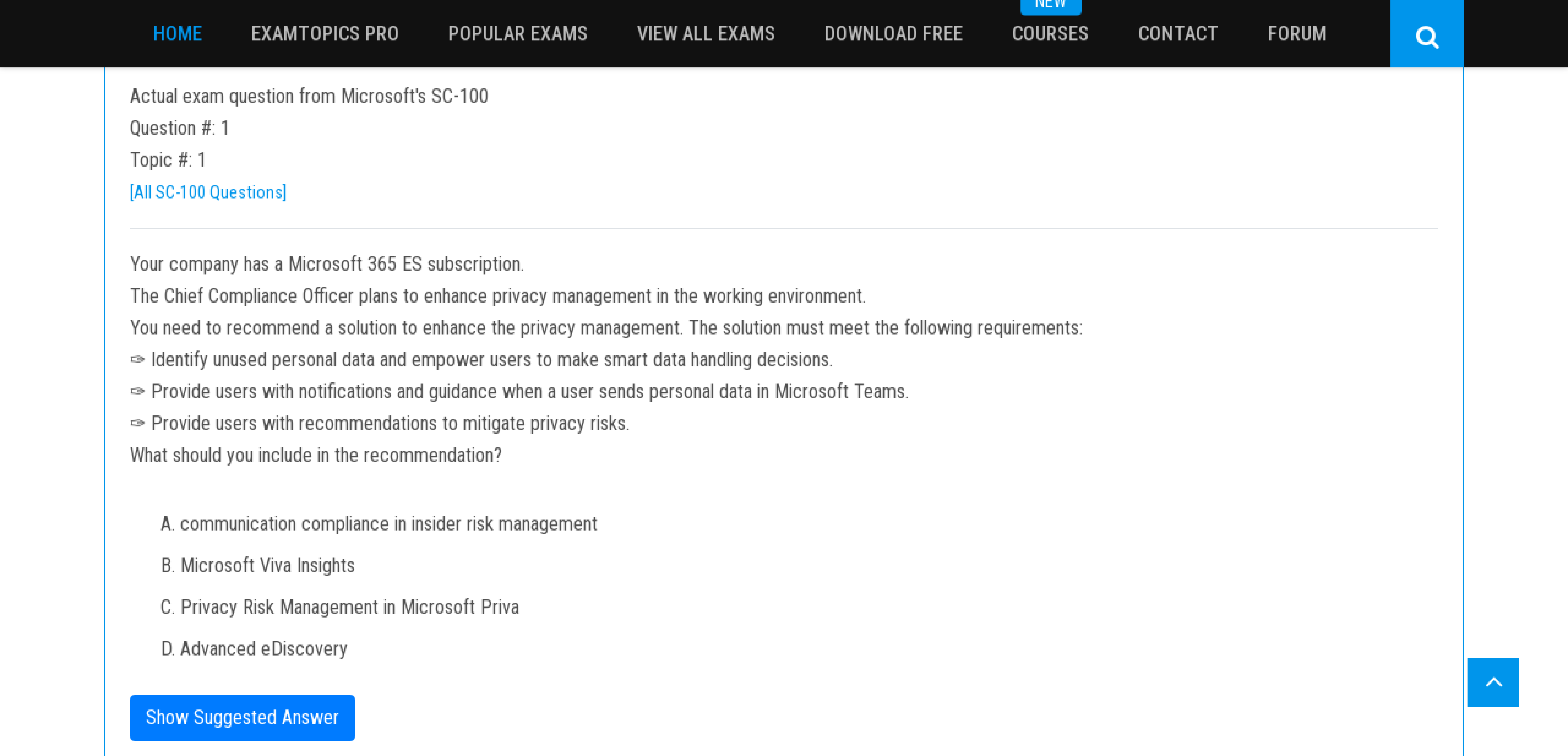


Actual exam question from Microsoft's SC-100

Question #: 1

Topic #: 1

[All SC-100 Questions]

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?

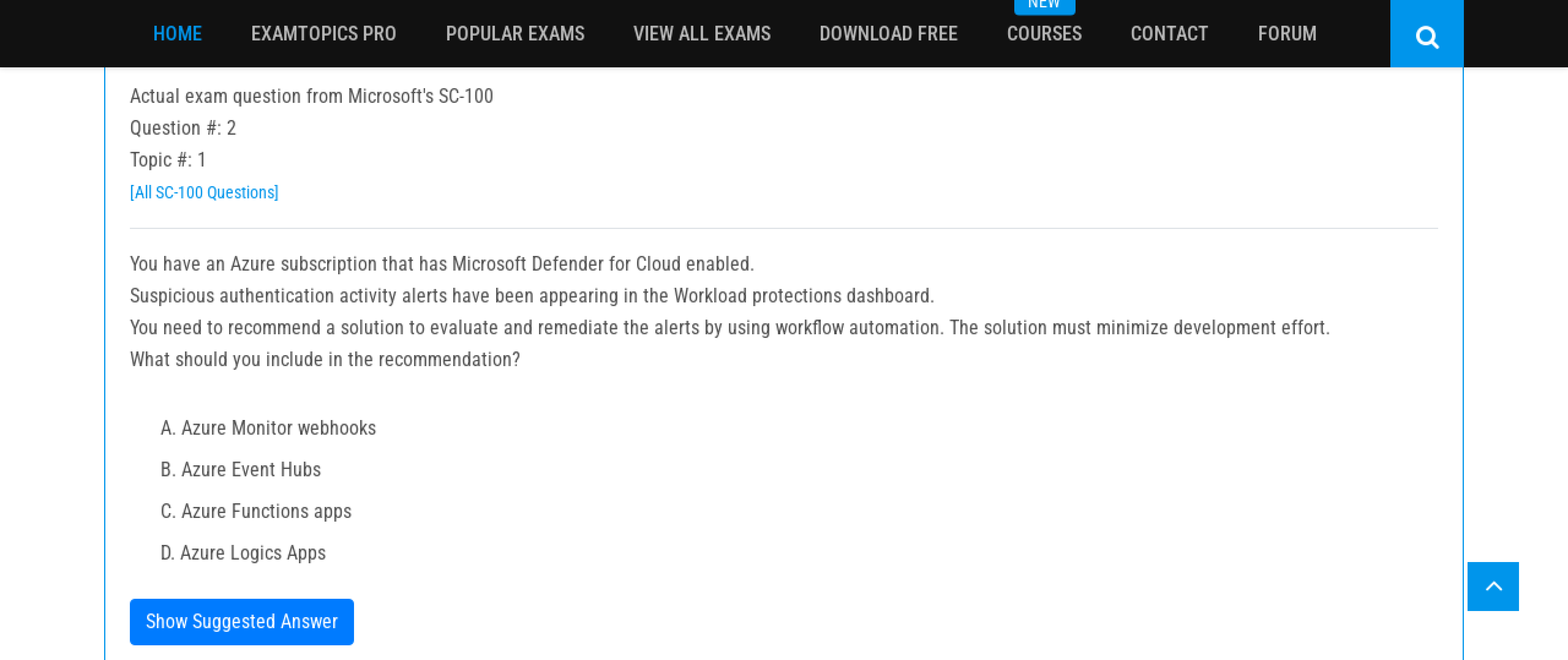
A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 2

Topic #: 1

[All SC-100 Questions]

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.

