1 times

bxlin 7 months ago

Agreed with your explanation. The question is asking "provide recommendations to secure the connection between the web app and the database". Creating a PE on webapp has nothing to do with that recommendation.

upvoted 1 times

cybrtrk 12 months ago

I think people are getting confused between the old infrastructure and the new.
The question relates to the new infrastructure in Azure, so the solution is WAF.
Private endpoints aren't related to this infrastructure.

upvoted 1 times

cyber_sa 1 year, 2 months ago

Selected Answer: A

got this in exam 6oct23. passed with 896 marks. I answered A

upvoted 3 times

bmulvIT 1 year, 7 months ago

Question in the exam today 19/05/2023

upvoted 4 times

bmulvIT 1 year, 7 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint
"Private endpoint is only used for incoming traffic to your app"
NO

upvoted 3 times

zellck 1 year, 7 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint
You can use private endpoint for your App Service apps to allow clients located in your private network to securely access the app over Azure Private Link. The private endpoint uses an IP address from your Azure virtual network address space. Network traffic between a client on your private network and the app traverses over the virtual network and a Private Link on the Microsoft backbone network, eliminating exposure from the public Internet.

upvoted 3 times

zellck 1 year, 7 months ago

Gotten this in May 2023 exam.

upvoted 5 times

Fal991l 1 year, 9 months ago

Selected Answer: A

ChatGPT: A. Yes, creating private endpoints for the web app and the database layer is a recommended solution to secure the connection between the two layers and meet the Zero Trust model.

Private endpoints allow you to access your Azure PaaS services over a private IP address within your virtual network. By creating private endpoints for both the web app and the MongoDB database, traffic between them can be routed through the private network, making it more secure by preventing access from the public internet.

This approach is recommended because it limits access to only the virtual network where the web app and database are deployed, and it helps to minimize the surface area of potential attacks. By implementing private endpoints, you can ensure that data is transmitted securely between the two layers and reduce the risk of data breaches.

Therefore, creating private endpoints for the web app and the database layer meets the goal of securing the connection between the two layers and follows the Zero Trust model.

upvoted 1 times

Ajdlfasudfo0 1 year, 10 months ago

I think this is incorrect. Private Endpoint would not be the solution here. The App service does need VNet Integration, not private endpoint in order to reach the cosmos DB via its private address. I think a lot of people just shout yes once they hear private endpoint and don't even understand what it is

upvoted 4 times

Azzzurrre 2 years ago

In addition to the private endpoint for the Cosmos DB, the Cosmos DB needs to have its "publicNetworkAccess" flag set to "Disabled" to prevent public network access to the Cosmos DB account when it is created, before its private endpoint is created.
Also,
(Just creating the private endpoint could be considered an incomplete solution.)
https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints#blocking-public-network-access-during-account-creation

upvoted 2 times

GetMonster 2 years, 3 months ago

Selected Answer: A

The answer is correct.

upvoted 3 times

tester18128075 2 years, 3 months ago

Private endpoint is correct. A is the correct answer

upvoted 2 times

prabhjot 2 years, 4 months ago

yes seems correct from NETWORK - zero trust principle point of view

upvoted 3 times

PlumpyTumbler 2 years, 4 months ago

I think this is right. It's always best to use official Microsoft documentation for answers. Other companies and blogs are not the source of truth.
https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints

upvoted 3 times

Alex_Burlachenko 2 years, 4 months ago

YES, correct

upvoted 4 times

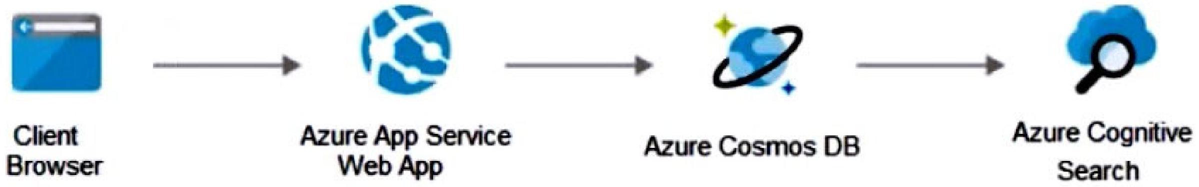
Question #21 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.

You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Key Vault to store credentials.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead use solution: You recommend creating private endpoints for the web app and the database layer.

Note:

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS

Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.

They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service

Bus, or Azure Automations.

Reference:

https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

B (59%) A (41%)

Alex_Burlachenko Highly Voted 2 years, 10 months ago

NO is correct answer

upvoted 19 times

Onimole 10 months, 1 week ago

or even the connection strings

upvoted 1 times

lt9898 1 year, 4 months ago

Agree with this, although having secrets stored in a key vault is a useful recommendation, in isolation it does not achieve the architectural goal stated by the question

upvoted 1 times

[Removed] Highly Voted 2 years, 9 months ago

Selected Answer: A

Landing zones are not only networking. Designing a proper authentication flow is also important, and in zero trust, no credentials should be unattended. Thats why using key vault and managed identities are important thin.gs when designing a zero trust architecture.
My answer is YES

upvoted 18 times

hw121693 1 year, 11 months ago

Even better solution is to use managed identity, so no credentials will be required. Even if you use key vault, you still need to grab the secret using managed identity

upvoted 3 times

MrsSunshine 2 years, 5 months ago

You have ro aecure the connection...For this question, it is networking only...

upvoted 2 times

JakeCallham 2 years, 8 months ago

I agree. Private endpoint is nice but if you use plain connectionsstrings without MI or keyvaults, it's not enough. So I would vote yes on this one. Yes private links are one of them, but using a keyvaults is another one.

upvoted 4 times

mtlpoly 2 years, 7 months ago

If using MI wasn't an option I would have said yes, but since MI is the way to go, then I wouldn't recommend using connection strings with secrets hence using the key vault would not be necessary.

upvoted 2 times

Nickname01 2 years, 7 months ago

agree with this, there should not be a need for a key vault. using secrets would only increase the risk unnecessary and make it more complex then necessary.

upvoted 1 times

AzureJobsTillRetire 2 years, 4 months ago

Not sure why you must have key vault. I think key vault is nice to have in this case. Manged identity may be a better solution.

upvoted 3 times

Avanade2023 2 years ago

You can keep the connection string to Database securely by the Key Vault.

upvoted 1 times

hw121693 1 year, 11 months ago

Using connection string to connect database has nothing to do with "Securing the connection". "Securing connection" means to secure data in transit to database such as using HTTPS connection to DB.

upvoted 2 times

Onimole Most Recent 10 months, 1 week ago

should be able to store certificates for secure connection in kv or am i missing something?

upvoted 1 times

jvallespin 11 months ago

Selected Answer: A

Azure KeyVault is part of a Zero trust strategy securing applications connectivity. Although a managed identity would be a better solution, Key Vault is a valid solution for this purpouse. Node.js for Mongo DB support this type of authentication as well.

https://learn.microsoft.com/en-us/azure/service-connector/how-to-integrate-cosmos-db?tabs=dotnet

upvoted 1 times

Ragdoll 1 year, 2 months ago

Selected Answer: B

This is about secure connectivity. Key Vault is not a networking solution.

upvoted 2 times

PierreTang 1 year, 3 months ago

Selected Answer: B

Do not require Key vault

upvoted 1 times

SFAY 1 year, 4 months ago

Selected Answer: B

The answer is No.

Key Vault is for data security whereas Private Link is for Network Security.

https://learn.microsoft.com/en-us/training/modules/specify-requirements-securing-saas-paas-iaas-services/3-specify-security-requirements-web-workloads

upvoted 3 times

Ramye 1 year, 5 months ago

you need to focus on what is exactly being asked and that is: "to secure the connection between the web app and the database."

So the answer is B - No

upvoted 3 times

Murtuza 1 year, 6 months ago

Selected Answer: B

Managed identity is the best way to secure connection between Azure services in this case cosmos DB and ASE

upvoted 2 times

cyber_sa 1 year, 8 months ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 9 times

ServerBrain 1 year, 10 months ago

B is the correct answer. The question is about securing the connection not about secure access. Key Vault will give you secure access...

upvoted 1 times

imsidrai 2 years ago

key vault also supports the "use least privilege access " principle, so yes

upvoted 1 times

PrettyFlyWifi 2 years, 1 month ago

Selected Answer: A

Considering the general overview of Azure Key Vault states a clear "note" on Zero Trust, I'd assume this answer should be "YES". E.g. Data protection, including key management, supports the "use least privilege access" principle.

https://learn.microsoft.com/en-us/azure/key-vault/general/overview

Got to be YES right??

upvoted 2 times

etblue 2 years, 3 months ago

My suggested answer is B, no.

Question being: Provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model

Zero Trust model guiding principle: Assume breach, Verify explicitly, Use least privilege.

Note that here the main point is about "secure the connection", which tend more towards network controls based "assumed breach prevention" rather than attack on credentials "verify explicitly".

Asking on the opposite side, if we secure the network connectivity between web and DB tier but using credentials that is not stored in Azure vault, does it necessarily raise risks? To a certain extend, if the relevant credentials are kept safe, I would think it does not raise a difference if store in vault or not, more importantly there is a secure network connectivity between the web and DB.

Plus the fact this is a continued series question where "private endpoint" seems to be the most "correct" answer. Hope it explains.

upvoted 6 times

Ram098 2 years, 3 months ago

B CORRECT

upvoted 2 times

Fal991l 2 years, 3 months ago

Selected Answer: A

ChatGPT: A. Yes, implementing Azure Key Vault to store credentials is a recommended solution to secure the connection between the web app and the MongoDB database, and it meets the goal of following the Zero Trust model.

upvoted 2 times

awssecuritynewbie 2 years, 4 months ago

Selected Answer: B

It asks for "secure connection" which is not the same thing as storing the key securely! so it would be B

upvoted 3 times

Aunehwet79 2 years, 4 months ago

Agree with you

upvoted 2 times

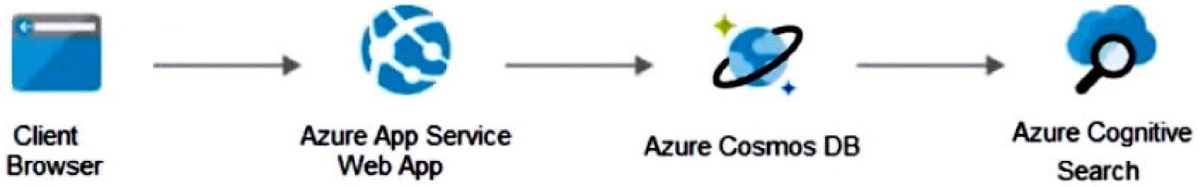
Question #22 Topic 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.

You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead use solution: You recommend creating private endpoints for the web app and the database layer.

Note:

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS

Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.

They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service

Bus, or Azure Automations.

Reference:

https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

B (64%) A (36%)

HardcodedCloud Highly Voted 2 years, 9 months ago

Selected Answer: B

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

upvoted 7 times

Alex_Burlachenko Highly Voted 2 years, 10 months ago

correct answer

upvoted 5 times

whh13 Most Recent 6 months, 3 weeks ago

Selected Answer: B

WAF is for external protection, not for backend comm with DB.

upvoted 2 times

SFAY 1 year, 4 months ago

Selected Answer: A

The answer is YES.

In the explicit guidance provided by Microsoft, deploying WAF is a Network Security control for securing web workloads. Also, WAF is a feature of Web Application Gateway.

Source: https://learn.microsoft.com/en-us/training/modules/specify-requirements-securing-saas-paas-iaas-services/3-specify-security-requirements-web-workloads

upvoted 2 times

> **SFAY** 1 year, 4 months ago
>
> Correction: Although the above statement is true, however the question is about securing connection BETWEEN the web app and the database and for that a private endpoint is the right solution. WAF only protects the web app.
> Therefore, the correct answer is 'No'
>
> upvoted 1 times

Murtuza 1 year, 5 months ago

This is a tricky question MS threw the word client connection to confuse us in picking the WAF component and App Gateway which is irrelevant here

upvoted 2 times

Victory007 1 year, 10 months ago

Selected Answer: A

Yes, implementing Azure Application Gateway with Azure Web Application Firewall (WAF) can help meet the goal of securing the connection between the web app and the database following the Zero Trust model. Azure Application Gateway is a load balancer that provides application-level routing and load balancing services. It can be configured with the optional addition of Azure Web Application Firewall (WAF), which provides inspection of HTTP requests and prevents malicious attacks at the web layer, such as SQL Injection or Cross-Site Scripting. https://learn.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway

upvoted 2 times

> **devop23** 2 months, 4 weeks ago
>
> can you people stop with the AI garbage and actually try to think the question?
>
> upvoted 1 times

tester18128075 2 years, 9 months ago

Answer is no, App gateway does not provide connectivity between webapp and cosmos DB

upvoted 2 times

> **ServerBrain** 1 year, 10 months ago
>
> Correct. WAF will give you connectivity between the client and the App.
>
> upvoted 1 times

Question #23 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure Security Benchmark compliance controls in Defender for Cloud

Suggested Answer: *A*
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
Incorrect:
Not B: App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.
Not C: Cloud Discovery anomaly detection policy reference. A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are considered for each cloud application.
Not D: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy
https://docs.microsoft.com/en-us/security/benchmark/azure/overview

Community vote distribution

A (96%) 4%

⊟ **PlumpyTumbler** Highly Voted 1 year, 10 months ago

Selected Answer: A

This question is on here twice. Each time it's asked the same way but the answer options are different so look out. In this case A is correct.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute-recommendations

upvoted 14 times

⊟ **cybrtrk** Most Recent 7 months, 1 week ago

Adaptive application controls don't block.
What am I missing here?

upvoted 3 times

⊟ **Intrudire** 7 months, 3 weeks ago

Selected Answer: A

Answer does not meet the requirements, but it seems to be the closest answer.

"If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application."

"No enforcement options are currently available. Adaptive application controls are intended to provide security alerts if any application runs other

than the ones you've defined as safe."
https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

upvoted 3 times

imsidrai 1 year ago

C is the correct answer
https://learn.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-policies

upvoted 2 times

imsidrai 1 year ago

No enforcement options are currently available. Adaptive application controls are intended to provide security alerts if any application runs other than the ones you've defined as safe.

upvoted 1 times

imsidrai 1 year ago

adaptive control wont block/deny , it would only suggest/recommend, so NO for adaptive controls

upvoted 2 times

imsidrai 1 year ago

Please disregard my comments above, The correct answer is B , Microsoft Endpoint manager which is now Intune Admin center has capability to block unauthorized applications and block all other executables, Adaptive control policies would only notify you.

upvoted 2 times

Intrudire 7 months, 3 weeks ago

Intune doesnt seem to support Server.
https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers

upvoted 1 times

zellck 1 year, 1 month ago

Same as Question 19.
https://www.examtopics.com/discussions/microsoft/view/94349-exam-sc-100-topic-4-question-19-discussion

upvoted 1 times

zellck 1 year, 1 month ago

Selected Answer: A

C is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the following instructions.

When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.

upvoted 1 times

vitodobra 1 year, 3 months ago

Selected Answer: B

La respuesta correcta es B. Debe recomendar políticas de protección de aplicaciones en Microsoft Endpoint Manager. Esta solución permite configurar y administrar las políticas de protección de aplicaciones en todas las máquinas virtuales de forma centralizada. Las políticas de protección de aplicaciones permiten controlar qué aplicaciones pueden ejecutarse o instalarse en las máquinas virtuales. Si una aplicación no autorizada intenta ejecutarse o instalarse, la aplicación se bloqueará automáticamente hasta que un administrador autorice la aplicación. Las políticas de protección de aplicaciones se pueden configurar para permitir aplicaciones específicas, bloquear aplicaciones específicas o permitir que los usuarios finales soliciten la instalación de aplicaciones no autorizadas.

upvoted 2 times

TJ001 1 year, 6 months ago

Perfect A

upvoted 1 times

Sec_Arch_Chn 1 year, 7 months ago

Selected Answer: A

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machine
Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

upvoted 3 times

Janusguru 1 year, 8 months ago

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

upvoted 1 times

SAMSH 1 year, 9 months ago

Correct answer. was in 20Sep2020 exam

upvoted 1 times

Jasper666 1 year, 9 months ago

https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls and the feature that does this is "Identify software that's banned by your organization but is nevertheless running on your machines"

upvoted 1 times

tester18128075 1 year, 9 months ago

A is the correct answer

upvoted 1 times

Granwizzard 1 year, 9 months ago

Selected Answer: A

The correct answer is A because you don't have any other option that will block applications from running.
But accordingly, with the latest info, the option to enforce adaptive applications is not available, so it will only alert.https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls#are-there-any-options-to-enforce-the-application-controls

The question is mentioning to block the application from running, and the adaptive application controls don't have this capability available, so the answer shouldn't be correct.

upvoted 3 times

Janusguru 1 year, 8 months ago

Adaptive application controls are intended to provide security alerts if any application runs other than the ones you've defined as safe. It does not block or enforce.

upvoted 3 times

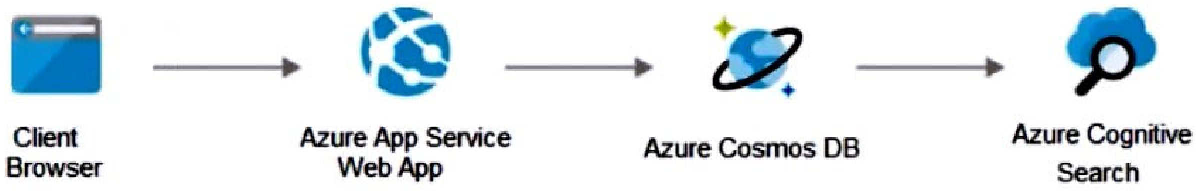
Alex_Burlachenko 1 year, 10 months ago

A. adaptive application controls - correct

upvoted 4 times

Question #24 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

B (92%) 8%

⊟ **neoalienson** Highly Voted 1 year ago

Selected Answer: B

The solution of implementing Azure Front Door with Azure Web Application Firewall (WAF) focuses on securing the web app against external threats and distributed denial-of-service (DDoS) attacks. While this is a valid security measure for protecting your web app, it does not directly address securing the connection between the web app and the database.

upvoted 7 times

⊟ **Learing** Highly Voted 1 year, 8 months ago

Selected Answer: B

Could make sense before web app but nut before DB

upvoted 6 times

Victory007 Most Recent 10 months, 4 weeks ago

Selected Answer: A

Yes, implementing Azure Front Door with Azure Web Application Firewall (WAF) can help meet the goal of securing the connection between the web app and the database following the Zero Trust model. Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely available web applications. With the integration of Azure Web Application Firewall (WAF), Azure Front Door can provide centralized protection for your web applications against common exploits and vulnerabilities.

upvoted 1 times

tester18128075 1 year, 9 months ago

correct

upvoted 2 times

Alex_Burlachenko 1 year, 10 months ago

correct

upvoted 6 times

Question #25 *Topic 2*

You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules.
What should you include in the solution?

A. Microsoft Defender for Endpoint

B. Microsoft Endpoint Manager

C. Microsoft Information Protection

D. Microsoft Sentinel

Suggested Answer: *B*
Microsoft Endpoint Manager includes Microsoft Intune.
Device compliance policies are a key feature when using Intune to protect your organization's resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version.
Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint
Manager includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.
Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co- management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk.
Note: Microsoft Defender for Endpoint Plan 2 protects your Windows and Linux machines whether they're hosted in Azure, hybrid clouds (on-premises), or multicloud.
Microsoft Defender for Endpoint on iOS offers protection against phishing and unsafe network connections from websites, emails, and apps.
Microsoft Defender for Endpoint on Android supports installation on both modes of enrolled devices - the legacy Device Administrator and Android Enterprise modes. Currently, Personally-owned devices with work profile and Corporate-owned fully managed user device enrollments are supported in Android Enterprise.
Reference:
https://docs.microsoft.com/en-us/mem/endpoint-manager-overview https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint

Community vote distribution

B (100%)

PlumpyTumbler Highly Voted 2 years, 4 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

upvoted 11 times

Itu2022 Highly Voted 1 year, 6 months ago

was on exam 15/06/23

upvoted 6 times

halrajeh Most Recent 1 month, 3 weeks ago

Selected Answer: B

Intune

upvoted 1 times

billo79152718 6 months, 3 weeks ago

Outdated. Microsoft Intune instead.

upvoted 5 times

TomHoff 1 year, 9 months ago

Selected Answer: B

yes, Intune MEM

upvoted 2 times

⊟ **AJ2021** 1 year, 9 months ago

Selected Answer: B

Correct

upvoted 1 times

⊟ **Azzzurrre** 2 years ago

Intune supports the listed device OS -- thus Endpoint Manager.

It's important to note that the explanation given is outdated. Microsoft Defender for Endpoint is not part of Microsoft Endpoint Manager, but integrating Defender for Endpoint with Intune allows Intune (and thus Endpoint Manager) to be the best answer.

upvoted 3 times

⊟ **Sec_Arch_Chn** 2 years, 1 month ago

Correct answer. Covers all of the below running devices

Android device administrator

Android (AOSP) (preview)

Android Enterprise

iOS/iPadOS

Linux - Ubuntu Desktop, version 20.04 LTS and 22.04 LTS

macOS

Windows 10 and later

Source: https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

upvoted 2 times

⊟ **SAMSH** 2 years, 3 months ago

Correct answer. was in 20Sep2020 exam

upvoted 2 times

⊟ **CaracasCCS1** 2 years, 3 months ago

Selected Answer: B

B... you need to create a compliance policy and check MDM devices with it.

upvoted 3 times

⊟ **prabhjot** 2 years, 4 months ago

Yes correct ans

upvoted 3 times

⊟ **Alex_Burlachenko** 2 years, 4 months ago

Selected Answer: B

correct answer

upvoted 3 times

Question #26 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Note: Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in- time VM access and network security groups.

Recommendations:

- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution

B (100%)

Alex_Burlachenko Highly Voted 1 year, 4 months ago

Selected Answer: B

100% correct

upvoted 6 times

pdnb Most Recent 6 months, 2 weeks ago

Selected Answer: B

defender detect/respond but not remediate ,open still will be opened. So it doesn't change anything - but if you tweek firewall rules... :)

upvoted 1 times

zellck 7 months, 2 weeks ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 2 times

tester18128075 1 year, 3 months ago

answer is correct

upvoted 1 times

Question #27 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

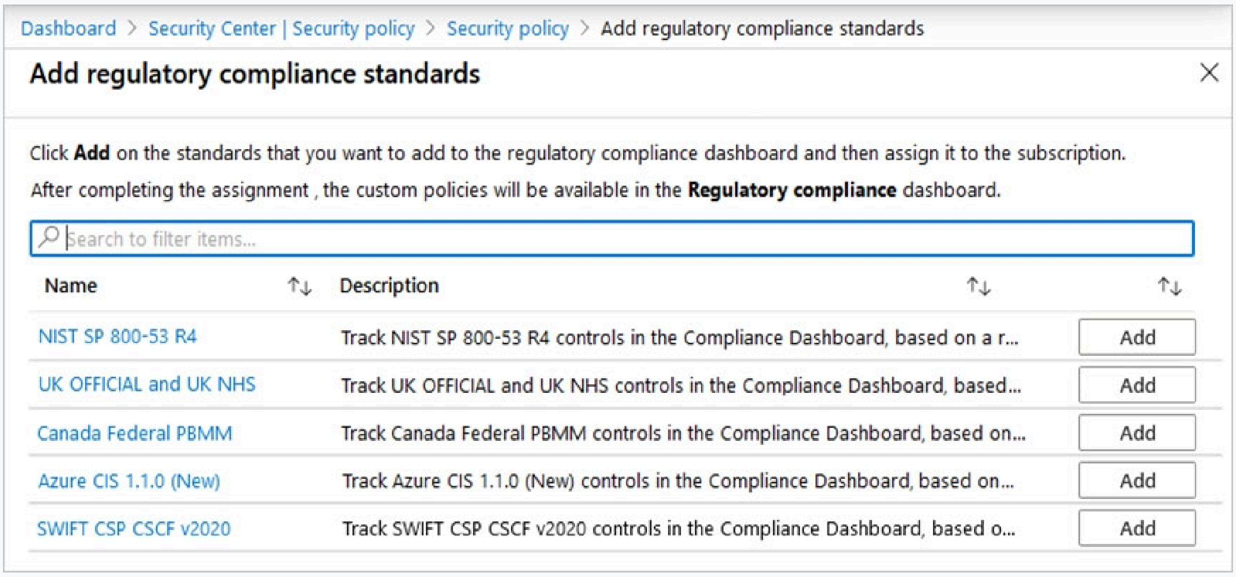
A. From Defender for Cloud, review the secure score recommendations.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Defender for Cloud, add a regulatory compliance standard.

Suggested Answer: *D*
Add a regulatory standard to your dashboard
The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.
Add a standard to your Azure resources
1. From Defender for Cloud's menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.
2. From the top of the page, select Manage compliance policies. The Policy Management page appears.
3. Select the subscription or management group for which you want to manage the regulatory compliance posture.
4. To add the standards relevant to your organization, expand the Industry & regulatory standards section and select Add more standards.
5. From the Add regulatory compliance standards page, you can search for any of the available standards:



Dashboard > Security Center | Security policy > Security policy > Add regulatory compliance standards

Add regulatory compliance standards

Click **Add** on the standards that you want to add to the regulatory compliance dashboard and then assign it to the subscription.
After completing the assignment , the custom policies will be available in the **Regulatory compliance** dashboard.

Search to filter items...