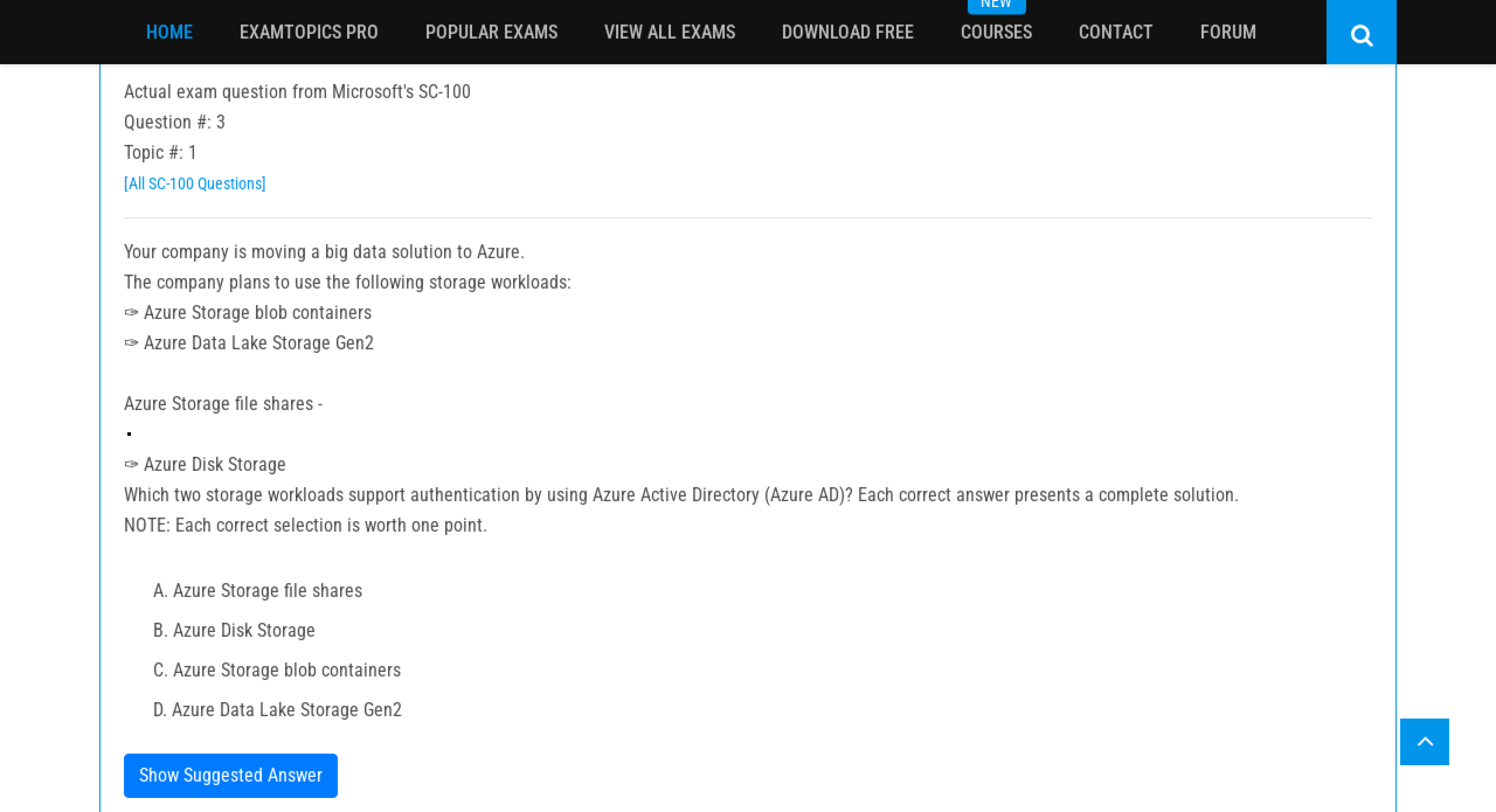
What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Event Hubs

C. Azure Functions apps

D. Azure Logics Apps



Actual exam question from Microsoft's SC-100
Question #: 3
Topic #: 1

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

Question #: 4

Topic #: 1

[All SC-100 Questions]

HOTSPOT -

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

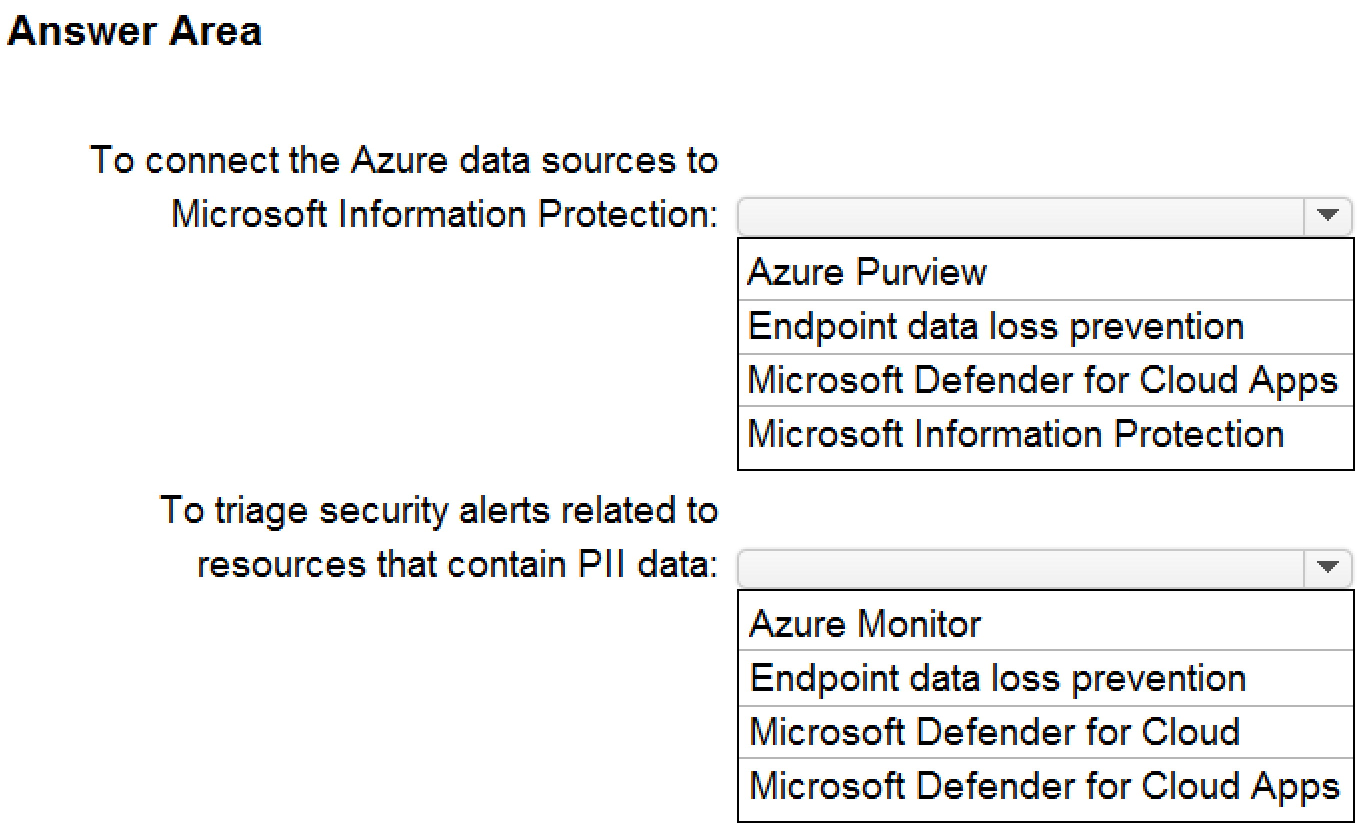
The company plans to use Microsoft Information Protection for the PII data store in Azure.

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 5

Topic #: 1

[All SC-100 Questions]

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?

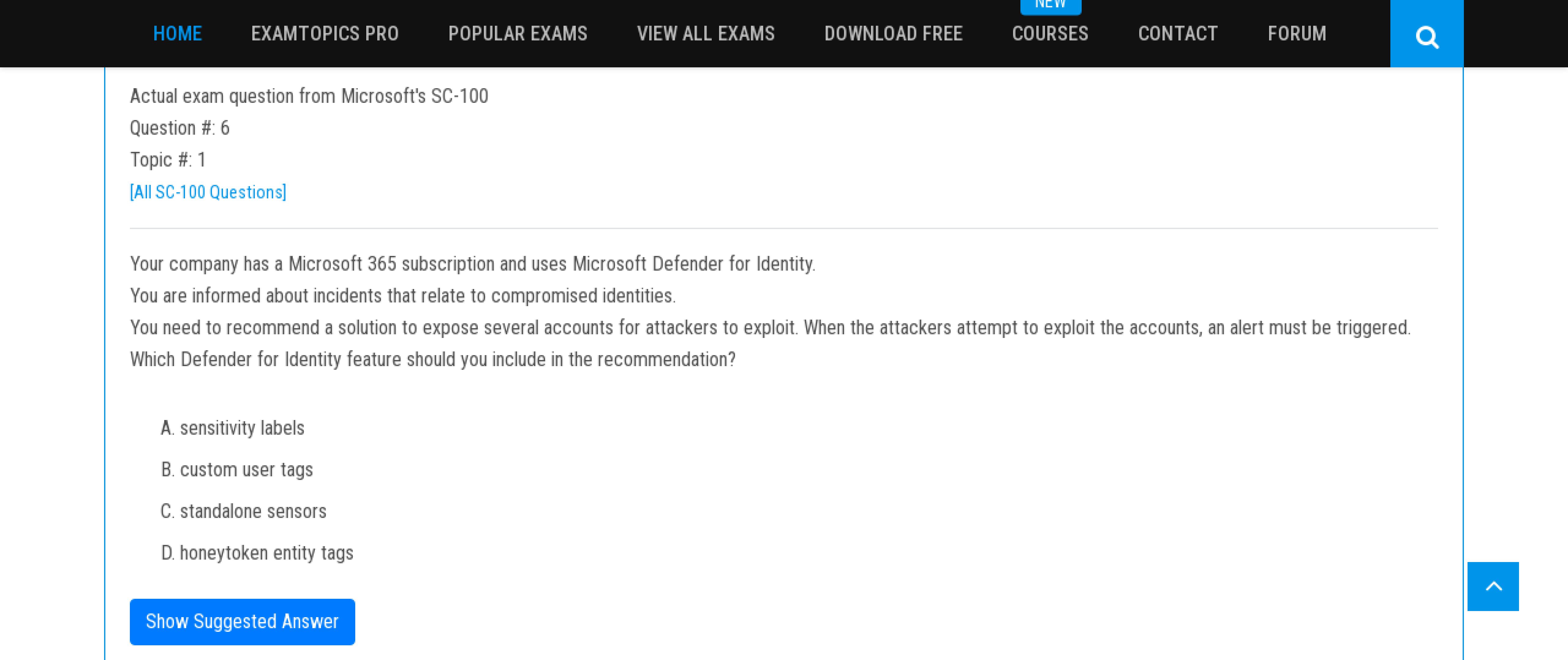
A. notebooks

B. playbooks

C. workbooks

D. threat intelligence

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 6

Topic #: 1

[All SC-100 Questions]

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.

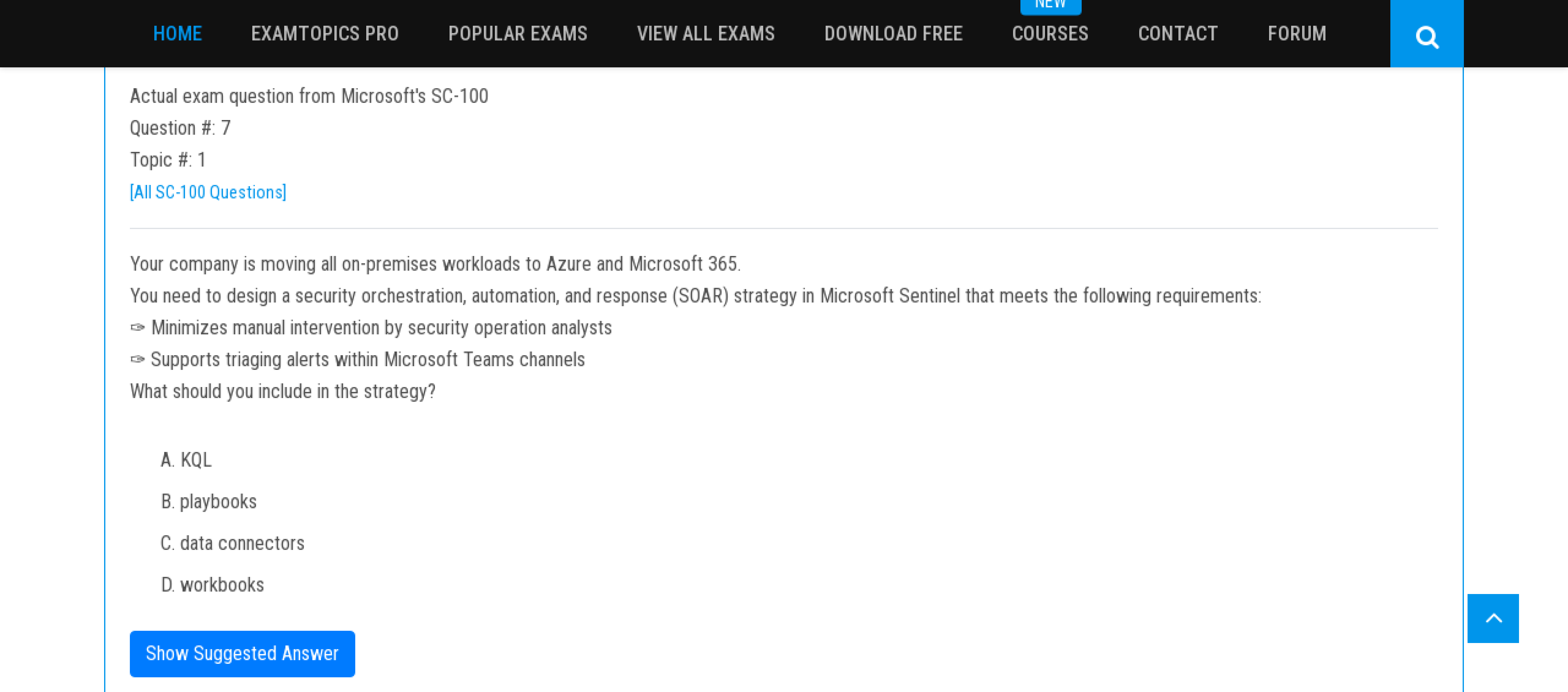
Which Defender for Identity feature should you include in the recommendation?

A. sensitivity labels

B. custom user tags

C. standalone sensors

D. honeytoken entity tags



Actual exam question from Microsoft's SC-100

Question #: 7

Topic #: 1

[All SC-100 Questions]

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

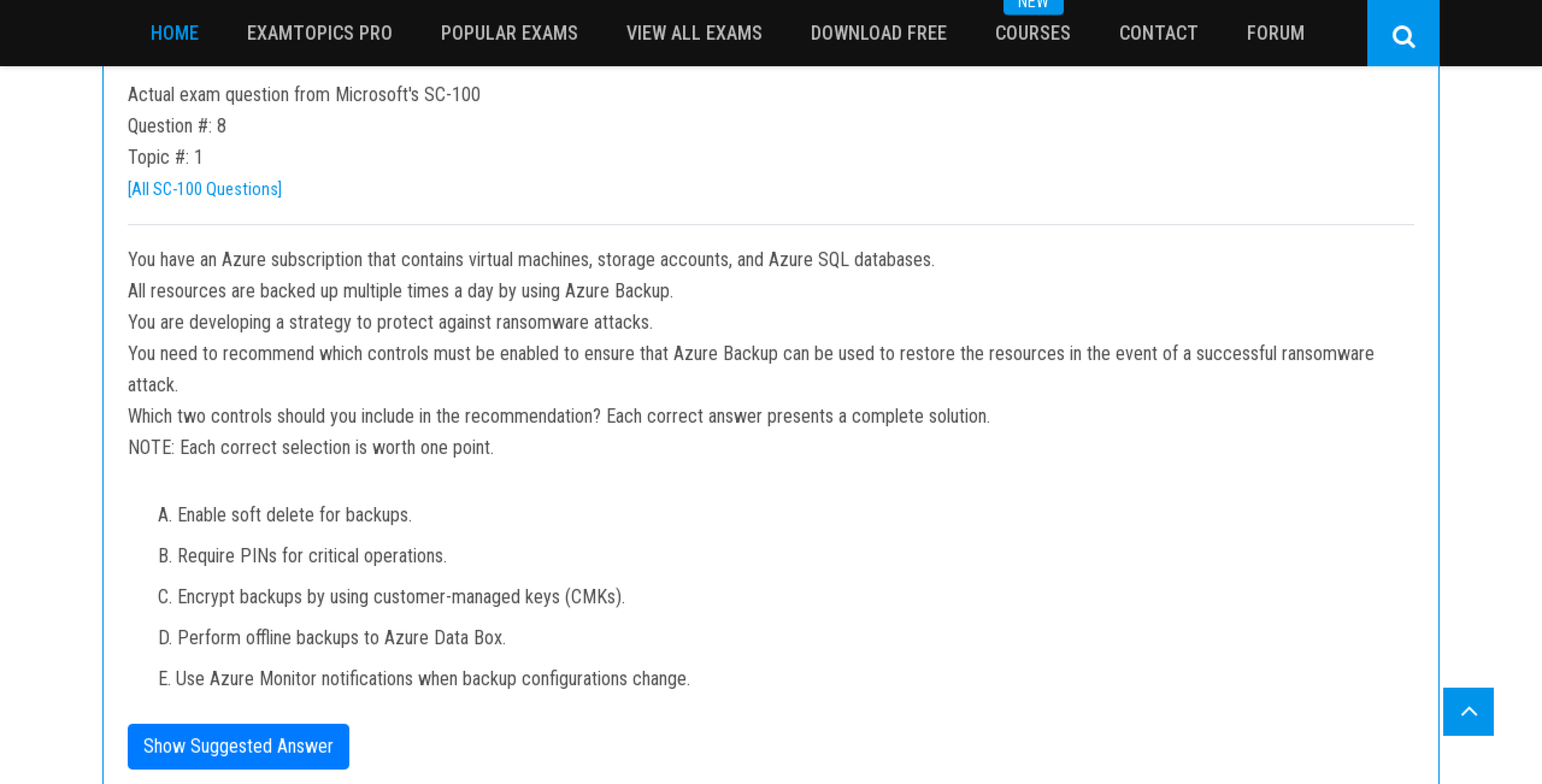
What should you include in the strategy?

A. KQL

B. playbooks

C. data connectors

D. workbooks



Actual exam question from Microsoft's SC-100

Question #: 8

Topic #: 1

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 9

Topic #: 1

[All SC-100 Questions]

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.