Name	Description	
NIST SP 800-53 R4	Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a r...	Add
UK OFFICIAL and UK NHS	Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based...	Add
Canada Federal PBMM	Track Canada Federal PBMM controls in the Compliance Dashboard, based on...	Add
Azure CIS 1.1.0 (New)	Track Azure CIS 1.1.0 (New) controls in the Compliance Dashboard, based on...	Add
SWIFT CSP CSCF v2020	Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based o...	Add

6. Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.
7. From Defender for Cloud's menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.
Your new standard appears in your list of Industry & regulatory standards.
Note: Customize the set of standards in your regulatory compliance dashboard.
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

Community vote distribution

D (100%)

⊟ **PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-are-available-in-defender-for-cloud

upvoted 14 times

zellck Most Recent 7 months, 2 weeks ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.

upvoted 1 times

awssecuritynewbie 10 months, 4 weeks ago

Selected Answer: D

The question asks to view .. but NIST is not added by default though... but i guess it is the best option between the given answers.

upvoted 1 times

Mo22 10 months, 4 weeks ago

Selected Answer: D

D. From Defender for Cloud, add a regulatory compliance standard.

The first step in reviewing the Azure subscription for NIST 800-53 compliance is to add the NIST 800-53 regulatory compliance standard in Defender for Cloud. This will allow you to see if your subscription meets the requirements for the NIST 800-53 standard. After adding the standard, you can review the compliance status and take appropriate actions to address any issues found.

upvoted 2 times

tester18128075 1 year, 3 months ago

D is correct

upvoted 2 times

prabhjot 1 year, 4 months ago

this is correct and (add a regulatory compliance standard from MS defender for cloud)

upvoted 3 times

Alex_Burlachenko 1 year, 4 months ago

actually exist the same question v.2.0 and answer there would be "From Defender for Cloud, enable Defender for Cloud plans." but that one is correct

upvoted 2 times

Question #28 *Topic 2*

Your company has devices that run either Windows 10, Windows 11, or Windows Server.
You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune

B. Local Group Policy Object (LGPO)

C. Windows Autopilot

D. Policy Analyzer

Suggested Answer: *D*
Microsoft Security Compliance Toolkit 1.0, Policy Analyzer.
The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:
Highlight when a set of Group Policies has redundant settings or internal inconsistencies.
Highlight the differences between versions or sets of Group Policies.
Compare GPOs against current local policy and local registry settings
Export results to a Microsoft Excel spreadsheet
Policy Analyzer lets you treat a set of GPOs as a single unit. This treatment makes it easy to determine whether particular settings are duplicated across the
GPOs or are set to conflicting values. Policy Analyzer also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.
Note: The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft- recommended security configuration baselines for Windows and other Microsoft products.
The SCT enables administrators to effectively manage their enterprise's Group Policy Objects (GPOs). Using the toolkit, administrators can compare their current
GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active
Directory or individually through local policy.
Security Compliance Toolkit Tools:

Policy Analyzer -
Local Group Policy Object (LGPO)

Set Object Security -

GPO to Policy Rules -
Incorrect:
Not B: Local Group Policy Object (LGPO)
What is the Local Group Policy Object (LGPO) tool?
LGPO.exe is a command-line utility that is designed to help automate management of Local Group Policy. Using local policy gives administrators a simple way to verify the effects of Group Policy settings, and is also useful for managing non-domain-joined systems.
LGPO.exe can import and apply settings from Registry
Policy (Registry.pol) files, security templates, Advanced Auditing backup files, as well as from formatted ג€LGPO textג€ files. It can export local policy to a GPO backup. It can export the contents of a Registry Policy file to the ג€LGPO textג€ format that can then be edited, and can build a Registry Policy file from an LGPO text file.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

Community vote distribution

D (100%)

⊟ **PlumpyTumbler** Highly Voted 1 year, 10 months ago

Selected Answer: D

Link referenced is good. Same one I used to study. D is correct.

upvoted 11 times

WRITER00347 Most Recent 11 months ago

The Microsoft Security Compliance Toolkit provides security baselines and allows you to view recommended and current system configurations. When it comes to comparing these baselines to the current device configurations, Policy Analyzer is the appropriate tool.

Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). It can identify whether current policies are compliant with the desired baselines, making it suitable for this task.

So the correct answer is:

D. Policy Analyzer

upvoted 4 times

Itu2022 1 year ago

was on exam 15/06/23

upvoted 1 times

zellck 1 year, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10#what-is-the-policy-analyzer-tool
The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:
- Compare GPOs against current local policy and local registry settings

upvoted 1 times

zellck 1 year, 1 month ago

Gotten this in May 2023 exam.

upvoted 1 times

Mo22 1 year, 4 months ago

Both the Local Group Policy Object (LGPO) tool and the Policy Analyzer tool support Windows 10, Windows 11, and Windows Server.

The LGPO tool is a Microsoft-supported command line tool that provides the ability to manage local group policies on Windows devices, including Windows 10, Windows 11, and Windows Server.

The Policy Analyzer tool is a Microsoft-supported graphical tool that provides the ability to compare and analyze different versions of Group Policy Objects (GPOs), including GPOs on Windows 10, Windows 11, and Windows Server.

upvoted 1 times

cast0r 1 year, 7 months ago

Selected Answer: D

Given answer is correct, also Intune does not support Server OS

upvoted 2 times

tester18128075 1 year, 9 months ago

Policy Analyser is correct

upvoted 1 times

HardcodedCloud 1 year, 9 months ago

Selected Answer: D

D is correct

upvoted 3 times

prabhjot 1 year, 10 months ago

the SCT also includes the Policy Analyzer and Local
Group Policy Object (LGPO) tools, which also help you manage your GPO settings (ANS is Policy analyzer)

upvoted 4 times

Alex_Burlachenko 1 year, 10 months ago

right, correct

upvoted 4 times

Question #29 *Topic 2*

You have an Azure subscription that is used as an Azure landing zone for an application.

You need to evaluate the security posture of all the workloads in the landing zone.

What should you do first?

A. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.

B. Obtain Azure AD Premium Plan 2 licenses.

C. Add Microsoft Sentinel data connectors.

D. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.

Suggested Answer: *D*

Community vote distribution

D (100%)

hanyahmed Highly Voted 11 months, 2 weeks ago

Selected Answer: D

security posture = MS Defender for Cloud

D is right answer

upvoted 15 times

zellck Highly Voted 7 months, 2 weeks ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction#improve-your-security-posture
The security of your cloud and on-premises resources depends on proper configuration and deployment. Defender for Cloud recommendations identify the steps that you can take to secure your environment.

Defender for Cloud includes Foundational CSPM capabilities for free. You can also enable advanced CSPM capabilities by enabling paid Defender plans.

upvoted 6 times

Pmonty4 Most Recent 3 months, 3 weeks ago

Selected Answer: D

Rixing man can.

upvoted 1 times

Ajdlfasudfo0 10 months, 1 week ago

Selected Answer: D

understand the current posture of the system. MDfC is correct

upvoted 2 times

killaK 11 months ago

Selected Answer: D

I dont like the wording. 'posture' is always related to recommendations (CSPM) which come free out of the box and dont require enabling any of the paid defender for cloud plans (CWPP), alerts.

upvoted 2 times

kiko90909 11 months, 2 weeks ago

i think this one is correct one Add Microsoft Sentinel data connectors

correct answer is A

upvoted 1 times

maku067 11 months, 2 weeks ago

"Add Microsoft Sentinel data connectors" is C but why? Could you explain?

upvoted 1 times

⊟ **purek77** 11 months, 3 weeks ago

Selected Answer: D

I guess D is the correct answer following below:
https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone

upvoted 4 times

Question #30 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Suggested Answer: *A*

Community vote distribution

A (69%) B (31%)

smosmo Highly Voted 1 year, 11 months ago

Selected Answer: A

Correct Answer

upvoted 6 times

Azerty1313 Most Recent 1 year ago

As enhanced security is already activated, the FIRST thing to do is C in my opinion.

upvoted 2 times

Ario 1 year, 6 months ago

Selected Answer: B

Azure Policy provides a centralized service for creating, assigning, and managing policies across Azure subscriptions. By assigning a built-in policy definition that aligns with NIST 800-53 compliance, you can evaluate the current state of the subscription against the required controls and identify any non-compliant resources

upvoted 4 times

epomatti 10 months, 2 weeks ago

Wrong answer. NIST is a collection of rules that is delivered as a policy initiative.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 3 times

zellck 1 year, 7 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 2 times

AzureJobsTillRetire 1 year, 10 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 2 times

Question #31 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **zellck** Highly Voted 👍 7 months, 2 weeks ago

Same as Question 30.

https://www.examtopics.com/discussions/microsoft/view/94937-exam-sc-100-topic-2-question-30-discussion

upvoted 5 times

⊟ **zellck** Most Recent ⊙ 7 months, 2 weeks ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 3 times

⊟ **03allen** 11 months, 1 week ago

I think this question appears 4 times so far in this dump.

upvoted 4 times

⊟ **airairo** 10 months, 2 weeks ago

for 3rd time. 2 are same. one in a different way.

upvoted 1 times

⊟ **fiol82** 11 months, 2 weeks ago

looks correct to me!

upvoted 2 times

⊟ **smosmo** 11 months, 2 weeks ago

I think it is D because you do not need to enable all the Cloud plans to review compliance (not 100% sure)

upvoted 2 times

⊟ **nieprotetkniteeetr** 11 months, 2 weeks ago

D Correct. https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 2 times

⊟ **maku067** 11 months, 3 weeks ago

Is it correct?

upvoted 1 times

Question #32 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Defender for Cloud, add a regulatory compliance standard.

Suggested Answer: *D*

Community vote distribution

D (75%) C (25%)

Ario 12 months ago

Selected Answer: C

FIRST STEP

upvoted 2 times

ServerBrain 10 months, 2 weeks ago

No, don't think like that, else you will think first step is to login to the portal

upvoted 6 times

zellck 1 year, 1 month ago

Same as Question 27.

https://www.examtopics.com/discussions/microsoft/view/78456-exam-sc-100-topic-2-question-27-discussion

upvoted 1 times

zellck 1 year, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.

upvoted 3 times

OrangeSG 1 year, 5 months ago

Selected Answer: D

Duplicate with question 27

upvoted 3 times

fiol82 1 year, 5 months ago

Selected Answer: D

D is correct according to me!

upvoted 1 times

maku067 1 year, 5 months ago

C or D?

upvoted 1 times

Question #32 *Topic 2*

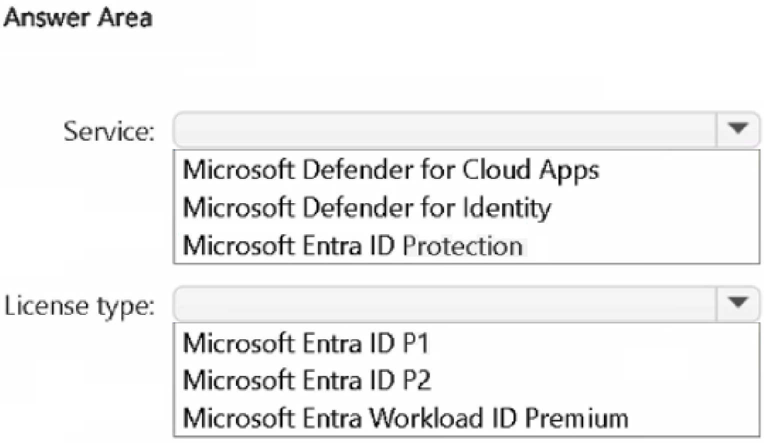
HOTSPOT -

You have a Microsoft Entra tenant that is linked to a Microsoft 365 subscription and an Azure subscription. The tenant contains service principals that are used to access applications in the Azure subscription.

You need to recommend a solution to detect risky sign-ins and other risky activities performed by the service principals in the tenant. The solution must minimize costs.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

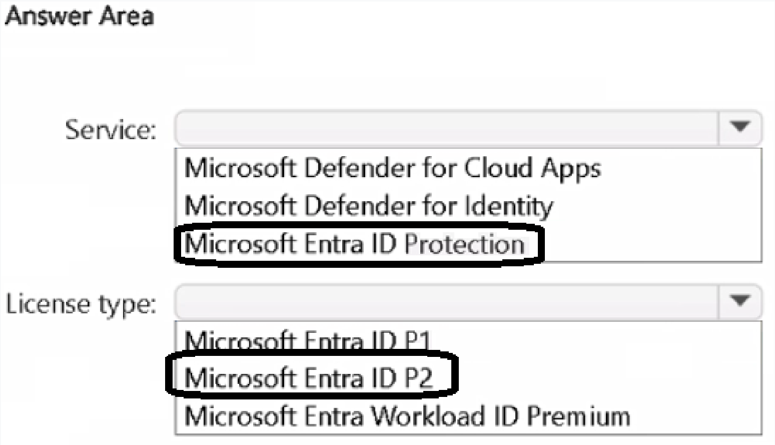


Answer Area

Service:
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Entra ID Protection

License type:
- Microsoft Entra ID P1
- Microsoft Entra ID P2
- Microsoft Entra Workload ID Premium

Suggested Answer:



Answer Area

Service:
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- [✓ Microsoft Entra ID Protection]

License type:
- Microsoft Entra ID P1
- [✓ Microsoft Entra ID P2]
- Microsoft Entra Workload ID Premium

cl1984 3 months, 1 week ago

Listed answers are correct - https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-risk-based-sspr-mfa

upvoted 1 times

676ae1a 5 months ago

Respuesta correcta

upvoted 1 times

Question #33 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Defender for Cloud, review the Azure security baseline for audit report.

C. From Defender for Cloud, add a regulatory compliance standard.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Suggested Answer: *C*

Community vote distribution

C (100%)

shahmitu 7 months, 4 weeks ago

Sorry, I meant A should be the answer

upvoted 1 times

shahmitu 7 months, 4 weeks ago

Adding a regulatory compliance needs to enable one of the paid defender plans at least . So, first step should be C. Answer =C

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: C

Adding a regulatory compliance standard allows you to assess the current state of the Azure subscription against specific compliance frameworks, such as NIST 800-53. This step enables you to evaluate the compliance posture and identify any gaps or areas that require attention to meet the compliance requirements.

upvoted 2 times

zellck 2 years, 1 month ago

Same as Question 27.

https://www.examtopics.com/discussions/microsoft/view/78456-exam-sc-100-topic-2-question-27-discussion

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.

upvoted 1 times

Ajdlfasudfo0 2 years, 4 months ago

Selected Answer: C

correct

upvoted 4 times

Question #33 *Topic 2*

HOTSPOT -

Your network contains an Active Directory Domain Services (AD DS) domain named Domain1.

You have a Microsoft Entra tenant.

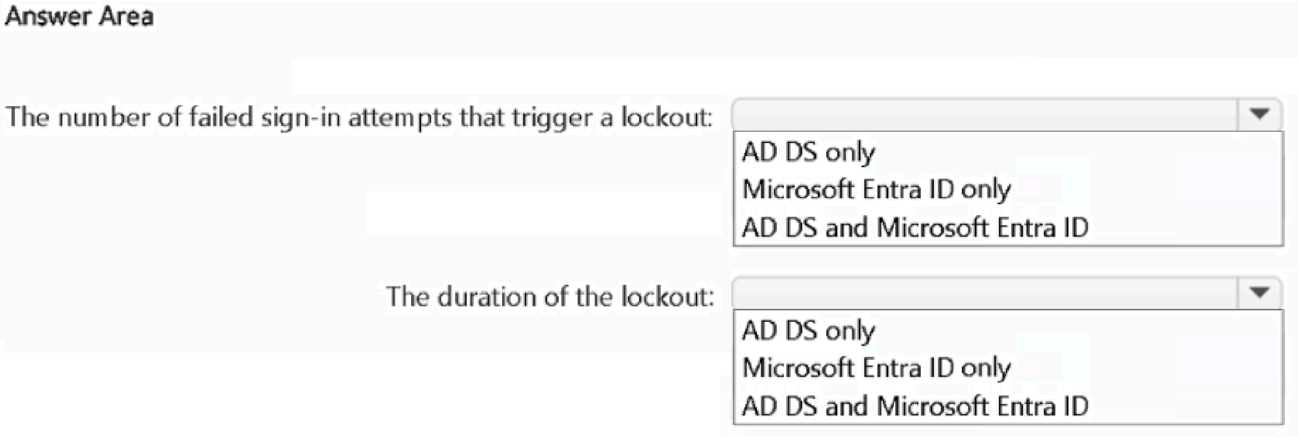
Domain1 syncs with the tenant by using Microsoft Entra Connect.

You need to evaluate Microsoft Entra smart lockout by testing the following account lockout considerations:

- The number of failed sign-in attempts that trigger a lockout
- The duration of the lockout

What should you use to test each consideration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

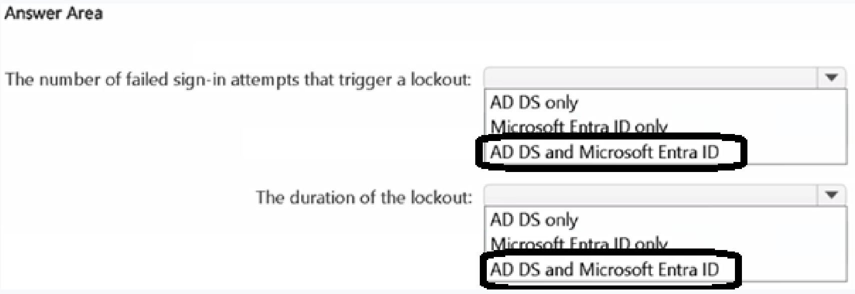


Answer Area

The number of failed sign-in attempts that trigger a lockout:
- AD DS only
- Microsoft Entra ID only
- AD DS and Microsoft Entra ID

The duration of the lockout:
- AD DS only
- Microsoft Entra ID only
- AD DS and Microsoft Entra ID

Suggested Answer:



Answer Area

The number of failed sign-in attempts that trigger a lockout:
- AD DS only
- Microsoft Entra ID only
- [✓ AD DS and Microsoft Entra ID]

The duration of the lockout:
- AD DS only
- Microsoft Entra ID only
- [✓ AD DS and Microsoft Entra ID]

RoboCock 2 months, 3 weeks ago

doesn't make sense to "test" against adds, smart lockout is entra feature. also auth is not mentioned, hybrid integration of smart lockout requires PTA or ADFS.

upvoted 1 times

424ede1 3 months ago

It's about Smart Lockout. Both are available on Entra ID only

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values

upvoted 2 times

jim85 4 months, 4 weeks ago

a) should be Entra ID only, the attempts happen there, as per https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout

upvoted 3 times

manognavenkat 4 months, 2 weeks ago

I agree too https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-troubleshoot-sign-in-errors

upvoted 1 times

⊟ **jim85** 4 months, 3 weeks ago

sorry, typo, b) should be Entra ID only, a) is ok

upvoted 2 times

⊟ **6c9ce39** 1 month, 2 weeks ago

The number of failed sign-in attempts that trigger a lockout: Microsoft Entra ID only

The duration of the lockout: Microsoft Entra ID only

upvoted 1 times

Question #34 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

C. From Defender for Cloud, review the secure score recommendations.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Suggested Answer: *B*

Community vote distribution

B (100%)

zellck 7 months, 2 weeks ago

Same as Question 30.

https://www.examtopics.com/discussions/microsoft/view/94937-exam-sc-100-topic-2-question-30-discussion

upvoted 1 times

zellck 7 months, 2 weeks ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 1 times

awssecuritynewbie 10 months, 2 weeks ago

Correct answer is selected

upvoted 2 times

Question #34 *Topic 2*

You have a Microsoft 365 subscription that contains 1,000 Microsoft Exchange Online mailboxes.

Incoming email from the internet is scanned for security threats by using a third-party cloud service.

You are evaluating whether to replace the third-party service with Microsoft Defender for Office 365.

What should you modify to ensure that all the incoming email is scanned by Defender for Office 365 only?

A. the accepted domains in Exchange Online

B. the DNS records

C. the Exchange Online transport rule

D. the Exchange Online connectors

Suggested Answer: *D*

Community vote distribution

B (100%)

SnowmanPapi 1 month, 2 weeks ago

Selected Answer: B

Definitely the DNS records. You would need to change the MX Records to make sure they point to Microsoft. i.e. - "0 <your domain>.mail.protection.outlook.com". The Exchange Online connectors would only reroute the email to Microsoft if you configure it that way but if the MX records are still pointing to the 3rd party filtering tool's domain (for example Proofpoint). the emails are still going to the 3rd party's filtering tool and not to Microsoft directly.

upvoted 1 times

RoboCock 2 months, 3 weeks ago

Selected Answer: B

To ensure that all incoming email is scanned exclusively by Microsoft Defender for Office 365, you need to modify the DNS records. Specifically, you should update the MX (Mail Exchange) records to point to Microsoft Defender for Office 365 instead of the third-party cloud service. This change will route all incoming email through Defender for Office 365 for scanning and protection.

upvoted 1 times

Saynot 3 months, 1 week ago

Selected Answer: B

Scan by Defender for Office ONLY, if i modify the connectors i cant guarantee that is scanned ONLY from Microsoft message can go thorugh other before. I must change DNS record (MX)

upvoted 1 times

skz94 3 months, 1 week ago

Selected Answer: D

the Exchange Online connectors

upvoted 1 times

Collecting 4 months, 1 week ago

Selected Answer: D

the Exchange Online connectors

upvoted 1 times

Ali96 5 months ago

Selected Answer: D

D. the Exchange Online connectors

upvoted 2 times

tuyi2 5 months ago

Selected Answer: B

The DNS Records should be the correct answer

upvoted 1 times

⊟ **Softeng** 5 months ago

Selected Answer: B

Should be: B- DNS Records?

To ensure that all incoming email is scanned exclusively by Microsoft Defender for Office 365, you need to modify your MX (Mail Exchange) records.

upvoted 2 times

Question #35 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

C. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

D. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

Suggested Answer: *B*

Community vote distribution

B (75%) D (25%)

baptista Highly Voted 1 year, 10 months ago

this question is repeated 3 times.

upvoted 13 times

techghostbarbie 11 months, 2 weeks ago

6 times actually

upvoted 4 times

billo79152718 Most Recent 9 months, 2 weeks ago

Selected Answer: B

B. is correct not D

upvoted 1 times

EmarOliva 1 year, 4 months ago

Selected Answer: B

It is repeated. So the answer is B (https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5)

upvoted 1 times

Ario 1 year, 6 months ago

Selected Answer: D

Azure Policy provides a centralized platform to enforce and assess compliance with a wide range of regulatory standards, including NIST 800-53. By assigning a built-in policy definition, you can evaluate the current configuration and compliance status of the Azure resources in the subscription against the specified requirements.

upvoted 1 times

zellck 1 year, 7 months ago

Same as Question 30.

https://www.examtopics.com/discussions/microsoft/view/94937-exam-sc-100-topic-2-question-30-discussion

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 1 times

Question #35 *Topic 2*

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.

You use Microsoft Defender XDR to manage the tenants of your company's customers.

You need to ensure that the users in Group1 can perform security tasks in the tenant of each customer. The solution must meet the following requirements:

- The Group1 users must only be assigned the Security Operator role for the customer tenants.
- The users in Group2 must be able to assign the Security Operators role to the Group1 users for the customer tenants.
- The use of quest accounts must be minimized.
- Administrative effort must be minimized.

What should you include in the solution?

A. multi-user authorization (MUA)

B. Azure Lighthouse

C. Privileged Identity Management (PIM)

D. Microsoft Entra B2B collaboration

Suggested Answer: *B*

Community vote distribution

B (100%)

skz94 3 months, 1 week ago

Selected Answer: B

Azure Lighthouse enables cross-tenant management, allowing users in Group1 to be assigned the Security Operator role for customer tenants without needing guest accounts1.
Users in Group2 can manage role assignments, including assigning the Security Operator role to Group1 users.
It simplifies administrative tasks and provides a scalable solution for managing multiple customer tenants.

upvoted 1 times

agroman09 3 months, 3 weeks ago

Selected Answer: C

My answer is PIM as it mentions use guest accounts to be minimized.

upvoted 1 times

Mick2024 5 months ago

Selected Answer: B

I found this somewhat confusing. It talks of 'a tenant' but further on talks about tenants, so which is it? If its tenants, option B makes sense, but if its tenant, is it not C?

upvoted 1 times

jim85 4 months, 4 weeks ago

I think, the mentioned tenant is a management tenant, and users from that tenant manage the other tenants. Guess, MS wanted to be tricky. Pls correct me, if I am mistaken.

upvoted 1 times

Question #36 *Topic 2*

You have an Azure subscription.

Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.

What should you recommend using to enforce the governance requirement?

A. Azure management groups

B. custom Azure roles

C. Azure Policy assignments

D. regulatory compliance standards in Microsoft Defender for Cloud

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **Gurulee** Highly Voted 👍 2 years, 2 months ago

Selected Answer: C

Specifically, some useful governance actions you can enforce with Azure Policy include:
Ensuring your team deploys Azure resources only to allowed regions,
Enforcing the consistent application of taxonomic tags, and
Requiring resources to send diagnostic logs to a Log Analytics workspace

upvoted 7 times

⊟ **ASP0505** Most Recent ⏱ 3 months ago

Selected Answer: C

Azure Policy has the capabilities to enforce specific policies/rules in your Azure subscription.

upvoted 1 times

⊟ **MidnightCrush** 6 months, 4 weeks ago

Selected Answer: C

Key word here is "enforce". Azure Policy has the capabilities to enforce specific policies/rules in your Azure subscription.

Answer is C.

upvoted 2 times

⊟ **WRITER00347** 1 year, 11 months ago

To enforce the governance requirement that resources must be created only in specific Azure regions (West Europe or North Europe), you should recommend using Azure Policy assignments.

Azure Policy enables you to create, assign, and manage policies that enforce different rules and effects over your resources. In this case, you can define a policy that restricts the creation of resources to the specified regions, and then assign that policy to the appropriate scope (subscription, resource group, etc.).

Therefore, the correct option is:

C. Azure Policy assignments.

upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 4 times

⊟ **kazaki** 2 years, 1 month ago

Why not D

upvoted 4 times

⊟ **ijunico** 2 years ago

because the question is about restrictions for regions for resources, not about any specific regulations.

upvoted 1 times

Question #37 Topic 2

HOTSPOT

-

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender.

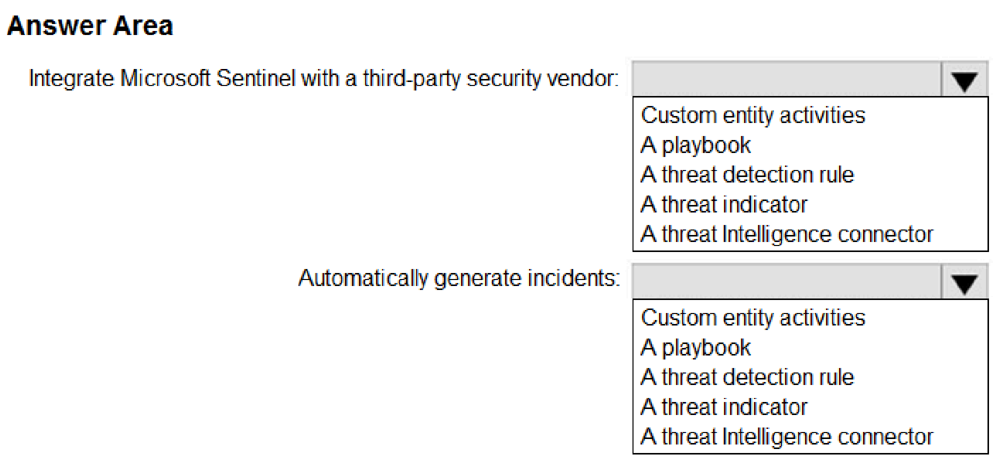
You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender.

You need to recommend a solution to meet the following requirements:

• Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware.
• Automatically generate incidents when the IP address of a command-and-control server is detected in the events.

What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

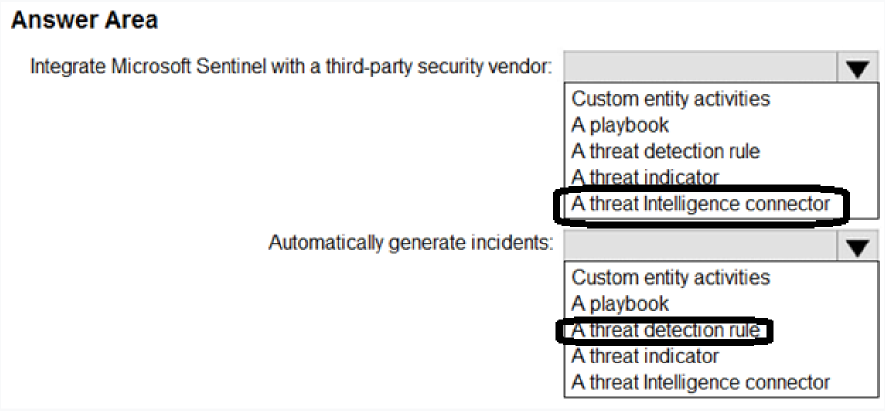
Integrate Microsoft Sentinel with a third-party security vendor: ▼

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat Intelligence connector

Automatically generate incidents: ▼

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat Intelligence connector

Suggested Answer:



Answer Area

Integrate Microsoft Sentinel with a third-party security vendor: ▼

Custom entity activities
A playbook
A threat detection rule
A threat indicator
[✓ A threat Intelligence connector]

Automatically generate incidents: ▼

Custom entity activities
A playbook
[✓ A threat detection rule]
A threat indicator
A threat Intelligence connector

⊟ **Victory007** Highly Voted 1 year, 10 months ago

1. Threat Intelligence connector - Allow you to integrate Microsoft Sentinel with third-party security vendors to access information about known threats, such as malware and command-and-control servers.
2. Threat detection rule- Allow you to define conditions that, when met, will automatically generate an incident in Microsoft Sentinel.
https://learn.microsoft.com/en-us/azure/sentinel/partner-integrations
https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts

upvoted 26 times

⊟ **Murtuza** Highly Voted 1 year, 5 months ago

Playbooks are used to automatically remediate the incidents after the rule has been created so playbook is not an answer here

upvoted 7 times

⊟ **dc864d4** Most Recent 7 months, 4 weeks ago

data connector and automation rules
upvoted 2 times

ayadmawla 1 year, 5 months ago
Given answers are correct
upvoted 2 times

ayadmawla 1 year, 5 months ago
Automation rules help you triage incidents in Microsoft Sentinel. You can use them to automatically assign incidents to the right personnel, close noisy incidents or known false positives, change their severity, and add tags. They are also the mechanism by which you can run playbooks in response to incidents or alerts.

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an entire incident, to an individual alert, or to a specific entity. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts are generated or when incidents are created or updated, by being attached to an automation rule. It can also be run manually on-demand on specific incidents, alerts, or entities.

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents
upvoted 1 times

Mblott77 1 year, 11 months ago
1. Playbook used to send data to 3rd party SIEM.
https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
2. Microsoft Threat Intelligence Analytics rule.
https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-built-in
upvoted 3 times

Ramye 1 year, 5 months ago
Playbook is NOT used to send data to 3rd party SIEM. Playbook is used for automatically remediate identified issues - SOAR
upvoted 2 times

Question #38 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You need to enforce ISO 27001:2013 standards for new resources deployed to the subscription. The solution must ensure that noncompliant resources are automatically detected.

What should you use?

A. Azure Blueprints

B. the regulatory compliance dashboard in Defender for Cloud

C. Azure Policy

D. Azure role-based access control (Azure RBAC)

Suggested Answer: *C*

Community vote distribution

C (71%) B (29%)

emartiy 1 year ago

Selected Answer: C

Azure Policy fulfill the question requirement!

upvoted 4 times

hellawaits111 1 year, 1 month ago

Selected Answer: B

I would say B

Azure Policy will be the enforcement part

upvoted 1 times

ayadmawla 1 year, 5 months ago

Selected Answer: B

They would like to "enforce" but first we need to detect non-compliance against the standard and therefore we must choose B to select the regulatory compliance in question and determine where the non-compliance is

see: https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

upvoted 1 times

ayadmawla 1 year, 5 months ago

Microsoft Defender for Cloud helps you to meet regulatory compliance requirements by continuously assessing resources against compliance controls, and identifying issues that are blocking you from achieving a particular compliance certification.

In the Regulatory compliance dashboard, you manage and interact with compliance standards. You can see which compliance standards are assigned, turn standards on and off for Azure, AWS, and GCP, review the status of assessments against standards, and more.

upvoted 1 times

ayadmawla 1 year, 4 months ago

I am wrong here; Policy detects and enforces see: https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

my apologies

upvoted 5 times

Ramye 1 year, 5 months ago

but it also says "You need to enforce standards for new resources deployed to the subscription." so how do you enforce? that would be via policy

upvoted 1 times

Murtuza 1 year, 5 months ago

enforce = azure policy

upvoted 3 times

⊟ **juanpe147** 1 year, 6 months ago

in my opinion, if they are new elements, it should be a BluePrint instead an azure Policy

upvoted 3 times

⊟ **Victory007** 1 year, 10 months ago

Selected Answer: C

same as before.

upvoted 3 times

Question #39 *Topic 2*

DRAG DROP
-

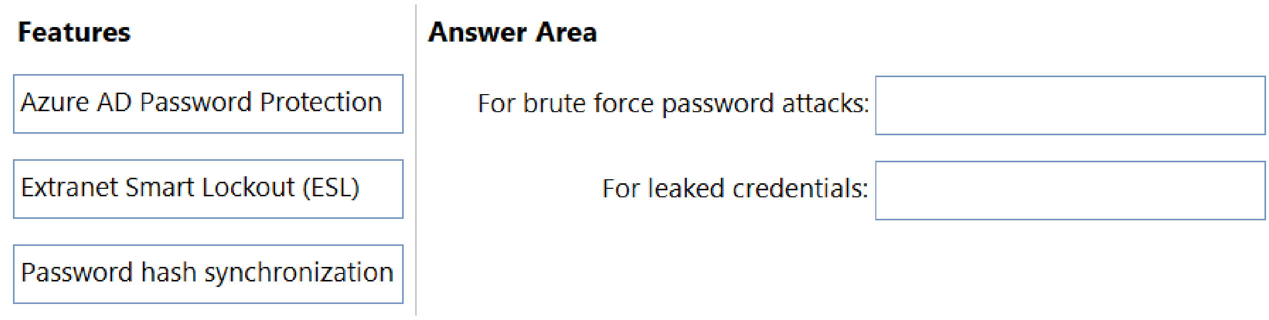
You have a hybrid Azure AD tenant that has pass-through authentication enabled.

You are designing an identity security strategy.

You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.

What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Features

Azure AD Password Protection

Extranet Smart Lockout (ESL)

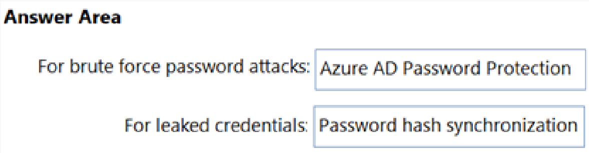
Password hash synchronization

Answer Area

For brute force password attacks:

For leaked credentials:

Suggested Answer:



Answer Area

For brute force password attacks: Azure AD Password Protection

For leaked credentials: Password hash synchronization

smanzana Highly Voted 1 year, 2 months ago

Box1: Azure AD Password Protection

Box2: Password hash syncronization

upvoted 16 times

PierreTang Most Recent 10 months, 1 week ago

Box1: Azure AD Password Protection

Box2: Password hash syncronization

As Azure AD Password Protection support "Custom smart lockout" Customize your smart lockout threshold (number of failures until the first lockout) and duration (how long the lockout period lasts).

upvoted 2 times

billo79152718 10 months, 1 week ago

Box1: Azure AD Password Protection

Box2: Password hash synchronization

There is no ADFS so no Extranet Smart Lockout for the first box.

upvoted 1 times

Charly80 11 months, 2 weeks ago

"Extranet Smart Lockout" is for ADFS, AAD PWd Protection help to prevent utilization of common password.

upvoted 2 times

RickySmith 11 months, 2 weeks ago

Entra Smart Lockout

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout

Password Hash Sync

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-phs

upvoted 1 times

ayadmawla 11 months, 3 weeks ago

Given Answer is wrong.

A: Brute Force Attack => SmartLock

B: Leaked Credentials => Password Hash

upvoted 2 times

Charly80 11 months, 2 weeks ago

Extranet Smart Lockout is for ADFS, there is no ADFS here.

upvoted 2 times

ayadmawla 11 months, 3 weeks ago

For Leaked Credentials, Microsoft recommends Password Hashing. See: https://learn.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity#protect-against-leaked-credentials-and-add-resilience-against-outages

The simplest and recommended method for enabling cloud authentication for on-premises directory objects in Microsoft Entra ID is to enable password hash synchronization (PHS). If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync

upvoted 2 times

Ramye 11 months, 2 weeks ago

Microsoft also says the below"

Note

"Hash tracking functionality isn't available for customers with pass-through authentication enabled as authentication happens on-premises not in the cloud."

in this question's scenario, pass-through authentication is enabled, for 2nd question The answer probably not Password Hash.. but not quite sure what should be the answer as there is info all over the place but not sure which one is they are looking for

upvoted 2 times

ayadmawla 11 months, 3 weeks ago

I agree with Luffysan91x, for Bruteforce attack, Smart Lockout is recommended by Microsoft. See: https://learn.microsoft.com/en-us/azure/active-directory-b2c/threat-management

Credential attacks lead to unauthorized access to resources. Passwords that are set by users are required to be reasonably complex. Azure AD B2C has mitigation techniques in place for credential attacks. Mitigation includes detection of brute-force credential attacks and dictionary credential attacks. By using various signals, Azure Active Directory B2C (Azure AD B2C) analyzes the integrity of requests. Azure AD B2C is designed to intelligently differentiate intended users from hackers and botnets.

How smart lockout works

Azure AD B2C uses a sophisticated strategy to lock accounts. The accounts are locked based on the IP of the request and the passwords entered. The duration of the lockout also increases based on the likelihood that it's an attack

upvoted 1 times

Luffysan91x 1 year ago

I chose ESL for the Second Option.

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout

Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers

upvoted 3 times

AbdallaAM 1 year, 3 months ago

Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers. By setting smart lockout policies in Azure AD appropriately, attacks can be filtered out before they reach on-premises AD DS.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

upvoted 4 times

calotta1 1 year, 4 months ago

based on the article ... https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

ESL is not possible when using PTA - "Hash tracking functionality isn't available for customers with pass-through authentication enabled as authentication happens on-premises not in the cloud"

Azure AD Password Protection seem to be the answer based on these recommendations:

When using pass-through authentication, the following considerations apply:*
*The Azure AD lockout threshold is less than the AD DS account lockout threshold. Set the values so that the AD DS account lockout threshold is at least two or three times greater than the Azure AD lockout threshold.
* The Azure AD lockout duration must be set longer than the AD DS account lockout duration. The Azure AD duration is set in seconds, while the AD duration is set in minutes.

upvoted 2 times

ruscomike 1 year, 1 month ago

from the same document:
"Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers"

ESL is available also for PTA, only the hash tracking is not available (purple box on the doc page).

upvoted 1 times

calotta1 1 year, 4 months ago

this means the current answers are correct.

upvoted 2 times

Doinitza 1 year, 3 months ago

Yes, it looks like that ESL is not available for a hybrid environment: "Finally, remember to start looking at moving to a Cloud Authentication model (either with Password Hash Sync or Pass-Through Authentication) so we can do the blocking for you at cloud scale in Azure Active Directory".
Link: https://www.linkedin.com/pulse/extranet-smart-lockout-ad-fs-2016-andres-canello

upvoted 1 times

KrissB 1 year, 4 months ago

For brute force password attacks: Extranet Smart Lockout (ESL)
For Leaked Credentials: Password Hash Sync. PHS needs to be enabled so Microsoft can compare Password hash' for cloud and hybrid identities to those available on the black market.

upvoted 1 times

KrissB 1 year, 4 months ago

Actually, This is a weird one. Extranet Smart Lockout is an ADFS feature, however here while talking about Hybrid identities, they mention that the set up is Pass-Through AUth so ADFS is not a solution without backtracking and going against the Microsoft recommended route (shift away from ADFS). Azure AD feature is Smart Lockout.

upvoted 3 times

kanag1 1 year, 4 months ago

For brute force password attacks: Extranet Smart Lockout (ESL)
For leaked Credentials: Azure AD Password Protection

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

upvoted 3 times

Cally46 1 year, 4 months ago

Looks correct:
1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
2. https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-phs

upvoted 3 times

Question #40 Topic 2

HOTSPOT

-

You are designing the security architecture for a cloud-only environment.

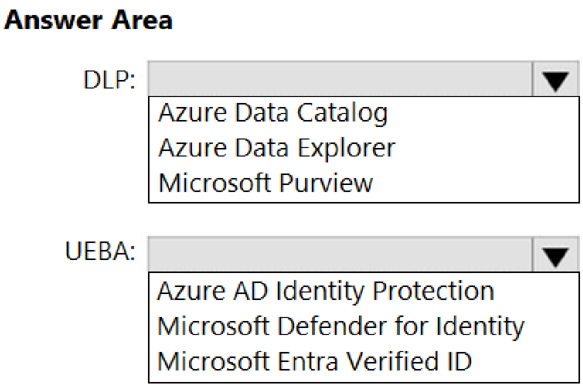
You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

• Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
• Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

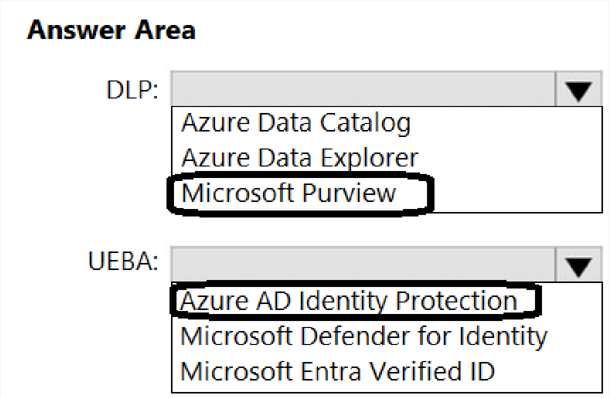


Answer Area

DLP:
- Azure Data Catalog
- Azure Data Explorer
- Microsoft Purview

UEBA:
- Azure AD Identity Protection
- Microsoft Defender for Identity
- Microsoft Entra Verified ID

Suggested Answer:



Answer Area

DLP:
- Azure Data Catalog
- Azure Data Explorer
- [✓ Microsoft Purview]

UEBA:
- [✓ Azure AD Identity Protection]
- Microsoft Defender for Identity
- Microsoft Entra Verified ID

Victory007 Highly Voted 1 year, 10 months ago

1. Purview- For the requirement to enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal, you should include Microsoft Purview in your recommendation. https://learn.microsoft.com/en-us/microsoft-365/security/defender/dlp-investigate-alerts-defender?view=o365-worldwide

2. MS Defender for Identity. Microsoft Defender for Cloud Apps provides user entity behavioral analytics (UEBA) in the cloud. This can be extended to your on-premises environment by integrating with Microsoft Defender for Identity. After you integrate with Defender for Identity, you'll also gain context around user identity from its native integration with Active Directory. https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-ueba

upvoted 19 times

hovlund Highly Voted 1 year, 8 months ago

It is NOT Defender for Identity because its a cloud only environment..., i agree with ServerBrian: Purview and Identity Protection

upvoted 16 times

RoboCock 2 months, 3 weeks ago

agreed! need to read carefully, for cloud-only MDI does not help. same time EIDP integration with XDR portal is not perfect, but it's the best choice to go w

upvoted 1 times

Azerty1313 1 year, 6 months ago

Agree. Azure ID protect is a better fit as it is Azure only.
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/introducing-investigation-priority-built-on-user-and-entity/ba-p/360853#:~:text=UEBA%20for%20Azure%20ATP%2C%20MCAS%2C%20and%20Azure%20AD%20Identity%20Protection&text=Activities%20and%20events

upvoted 1 times

Socgen1 Most Recent 11 months, 3 weeks ago

DLP - Purview
UEBA - Identity Protection as it is cloud only environment - because Microsoft Defender for Identity (formerly Azure Advanced Threat Protection or Azure ATP) is a cloud-based security solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. To detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting using Defender for Identity

upvoted 2 times

emartiy 1 year ago

As other mentioned..
DLP > Microsoft Purview other options do not fulfill requirement
UEBA > for cloud based checks Azure AD Identity protection when you refer to question and given environment... Don't miss point.

upvoted 3 times

macka2005 1 year ago

1. Purview

2. Microsoft Defender for Identity - "Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization."
https://learn.microsoft.com/en-us/defender-for-identity/what-is

upvoted 1 times

ubiquituz 1 year, 3 months ago

Microsoft Defender for Identity
To help you focus on user identity, Microsoft Defender for Cloud Apps provides user entity behavioral analytics (UEBA) in the cloud. This can be extended to your on-premises environment by integrating with Microsoft Defender for Identity. After you integrate with Defender for Identity, you'll also gain context around user identity from its native integration with Active Directory.

upvoted 2 times

ayadmawla 1 year, 5 months ago

Just remember that "MS Defender for Identity" is for on premise AD identity protection and not the Cloud Identity as the case in this question.

see: https://learn.microsoft.com/en-us/defender-for-identity/what-is#detect-threats-across-modern-identity-environments

Defender for Identity uses data from across your environment, including domain controllers, Active Directory Federation Services (AD FS), and Active Directory Certificate services (AD CS), to provide you with a complete view of your identity environment.

Defender for Identity sensors monitor domain controller traffic by default. For AD FS / AD CS servers, make sure to install the relevant sensor type for complete identity monitoring.

upvoted 3 times

cybrtrk 1 year, 6 months ago

Purview is correct
No active directory in this question, so UEBA should be Azure AD Identity Protection.

upvoted 4 times

summut 1 year, 6 months ago

1 = Purview
2 = Identity Protection (MDI is a Hybrid solution mainly for monitoring and protecting on-prem identities)

upvoted 3 times

Arjanussie 1 year, 6 months ago

It is a design of a cloud only environment and Yes, Azure AD Identity Protection provides User and Entity Behavior Analytics (UEBA) functionality .
UEBA uses artificial intelligence and machine learning to model how users and devices typically behave. It then compares future behavior against the baseline to create a risk score. This allows you to analyze large data sets and elevate the highest-priority alerts

upvoted 3 times

smanzana 1 year, 8 months ago

Microsoft Purview and Microsoft Defender for Identity

upvoted 1 times

KrissB 1 year, 10 months ago

Purview and Microsoft Defender for Identity. MDI is a pre-requisite UEBA across various security workloads.

upvoted 6 times

ServerBrain 1 year, 10 months ago

Purview and Identity Protection

https://learn.microsoft.com/en-us/azure/security/fundamentals/threat-detection

upvoted 2 times

sbnpj 1 year, 10 months ago

Purview and Defender for Identity

https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-suspicious-activity

upvoted 2 times

Question #41 Topic 2

HOTSPOT

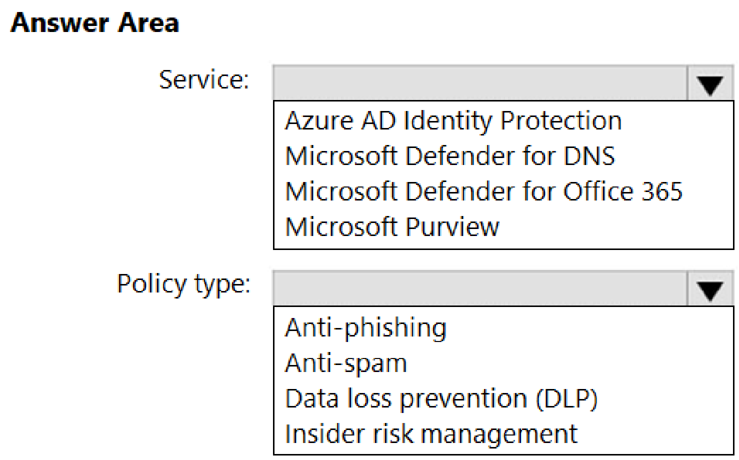
-

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

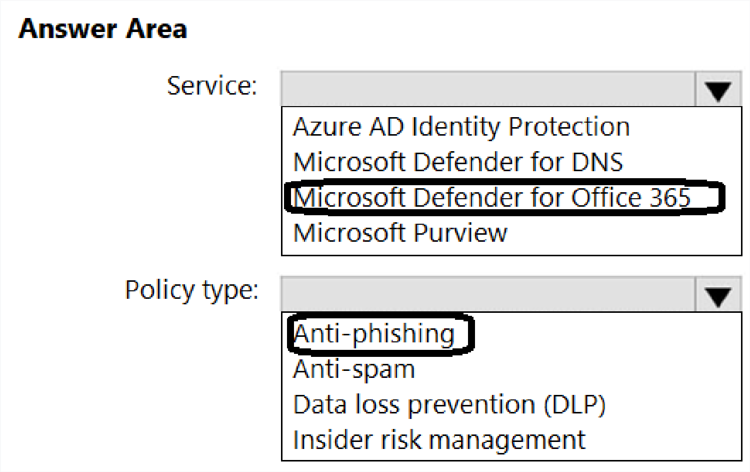


Answer Area

Service:
- Azure AD Identity Protection
- Microsoft Defender for DNS
- Microsoft Defender for Office 365
- Microsoft Purview

Policy type:
- Anti-phishing
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

Suggested Answer:



Answer Area

Service:
- Azure AD Identity Protection
- Microsoft Defender for DNS
- [✓ Microsoft Defender for Office 365]
- Microsoft Purview

Policy type:
- [✓ Anti-phishing]
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

⊟ **ServerBrain** Highly Voted 1 year, 4 months ago

Given answers are 100% correct

upvoted 16 times

⊟ **Victory007** Highly Voted 1 year, 4 months ago

1. MS Defender for Office 365. 2. Anti-Phishing . To prevent malicious actors from impersonating the email addresses of internal senders, you should use Microsoft Defender for Office 365 and configure an Anti-phishing policy. Microsoft Defender for Office 365 provides protection against phishing attacks, including spoofing and impersonation. You can customize the anti-phishing policy to specify the actions to take when a message is identified as a phishing attempt. This includes configuring anti-spoofing protection, which helps protect against exact domain spoofing, where attackers forge the domain to look exactly like the domain of the victim's organization or like their business partner's.

upvoted 9 times

⊟ **morito** Most Recent 1 year ago

For people like me who are unsure whether this belongs to EOP or to Defender for Office 365, here a good comparision: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about?view=o365-worldwide. TLDR: EOP contains some anti-phishing functionality, but only Defender for Office 365 has impersonation protection.

upvoted 3 times

⊟ **smanzana** 1 year, 2 months ago

Microsoft Defender for Office 365 y Anti-Phishing

upvoted 4 times

Question #42 *Topic 2*

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

You have multiple project teams. Each team has an AD DS group that syncs with Azure AD.

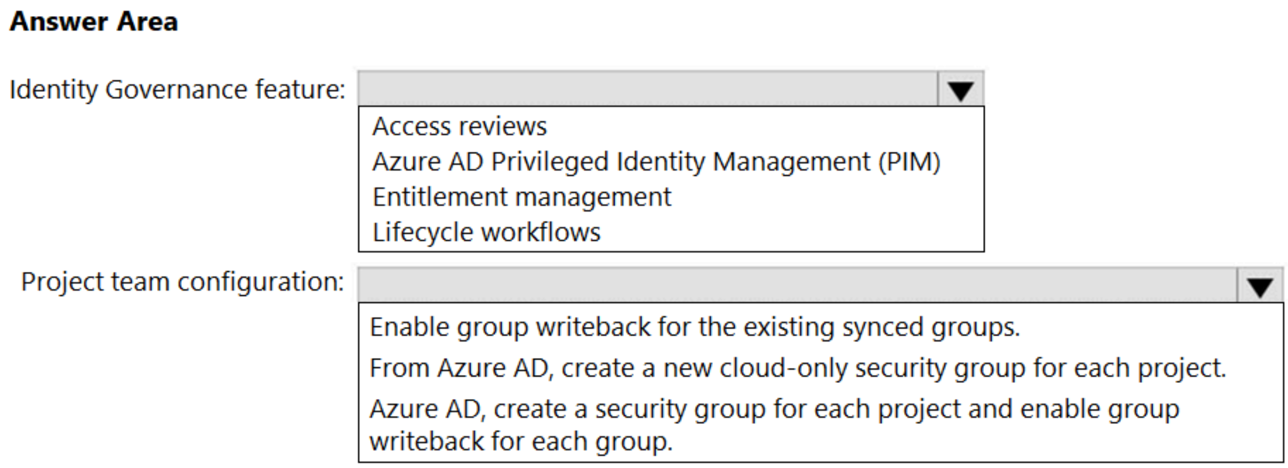
Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

You need to recommend an Azure AD Identity Governance solution that meets the following requirements:

- Project managers must verify that their project group contains only the current members of their project team.
- The members of each project team must only have access to the resources of the project to which they are assigned.
- Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days.
- Administrative effort must be minimized.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

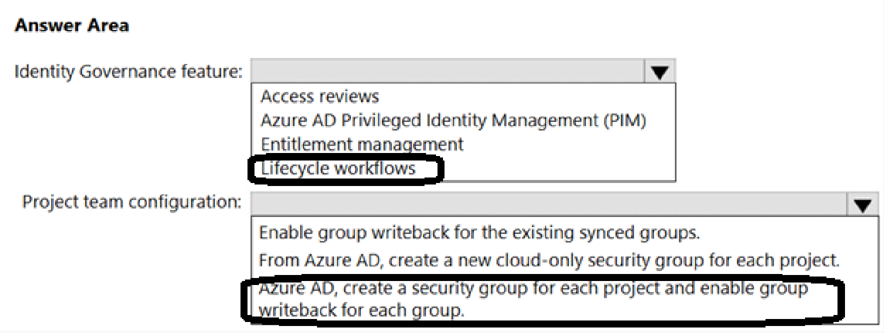
Identity Governance feature: ▼

- Access reviews
- Azure AD Privileged Identity Management (PIM)
- Entitlement management
- Lifecycle workflows

Project team configuration: ▼

- Enable group writeback for the existing synced groups.
- From Azure AD, create a new cloud-only security group for each project.
- Azure AD, create a security group for each project and enable group writeback for each group.