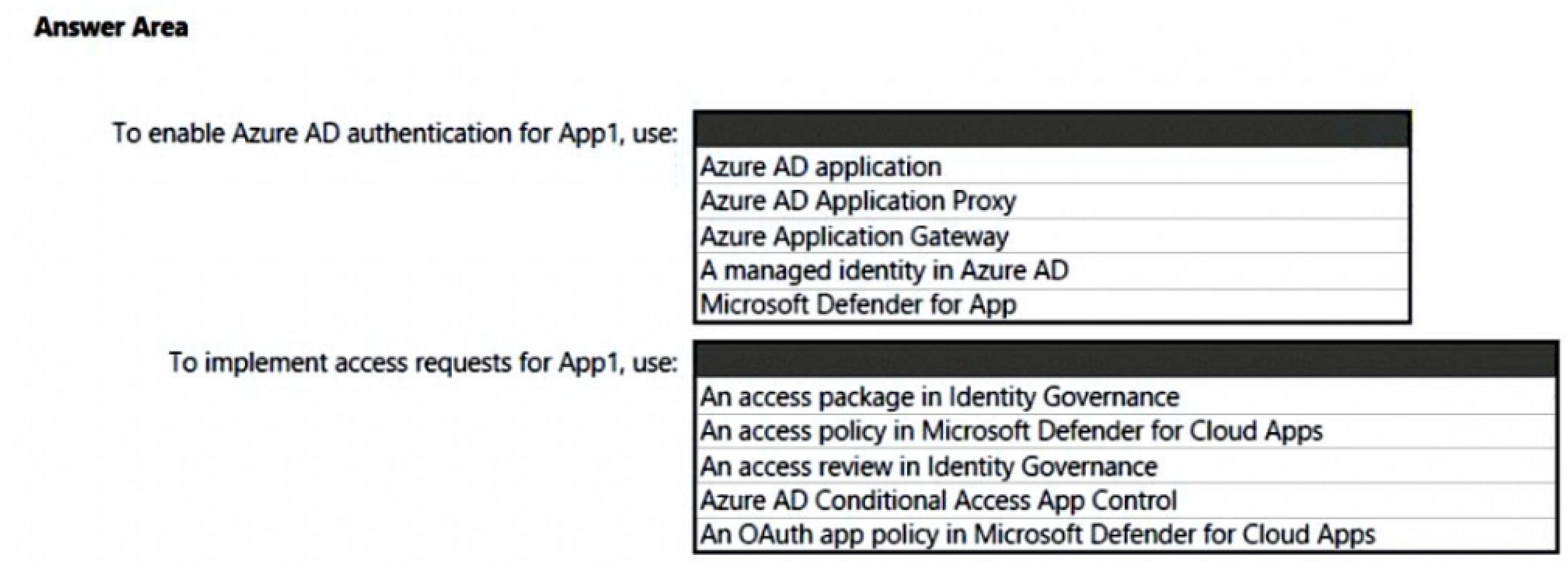
✑ Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

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

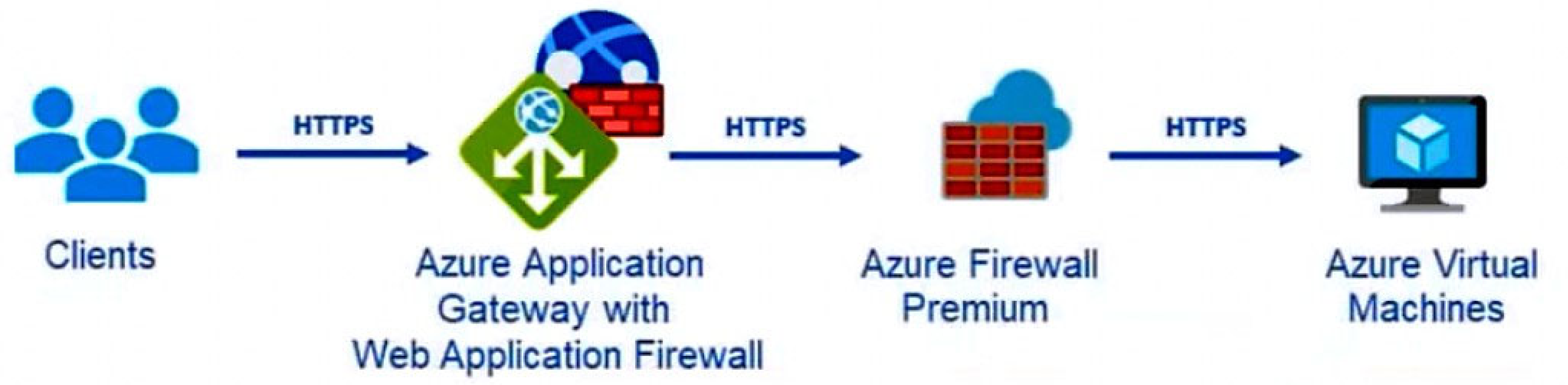
To implement access requests for App1, use:

- 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

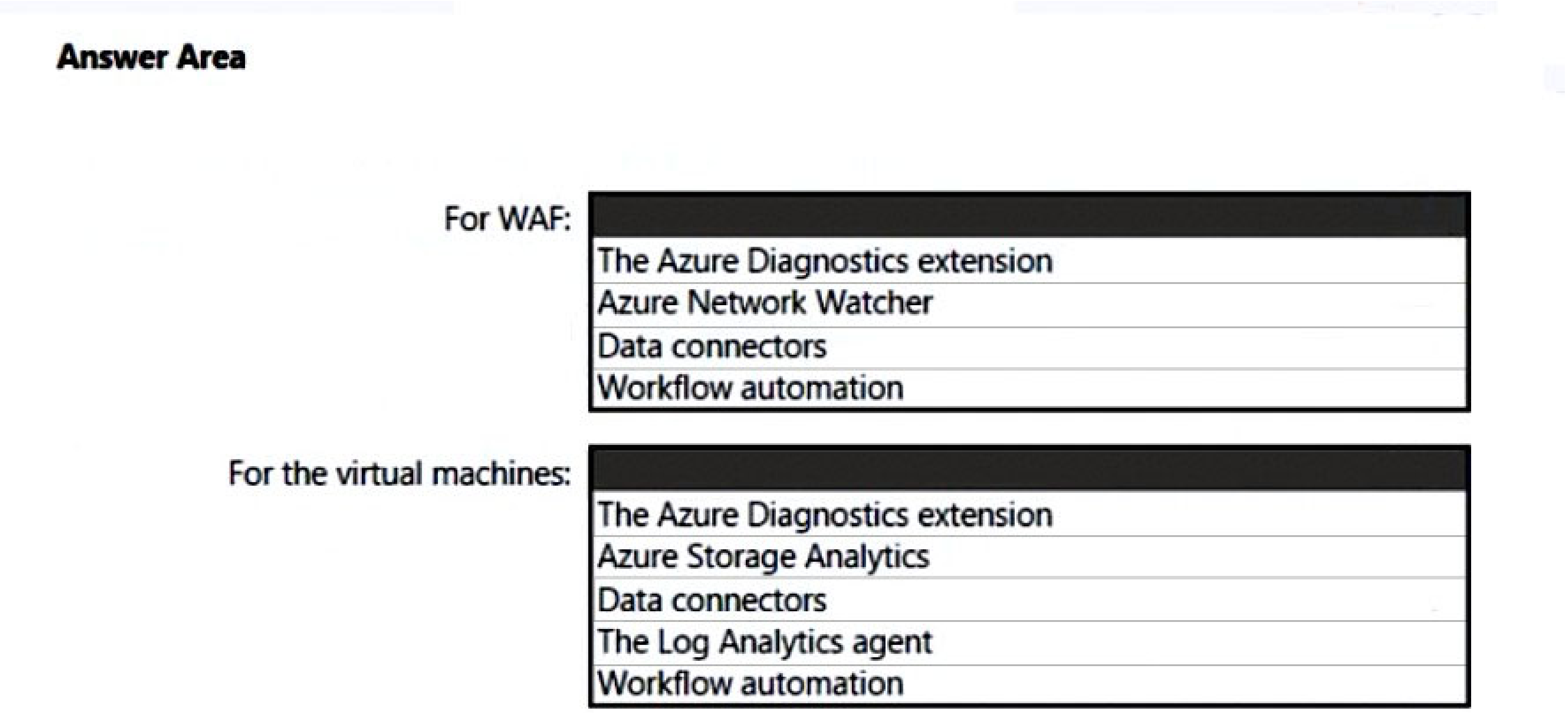
Show Suggested Answer

Actual exam question from Microsoft's SC-100
Question #: 10
Topic #: 1
[All SC-100 Questions]

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 11

Topic #: 1

[All SC-100 Questions]

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?