Suggested Answer:



Answer Area

Identity Governance feature: ▼

- Access reviews
- Azure AD Privileged Identity Management (PIM)
- Entitlement management
- [✓ Lifecycle workflows]

Project team configuration: ▼

- Enable group writeback for the existing synced groups.
- From Azure AD, create a new cloud-only security group for each project.
- [✓ Azure AD, create a security group for each project and enable group writeback for each group.]

⊟ **Victory007** Highly Voted 1 year, 10 months ago

1. Access Reviews. 2. Enable group write back for the existing synced group. https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview.

upvoted 45 times

⊟ **Er_01** 4 months, 3 weeks ago

In looking at the Interface it asks which feature in ID gov can do this. You can configure an access review in an access package under EM or as a stand alone option in an AR. However, part 2 of the question is ensuring only a group has access. So is it inferring access by the nature of the AR or it is explicit as with an AP under EM. With the 2nd line being vague could be either one based on unstated assumptions. Admin effort leans toward EM as you do all in a package, still it is based on the implicit or explicit view of access.

upvoted 1 times

casualbork 1 year, 9 months ago

• Project managers must verify that their project group contains only the current members of their project team.
This means access reviews, Lifecycle Workflow would do all of this automatically based on the user attributes (such as department or team)

You have multiple project teams. Each team has an **AD DS group** that **syncs with Azure AD.** (these being the key to find the correct answer)
Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

The correct answer is "Enable group write back for the existing synced group."

Therefor, the answer Victory007 have provided is the correct answer.

upvoted 10 times

ServerBrain 1 year, 10 months ago

You are correct. Azure AD Connect has group writeback enabled, no need to create new groups.

upvoted 3 times

NICKTON81 Highly Voted 👍 1 year, 6 months ago

1 - Entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview
2. Enable group write back for the existing synced group.

upvoted 7 times

6c0ca3d Most Recent 🕘 1 month, 2 weeks ago

1. Access Reviews
Ensures periodic verification by project managers to confirm that each group contains the correct members.

Users are automatically removed if the group membership is not reviewed for 30 days, enforcing compliance.

upvoted 1 times

424ede1 3 months ago

entitlement management

The link below contains all requirements!
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview#what-can-i-do-with-entitlement-management

upvoted 1 times

Er_01 4 months, 3 weeks ago

Access Reviews do not meet the 2nd requirement of insuring access to resources.
AR does 1 and 3. Identity Governance does all 3 as Reviews and Packages are part of it.

upvoted 1 times

Dan91 8 months ago

To meet the requirements of the question. The answer has to be:
1. Entitlement Management - there is a requirement to restrict access only to resources that the user is required to access. Whilst this can be done through various methods, the only option provided that achieves this is Entitlement Managment. Secondly, access reviews must be conducted where if there is no response the access is automatically removed. This also can be achieved through Entitlement Managment (see below link).
2. Enable group write back for the existing synced group.

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-reviews-create?source=recommendations
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview
https://learn.microsoft.com/en-us/entra/identity/hybrid/group-writeback-cloud-sync

upvoted 1 times

RenegadeOrange 9 months, 1 week ago

1. Access Reviews
You can set it to remove if there is no response from the reviewer.
2. Entra ID, create a security group for each project and enable group writeback for each group:
It has to be a cloud group, on premises cannot be configured with writeback.

That feature is depricated back in June 24 but the new Microsoft Entra Cloud Sync called Group Provision to Active Directory that you can use instead of Group Writeback
https://learn.microsoft.com/en-us/entra/identity/hybrid/group-writeback-cloud-sync
upvoted 1 times

jvallespin 11 months ago
1. Access Reviews: When the approver does not reply to the access review you can configure an action like remove users.
2. Azure AD, create a security group for each project and enable group writeback for each group: Already created Synced Groups from on premises cannot be configured with writeback. Create new cloud groups only would work if cloud sync would have been configured for all groups, that is not mentioned in the question text.
upvoted 2 times

pokus00132 11 months, 2 weeks ago
1. Access Reviews
2. Azure AD, create a security group for each project and enable group writeback for each group

You need to create cloud Entra Id (Azure AD) group and then select group and enable it for writeback.
You can't enable writeback for group which is synchronized from Windows AD to Entra Id.
If you create new cloud-only security group for each project, group writeback is not automatically enabled.
upvoted 1 times

emartiy 1 year ago
Box1: Access review (Under the Entitlement management of Identity Governance)
Box2: From Azure AD, create a new cloud-only security group for each project)

Group Writeback v2:
With the release of provisioning agent 1.1.1370.0, Cloud Sync now supports group writeback.
Cloud Sync provisions groups directly to your on-premises AD environment.
You can use identity governance features to manage access to AD-based applications by including a group in an entitlement management access package.
upvoted 2 times

> **emartiy** 1 year ago
> You can't update on-prem AD groups via Azure AD. Therefore, you need a cloud-only group and also it will be synced to on-prem thanks to Azure AD Connect tool's group writeback feature..
> upvoted 2 times

jayek 1 year ago
https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews#review-access-to-on-premises-groups
upvoted 1 times

ayadmawla 1 year, 4 months ago
I am sorry to contradict but Lifecycle Workflow is exactly what is needed

see: https://learn.microsoft.com/en-us/entra/id-governance/what-are-lifecycle-workflows#when-to-use-lifecycle-workflows

Automating group membership: When groups in your organization are well defined, you can automate user membership in those groups.
Lifecycle workflows manage static groups, where you don't need a dynamic group rule.
There's no need to have one rule per group. Lifecycle workflow rules determine the scope of users to execute workflows against, not which group.
upvoted 1 times

> **Mnguyen0503** 1 year, 2 months ago
> You're missing the point here. The key info is manages must approve group membership. This is what access reviews are designed to do. In access review configuration, you can determine what to do when access review is not completed, which meet the other requirement as well.
> upvoted 1 times

Murtuza 1 year, 5 months ago
Project managers must verify = IMPLIES ACCESS REVIEW

upvoted 2 times

⊟ **Ramye** 1 year, 5 months ago

but how does this satisfies this requirement ---> "Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days"

see it says automatically

upvoted 1 times

⊟ **harimurti20** 1 year, 6 months ago

Given Answer is correct: Lifecycle Workflow is correct, as per the requirement-Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days.

upvoted 1 times

⊟ **jvallespin** 11 months, 1 week ago

This is a setting: "Remove Access if reviewers don't respond" in the Access review configuration https://learn.microsoft.com/en-us/entra/id-governance/create-access-review#next-settings

upvoted 2 times

⊟ **smanzana** 1 year, 8 months ago

Box1:Access Reviews

Box2: Enable group write back for the existing synced group.

upvoted 3 times

⊟ **ConanBarb** 1 year, 9 months ago

To add some detail to the discussion: Lifecycle Workflows could have been an option, and actually a better one than Access Reviews, but isn't due to

1) The requirements says "Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days."

2) LC Workflows requires Microsoft Entra ID Governance licenses (which we can't assume)

Lifecycle Workflows, if valid, would have been better as they are automatic and event driven, (happen instantly) and not every 30 days or so

upvoted 1 times

⊟ **ayadmawla** 1 year, 4 months ago

This is a logic apps functionality that can be included within Lifecycle Workflows

upvoted 1 times

⊟ **sbnpj** 1 year, 10 months ago

I agree with Victory007, its 1- Access reviews and Enabled Group write back for the existing synced group.

upvoted 2 times

Question #43 *Topic 2*

HOTSPOT

-

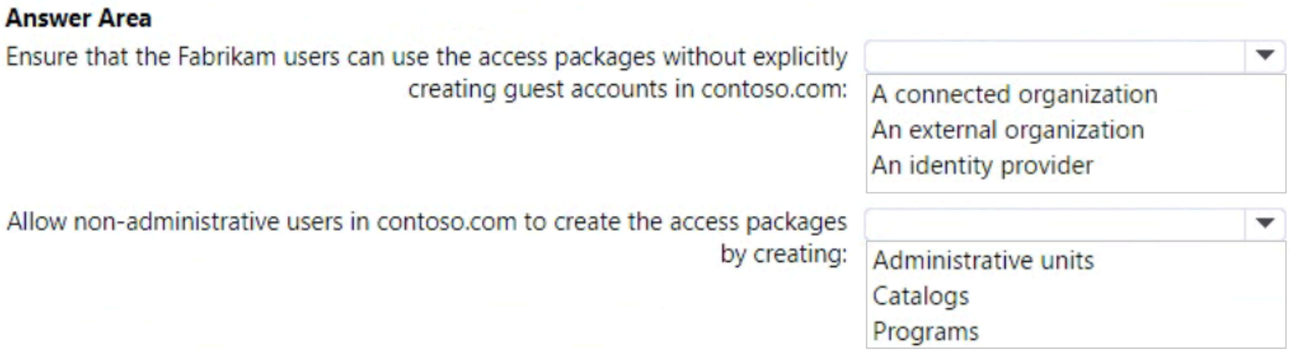
You are designing a privileged access strategy for a company named Contoso, Ltd. and its partner company named Fabrikam, Inc. Contoso has an Azure AD tenant named contoso.com. Fabrikam has an Azure AD tenant named fabrikam.com. Users at Fabrikam must access the resources in contoso.com.

You need to provide the Fabrikam users with access to the Contoso resources by using access packages. The solution must meet the following requirements:

• Ensure that the Fabrikam users can use the Contoso access packages without explicitly creating guest accounts in contoso.com.
• Allow non-administrative users in contoso.com to create the access packages.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

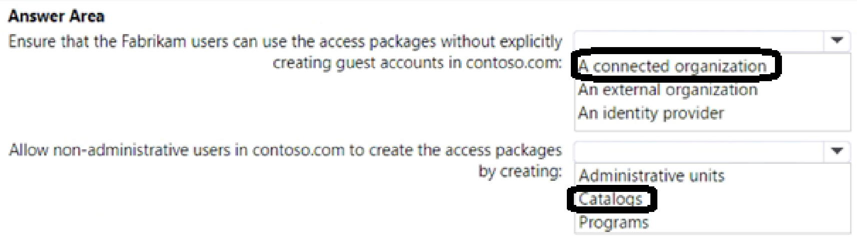
Ensure that the Fabrikam users can use the access packages without explicitly creating guest accounts in contoso.com:

- A connected organization
- An external organization
- An identity provider

Allow non-administrative users in contoso.com to create the access packages by creating:

- Administrative units
- Catalogs
- Programs

Suggested Answer:



Answer Area

Ensure that the Fabrikam users can use the access packages without explicitly creating guest accounts in contoso.com:

- [✓ A connected organization]
- An external organization
- An identity provider

Allow non-administrative users in contoso.com to create the access packages by creating:

- Administrative units
- [✓ Catalogs]
- Programs

RickySmith Highly Voted 11 months, 2 weeks ago

A connected organization

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-organization

Catalogs

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-delegate-catalog

upvoted 8 times

harimurti20 Highly Voted 1 year ago

Answer is correct

upvoted 5 times

xavi1 Most Recent 1 year, 2 months ago

Correct:

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-organization

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-external-users

upvoted 3 times

Question #44 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app registrations in Azure AD

D. application control policies in Microsoft Defender for Endpoint

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **PKPKPK** 8 months, 1 week ago

Selected Answer: D

correct, There are several questions on the same scenario

upvoted 4 times

⊟ **Ramye** 11 months, 3 weeks ago

Yes, Microsoft Defender for Endpoint can do the job, but it is not mentioned in the question at all. So, can this really be the answer?

upvoted 1 times

⊟ **Ramye** 11 months, 3 weeks ago

Never mind ☝this inquiry. It is mentioned in choice D. Thx

upvoted 1 times

⊟ **harimurti20** 1 year ago

D (Application control policies in Microsoft Defender for Endpoint) is correct.

upvoted 2 times

⊟ **smanzana** 1 year, 2 months ago

D (Application control policies in Microsoft Defender for Endpoint)

upvoted 3 times

⊟ **theugly23** 1 year, 2 months ago

D is correct

upvoted 1 times

Question #45 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, add a regulatory compliance standard.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Suggested Answer: *A*

Community vote distribution

A (100%)

tuyi2 5 months, 1 week ago

Selected Answer: A

This question has been repeated more than 6 times.

upvoted 1 times

Murtuza 12 months ago

Selected Answer: A

A is correct

upvoted 4 times

Arockia 12 months ago

A. From Defender for Cloud, add a regulatory compliance standard.

To review the subscription for NIST 800-53 compliance, you should start by adding the NIST 800-53 regulatory compliance standard within Defender for Cloud. This will ensure that the appropriate compliance checks and assessments are performed against the NIST 800-53 controls for your Azure resources.

The other options are not the correct first step for reviewing NIST 800-53 compliance:

upvoted 4 times

harimurti20 1 year ago

Answer is B

upvoted 1 times

harimurti20 1 year ago

Answer A is correct:

Answer B will be correct if it contains Azure Policy initiative

upvoted 3 times

Glorpy 1 year ago

Selected Answer: A

Answer is correct:

Defender for Cloud's regulatory standards and benchmarks are represented as security standards.

Defender for Cloud continually assesses the environment-in-scope against standards. Based on assessments, it shows in-scope resources as being compliant or noncompliant with the standard, and provides remediation recommendations.

upvoted 3 times

Azerty1313 1 year ago

Answer is B

upvoted 1 times

theugly23 1 year, 2 months ago

Answer A Correct

upvoted 1 times

Question #45 Topic 2

You have a Microsoft Entra tenant. The tenant contains 500 Windows devices that have the Global Secure Access client deployed.

You have a third-party software as a service (SaaS) app named App1.

You plan to implement Global Secure Access to manage access to App1.

You need to recommend a solution to manage connections to App1. The solution must ensure that users authenticate by using their Microsoft Entra credentials before they can connect to App1.

What should you include the recommendation?

A. a Global Secure Access app

B. a private access traffic forwarding profile

C. an internet access traffic forwarding profile

D. a Quick Access app

Suggested Answer: *A*

Community vote distribution

A (100%)

SMHcalicut 3 months, 1 week ago

Selected Answer: C

Internet access traffic forwarding profiles are designed for managing access to public cloud-based services like SaaS apps.

upvoted 1 times

AlbertE1nstein 5 months ago

Selected Answer: A

A Global Secure Access app allows you to manage access to third-party SaaS apps, like App1, by integrating with Microsoft Entra for authentication.

This solution ensures that users must authenticate with their Microsoft Entra credentials before they can access App1, providing a secure and managed access solution.

upvoted 4 times

Question #46 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app registrations in Azure AD

B. Azure AD Conditional Access App Control policies

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. adaptive application controls in Defender for Cloud

Suggested Answer: *D*

Community vote distribution

D (100%)

Ramye 11 months, 3 weeks ago

Can someone explain pls - how does adaptive control meet this requirements? Thx

upvoted 2 times

frankokabbb 10 months, 3 weeks ago

Because i think it is referring to an application and so adaptive appliation control would be the best

upvoted 2 times

Murtuza 12 months ago

Selected Answer: D

D is correct

upvoted 3 times

Murtuza 1 year ago

Selected Answer: D

D is correct questions keeps repeating in this dump

upvoted 4 times

theugly23 1 year, 2 months ago

D is correct

upvoted 4 times

Question #47 *Topic 2*

You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.

You need to design a security solution to assess whether all the devices meet the customer's compliance rules.

What should you include in the solution?

A. Microsoft Sentinel

B. Microsoft Purview Information Protection

C. Microsoft Intune

D. Microsoft Defender for Endpoint

Suggested Answer: *D*

Community vote distribution

C (97%)

cyber_sa Highly Voted 👍 1 year, 8 months ago

Selected Answer: C

got this in exam 6oct23. passed with 896 marks. I answered C

upvoted 9 times

shanti0091 Highly Voted 👍 1 year, 8 months ago

Selected Answer: C

Microsoft Intune same repeated question as #25 Microsoft Endpoint Manager.

upvoted 8 times

Faiz9876 Most Recent 🕓 1 year ago

Selected Answer: C

Intune

Microsoft Sentinel and Microsoft Purview Information Protection—are not directly related to assessing device compliance. Microsoft Defender for Endpoint focuses on threat protection rather than compliance evaluation

upvoted 2 times

harimurti20 1 year, 6 months ago

Answer C, Microsoft Intue is correct

upvoted 3 times

Glorpy 1 year, 7 months ago

Selected Answer: C

Intune as compliance is assessed through it and not MDE

upvoted 2 times

DuckChuck 1 year, 8 months ago

Selected Answer: C

Intune is correct

upvoted 4 times

Igglepiggle 1 year, 8 months ago

Selected Answer: C

"solution to assess whether all the devices meet the customer's compliance rules"

Answer is MS Intune.

Defender for endpoint is for detection and response (EDR).

upvoted 4 times

cyber_sa 1 year, 8 months ago

Selected Answer: D

Repeated Q#25. MD for endpoint is answer

upvoted 1 times

⊟ **cyber_sa** 1 year, 8 months ago

Sorry this is wrong comment by me. i don't know how to remove it. please ignore this ans D. correct is C

upvoted 3 times

Question #48 *Topic 2*

You have a Microsoft 365 subscription.

You have an Azure subscription.

You need to implement a Microsoft Purview communication compliance solution for Microsoft Teams and Yammer. The solution must meet the following requirements:

- Assign compliance policies to Microsoft 365 groups based on custom Microsoft Exchange Online attributes.
- Minimize the number of compliance policies.
- Minimize administrative effort.

What should you include in the solution?

A. Microsoft Purview Information Protection

B. Microsoft 365 Defender user tags

C. adaptive scopes

D. administrative units

Suggested Answer: *C*

Community vote distribution

C (100%)

AlbertE1nstein Highly Voted 👍 5 months ago

Selected Answer: C

Adaptive scopes allow you to assign compliance policies based on custom attributes, such as those in Microsoft Exchange Online.

They help minimize the number of compliance policies by dynamically applying policies based on the attributes of the groups.

This approach reduces administrative effort by automating the assignment of policies based on the defined criteria.

Does this align with what you were l

upvoted 5 times

Question #49 Topic 2

HOTSPOT

-

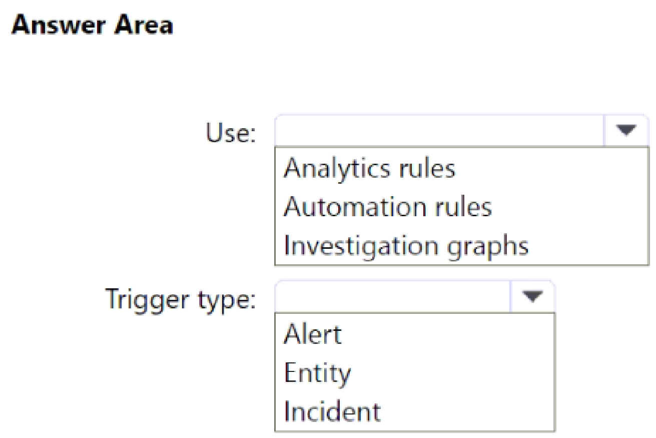
You have an Azure subscription that contains a Microsoft Sentinel workspace named MSW1. MSW11 includes 50 scheduled analytics rules.

You need to design a security orchestration automated response (SOAR) solution by using Microsoft Sentinel playbooks. The solution must meet the following requirements:

• Ensure that expiration dates can be configured when a playbook runs.
• Minimize the administrative effort required to configure individual analytics rules.

What should you use to invoke the playbooks, and which type of Microsoft Sentinel trigger should you use? To answer, select the options in the answer area.

NOTE: Each correct selection is worth one point.

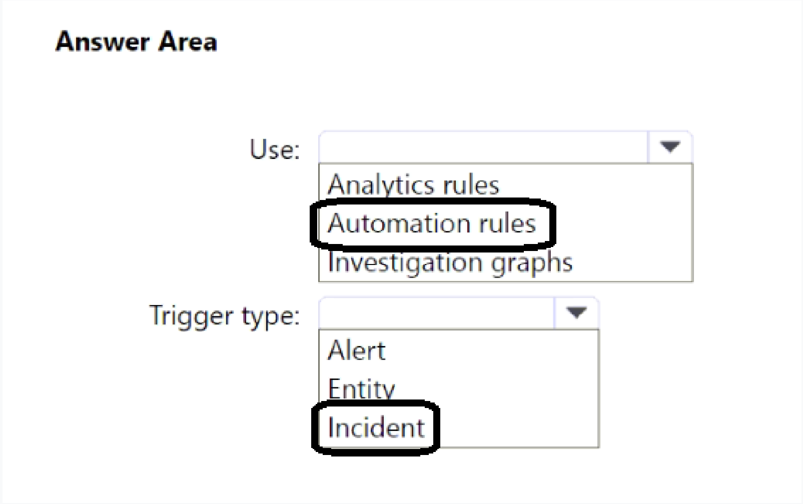


Answer Area

Use:
- Analytics rules
- Automation rules
- Investigation graphs

Trigger type:
- Alert
- Entity
- Incident

Suggested Answer:



Answer Area

Use:
- Analytics rules
- [✓ Automation rules]
- Investigation graphs

Trigger type:
- Alert
- Entity
- [✓ Incident]

cl1984 3 months, 1 week ago

Answers are:

Use: Automation Rules
Trigger Type: Incident

https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules?tabs=onboarded
upvoted 2 times

Question #50 *Topic 2*

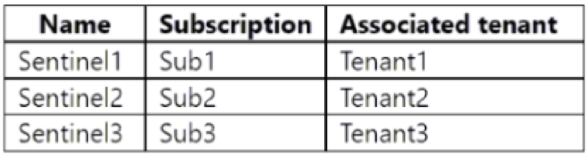
HOTSPOT

-

You have three Microsoft Entra tenants named Tenant1, Tenant2, and Tenant3.

You have three Azure subscriptions named Sub1, Sub2, and Sub3. Each tenant is associated with multiple Azure subscriptions.

Each subscription contains a single Microsoft Sentinel workspace as shown in the following table.



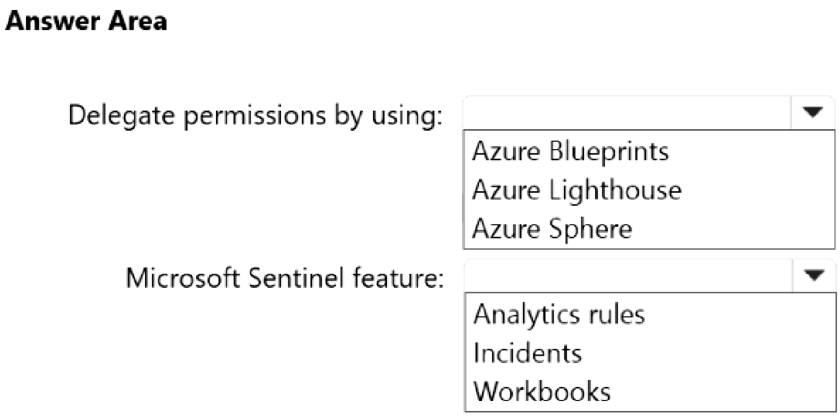
Name	Subscription	Associated tenant
Sentinel1	Sub1	Tenant1
Sentinel2	Sub2	Tenant2
Sentinel3	Sub3	Tenant3

You need to recommend a solution that meets the following requirements:

• Ensures that the users in Tenant1 can manage the resources in Sub2 and Sub3 without having to switch subscriptions or sign in to a different tenant.
• Implements multiple workspace view for Sentinel2 and Sentinel3.

What should you use to delegate permissions, and which Microsoft Sentinel feature will users be able to manage in multiple workspace view? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

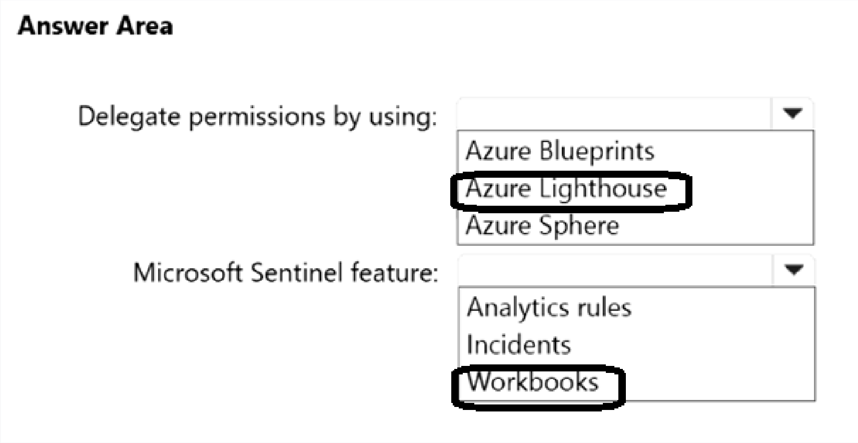


Answer Area

Delegate permissions by using:
- Azure Blueprints
- Azure Lighthouse
- Azure Sphere

Microsoft Sentinel feature:
- Analytics rules
- Incidents
- Workbooks

Suggested Answer:



Answer Area

Delegate permissions by using:
- Azure Blueprints
- [✓ Azure Lighthouse]
- Azure Sphere

Microsoft Sentinel feature:
- Analytics rules
- Incidents
- [✓ Workbooks]

424ede1 3 months ago

1- Lighthouse
https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants#manage-workspaces-across-tenants-using-azure-lighthouse

2- Incidents
https://learn.microsoft.com/en-us/azure/sentinel/multiple-workspace-view
upvoted 2 times

⊟ **Saynot** 3 months, 3 weeks ago
1- Lighthouse
2- Incidents
upvoted 3 times

Question #51 *Topic 2*

HOTSPOT

-

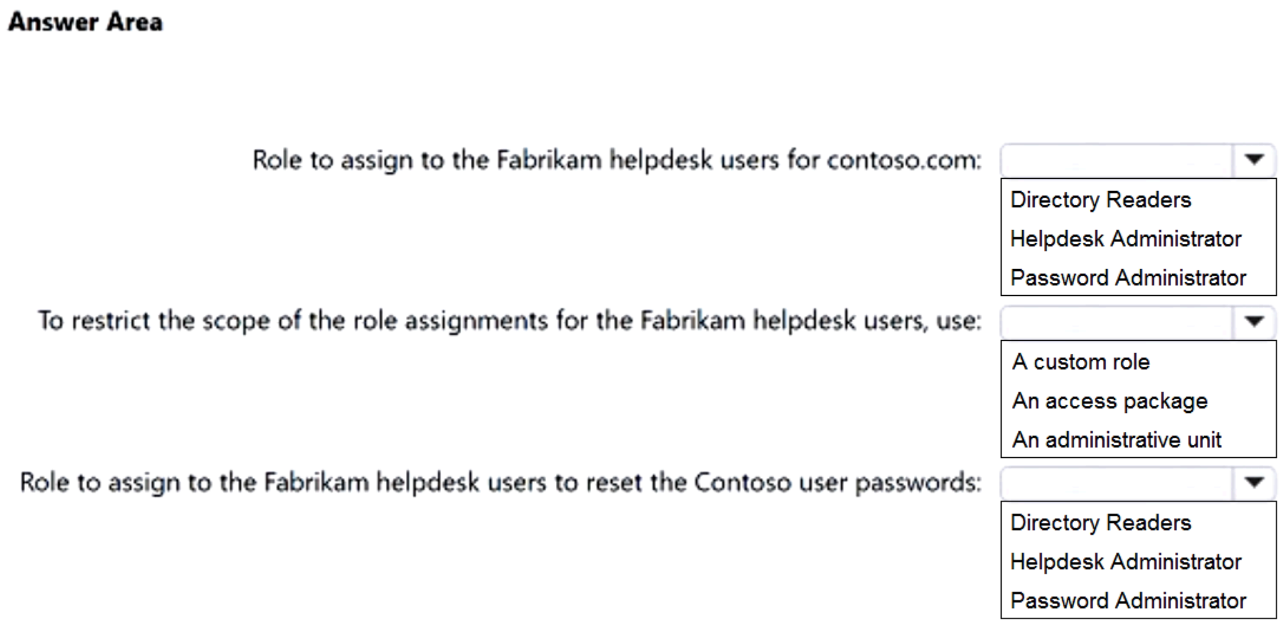
Your company, named Contoso, Ltd., has a Microsoft Entra tenant named contoso.com. Contoso has a partner company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabrikam.com.

You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:

• Follow the principle of least privilege.
• Minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



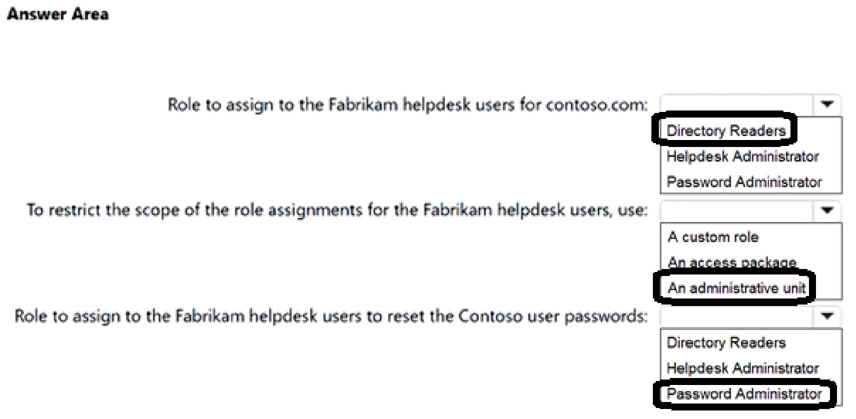
Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com:
- Directory Readers
- Helpdesk Administrator
- Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:
- A custom role
- An access package
- An administrative unit

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:
- Directory Readers
- Helpdesk Administrator
- Password Administrator

Suggested Answer:



Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com:
- [✓ Directory Readers]
- Helpdesk Administrator
- Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:
- A custom role
- An access package
- [✓ An administrative unit]

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:
- Directory Readers
- Helpdesk Administrator
- [✓ Password Administrator]

cl1984 3 months, 1 week ago

The given answers look good to me

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#directory-readers
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#password-administrator

upvoted 1 times

Question #52 *Topic 2*

HOTSPOT

-

You have multiple on-premises Hyper-V hosts that contain virtual machines. The virtual machines run Windows Server 2022.

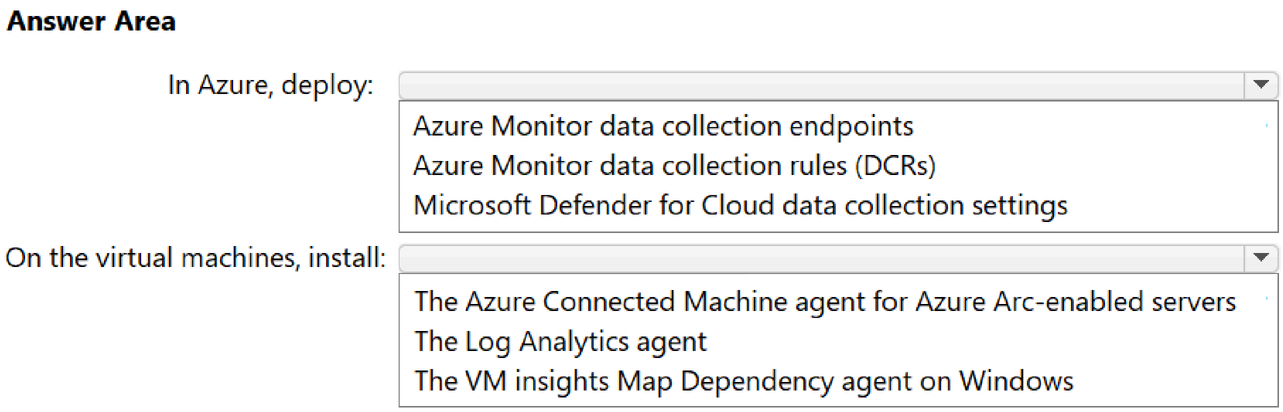
You have an Azure subscription.

You need to recommend a solution to collect Security event logs from the virtual machines by using Microsoft Sentinel. The Solution must meet the following requirements:

- Leverage the Windows Security Events via AMA data connector.
- Ensure that only specific events are collected.
- Minimize costs.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one port.



Answer Area

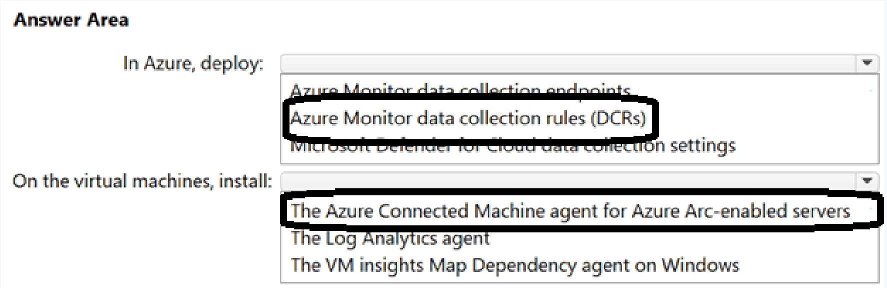
In Azure, deploy:

- Azure Monitor data collection endpoints
- Azure Monitor data collection rules (DCRs)
- Microsoft Defender for Cloud data collection settings

On the virtual machines, install:

- The Azure Connected Machine agent for Azure Arc-enabled servers
- The Log Analytics agent
- The VM insights Map Dependency agent on Windows

Suggested Answer:



Answer Area

In Azure, deploy:

- Azure Monitor data collection endpoints
- [✓ Azure Monitor data collection rules (DCRs)]
- Microsoft Defender for Cloud data collection settings

On the virtual machines, install:

- [✓ The Azure Connected Machine agent for Azure Arc-enabled servers]
- The Log Analytics agent
- The VM insights Map Dependency agent on Windows

424ede1 3 months ago

Data Collection Rule

Log Analytics agent (Now Azure Monitor agent)

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

upvoted 1 times

424ede1 3 months ago

Correct!

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

upvoted 1 times

reyreyg 5 months ago

1. DCR 2. Azure arc now

*Log analytics agent is depreciated *

upvoted 3 times

⊟ **676ae1a** 5 months ago

1.DCR 2.Log analytics agent

upvoted 1 times

Question #53 *Topic 2*

HOTSPOT

-

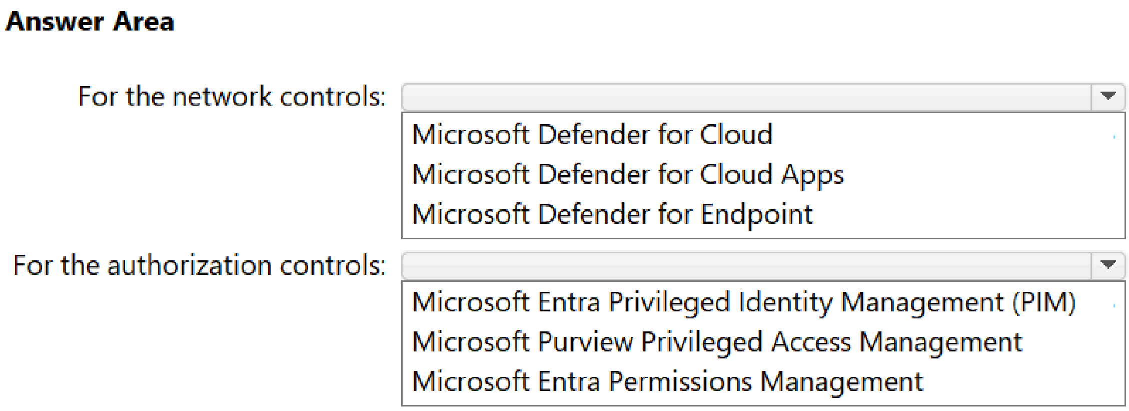
You have an Azure subscription that contains 100 virtual machines. The virtual machines are accessed by using Azure Bastion.

You need to recommend a solution to ensure that only specific users in specific locations can access the virtual machines. The solution must meet the following requirements:

• Restrict access to the virtual machines based on an originating IP address or a connection request by using just-in-time (JIT) VM access network-based controls.
• Restrict access to the virtual machines based on role-based access control (RBAC) role assignments by using JIT VM access authorization controls.

Which Microsoft cloud services should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

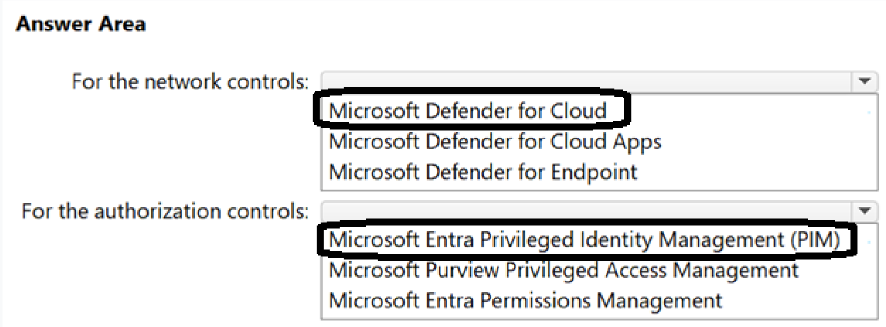


Answer Area

For the network controls:
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint

For the authorization controls:
- Microsoft Entra Privileged Identity Management (PIM)
- Microsoft Purview Privileged Access Management
- Microsoft Entra Permissions Management

Suggested Answer:



Answer Area

For the network controls:
- [✓ Microsoft Defender for Cloud]
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint

For the authorization controls:
- [✓ Microsoft Entra Privileged Identity Management (PIM)]
- Microsoft Purview Privileged Access Management
- Microsoft Entra Permissions Management

Ali96 4 months, 3 weeks ago

For network controls: Microsoft Defender for Cloud

For authorization controls: Microsoft Entra Privileged Identity Management (PIM)

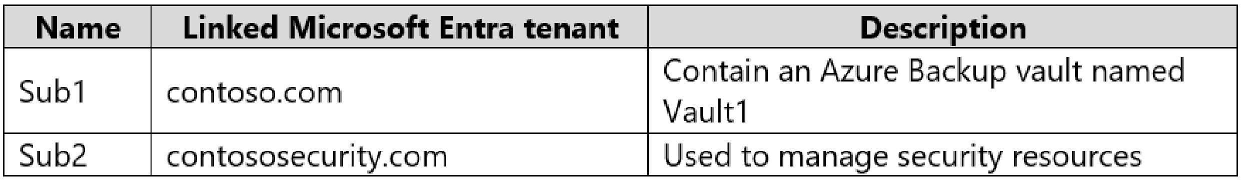
upvoted 1 times

Question #54 Topic 2

HOTSPOT

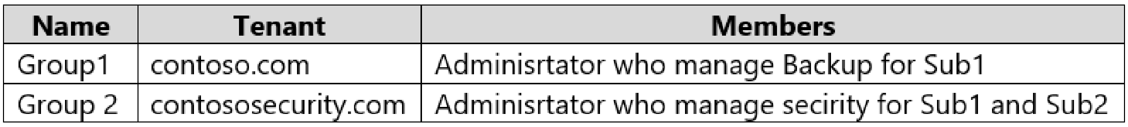
-

You have the Azure subscriptions shown in the following table.



Name	Linked Microsoft Entra tenant	Description
Sub1	contoso.com	Contain an Azure Backup vault named Vault1
Sub2	contososecurity.com	Used to manage security resources

The tenants contain the groups shown in the following table.



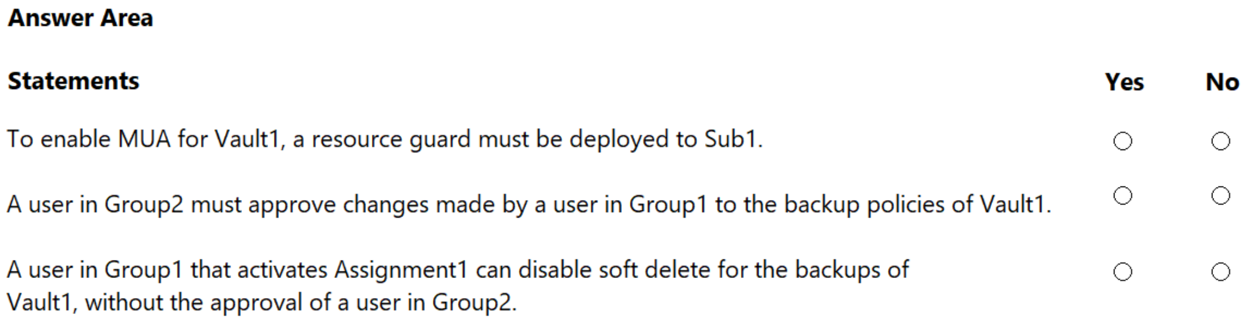
Name	Tenant	Members
Group1	contoso.com	Adminisrtator who manage Backup for Sub1
Group 2	contososecurity.com	Adminisrtator who manage secirity for Sub1 and Sub2

You perform the flowing actions:

- Configure multi-user authorization (MUA) for Vault1 by using a resource guard deployed to Sub2.
- Enable all available MUA controls for Vault1.
- In contoso.com, create a Privileged Identity Management (PIM) assignment named Assignment1.
- Configure Assignment1 to enable Group1 to activate the Contributor role for Vault1.

For each of the following statements, select Yes if the statements is true. Otherwise, select No.

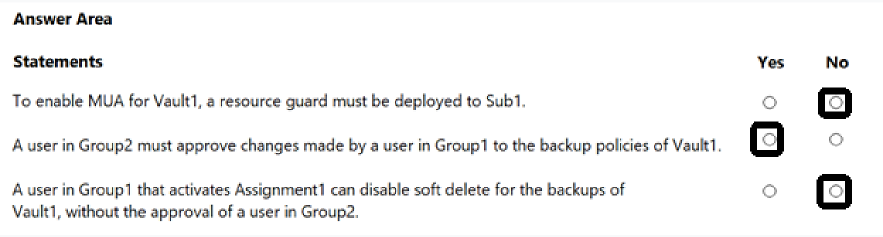
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
To enable MUA for Vault1, a resource guard must be deployed to Sub1.	○	○
A user in Group2 must approve changes made by a user in Group1 to the backup policies of Vault1.	○	○
A user in Group1 that activates Assignment1 can disable soft delete for the backups of Vault1, without the approval of a user in Group2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
To enable MUA for Vault1, a resource guard must be deployed to Sub1.	○	[✓ ○]
A user in Group2 must approve changes made by a user in Group1 to the backup policies of Vault1.	[✓ ○]	○
A user in Group1 that activates Assignment1 can disable soft delete for the backups of Vault1, without the approval of a user in Group2.	○	[✓ ○]

ca7859c 3 days, 4 hours ago

N "You can place Resource Guard in a subscription or tenant different from the one containing the vaults to provide better protection."

Y more than one user approves changes, not just one with the RBAC/access policy

N same logic, another user must approve the change

upvoted 1 times

Saynot 3 months, 3 weeks ago

false, true, false

upvoted 3 times

Question #55 *Topic 2*

HOTSPOT

-

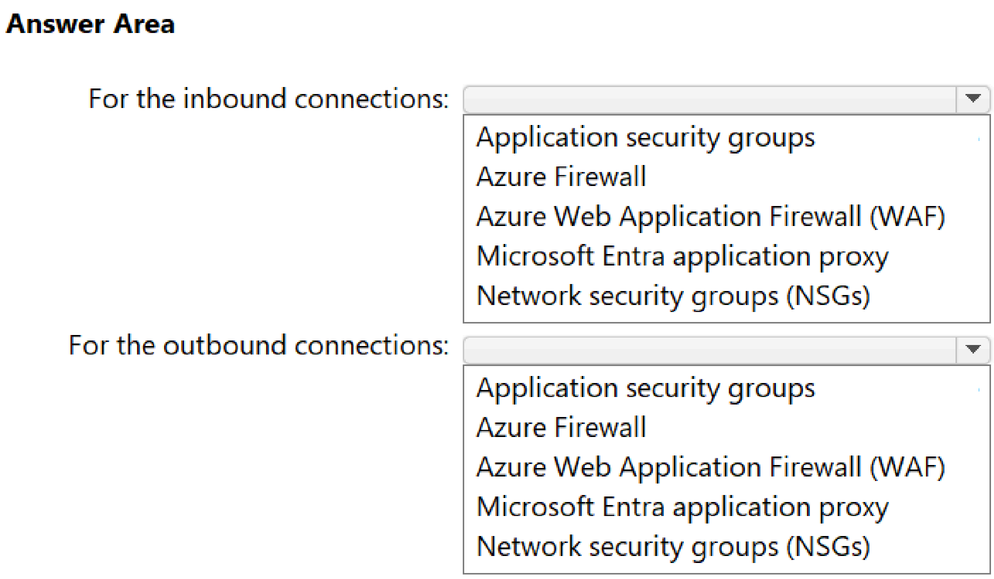
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a 10-node virtual machine scale set that hosts a web search app named App1. Customers access App1 from the internet. The nodes establish outbound HTTP and HTTPS connections to the internet.

You need to recommend a network security solution for App1. The solution must meet the following requirements:

• Inbound connections to App1 that contain security threats specified in the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP) must be blocked.
• Outbound HTTP and HTTPS connections from the virtual machine scale set that contain security threats identified by the Microsoft Defender Threat Intelligence (Defender TI) feed must be blocked.

What should you include in the recommendation? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

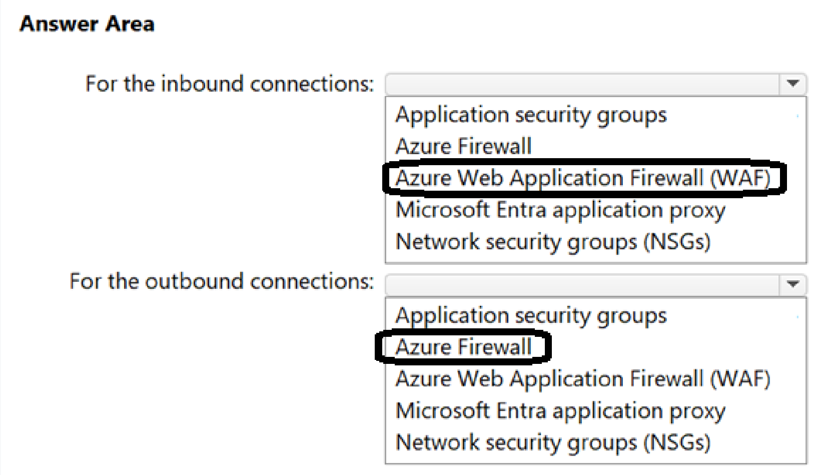


Answer Area

For the inbound connections:
- Application security groups
- Azure Firewall
- Azure Web Application Firewall (WAF)
- Microsoft Entra application proxy
- Network security groups (NSGs)

For the outbound connections:
- Application security groups
- Azure Firewall
- Azure Web Application Firewall (WAF)
- Microsoft Entra application proxy
- Network security groups (NSGs)

Suggested Answer:



Answer Area

For the inbound connections:
- Application security groups
- Azure Firewall
- [✓ Azure Web Application Firewall (WAF)]
- Microsoft Entra application proxy
- Network security groups (NSGs)

For the outbound connections:
- Application security groups
- [✓ Azure Firewall]
- Azure Web Application Firewall (WAF)
- Microsoft Entra application proxy
- Network security groups (NSGs)

jim85 4 months, 4 weeks ago

Looks correct:
a) https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=drs21
b) https://learn.microsoft.com/en-us/azure/firewall-manager/threat-intelligence-settings

upvoted 4 times

Question #56 *Topic 2*

You have a Microsoft Entra tenant named contoso.com.

You have an external partner that has a Microsoft Entra tenant named fabnkam.com.

You need to recommend an identity governance solution for contoso.com that meets the following requirements:

- Enables the users in contoso.com and fabrikam.com to communicate by using shared Microsoft Teams channels
- Manages access to shared Teams channels in contoso.com by using groups in fabrikam.com
- Supports single sign-on (SSO)
- Minimizes administrative effort
- Maximizes security

What should you include in the recommendation?

A. Cross-tenant synchronization

B. Microsoft Entra B2B collaboration

C. B2B direct connect

D. Microsoft Entra Connect Sync

Suggested Answer: *C*

Community vote distribution

B (100%)

424ede1 3 months ago

Selected Answer: C

B2B direct connect requires a mutual trust relationship between two Microsoft Entra organizations to allow access to each other's resources. Both the resource organization and the external organization need to enable B2B direct connect in their cross-tenant access settings. When the trust is established, the B2B direct connect user has single sign-on access to resources outside their organization using credentials from their home Microsoft Entra organization.

https://learn.microsoft.com/en-us/entra/external-id/b2b-direct-connect-overview

upvoted 1 times

AleFerrillo 3 months, 2 weeks ago

Selected Answer: C

"B2B direct connect is a feature of Microsoft Entra External ID that lets you set up a mutual trust relationship with another Microsoft Entra organization for seamless collaboration. This feature currently works with Microsoft Teams shared channels."

https://learn.microsoft.com/en-us/entra/external-id/b2b-direct-connect-overview

upvoted 1 times

Collecting 4 months, 1 week ago

Selected Answer: C

B2B Direct Connect allows seamless collaboration between users in different Microsoft Entra tenants (Contoso and Fabrikam) without requiring guest accounts. It is specifically designed for shared Microsoft Teams channels and enables:

upvoted 1 times

Ali96 4 months, 1 week ago

B2B direct connect is not the correct answer, as it is more related to network connectivity rather than managing shared resources like Teams channels

upvoted 1 times

Er_01 4 months, 3 weeks ago

Selected Answer: C

B2B collaboration involves adding users as guest to contoso. Direct connect allows for access using fabrikam accounts.

upvoted 4 times

Ali96 5 months ago

Selected Answer: B

Microsoft Entra B2B collaboration allows external partners (in this case, fabrikam.com) to securely access resources in contoso.com, including shared Teams channels.

upvoted 1 times

⊟ **676ae1a** 5 months ago

Selected Answer: B

Colaboración B2B de Microsoft Entra

upvoted 1 times

Question #57 *Topic 2*

You have a multicloud environment that contains Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) subscriptions.

You need to discover and review role assignments across the subscriptions.

What should you use?

A. Azure Lighthouse

B. Microsoft Defender for Identity

C. Microsoft Entra ID Governance

D. Microsoft Entra Permissions Management

Suggested Answer: *D*

Community vote distribution

C (50%) D (50%)

Ali96 5 months ago

Selected Answer: D

Microsoft Entra Permissions Management is designed to provide visibility and management of permissions across multiple cloud platforms, including Azure, AWS, and GCP.

upvoted 3 times

tuyi2 5 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/entra/permissions-management/overview

upvoted 2 times

676ae1a 5 months ago

Selected Answer: C

La opción correcta es Gobernanza de identidades de Microsoft Entra

La **Gobernanza de identidades de Microsoft Entra** te permite descubrir y revisar las asignaciones de roles en todas las suscripciones de Azure, AWS y GCP de manera centralizada y eficiente.

upvoted 1 times

Question #58 Topic 2

HOTSPOT

-

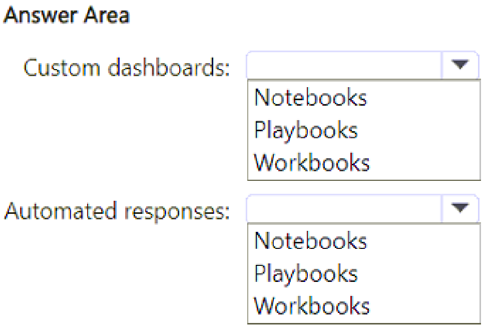
You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1.