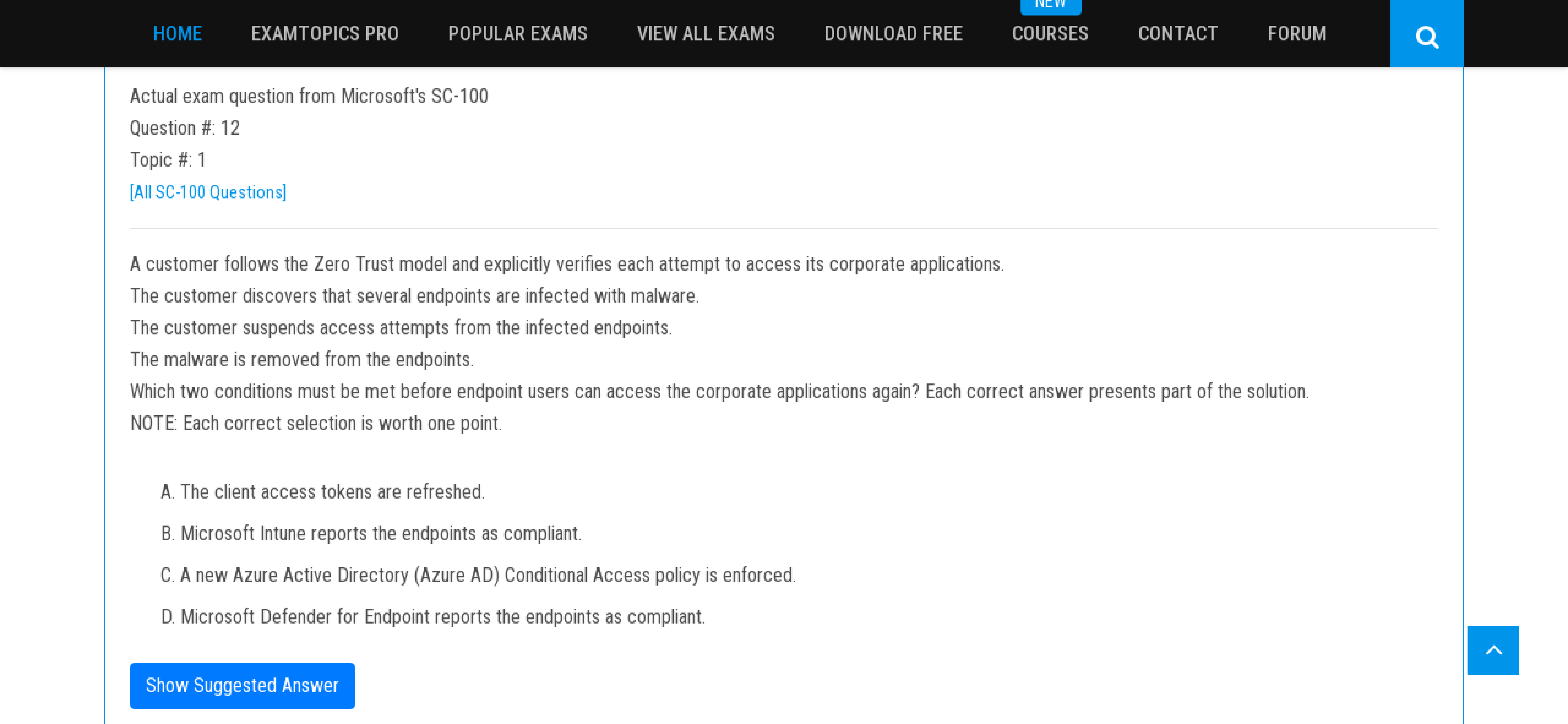
A. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 12

Topic #: 1

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 13

Topic #: 1

[All SC-100 Questions]

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.

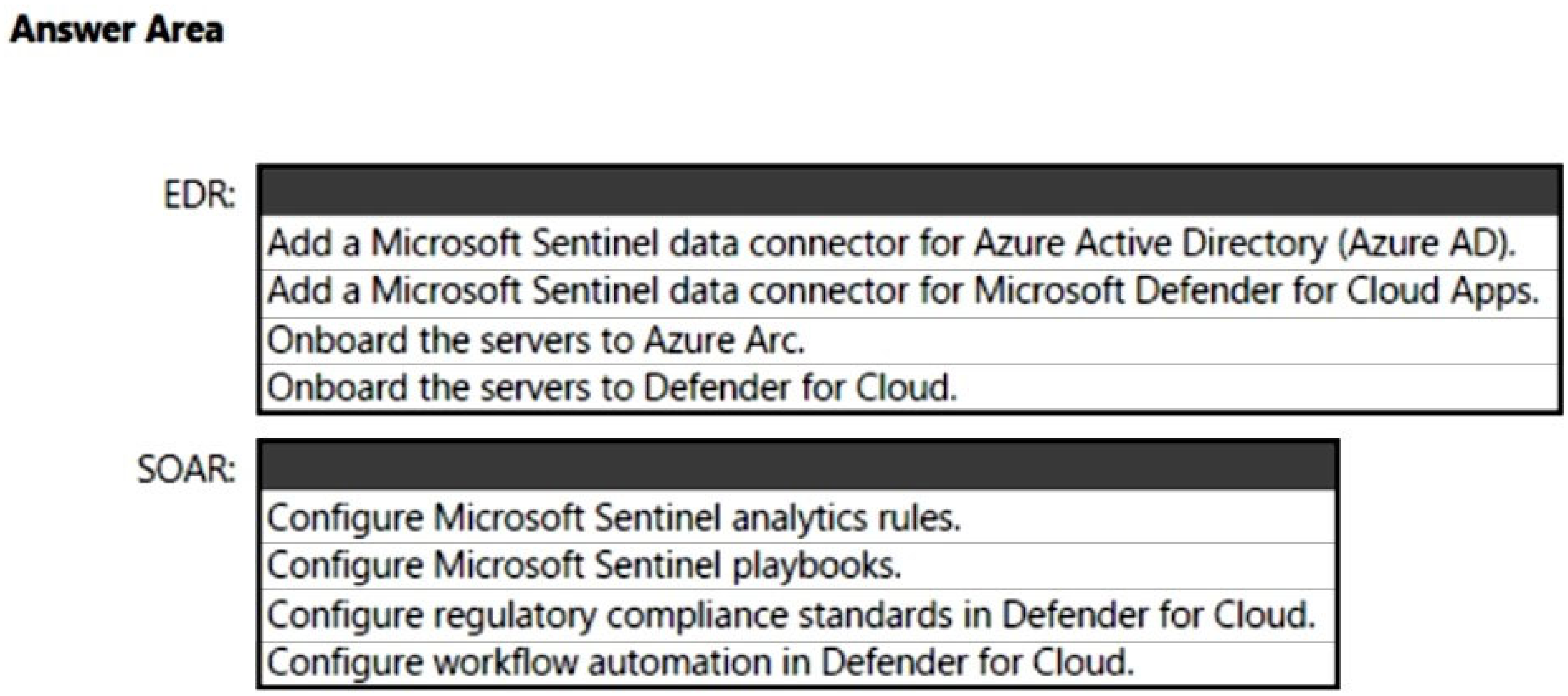
You plan to deploy Azure virtual machines that will run Windows Server.

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:

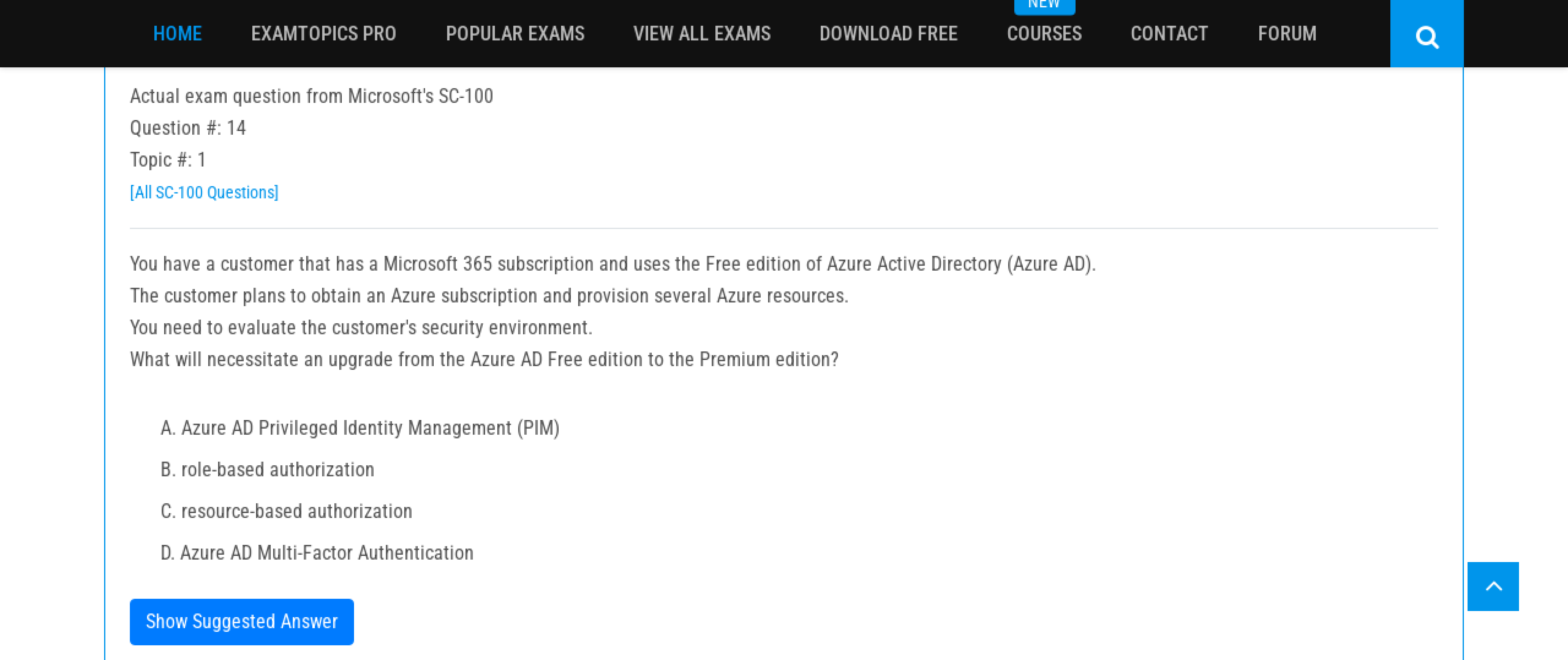


Answer Area

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.