You need to configure WS1 to meet the following requirements:

• Create custom dashboards to visualize the workload of security analysts that use Microsoft Sentinel.
• Enable automated responses for the security alerts generated by Microsoft Sentinel analytics rules.

What should you use for each requirement? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

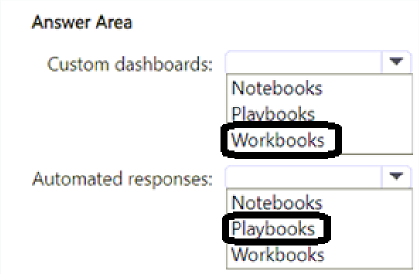


Answer Area

Custom dashboards:
Notebooks
Playbooks
Workbooks

Automated responses:
Notebooks
Playbooks
Workbooks

Suggested Answer:



Answer Area

Custom dashboards:
Notebooks
Playbooks
[✓ Workbooks]

Automated responses:
Notebooks
[✓ Playbooks]
Workbooks

cl1984 3 months, 1 week ago

Given answers are correct:

Workbooks
Playbooks

https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/sentinel/automation/automate-responses-with-playbooks

upvoted 4 times

Question #59 *Topic 2*

You have multiple Azure subscriptions that each contains multiple resource groups.

You need to identify the privileged role assignments in each subscription and any associated security risks. The solution must minimize administrative effort.

What should you use?

A. access reviews in Privileged Identity Management (PIM)

B. access reviews in Microsoft Entra ID Identity Governance

C. Microsoft Defender External Attack Surface Management (Defender EASM) discovery

D. the Analytics dashboard in Microsoft Entra Permissions Management

Suggested Answer: *A*

Community vote distribution

D (100%)

424ede1 3 months ago

Selected Answer: D

D. the Analytics dashboard in Microsoft Entra Permissions Management
https://learn.microsoft.com/en-us/entra/permissions-management/usage-analytics-users#apply-filters-by-identity-type

upvoted 1 times

Gagi79 1 month, 3 weeks ago

https://techcommunity.microsoft.com/blog/microsoft-entra-blog/important-change-announcement-microsoft-entra-permissions-management-end-of-sale/4399382

upvoted 1 times

sweetykaur 4 months, 3 weeks ago

Selected Answer: A

A. Microsoft Defender for Identity

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection) can help you mark sensitive groups and monitor changes to these groups. By integrating it with Microsoft Sentinel, you can set up alerts to be triggered whenever there are changes to Group1, ensuring that any modifications are promptly detected and addressed.

upvoted 2 times

Gagi79 1 month, 3 weeks ago

MDI is for on-prem...

upvoted 1 times

Ali96 5 months ago

Selected Answer: A

A. access reviews in Privileged Identity Management (PIM)

upvoted 3 times

AlbertE1nstein 5 months ago

Selected Answer: D

D. the Analytics dashboard in Microsoft Entra Permissions Management

upvoted 2 times

oscarpopi 5 months ago

Selected Answer: D

Identify the p[riviledged role in multiple subscriptions, Access Reviews does not do that. EPM does.

upvoted 4 times

Question #60 *Topic 2*

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a hybrid deployment between a Microsoft Exchange Server 2019 organization and an Exchange Online tenant. The AD DS domain contains a group named Group1. Group1 is a member of the Organization Management role group for the Exchange deployment.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender.

You have an Azure subscription that uses Microsoft Sentinel.

You need to recommend a solution to ensure that Group1 is marked as a sensitive group and that any changes made to Group1 raises an alert in Microsoft Sentinel. The solution must minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Defender for Identity

B. Microsoft Entra ID Protection

C. Microsoft Entra Privileged Identity Management (PIM)

D. Microsoft Defender for Office 365

Suggested Answer: *A*

Community vote distribution

C (50%) A (50%)

oscarpopi 4 months, 4 weeks ago

Selected Answer: A

MDI is the correct answer, Exchange Hybrid, means OM group is being synced from the on-prem. and it needs to be protected .

upvoted 1 times

jim85 4 months, 4 weeks ago

Selected Answer: A

Microsoft Defender for Identity is a cloud-based security solution that helps secure your identity monitoring across your organization.

Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.

upvoted 1 times

676ae1a 5 months ago

Selected Answer: A

Respuesta correcta

upvoted 2 times

Ali96 5 months ago

Selected Answer: C

C. Microsoft Entra Privileged Identity Management (PIM)

upvoted 1 times

Question #61

Topic 2

HOTSPOT

-

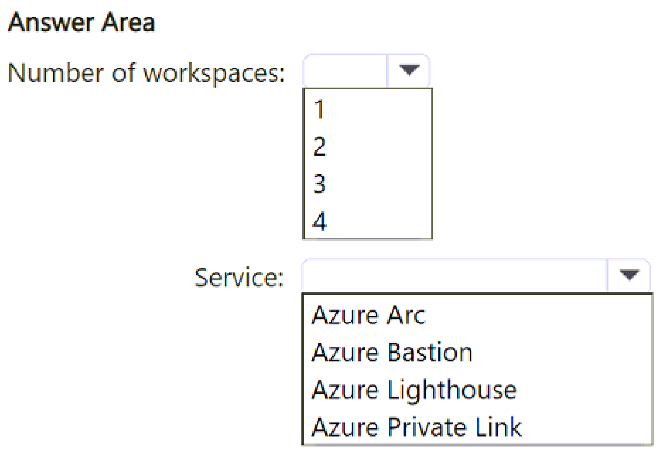
You have four Azure subscriptions named Sub1, Sub2, Sub3, and Sub4. Each subscription has a unique Microsoft Entra tenant that is linked to a Microsoft 365 subscription. Sub1 contains a user named User1.

You plan to implement Microsoft Sentinel.

You need to ensure that User1 can monitor Microsoft Entra ID events and Microsoft 365 events for Sub2, Sub3, and Sub4 by using Microsoft Sentinel. The solution must minimize administrative effort.

What is the minimum number of Microsoft Sentinel workspaces you should create, and which Azure service should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

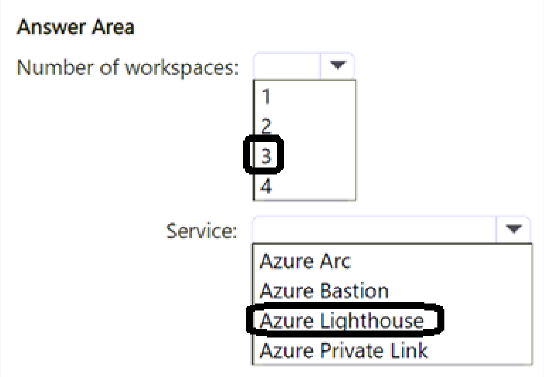


Answer Area

Number of workspaces:
1
2
3
4

Service:
Azure Arc
Azure Bastion
Azure Lighthouse
Azure Private Link

Suggested Answer:



Answer Area

Number of workspaces:
1
2
[✓ 3]
4

Service:
Azure Arc
Azure Bastion
[✓ Azure Lighthouse]
Azure Private Link

⊟ **ca7859c** 3 days, 4 hours ago

1 Workspace is enough

Lighthouse

upvoted 1 times

⊟ **SnowmanPapi** 1 month, 2 weeks ago

1 workspace and Azure Lighthouse. As the questions says, this is a single Entra ID tenant which means only a single workspace is needed, as you would integrate Microsoft XDR to Sentinel. All the subscriptions are tied to the same Entra ID tenant.

upvoted 1 times

⊟ **SnowmanPapi** 1 month, 1 week ago

Correction. It is 3 workspaces. Each sub has a unique tenant.

upvoted 1 times

⊟ **6c0ca3d** 1 month, 2 weeks ago

To centralize management, you can use Azure Lighthouse to monitor multiple Sentinel workspaces from a single SOC environment.

1 workspace

services: lighthouse

upvoted 1 times

⊟ **Sails71** 2 months, 2 weeks ago

A single workspace can be used to monitor events across multiple subscriptions and tenants, reducing administrative effort - 1 Workspace & Azure Lighthouse.

upvoted 2 times

⊟ **Collecting** 4 months, 1 week ago

Each Microsoft Sentinel workspace is tied to a SINGLE Microsoft Entra tenant.

Answers:

Number of workspaces: 3

Service: Lighthouse

upvoted 4 times

⊟ **Coolcat2023** 3 months, 1 week ago

Why 3 workspaces ?

upvoted 2 times

⊟ **tuyi2** 4 months, 3 weeks ago

1 workspace

Azure Lighthouse

upvoted 4 times

⊟ **Ali96** 5 months ago

1, Azure Lighthouse

upvoted 3 times

Question #62 *Topic 2*

You have a Microsoft 365 subscription that contains 1,000 users and a group named Group1. All the users have Windows 11 devices. The users sign in to their devices by using their Microsoft Entra account. The users do NOT have administrative rights to their devices.

The members of Group1 remotely assist the users by taking control of user sessions. The remote control sessions run in the security context of the users they are assisting.

You need to recommend a solution that will enable the Group1 members to run apps that require administrative rights to the users' devices. The solution must ensure that the apps are run in the context of each signed-in standard user.

What should you include in the recommendation?

A. Windows Local Administrator Password Solution (Windows LAPS)

B. Microsoft Entra Permissions Management

C. Microsoft Intune Endpoint Privilege Management

D. Privileged Identity Management (PIM) in Microsoft Entra ID

Suggested Answer: *C*

Community vote distribution

C (100%)

AleFerrillo 3 months, 2 weeks ago

Selected Answer: C

"With Microsoft Intune Endpoint Privilege Management (EPM) your organization’s users can run as a standard user (without administrator rights) and complete tasks that require elevated privileges"
https://learn.microsoft.com/en-us/mem/intune-service/protect/epm-overview

upvoted 3 times

676ae1a 5 months ago

Selected Answer: C

Respuesta correcta

upvoted 2 times

Ali96 5 months ago

Selected Answer: C

C. Microsoft Intune Endpoint Privilege Management.

upvoted 2 times

Question #63 *Topic 2*

HOTSPOT

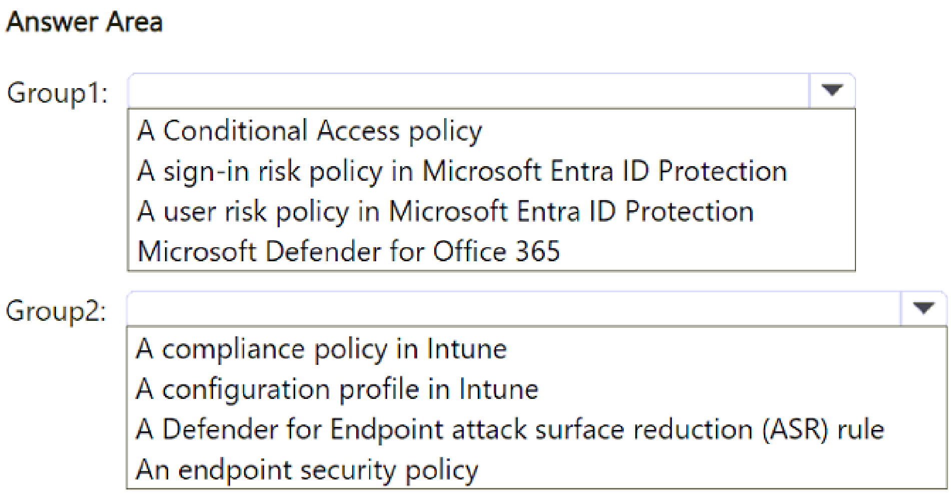
-

You have a Microsoft 365 subscription that contains 1,000 users and two groups named Group1 and Group2. All the users have devices that are onboarded to Microsoft Intune and Microsoft Defender for Endpoint. Group1 manages Microsoft Entra and Microsoft 365 services. Group2 manages Intune and Defender for Endpoint.

You need to recommend a solution to prevent users from connecting to Microsoft 365 services from devices that have encryption disabled.

What should you recommend implementing for each group? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

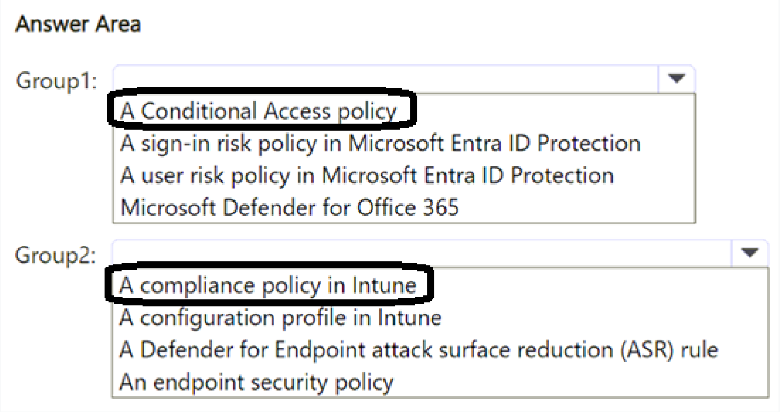


Answer Area

Group1:
- A Conditional Access policy
- A sign-in risk policy in Microsoft Entra ID Protection
- A user risk policy in Microsoft Entra ID Protection
- Microsoft Defender for Office 365

Group2:
- A compliance policy in Intune
- A configuration profile in Intune
- A Defender for Endpoint attack surface reduction (ASR) rule
- An endpoint security policy

Suggested Answer:



Answer Area

Group1:
- [✓ A Conditional Access policy]
- A sign-in risk policy in Microsoft Entra ID Protection
- A user risk policy in Microsoft Entra ID Protection
- Microsoft Defender for Office 365

Group2:
- [✓ A compliance policy in Intune]
- A configuration profile in Intune
- A Defender for Endpoint attack surface reduction (ASR) rule
- An endpoint security policy

676ae1a 5 months ago

Respuesta correcta

upvoted 3 times

Ali96 5 months ago

A Conditional Access policy

Group2: A compliance policy in Intune

upvoted 4 times

Question #64 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app registrations in the Microsoft Entra tenant

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. app protection policies in Microsoft Endpoint Manager

D. application control policies in Microsoft Defender for Endpoint

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **Ali96** 5 months ago

Selected Answer: D

D. application control policies in Microsoft Defender for Endpoint

upvoted 2 times

Question #65 *Topic 2*

You have a Microsoft 365 subscription that contains 1,000 users. Each user is assigned a Microsoft 365 E5 license.

The subscription uses sensitivity labels to classify corporate documents. All the users have Windows 11 devices that are onboarded to Microsoft Defender for Endpoint and are configured to sync files to Microsoft OneDrive.

You need to prevent the users from uploading the documents from OneDrive to external websites.

What should you include in the solution?

A. Microsoft Purview Information Protection

B. Microsoft Purview data loss prevention (DLP)

C. web content filtering in Defender for Endpoint

D. an endpoint security policy

Suggested Answer: *B*

Community vote distribution

B (100%)

676ae1a 5 months ago

Selected Answer: B

La funcionalidad DLP de Microsoft Purview permite crear políticas que previenen la transferencia de información sensible o clasificada a ubicaciones no autorizadas, como sitios web externos

upvoted 2 times

Ali96 5 months ago

Selected Answer: B

B. Microsoft Purview data loss prevention (DLP).

upvoted 2 times

Question #1 *Topic 3*

You have Microsoft Defender for Cloud assigned to Azure management groups.
You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation.
Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel threat intelligence workbooks

B. Microsoft Sentinel notebooks

C. threat intelligence reports in Defender for Cloud

D. workload protections in Defender for Cloud

Suggested Answer: *AC*
A: Workbooks provide insights about your threat intelligence
Workbooks provide powerful interactive dashboards that give you insights into all aspects of Microsoft Sentinel, and threat intelligence is no exception. You can use the built-in Threat Intelligence workbook to visualize key information about your threat intelligence, and you can easily customize the workbook according to your business needs. You can even create new dashboards combining many different data sources so you can visualize your data in unique ways. Since
Microsoft Sentinel workbooks are based on Azure Monitor workbooks, there is already extensive documentation available, and many more templates.
C: What is a threat intelligence report?
Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.
Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:
Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
Campaign Report: focuses on details of specific attack campaigns.
Threat Summary Report: covers all of the items in the previous two reports.
This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future.
Incorrect:
Not B: When to use Jupyter notebooks
While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data.
For example, use notebooks to:
Perform analytics that aren't provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features
Create data visualizations that aren't provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees
Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.
Not D: Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. For example, you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Community vote distribution

AC (100%)

⊟ **zts** Highly Voted 2 years, 9 months ago

Selected Answer: AC

answer is correct.

upvoted 12 times

⊟ **Alex_Burlachenko** Highly Voted 2 years, 10 months ago

correct ans

upvoted 6 times

SMHcalicut Most Recent 3 months, 1 week ago

Selected Answer: CD

A. Microsoft Sentinel threat intelligence workbooks:
While workbooks in Microsoft Sentinel are valuable for visualizing and analyzing data, they do not provide direct remediation suggestions or detailed security event information. They're more for interactive investigation rather than detailed threat intelligence or actionable security event context.

B. Microsoft Sentinel notebooks:
Notebooks in Microsoft Sentinel are useful for custom queries and analysis but do not provide out-of-the-box detailed information or suggestions for remediation of security events. They are primarily a tool for analysts to run custom queries and visualize data in a flexible format.

upvoted 2 times

Cyko 4 months, 3 weeks ago

Selected Answer: BD

I think B and D are correct

upvoted 2 times

sweetykaur 4 months, 3 weeks ago

Selected Answer: BC

Microsoft Sentinel notebooks: Notebooks allow you to analyze and investigate security events in more detail, providing a flexible environment for data exploration and threat hunting. They can also provide insights and remediation suggestions based on the analyzed data.

Threat intelligence reports in Defender for Cloud: These reports offer detailed information about security threats, including context and remediation recommendations. By leveraging threat intelligence reports, you can gain a better understanding of the security events and take appropriate actions to address them.

upvoted 1 times

Delatalase 6 months, 2 weeks ago

Selected Answer: BC

Microsoft Sentinel notebooks: These provide detailed analysis and investigation capabilities, allowing you to explore security events and gain insights into potential threats and remediation steps.
Threat intelligence reports in Defender for Cloud: These reports offer valuable information about security threats and vulnerabilities, along with recommendations for mitigating those threats

upvoted 1 times

whh13 6 months, 3 weeks ago

Selected Answer: CD

A is not correct.
While Microsoft Sentinel provides workbooks for visualizing and analyzing threat intelligence data, these workbooks focus more on providing insights into your organization's threat landscape rather than offering specific remediation suggestions during alert triage. Sentinel workbooks are useful for monitoring and visualizing threat data but are not directly focused on remediation actions.

upvoted 2 times

yakinikuman 1 year, 1 month ago

Can't we achieve this with D:Defender for Cloud as well?
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workload-protections-dashboard

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence#add-threat-indicators-to-microsoft-sentinel-with-the-microsoft-defender-threat-intelligence-data-connector
Bring high fidelity indicators of compromise (IOC) generated by Microsoft Defender Threat Intelligence (MDTI) into your Microsoft Sentinel workspace. The MDTI data connector ingests these IOCs with a simple one-click setup. Then monitor, alert and hunt based on the threat intelligence in the same way you utilize other feeds.

upvoted 5 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 4 times

⊟ **zellck** 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence#introduction-to-threat-intelligence

For SIEM solutions like Microsoft Sentinel, the most common forms of CTI are threat indicators, also known as Indicators of Compromise (IoC) or Indicators of Attack (IoA). Threat indicators are data that associate observed artifacts such as URLs, file hashes, or IP addresses with known threat activity such as phishing, botnets, or malware. This form of threat intelligence is often called tactical threat intelligence because it's' applied to security products and automation in large scale to detect potential threats to an organization and protect against them. Use threat indicators in Microsoft Sentinel, to detect malicious activity observed in your environment and provide context to security investigators to inform response decisions.

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports#what-is-a-threat-intelligence-report

When Defender for Cloud identifies a threat, it triggers a security alert, which contains detailed information regarding the event, including suggestions for remediation. To help incident response teams investigate and remediate threats, Defender for Cloud provides threat intelligence reports containing information about detected threats.

upvoted 1 times

⊟ **uffman** 2 years, 2 months ago

Selected Answer: AC

Correct.

upvoted 1 times

⊟ **tester18128075** 2 years, 9 months ago

A and C

upvoted 4 times

Question #2 *Topic 3*

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions.
You are evaluating the security posture of the customer.
You discover that the AKS resources are excluded from the secure score recommendations.
You need to produce accurate recommendations and update the secure score.
Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Defender plans.

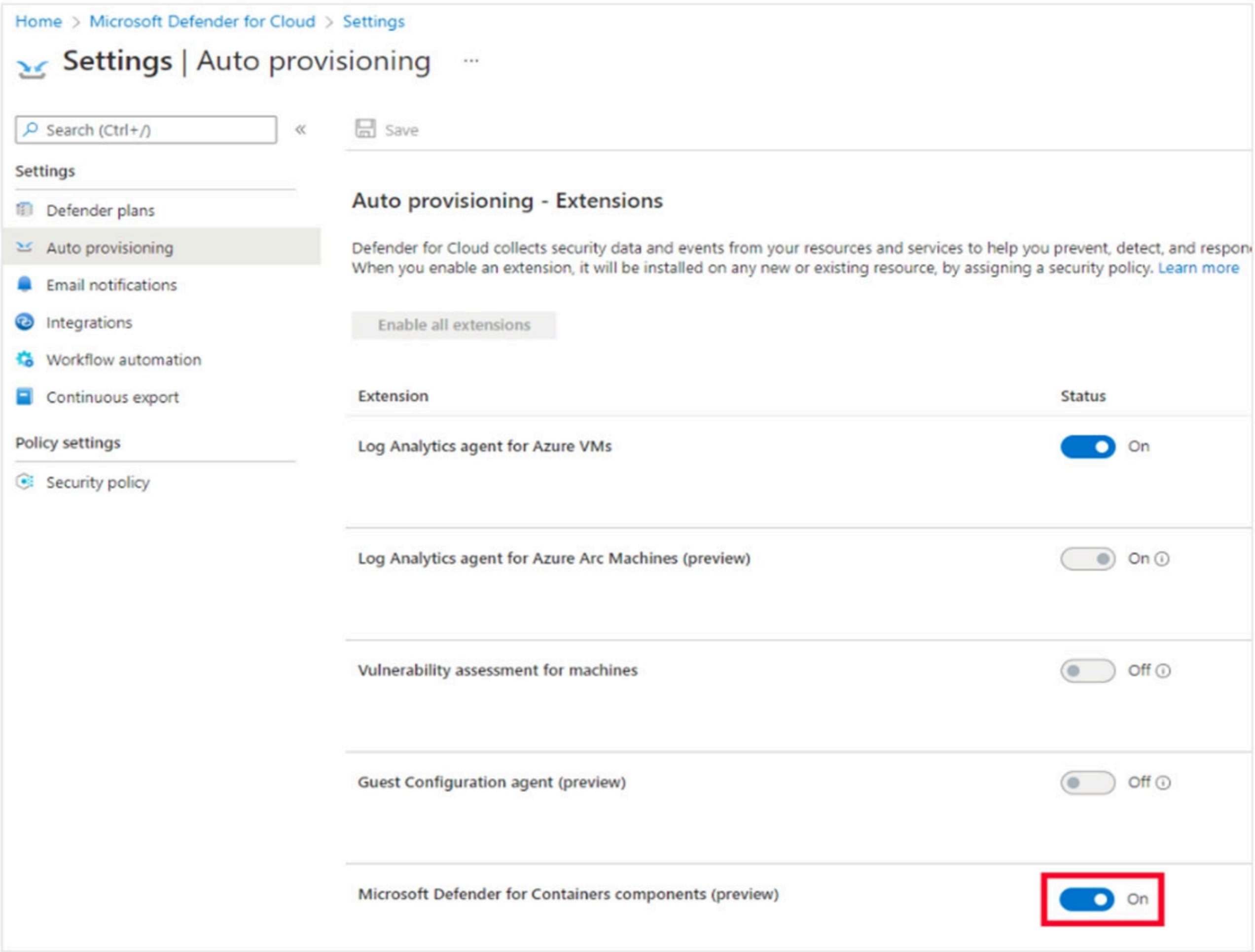
B. Configure auto provisioning.

C. Add a workflow automation.

D. Assign regulatory compliance policies.

E. Review the inventory.

Suggested Answer: *BD*
D: How are regulatory compliance standards represented in Defender for Cloud?
Industry standards, regulatory standards, and benchmarks are represented in Defender for Cloud's regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.
To see compliance data mapped as assessments in your dashboard, add a compliance standard to your management group or subscription from within the
Security policy page.
When you've assigned a standard or benchmark to your selected scope, the standard appears in your regulatory compliance dashboard with all associated compliance data mapped as assessments.
B: Configure Defender for Containers components
If you disabled any of the default protections when you enabled Microsoft Defender for Containers, you can change the configurations and reenable them via auto provisioning.
1. To configure the Defender for Containers components:
2. Sign in to the Azure portal.
3. Navigate to Microsoft Defender for Cloud > Environment settings.
4. Select the relevant subscription.
5. From the left side tool bar, select Auto provisioning.
6. Ensure that Microsoft Defenders for Containers components (preview) is toggled to On.



Settings | Auto provisioning ...

Auto provisioning - Extensions

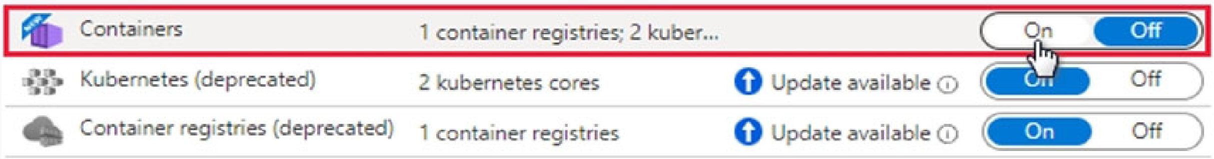
Defender for Cloud collects security data and events from your resources and services to help you prevent, detect, and respon
When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy. Learn more

Extension	Status
Log Analytics agent for Azure VMs	On
Log Analytics agent for Azure Arc Machines (preview)	On ⓘ
Vulnerability assessment for machines	Off ⓘ
Guest Configuration agent (preview)	Off ⓘ
Microsoft Defender for Containers components (preview)	On

Incorrect:

Not A: When you enable Microsoft Defender for Containers, Azure Kubernetes Service clusters, and Azure Arc enabled Kubernetes clusters (Preview) protection are both enabled by default.

To upgrade to Microsoft Defender for Containers, open the Defender plans page in the portal and enable the new plan:



Containers	1 container registries; 2 kuber...		On / Off
Kubernetes (deprecated)	2 kubernetes cores	Update available ⓘ	On / Off
Container registries (deprecated)	1 container registries	Update available ⓘ	On / Off

Not C: No need for automation.

Note: Automate responses to Microsoft Defender for Cloud triggers.

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can.

Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Community vote distribution

AB (73%) AD (15%) 13%

⊟ **Alex_Burlachenko** Highly Voted 2 years, 10 months ago

I would select A and B

upvoted 45 times

⊟ **foxtrott** Highly Voted 2 years, 9 months ago

Selected Answer: AB

I like A and B for this one - enable the defender for containers plan - then ensure it deploys to your container resources with auto provision.

upvoted 34 times

⊟ **AWSPro24** 5 months, 1 week ago

Defender for Containers is agentless:

Agentless discovery for Kubernetes - provides zero footprint, API-based discovery of your Kubernetes clusters, configurations, and deployments.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction

upvoted 1 times

orrery Most Recent 11 months, 2 weeks ago

Selected Answer: AD

I would select A and D.
Enable Defender plans: By enabling Defender plans in Microsoft Defender for Cloud, you can provide security assessments and recommendations for all resources, including AKS resources.
Assign regulatory compliance policies: By assigning regulatory compliance policies, AKS resources will be evaluated according to security standards and reflected in the Secure Score.

B is for setting up automatic provisioning of resources and is not directly involved in updating the Secure Score.
E also is not directly involved in updating the Secure Score.

upvoted 2 times

JHJ44 1 year, 2 months ago

Selected Answer: AE

Enable Defender Plans:
Enable Defender plans for your AKS resources.
Defender plans provide security recommendations and insights specific to the services you use.
By enabling Defender plans, you ensure that AKS is included in the secure score calculations.
Points: 1
Review the Inventory:
Ensure that all AKS resources are correctly identified and included in your inventory.
Review the list of resources to verify their inclusion.
Any missing resources should be added to the inventory.
Points: 1

upvoted 2 times

Jonny_Cage 1 year, 5 months ago

To produce accurate recommendations and update the secure score for AKS resources in Microsoft Defender for Cloud, you should:

A. Enable Defender plans: This will ensure that the AKS resources are being monitored by Microsoft Defender for Cloud, which will include them in the secure score recommendations.

D. Assign regulatory compliance policies: This will apply the necessary compliance controls against the AKS resources, which can help in identifying security configurations that are not in compliance with the required standards, thus affecting the secure score.

upvoted 3 times

sbnpj 1 year, 11 months ago

Selected Answer: AB

I would go with A&B

upvoted 4 times

Ario 1 year, 12 months ago

Selected Answer: AE

By enabling Defender plans and reviewing the inventory, you can ensure that the AKS resources are properly evaluated, and their security posture is reflected in the secure score.

upvoted 4 times

MS_ExamsRule 2 years ago

Although by default Enabling the Defender plan also configures auto-provisioning, to align with CAF you would then configure auto-provisioning to use a centralised rather than the default log analytics workspace.
So its A&B

upvoted 4 times

zellck 2 years, 1 month ago

Selected Answer: AB

AB is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-enable

upvoted 6 times

⊟ **zellck** 2 years, 1 month ago

A streamlined, frictionless, process lets you use the Azure portal pages to enable the Defender for Cloud plan and setup auto provisioning of all the necessary components for defending your Kubernetes clusters at scale.

upvoted 1 times

⊟ **Tictactoe** 2 years, 1 month ago

AE CORRECT

upvoted 2 times

⊟ **alifrancos** 2 years, 2 months ago

Selected Answer: AD

For me it's A & D,
it's simple, first you should active the Defender Plan, and microsoft say that auto provisioned id activated by default, so, we cannot shoose it because it's given by microsoft,
and for the secure score, we should have policy defenition assigned, else we will not increase secure score

upvoted 3 times

⊟ **Gurulee** 2 years, 2 months ago

Selected Answer: AB

Since AKS was observed as excluded, it needs to be re-enabled and auto provisioned.

upvoted 6 times

⊟ **vitodobra** 2 years, 3 months ago

Selected Answer: AE

Para producir recomendaciones precisas y actualizar la puntuación segura en Microsoft Defender para la nube en relación con los recursos de AKS, se recomienda:

A. Habilitar los planes de Defender para la suscripción de Azure que contiene los recursos de AKS. Esto permitirá que Microsoft Defender para la nube recolecte datos de seguridad de los recursos y proporcionará recomendaciones específicas de seguridad.

E. Revisar el inventario de recursos de AKS en cada suscripción de Azure y asegurarse de que se están siguiendo las mejores prácticas de seguridad. Esto ayudará a identificar cualquier problema de seguridad que pueda existir y tomar medidas para abordarlos.

upvoted 1 times

⊟ **josh_josh** 2 years, 3 months ago

Selected Answer: AE

The correct answer is A and E. No one can counter this statement. prove me wrong

upvoted 2 times

⊟ **ChaBum** 2 years, 3 months ago

so, you're guessing!

upvoted 2 times

⊟ **Fal991l** 2 years, 3 months ago

Selected Answer: AE

The two actions that should be recommended in Microsoft Defender for Cloud to produce accurate recommendations and update the secure score are:

A. Enable Defender plans: Enabling Defender plans for Azure Kubernetes Service will enable the Defender for Kubernetes solution to collect and analyze security events and provide recommendations for improving the security posture of the AKS resources. Defender for Kubernetes integrates with Azure Security Center and Azure Monitor to provide a unified view of security posture and insights.

E. Review the inventory: Reviewing the inventory in Microsoft Defender for Cloud will enable you to identify all the AKS resources and Docker images deployed across the four Azure subscriptions. This will help you assess the security posture of the resources, identify potential vulnerabilities and misconfigurations, and prioritize remediation actions.

upvoted 7 times

⊟ **Fal991l** 2 years, 3 months ago

Option B (Configure auto provisioning), option C (Add a workflow automation), and option D (Assign regulatory compliance policies) are not directly related to addressing the issue of excluded AKS resources from secure score recommendations. These options may be helpful in other scenarios, such as automating remediation actions or ensuring compliance with specific regulations. However, for the given scenario, enabling Defender plans and reviewing the inventory are the most relevant actions.

upvoted 2 times

Fal991l 2 years, 3 months ago

That's from ChatGPT. Does it sound interesting?

upvoted 1 times

Gurulee 2 years, 4 months ago

Tricky…I can understand B,D. “ When you enable Microsoft Defender for Containers, Azure Kubernetes Service clusters, and Azure Arc enabled Kubernetes clusters (Preview) protection are both enabled by default.”

upvoted 1 times

Gurulee 2 years, 2 months ago

After reviewing closer, since AKS was found excluded, my answer would be A, B

upvoted 3 times

awssecuritynewbie 2 years, 4 months ago

Selected Answer: AB

A and B for sure! I have tested it in the lab trust me

upvoted 6 times

Question #3 *Topic 3*

Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks.
The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:
✑ Prevent exposing the public IP addresses of the virtual machines.
✑ Provide the ability to connect without using a VPN.
✑ Minimize costs.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a hub and spoke network by using virtual network peering.

B. Deploy Azure Bastion to each virtual network.

C. Deploy Azure Bastion to one virtual network.

D. Create NAT rules and network rules in Azure Firewall.

E. Enable just-in-time VM access on the virtual machines.

Suggested Answer: *AC*
Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
Incorrect:
Not B: Two Azure Bastions would increase the cost.
Reference:
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

Community vote distribution
AC (90%) 10%

PlumpyTumbler Highly Voted 👍 2 years, 10 months ago
Selected Answer: AC
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion
upvoted 26 times

Alex_Burlachenko Highly Voted 👍 2 years, 10 months ago
correct answer (so good job Guys!)
upvoted 14 times

ca7859c Most Recent 🕓 3 days, 4 hours ago
Selected Answer: AC
Correct.
Hub & spoke
Deploy bastion for the hub vnet
Then do network peering from the hub vnet with all the spokes so they are all treated as one vnet and you'll be paying and deploying a single bastion
upvoted 1 times

JHJ44 1 year, 2 months ago
Selected Answer: BE
Deploy Azure Bastion: Azure Bastion is a secure and convenient way to access Azure VMs without exposing public IP addresses. It uses TLS encryption and firewall traversal for RDP connections, ensuring traffic security. By deploying Azure Bastion, you can connect to your VMs directly from the Azure portal using a web browser, eliminating the need for VPNs and minimizing costs. You can configure Azure Bastion for each virtual network or use a single instance for multiple virtual networks.

Enable just-in-time VM access: By enabling just-in-time VM access, you can restrict RDP or SSH access to your VMs based on specific conditions (such as time window and source IP). This feature enhances security by reducing exposure to potential attacks. It allows authorized users to request access to VMs only when needed, minimizing the attack surface and adhering to the principle of least privilege

upvoted 4 times

Onimole 10 months, 1 week ago

bastion is expensive

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: BE

By deploying Azure Bastion to each virtual network and enabling JIT VM access on the virtual machines, you can provide the developers with secure and convenient access to the virtual machines over SSL from the Azure portal, while also meeting the requirements of preventing public IP exposure, avoiding the use of a VPN, and minimizing costs.

upvoted 1 times

edurakhan 2 years, 1 month ago

Exam 5/25/2023

upvoted 3 times

zellck 2 years, 1 month ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

upvoted 4 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 2 times

Ajdlfasudfo0 2 years, 4 months ago

Selected Answer: AC

This seems the only logical combination.

upvoted 1 times

awssecuritynewbie 2 years, 4 months ago

Selected Answer: AC

Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.

Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Incorrect:

Not B: Two Azure Bastions would increase the cos

upvoted 2 times

JeeBi 2 years, 5 months ago

Why not C and E? Because E costs more? It would be safer...

upvoted 1 times

walkaway 2 years, 5 months ago

Then you will need two different Azure Bastion hosts.

upvoted 2 times

tester18128075 2 years, 9 months ago

A and C is cost optimal solution

upvoted 4 times

HardcodedCloud 2 years, 9 months ago

Selected Answer: AC

Perfect answer

upvoted 7 times

Question #4 *Topic 3*

HOTSPOT -

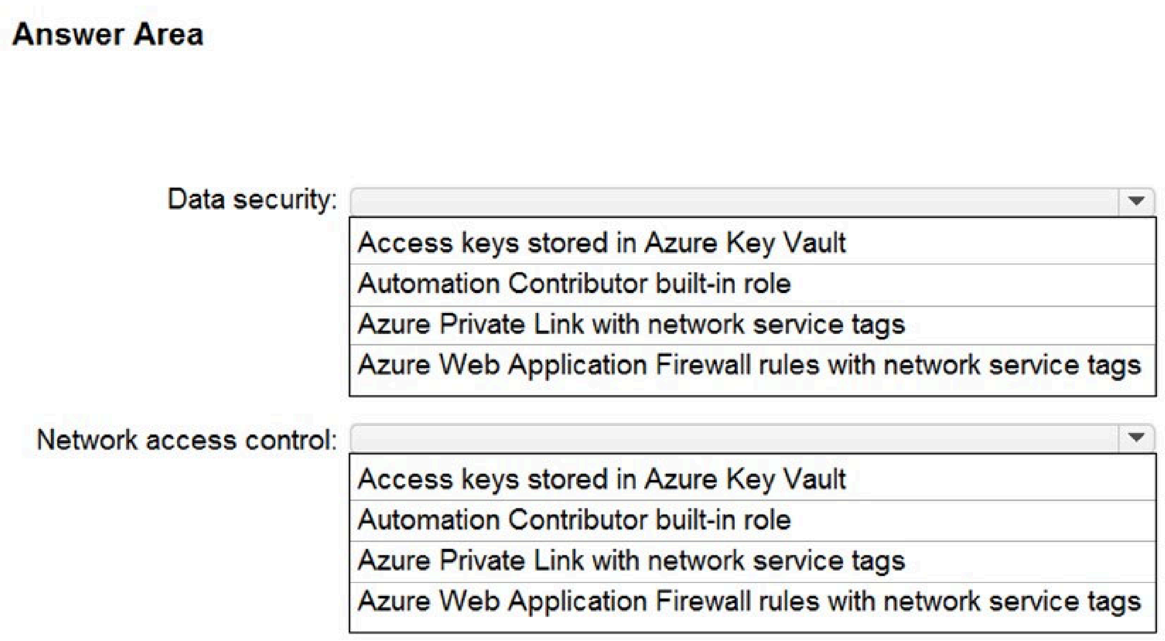
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

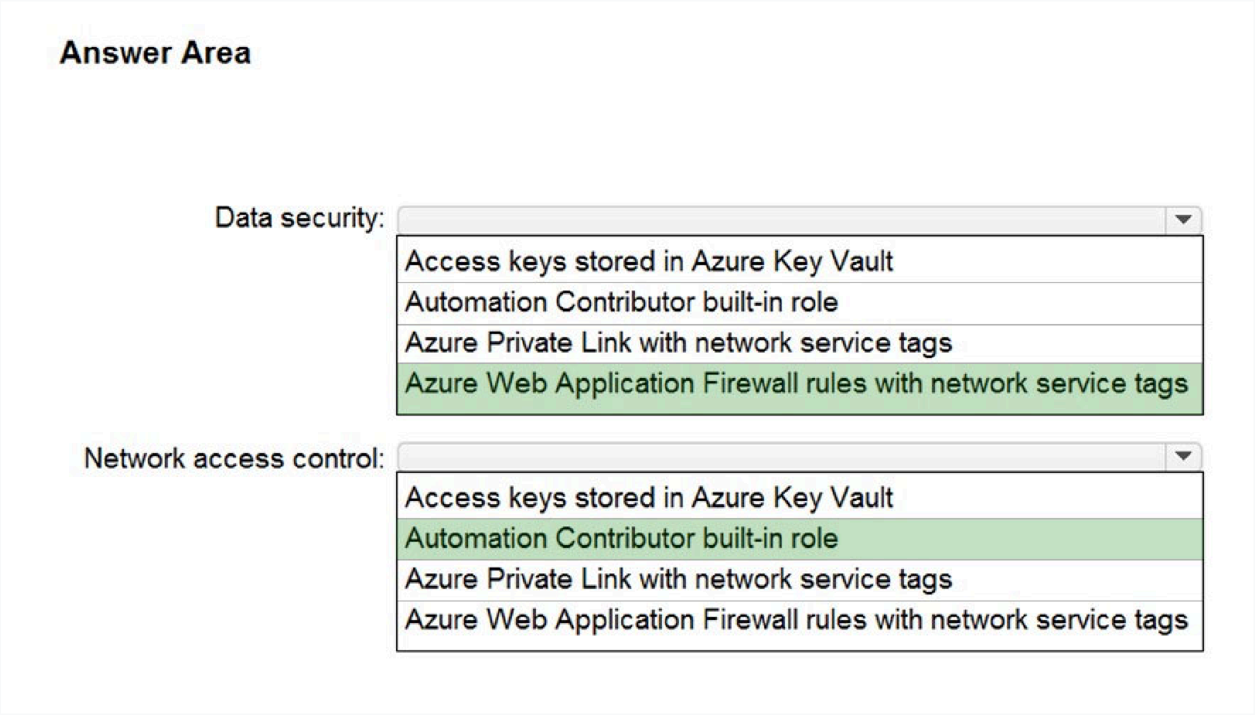


Answer Area

Data security:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Network access control:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Suggested Answer:



Answer Area

Data security:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- [✓ Azure Web Application Firewall rules with network service tags]

Network access control:
- Access keys stored in Azure Key Vault
- [✓ Automation Contributor built-in role]
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Box 1: Azure Web Application Firewall with network service tags

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to define network access controls on network security groups, Azure Firewall, and user-defined routes.

Incorrect:

* Not Azure private link with network service tags

Network service tags are not used with Private links.

Box 2: Automation Contributor built-in role

The Automation Contributor role allows you to manage all resources in the Automation account, except modifying other user's access permissions to an

Automation account.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control

Alex_Burlachenko Highly Voted 👍 2 years, 10 months ago

wrong one, I would select - Key Vault for box1 and for box 2 is Private Link

upvoted 109 times

> **prabhjot** 2 years, 10 months ago
>
> Ans is wrong - Azure key vault is for Application ad Data Security so key vault - Box1 and Private link is for Vnet security so Box2 =Private link
>
> upvoted 18 times
>
> > **Ramye** 1 year, 5 months ago
> >
> > Yes, Private Link is for VNet security, but there's no reference to VNet here. What am I missing? thx
> >
> > upvoted 1 times

HardcodedCloud Highly Voted 👍 2 years, 9 months ago

Data Security : Access Keys stored in Azure Key Vault

Network access control : Azure Private Link with network service tags

upvoted 49 times

6c0ca3d Most Recent 🕐 1 month, 3 weeks ago

access keys stored..

azure private link

appear to be the correct response

upvoted 1 times

orrery 11 months, 2 weeks ago

Data security:

Access keys stored in Azure Key Vault: This ensures that sensitive keys are securely stored and managed, reducing the risk of unauthorized access.

Network access control:

Azure Private Link with network service tags: This provides secure and private connectivity to Azure services, ensuring that data transfer occurs over a private network rather than the public internet.

upvoted 1 times

Arockia 1 year, 5 months ago

• Data safety: Lock keys in Key Vault, network isolation with Private Link & service tags for secured Azure Data Lake Gen2 copy via Automation runbook.

• Network control: Private Link & service tags shield your Azure Data Lake Gen2 copy process from the public internet for enhanced security.

upvoted 2 times

Murtuza 1 year, 5 months ago

App GW with WAF cant play a role because it applies to client facing which is not the ASK in the question.

upvoted 2 times

JG56 1 year, 7 months ago

in exam Nov 23, Agree with Alex

upvoted 4 times

smanzana 1 year, 8 months ago

Box1:Key Vault

Box2:Private Link

upvoted 3 times

ian2387 1 year, 8 months ago

Have we managed to figure out the correct answer?

Data: Azure key vault

Network: Private link with service tags. I have my doubts if service tags are supported by azure private links.

upvoted 2 times

⊟ **rahulnair** 1 year, 8 months ago

A & C -

Secure the assets in Azure Automation including credentials, certificates, connections and encrypted variables. These assets are protected in Azure Automation using multiple levels of encryption. By default, data is encrypted with Microsoft-managed keys. For additional control over encryption keys, you can supply customer-managed keys to use for encryption of Automation assets. These keys must be present in Azure Key Vault for Automation service to be able to access the keys.

Use Azure Private Link to securely connect Hybrid runbook workers to Azure Automation. Azure Private Endpoint is a network interface that connects you privately and securely to a an Azure Automation service powered by Azure Private Link. Private Endpoint uses a private IP address from your Virtual Network (VNet), to effectively bring the Automation service into your VNet.

https://learn.microsoft.com/en-us/azure/automation/automation-security-guidelines

upvoted 2 times

⊟ **ConanBarb** 1 year, 9 months ago

Hey all,

Lets exclude the nonsensical options first:

Automation Contributor role is the RBAC role for working with the Automation service, "design-time" if you will, and hence has nothing to do with securing data run-time.

Private link with network service tags is nonse for N/W security. There is no such thing. Network service tags is used in NSGs and firewall rules.

Hence, even though these options seem strange as well but in theory relevant:

Data Security: Key vault

N/W Security: App GW with WAF

upvoted 3 times

⊟ **uffman** 2 years, 2 months ago

Box1: Key Vault

Box2: Private Link

upvoted 1 times

⊟ **KrisDeb** 2 years, 4 months ago

Azure Automation Run As Account will retire on September 30, 2023 and will be replaced with Managed Identities. Before that date, you'll need to start migrating your runbooks to use managed identities. For more information, see migrating from an existing Run As accounts to managed identity to start migrating the runbooks from Run As account to managed identities before 30 September 2023.

upvoted 3 times

⊟ **Toschu** 2 years, 3 months ago

Note: This has nothing to do with the question

upvoted 4 times

⊟ **janesb** 2 years, 5 months ago

Data Security : Access Keys stored in Azure Key Vault

Network access control : Azure Private Link with network service tags

https://learn.microsoft.com/en-us/azure/automation/automation-security-guidelines

upvoted 6 times

⊟ **Azzzurrre** 2 years, 6 months ago

None of the answers provided is a good answer. They are fragmentary or just wrong.

Key Vault with access keys is a bad answer because using shared access keys is only recommended if a service accessing the storage cannot use a managed identity or a certificate to authenticate.

"Azure Private Link with network service tags" doesn't mean anything. Network Service Tags can be used in NSG rules, and in routing rules, if either were specified, but they aren't.

upvoted 6 times

⊟ **EM1234** 2 years, 1 month ago

these are both good points. I was also confused how everyone keeps saying to use private link with service tags. Service tags are not used with private links / endpoints.

I would still go with A for data security since key vault can be very explicitly secured but the point you made is great.

For the second question, I would go with the app gateway with WAF since it is at least controlling network access. Honestly though, I think something has been written wrong here. The answers dont make sense.

upvoted 1 times

⊟ **TJ001** 2 years, 6 months ago

Data Security : Access Keys stored in Azure Key Vault

Network access control : Azure Private Link with network service tags

upvoted 3 times

⊟ **cychoia** 2 years, 7 months ago

https://learn.microsoft.com/en-us/azure/automation/automation-security-guidelines

upvoted 6 times

Question #5 *Topic 3*

You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.
What should you include in the recommendation?

A. Compliance Manager

B. Microsoft Defender for Cloud Apps

C. Microsoft Endpoint Manager

D. Microsoft Defender for Endpoint

Suggested Answer: *D*
Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.
Note: Turn on web content filtering
From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering. Switch the toggle to On and Save preferences.
Configure web content filtering policies
Web content filtering policies specify which site categories are blocked on which device groups. To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering

Community vote distribution
D (93%) 7%

PlumpyTumbler Highly Voted 2 years, 4 months ago
Selected Answer: D
Click on the arrow next to "Adult content" and Gambling is explicitly named as a Defender for Endpoint content filtering site category.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#configure-web-content-filtering-policies
upvoted 17 times

francescoc Most Recent 2 months, 3 weeks ago
Selected Answer: D
In the navigation pane, select Settings > Endpoints > General > Advanced Features.
Scroll down until you see Web content filtering.
Switch the toggle to On, and then select Save preferences.
Web content filtering policies specify which site categories are blocked on which device groups. To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#configure-web-content-filtering-policies
upvoted 2 times

Ramye 11 months, 2 weeks ago
D confirmed

Tried the below steps
Note: Turn on web content filtering
From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering. Switch the toggle to On and Save preferences.
upvoted 1 times

zellck 1 year, 7 months ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#what-is-web-content-filtering
Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint and Microsoft Defender for Business. Web content filtering enables your organization to track and regulate access to websites based on their content categories. Many of these websites (even if they're not malicious) might be problematic because of compliance regulations, bandwidth usage, or other concerns.

upvoted 3 times

Shaz 1 year, 7 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide

upvoted 2 times

AWS56 1 year, 9 months ago

Selected Answer: B

B. Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a cloud-native security solution that helps protect your organization from cyber threats across cloud applications and services, including web browsing. It includes web content filtering capabilities that allow you to block access to websites that contain adult content, such as gambling sites, and other categories of websites that you want to block.

To implement this solution, you can configure web content filtering policies in Microsoft Defender for Cloud Apps and apply them to your Windows 11 devices. This will prevent users from accessing websites that are not allowed by the policy.

Compliance Manager is a solution that helps you manage regulatory compliance requirements for Microsoft cloud services, and Microsoft Endpoint Manager and Microsoft Defender for Endpoint are solutions for securing and managing endpoint devices, but neither of these solutions specifically provide web content filtering capabilities.

upvoted 2 times

Toschu 1 year, 9 months ago

Defender for Endpoint has a basic web filter included, and Microsoft Defender for Cloud Apps needs for the web filter to run Defender for Endpoint on the client.
Fun fact: When Defender for Endpoint was first released, a web filter was not included in the price and they wanted that customers pay extra for it because it was provided by 3rd party. In the end, after an outcry, it was added as part of the package.

upvoted 1 times

awssecuritynewbie 1 year, 10 months ago

Selected Answer: B

this is is also correct with cloudapps you can filter based on category so i would say B

upvoted 2 times

tester18128075 2 years, 3 months ago

D is correct

upvoted 2 times

NNavee 2 years, 3 months ago

Correct Answer

upvoted 1 times

JMuller 2 years, 3 months ago

Selected Answer: D

correct

upvoted 2 times

re213 2 years, 3 months ago

Selected Answer: D

Correct Ans

upvoted 3 times

Alex_Burlachenko 2 years, 4 months ago

defo correct

upvoted 2 times

K1SMM 2 years, 4 months ago

D is correct !

upvoted 2 times

Question #6 *Topic 3*

Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10.
You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
✑ Ensure that only authorized applications can run on the kiosks.
✑ Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Implement Automated investigation and Remediation (AIR) in Microsoft Defender for Endpoint.