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 14

Topic #: 1

[All SC-100 Questions]

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.

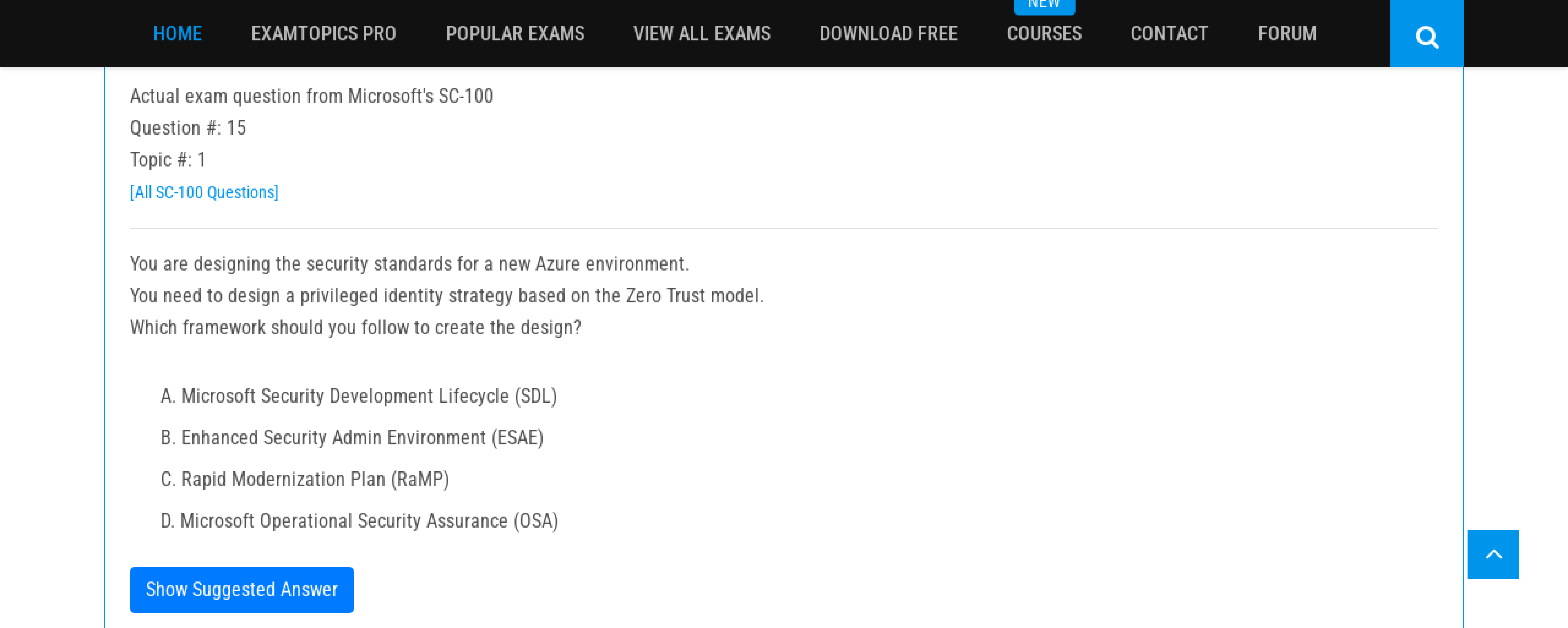
What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

A. Azure AD Privileged Identity Management (PIM)

B. role-based authorization

C. resource-based authorization

D. Azure AD Multi-Factor Authentication



Actual exam question from Microsoft's SC-100

Question #: 15

Topic #: 1

[All SC-100 Questions]

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.

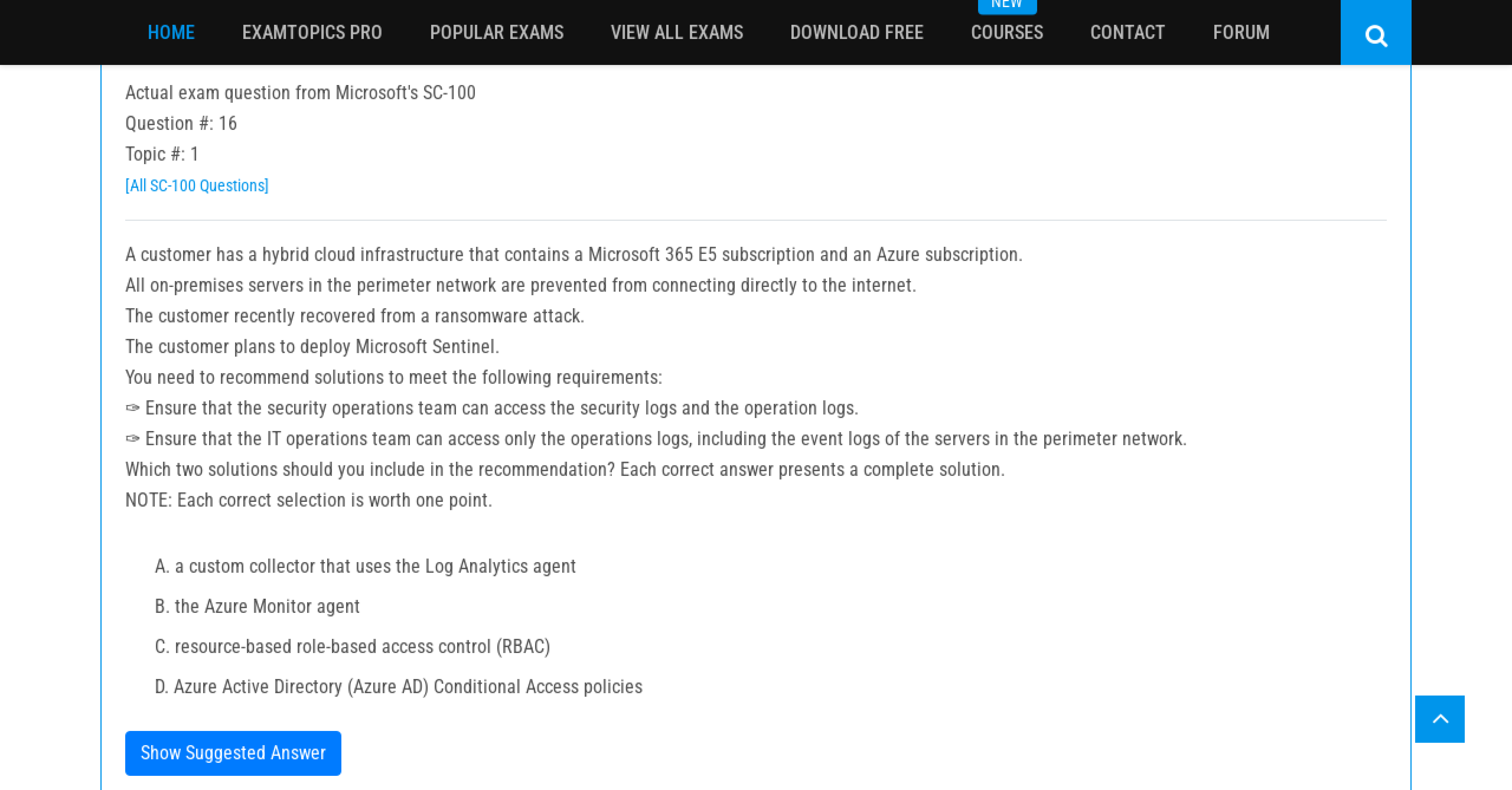
Which framework should you follow to create the design?