B. Onboard the kiosks to Microsoft intune and Microsoft Defender for Endpoint.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

D. Onboard the kiosks to Azure Monitor.

E. Implement Privileged Access Workstation (PAW) for the kiosks.

Suggested Answer: *BE*
Onboard devices and configure Microsoft Defender for Endpoint capabilities.
Deploying Microsoft Defender for Endpoint is a two-step process.
* Onboard devices to the service
* Configure capabilities of the service
B: Depending on the device, follow the configuration steps provided in the onboarding section of the Defender for Endpoint portal.
E: A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses credential guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and web traffic is restricted to a limit set of permitted destinations (Deny all).
Note: Privileged Access Workstation (PAW) ג€" This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised. The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive job tasks. This makes the
PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing. To provide productivity to these users, separate accounts and workstations must be provided for productivity applications and web browsing. While inconvenient, this is a necessary control to protect users whose account could inflict damage to most or all resources in the organization.
Incorrect:
Not A: What is automated investigation and remediation?
Automated investigation and response capabilities help your security operations team by: Determining whether a threat requires action. Taking (or recommending) any necessary remediation actions. Determining whether and what other investigations should occur. Repeating the process as necessary for other alerts.
Not C: Threat & Vulnerability Management is a component of Microsoft Defender for Endpoint, and provides both security administrators and security operations teams with unique value, including:
- Real-time endpoint detection and response (EDR) insights correlated with endpoint vulnerabilities.
- Invaluable device vulnerability context during incident investigations.
- Built-in remediation processes through Microsoft Intune and Microsoft System Center Configuration Manager.
Note: Microsoft's threat and vulnerability management is a built-in module in Microsoft Defender for Endpoint that can:
Discover vulnerabilities and misconfigurations in near real time.
Prioritize vulnerabilities based on the threat landscape and detections in your organization.
If you've enabled the integration with Microsoft Defender for Endpoint, you'll automatically get the threat and vulnerability management findings without the need for additional agents.
As it's a built-in module for Microsoft Defender for Endpoint, threat and vulnerability management doesn't require periodic scans.
Not D: You do not use Azure Monitor for onboarding.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure https://docs.microsoft.com/en-us/security/compass/privileged-access-devices https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-tvm

Community vote distribution

BC (82%) BE (18%)

Jasper666 Highly Voted 2 years, 4 months ago

I would go for B and C. Vuln management sits on top of defender for endpoint. (https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide)

upvoted 49 times

cdizzle 2 years, 1 month ago

Agree with you, I think PAW could get the job done as well but the spirit of the question is for kiosks endpoint. PAW implementations are typical for admin workstations.

upvoted 21 times

HardcodedCloud Highly Voted 2 years, 3 months ago

Selected Answer: BC

B & C based on the requirements.

upvoted 25 times

masby661 Most Recent 9 months, 3 weeks ago

Selected Answer: BC

B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint:

Onboarding the kiosks to Microsoft Intune allows for centralized management of device configurations, compliance policies, and application control to ensure that only authorized applications can run on the kiosks.

Onboarding to Microsoft Defender for Endpoint provides advanced threat protection, endpoint security, and vulnerability management to regularly harden the kiosks against new threats.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint:

Implementing threat and vulnerability management in Microsoft Defender for Endpoint enables continuous monitoring, detection, and remediation of security vulnerabilities and threats on the kiosks, ensuring proactive security measures are in place

upvoted 3 times

JG56 1 year, 1 month ago

in exam Nov 23, Answer, B,C

upvoted 6 times

theplaceholder 1 year, 3 months ago

Selected Answer: BC

B&C for sure.

upvoted 4 times

WRITER00347 1 year, 4 months ago

The requirements provided emphasize controlling the applications that can run on the kiosks and regularly hardening them against new threats. With this focus on application control and threat protection, the correct actions would be:

B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Microsoft Intune can manage and configure the kiosks, allowing control over which applications can run. Microsoft Defender for Endpoint will help to protect the kiosks against threats.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

This feature of Microsoft Defender for Endpoint helps to discover, prioritize, and remediate threats and vulnerabilities, helping to harden the kiosks against new and emerging threats.

So the correct answers are:

B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

upvoted 2 times

sbnpj 1 year, 4 months ago

Selected Answer: BC

it has to be BC, other options dont provide the best solution.

upvoted 3 times

Ario 1 year, 6 months ago

Selected Answer: BC

Microsoft Intune and Microsoft Defender for Endpoint provide a comprehensive set of security capabilities to manage and protect the Windows 10 kiosks, while threat and vulnerability management helps to proactively identify and remediate vulnerabilities.

upvoted 3 times

imsidrai 1 year, 6 months ago

recommended solution is not asking for least privilege, so no for PAW

B&C definitely correct

upvoted 1 times

Gurulee 1 year, 8 months ago

Selected Answer: BC

PAW are for admin privileged purposes.

upvoted 5 times

JayLearn2022 1 year, 9 months ago

Answer: BC

B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint to ensure that only authorized applications can run on the kiosks. This allows for the creation of a custom device configuration profile that can restrict which apps are allowed to run on the kiosks. Intune can also be used to regularly harden the kiosks against new threats.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint to provide a centralized view of the security posture of the kiosks. This feature identifies potential vulnerabilities and provides guidance on how to mitigate them, allowing for regular hardening of the kiosks against new threats.

Option E (Implement Privileged Access Workstation (PAW) for the kiosks) is not a suitable recommendation for securing the mobile self-service kiosks. PAWs are typically used for highly privileged users who need access to sensitive information or systems, and not for standard kiosks. Instead, implementing Microsoft Intune and Microsoft Defender for Endpoint as suggested in option B would provide better security measures for the kiosks.

upvoted 2 times

OK2020 1 year, 9 months ago

I would go B & E:

B: Microsoft Defender for Endpoint Intune integration

Microsoft Defender for Endpoint and Microsoft Intune work together to help prevent security breaches. They can also limit the impact of breaches. ATP capabilities provide real-time threat detection as well as enable extensive auditing and logging of the end-point devices.

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment

E: PAW

A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses credential guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and web traffic is restricted to a limit set of permitted destinations (Deny all).

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices

upvoted 2 times

awssecuritynewbie 1 year, 10 months ago

Selected Answer: BC

It has to be B because you do need to onboard MDE come on guys

C = it has vulnerability scanning enabled

upvoted 4 times

Mo22 1 year, 10 months ago

Selected Answer: BC

B and C are the recommended actions to secure the kiosks. Implementing threat and vulnerability management in Microsoft Defender for Endpoint and onboarding the kiosks to Microsoft Intune and Microsoft Defender for Endpoint will help ensure that only authorized applications can run on the kiosks and that the kiosks are regularly hardened against new threats.

upvoted 4 times

m7medcs 1 year, 11 months ago

B & C 100%

upvoted 3 times

walkaway 1 year, 11 months ago

Selected Answer: BC

kiosks are NOT administrative workstations lol. We don't need PAW for kiosks.

upvoted 4 times

yaza85 1 year, 11 months ago

Selected Answer: BC

PAW is the name of the admin workstation concept. Its not a technology and has nothing to do with kiosk. B and C

upvoted 4 times

Question #7 *Topic 3*

You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data.
What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps

B. Microsoft Information Protection

C. insider risk management

D. Azure Purview

Suggested Answer: *A*
Microsoft Defender for Cloud Apps File policies.
File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases. Defender for Cloud Apps can monitor any file type based on more than 20 metadata filters (for example, access level, file type).
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

Community vote distribution
B (91%) 7%

Alex_Burlachenko Highly Voted 2 years, 4 months ago
Better to select B - https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide like for example You can use sensitivity labels to:

Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android.

Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as SalesForce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.
upvoted 45 times

HardcodedCloud Highly Voted 2 years, 3 months ago
Selected Answer: B
B is part of Microsoft Information Protection to add Visual markings e.g. watermark for sensitive information.
upvoted 21 times

MWP Most Recent 8 months ago
It's B and not A. "When a document is labeled by Defender for Cloud Apps, visual markings, such as headers, footers, or watermarks, are not applied". https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-information-protection#validate-your-policy
upvoted 1 times

JHJ44 8 months, 3 weeks ago
Selected Answer: B
To add a watermark to email attachments containing sensitive data in your Microsoft 365 E5 subscription, I recommend using Microsoft Information Protection. This solution allows you to apply watermarks to files and emails, ensuring that sensitive content is clearly marked and protected. By configuring content marking options, you can add watermarks, headers, or footers to attachments, helping meet compliance requirements and enhance security
upvoted 2 times

PierreTang 10 months, 2 weeks ago

Azure Purview is now Microsoft Purview, and sensitivity labels are part of Microsoft Purview, and there are no "Microsoft Information Protection" it call "Microsoft Purview Information Protection"

upvoted 7 times

PierreTang 10 months, 1 week ago

So, it should D

upvoted 3 times

Naqsh27 11 months, 3 weeks ago

Selected Answer: B

Definitely B - I accidentally enabled this for the entire organisation :-P

upvoted 3 times

JG56 1 year, 1 month ago

Answer B, in exam Nov 23

upvoted 6 times

sherifhamed 1 year, 3 months ago

Selected Answer: B

To add a watermark to email attachments that contain sensitive data in a Microsoft 365 E5 subscription, you should recommend B. Microsoft Information Protection.

Microsoft Information Protection (MIP) is a comprehensive solution that allows you to classify, label, and protect sensitive information in emails and documents. It includes the ability to apply watermarks to documents and emails based on sensitivity labels. By configuring sensitivity labels and associated policies, you can automatically add watermarks to email attachments containing sensitive data, helping to protect the information and ensure it is appropriately labeled.

upvoted 3 times

[Removed] 1 year, 5 months ago

A: https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-dlp

Define which information is sensitive: Before looking for sensitive information in your files, you first need to define what counts as sensitive for your organization. As part of our data classification service, we offer over 100 out-of-the-box sensitive information types, or you can create your own to suit to your company policy. Defender for Cloud Apps is natively integrated with Microsoft Purview Information Protection and the same sensitive types and labels are available throughout both services. So when you want to define sensitive information, head over to the Microsoft Purview Information Protection portal to create them, and once defined they'll be available in Defender for Cloud Apps. You can also use advanced classifications types such as fingerprint or Exact Data Match (EDM).

upvoted 1 times

Ario 1 year, 6 months ago

Selected Answer: B

Microsoft Defender for Cloud Apps, insider risk management, and Azure Purview, are not specifically designed to add watermarks to email attachments.

upvoted 1 times

Ramye 11 months, 3 weeks ago

Information Protection is part of Purview, so Information Protection is specifically mentioned hence this is the best choice, otherwise, Purview.

upvoted 1 times

Holii 1 year, 6 months ago

Well, now it's called Microsoft Purview Information Protection-
and there is no Azure Purview.

upvoted 3 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered.

You can use sensitivity labels to:

- Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

upvoted 2 times

oscarmh 1 year, 9 months ago

I would chose AIP always for watermarks

upvoted 1 times

OK2020 1 year, 9 months ago

I would select D:

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Anyone knows a reason why it's not D: Azure Purview?

Purview You can use sensitivity labels to:

Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

upvoted 3 times

AJ2021 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 2 times

God2029 1 year, 10 months ago

B is the right choice. A is more for thirdparty App information you have 365 E5 so using 365 Email not of any 3rd Party. Information Protection will help you here to apply the water mark based on the classification of Labels, (Ex:Internal/confidential/Public)

upvoted 1 times

Gurulee 1 year, 10 months ago

Selected Answer: B

Information protection

upvoted 2 times

Question #8 *Topic 3*

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface.

What should you include in the recommendation?

A. Azure Firewall Premium

B. Azure Traffic Manager and application security groups

C. Azure Application Gateway Web Application Firewall (WAF)

D. network security groups (NSGs)

Suggested Answer: *B*

* Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

* Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint.

Incorrect:

Not C: Azure Application Gateway Web Application Firewall is too small a scale solution in this scenario.

Note: Attacks against a web application can be monitored by using a real-time Application Gateway that has Web Application Firewall, enabled with integrated logging from Azure Monitor to track Web Application Firewall alerts and easily monitor trends.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

Community vote distribution

C (100%)

PlumpyTumbler Highly Voted 2 years, 4 months ago

Selected Answer: C

https://docs.microsoft.com/en-us/learn/modules/specify-security-requirements-for-applications/5-specify-security-strategy-apis

upvoted 31 times

JaySapkota Highly Voted 2 years, 4 months ago

I would choose C, Application Gateway with WAF. Not Traffic Manager.

Traffic Manager is a DNS based routing for performance and speed.

upvoted 19 times

ian2387 Most Recent 1 year, 2 months ago

This answer needs to be rectified

upvoted 4 times

Ramye 11 months, 4 weeks ago

And many others really

upvoted 4 times

sherifhamed 1 year, 3 months ago

Selected Answer: C

To prevent malicious bots from scanning Azure App Service web apps for vulnerabilities while minimizing the attack surface for customers in Europe and the United States, you should recommend C. Azure Application Gateway Web Application Firewall (WAF).

C. Azure Application Gateway Web Application Firewall (WAF): Azure Application Gateway with the Web Application Firewall (WAF) is specifically designed for web application security. It provides protection against common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It also includes bot protection capabilities, which can help prevent malicious bots from scanning web apps for vulnerabilities. This aligns with the requirement to prevent bot scanning while minimizing the attack surface.

upvoted 4 times

Ario 1 year, 6 months ago

Selected Answer: C

to prevent malicious bot scanning and minimize the attack surface for the web apps, Azure Application Gateway Web Application Firewall (WAF) is the recommended solution.

upvoted 3 times

Linuxieux 1 year, 6 months ago

The answer is Clear WAF- Azure Web Application Firewall on Azure Application Gateway bot protection overview: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 2 times

PrettyFlyWifi 1 year, 7 months ago

Selected Answer: C

Looks like C to me, check out:
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 2 times

zellck 1 year, 7 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview
Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

upvoted 1 times

Gurulee 1 year, 10 months ago

Selected Answer: C

Application gateway with waf

upvoted 2 times

tech_rum 1 year, 10 months ago

Selected Answer: C

App gw waf

upvoted 1 times

buguinha 1 year, 10 months ago

Selected Answer: C

https://azure.microsoft.com/en-us/updates/new-bot-protection-rule-set-in-public-preview-for-web-application-firewall-waf-with-azure-front-door-service/

upvoted 1 times

Mo22 1 year, 10 months ago

Selected Answer: C

Azure Application Gateway Web Application Firewall (WAF) provides centralized protection for your web applications, helps block common attacks like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), and helps minimize the attack surface by blocking malicious bots from scanning your web apps for vulnerabilities. By using WAF, you can ensure that the web apps are protected against common web application attacks while minimizing the attack surface.

upvoted 2 times

ad77 1 year, 11 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 2 times

nieprotetkniteeetr 1 year, 11 months ago

C. Traffic Manager has no anti-bot capability.

upvoted 2 times

Hullstar 1 year, 11 months ago

Selected Answer: C

WAF is the answer here.

upvoted 1 times

⊟ **purek77** 1 year, 11 months ago

Selected Answer: C

It is WAF on Azure Application Gateway.

Ref: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 1 times

⊟ **cychoia** 2 years, 1 month ago

Selected Answer: C

Use Geomatch custom rules.
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/geomatch-custom-rules

upvoted 3 times

Question #9 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Need to use customer-managed keys instead.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution

B (88%) 12%

zts Highly Voted 2 years, 3 months ago

Selected Answer: B

This is the link on how-to.
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

upvoted 8 times

prabhjot Highly Voted 2 years, 4 months ago

Ans is correct (it is No)

upvoted 5 times

SFAY Most Recent 10 months, 1 week ago

Selected Answer: B

The answer is B
MMK rotation frequency is not disclosed by Microsoft and is not mentioned in any MS documentation. For custom requirements, Microsoft suggests to use CMK.

https://learn.microsoft.com/en-us/answers/questions/1286740/what-is-the-frequency-of-key-rotation-in-platform

upvoted 3 times

Murtuza 1 year ago

The frequency of key rotation for Platform Managed Keys (PMKs) in Azure depends on the specific service or feature you are using. Azure manages the key rotation process for you, but the actual rotation interval may vary.

upvoted 2 times

Glorpy 1 year ago

Selected Answer: B

Answer is B...while the solution of using Microsoft-managed keys within an encryption scope for blob containers in Azure Storage supports AES-256 encryption for data at rest, for monthly rotation of the encryption keys, the solution would need to be slightly adjusted to use customer-managed keys to meet the specific rotation requirement.

upvoted 4 times

JG56 1 year, 1 month ago

Answer : No , in exam Nov 23

upvoted 4 times

shanti0091 1 year, 2 months ago

Selected Answer: A

A is the answer.

upvoted 1 times

shanti0091 1 year, 2 months ago

To backup my point, here is a link - https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption#about-encryption-key-management

upvoted 1 times

Ario 1 year, 6 months ago

Selected Answer: A

Yes, the solution of using Microsoft-managed keys within an encryption scope for blob containers in Azure Storage meets the goal of encrypting the data at rest with AES-256 keys and supporting monthly key rotation

upvoted 2 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version

Following cryptographic best practices means rotating the key that is protecting your storage account on a regular schedule, typically at least every two years. Azure Storage never modifies the key in the key vault, but you can configure a key rotation policy to rotate the key according to your compliance requirements.

upvoted 4 times

Ajdlfasudfo0 1 year, 10 months ago

The thing is, keys are rotated with microsoft managed keys, but I think you don't know exactly when

upvoted 2 times

Fal991l 1 year, 9 months ago

Azure Storage encryption with Microsoft-managed keys allows for automatic and seamless key rotation every 30 days by default, which meets the requirement of rotating encryption keys monthly.

upvoted 2 times

JakeCallham 2 years, 2 months ago

Selected Answer: B

Nope, answer is B

upvoted 4 times

Question #10 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses Microsoft-managed keys.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Need to use customer-managed keys instead.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution
B (85%) A (15%)

zts Highly Voted 2 years, 3 months ago
Selected Answer: B
To provide Azure SQL customers with two layers of encryption of data at rest, infrastructure encryption (using AES-256 encryption algorithm) with platform managed keys is being rolled out. This provides an addition layer of encryption at rest along with TDE with customer-managed keys, which is already available. ---- Derived from the link below:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql&viewFallbackFrom=sql-server-ver16
upvoted 5 times

masby661 Most Recent 9 months, 2 weeks ago
Selected Answer: A
You can rotate (or just Microsoft do their thing) with MMK. Remember with these type of questions 1 or more of the scenario's may be correct
upvoted 1 times

Murtuza 1 year ago
The frequency of key rotation for Platform Managed Keys (PMKs) in Azure depends on the specific service or feature you are using. Azure manages the key rotation process for you, but the actual rotation interval may vary.
upvoted 1 times

Ario 1 year, 6 months ago
Selected Answer: A
By adopting TDE with Microsoft-managed keys, you can easily implement and maintain data encryption at rest for your Azure SQL databases, while also meeting the goal of supporting monthly key rotation and using AES-256 keys for encryption.
upvoted 1 times

zellck 1 year, 7 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql
Azure SQL transparent data encryption (TDE) with customer-managed key (CMK) enables Bring Your Own Key (BYOK) scenario for data protection at rest, and allows organizations to implement separation of duties in the management of keys and data. With customer-managed TDE, the customer is

responsible for and in a full control of a key lifecycle management (key creation, upload, rotation, deletion), key usage permissions, and auditing of operations on keys.

upvoted 3 times

Gurulee 1 year, 10 months ago

Selected Answer: B

Customer managed key

upvoted 3 times

Philthetill 2 years, 3 months ago

correct

upvoted 3 times

Question #11 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
We need to use customer-managed keys.
Azure Storage encryption for data at rest.
Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments.
Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.
Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to manage encryption with your own keys, you have two options. You can use either type of key management, or both:
* You can specify a customer-managed key to use for encrypting and decrypting data in Blob Storage and in Azure Files.
* You can specify a customer-provided key on Blob Storage operations. A client making a read or write request against Blob Storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution
A (100%)

aiczuki 10 months, 1 week ago
In addition to this question, the actual exam had a trick question that used the word "CMK" in "Solution."
It's a good idea to remember the content of the question: Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).
upvoted 1 times

Murtuza 1 year, 6 months ago
Unfortunately, the exact frequency of key rotation for PMKs in Azure may not be publicly disclosed.
upvoted 1 times

JG56 1 year, 7 months ago
in exam Nov 23, agree with zellck.
upvoted 2 times

zellck 2 years, 1 month ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version
Following cryptographic best practices means rotating the key that is protecting your storage account on a regular schedule, typically at least every

two years. Azure Storage never modifies the key in the key vault, but you can configure a key rotation policy to rotate the key according to your compliance requirements.

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 3 times

⊟ **purek77** 2 years, 5 months ago

Selected Answer: A

Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when you retrieve it. The process is completely transparent to users. Storage Service Encryption uses 256-bit Advanced Encryption Standard (AES) encryption.

SSE ref: https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption

Finally: Microsoft-managed keys are rotated appropriately per compliance requirements. If you have specific key rotation requirements, Microsoft recommends that you move to customer-managed keys so that you can manage and audit the rotation yourself.

upvoted 1 times

⊟ **Rocky83** 2 years, 5 months ago

Selected Answer: A

The Microsoft-managed key is rotated appropriately per compliance requirements. Note that the frequency may change without notice. Azure does not expose the logs to indicate rotation to customers. If you have specific key rotation requirements, then we recommend that you move to customer-managed keys. That way, you can manage and audit the rotation yourself.

upvoted 2 times

⊟ **Yeero** 2 years, 7 months ago

Selected Answer: A

Correct

upvoted 2 times

⊟ **damiandeny** 2 years, 7 months ago

Selected Answer: A

correct

upvoted 2 times

⊟ **Philthetill** 2 years, 9 months ago

correct

upvoted 4 times

⊟ **zts** 2 years, 9 months ago

Selected Answer: A

seems correct.

upvoted 3 times

Question #12 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.

Does this meet the goal?

A. Yes

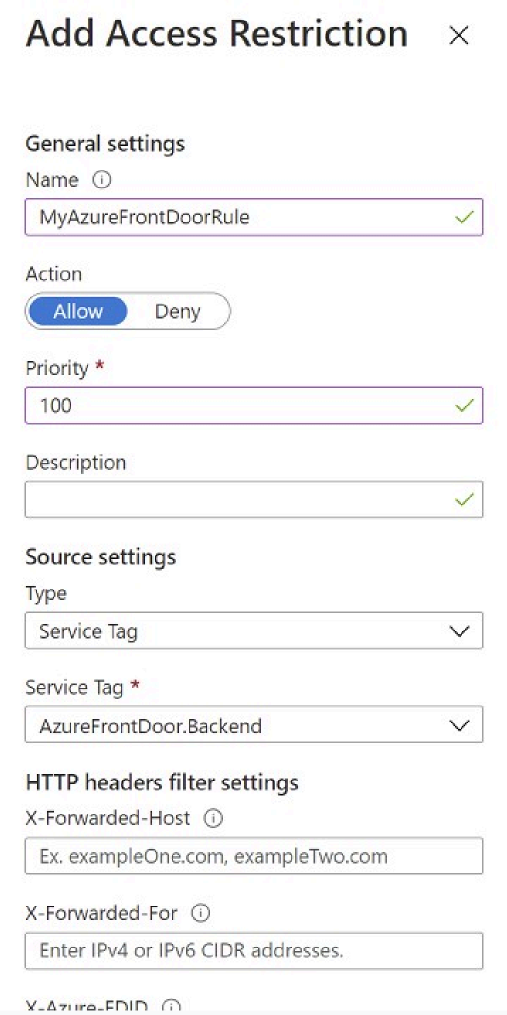
B. No

Suggested Answer: *B*

Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.

Restrict access to a specific Azure Front Door instance.

Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.



Add Access Restriction ✕

General settings

Name ⓘ

MyAzureFrontDoorRule ✓

Action

● Allow ○ Deny

Priority *

100 ✓

Description

✓

Source settings

Type

Service Tag

Service Tag *

AzureFrontDoor.Backend

HTTP headers filter settings

X-Forwarded-Host ⓘ

Ex. exampleOne.com, exampleTwo.com

X-Forwarded-For ⓘ

Enter IPv4 or IPv6 CIDR addresses.

X-Azure-FDID ⓘ

Reference:

https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

Community vote distribution

B (79%) A (21%)

PlumpyTumbler Highly Voted 2 years, 4 months ago

These questions repeat in this exam dump. They are found again in a later section. The answer is SERVICE TAGS. The explanations are confused. They say the correct answer in some places and incorrect in others. Focus on the screenshot provided. It shows you the answer. A picture is worth a thousand words.

upvoted 13 times

AzureJobsTillRetire 1 year, 9 months ago

This cannot be correct. Service tag is just a list of IP addresses.

upvoted 1 times

[Removed] 1 year, 9 months ago

This must be correct, as service tag is precisely what we need. Definition of service tag:
A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.
Link to the screenshot, you can see the type of service tag which in our case is AzureFrontDoor.Backend:
https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli#set-a-service-tag-based-rule

upvoted 1 times

zellck Highly Voted 👍 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.

upvoted 6 times

Arockia Most Recent 12 months ago

To securely restrict access to Azure App Service web apps through Azure Front Door, a more robust approach is required:

1. Service Tag-Based Access Restrictions
2. Custom Headers

upvoted 1 times

EM1234 1 year, 7 months ago

Selected Answer: B

When you read the doc you will see that the header filter is critical:

"IP address filtering alone isn't sufficient to secure traffic to your origin, because other Azure customers use the same IP addresses. You should also configure your origin to ensure that traffic has originated from your Front Door profile.

Azure generates a unique identifier for each Front Door profile. You can find the identifier in the Azure portal, by looking for the Front Door ID value in the Overview page of your profile.

When Front Door makes a request to your origin, it adds the X-Azure-FDID request header. Your origin should inspect the header on incoming requests, and reject requests where the value doesn't match your Front Door profile's identifier."

https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?pivots=front-door-standard-premium&tabs=app-service-functions#front-door-identifier

upvoted 4 times

Ajdlfasudfo0 1 year, 10 months ago

Selected Answer: A

You have to restrict traffic to front door backend pool only. This can be done via IP Range, HTTP Header or service tag. So I would go with A.

upvoted 4 times

omarrob 2 years, 1 month ago

A is correct and i was using this method based on an opened ticket with Microsoft Support three years ago where they recommend to do access restriction using the Frontdoor instance ipv4 and ipv6. that time the frontdoor service tag was not yet available.

so this particular question is correct using the frontdoor backend IP or the service tag or the HTTP header, ALL ARE CORRECT
Below are the front door IP range provided by Microsoft support