A. Microsoft Security Development Lifecycle (SDL)

B. Enhanced Security Admin Environment (ESAE)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)



Actual exam question from Microsoft's SC-100

Question #: 16

Topic #: 1

[All SC-100 Questions]

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

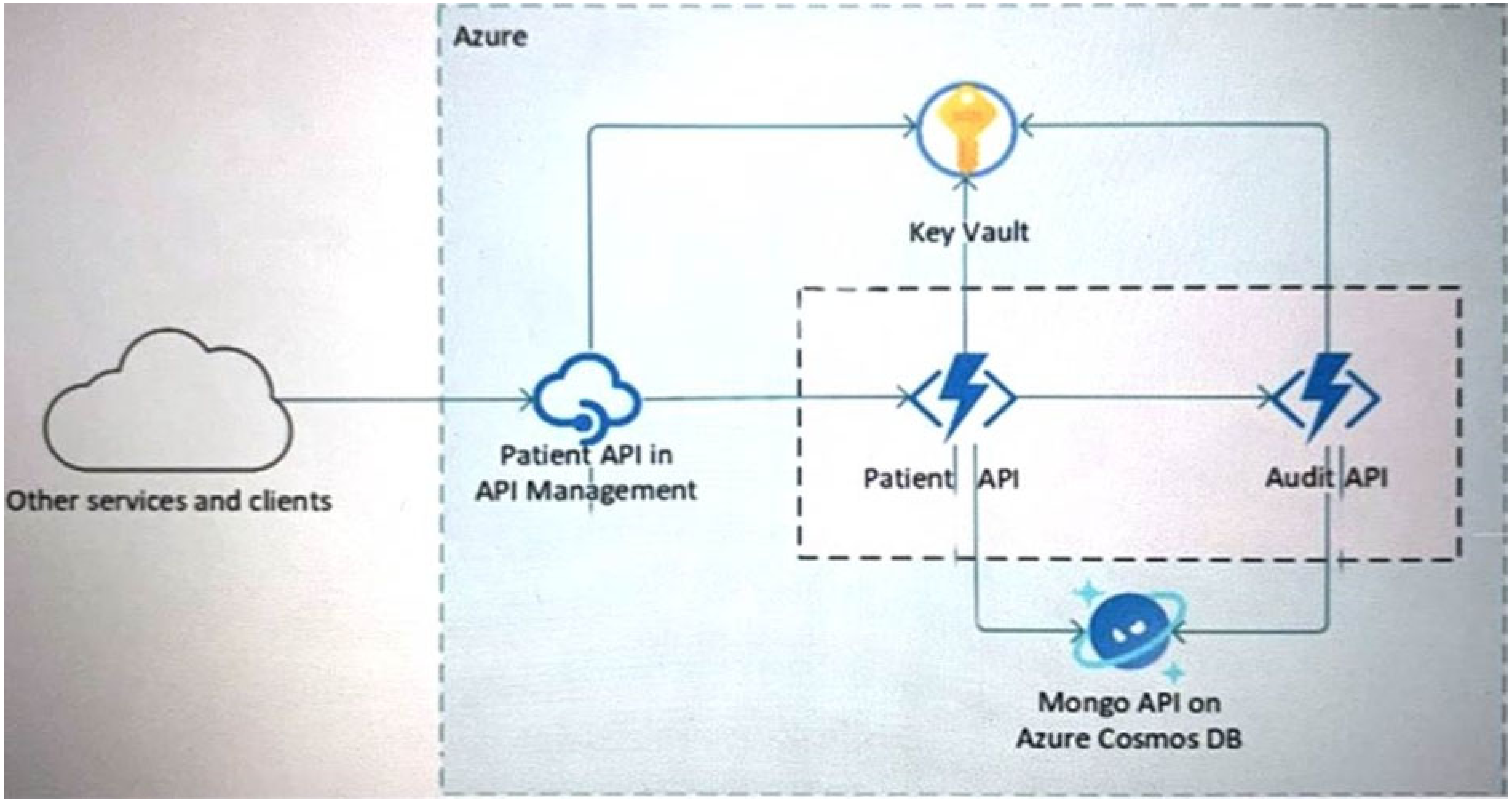
Actual exam question from Microsoft's SC-100

Question #: 17

Topic #: 1

[All SC-100 Questions]

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



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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 18

Topic #: 1

[All SC-100 Questions]

HOTSPOT

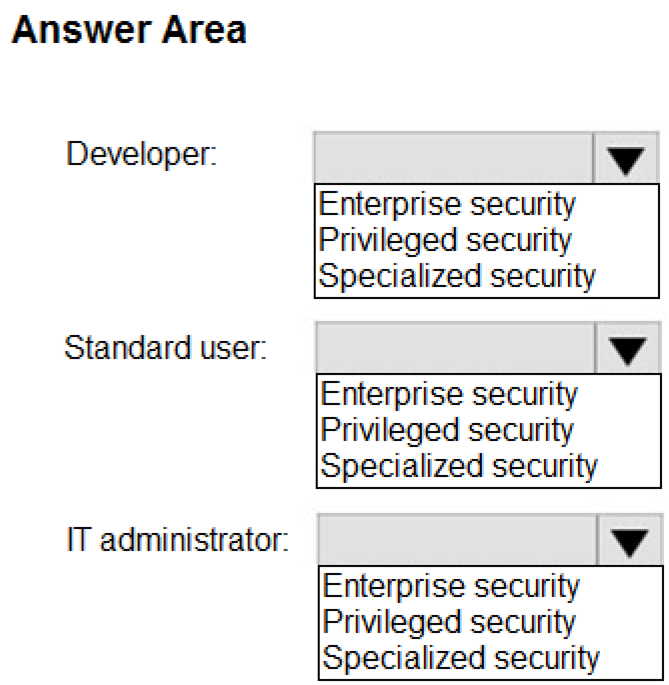
-

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.



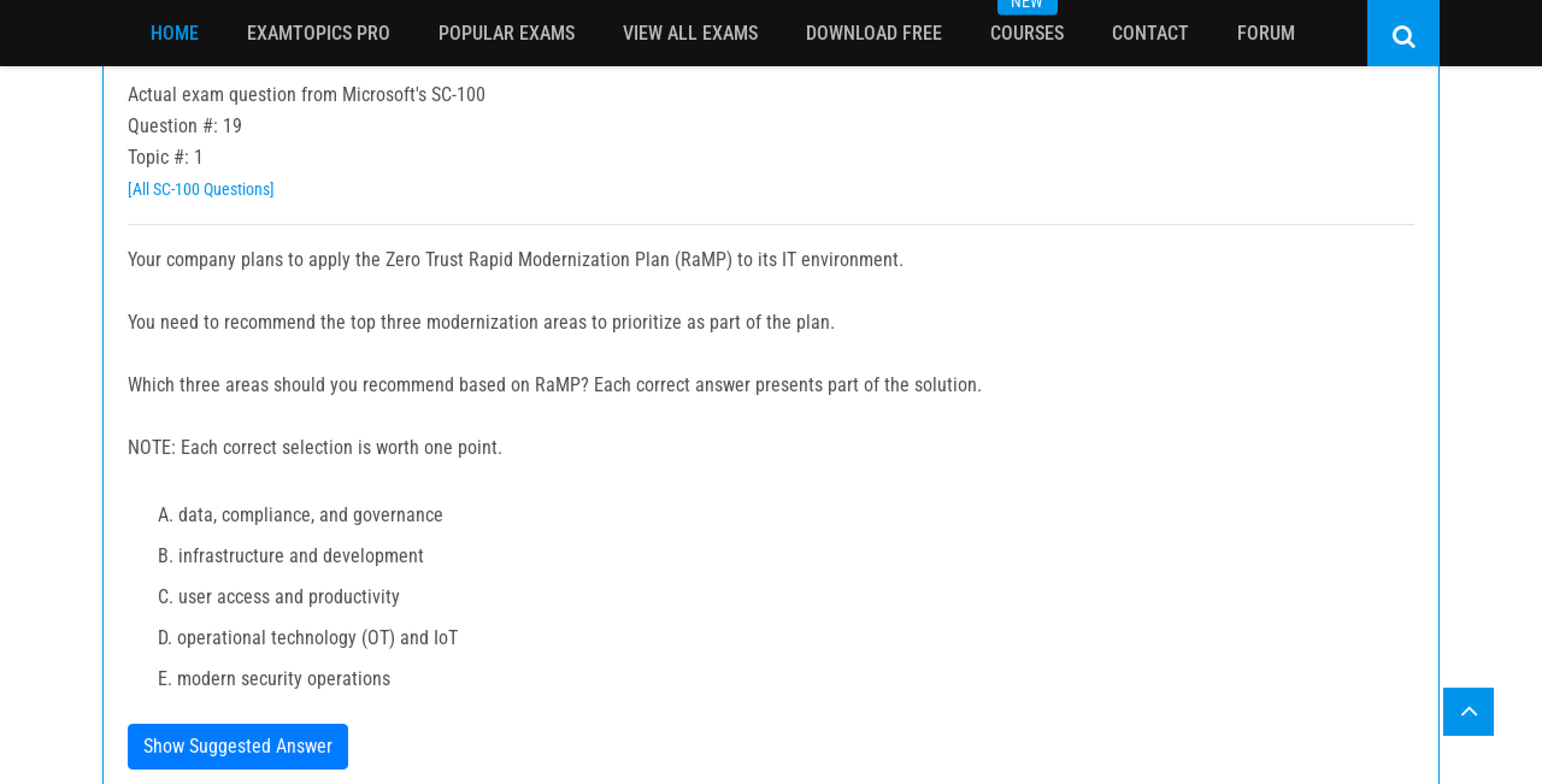
Answer Area

Developer:
- Enterprise security
- Privileged security
- Specialized security

Standard user:
- Enterprise security
- Privileged security
- Specialized security

IT administrator:
- Enterprise security
- Privileged security
- Specialized security

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 19
Topic #: 1
[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

Question #: 20

Topic #: 1

[All SC-100 Questions]

HOTSPOT

-

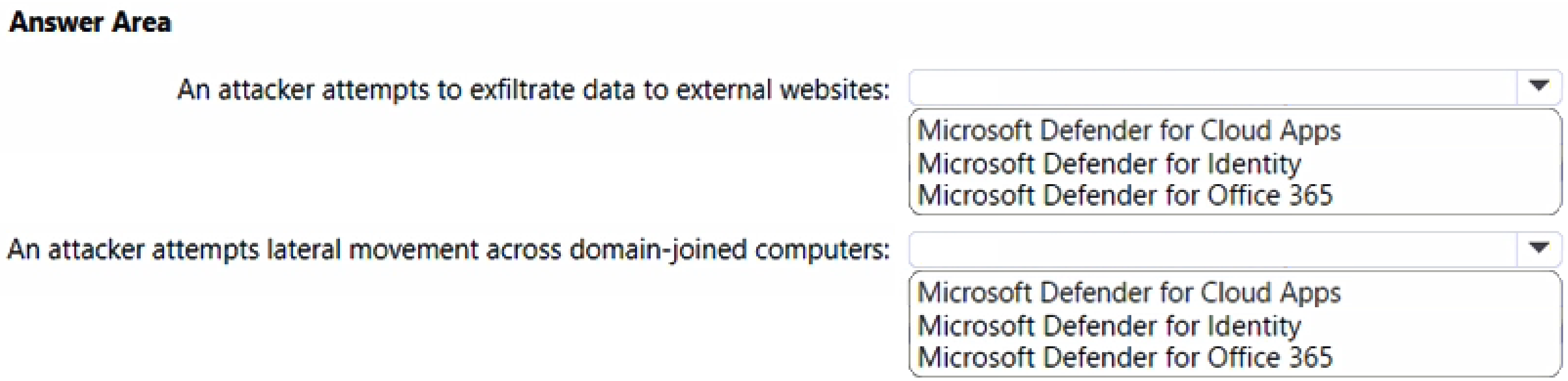
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA).

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 21

Topic #: 1

[All SC-100 Questions]

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

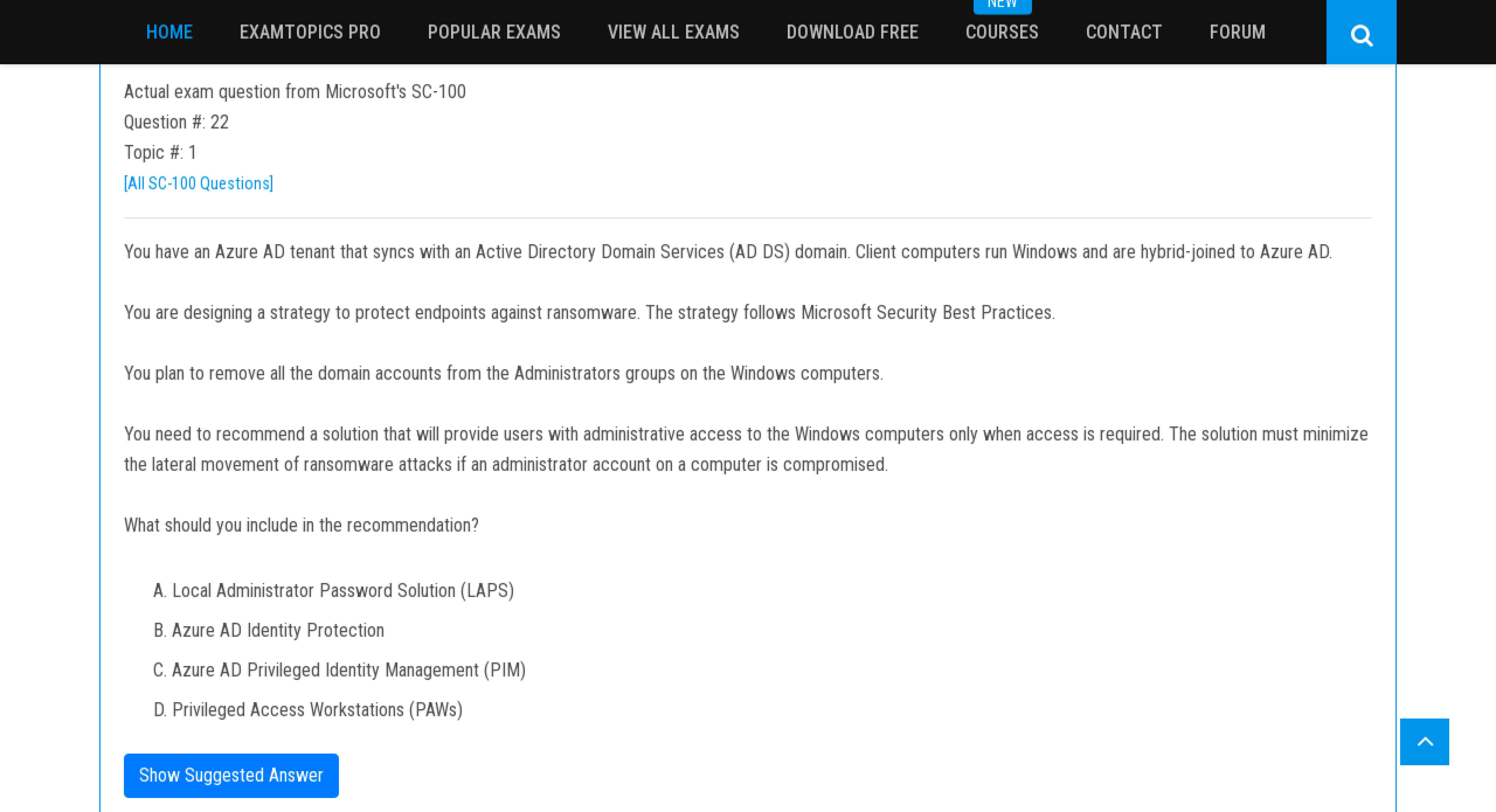
B. managed identities in Azure

C. Azure service principals with usernames and passwords

D. device registrations in Azure AD

E. Azure service principals with certificate credentials

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 22
Topic #: 1
[All SC-100 Questions]

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)

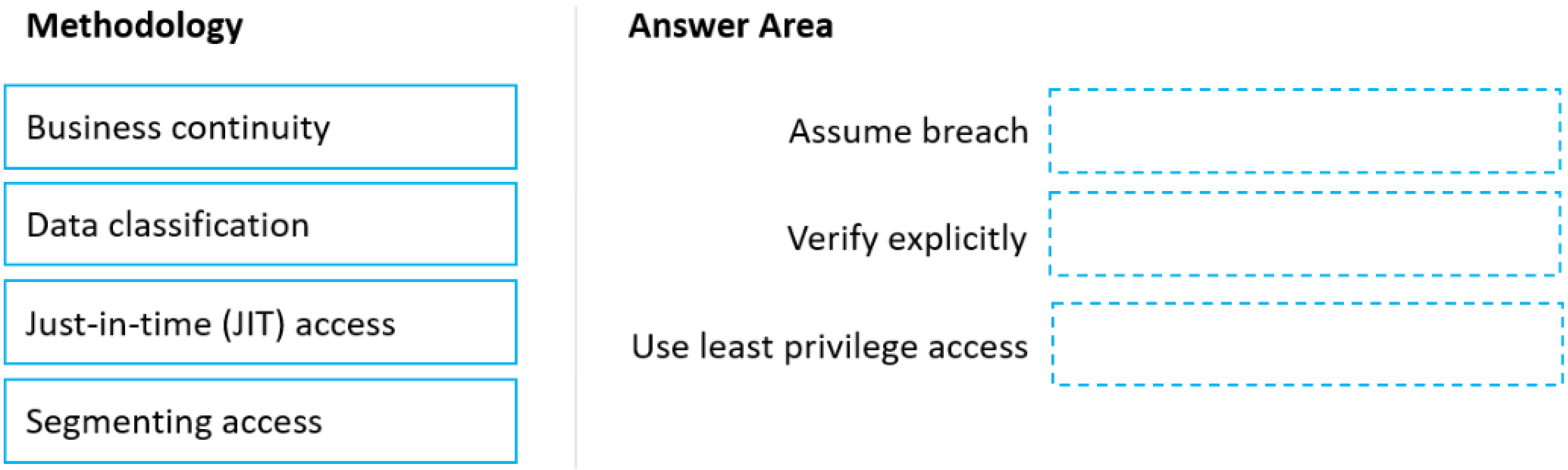
Actual exam question from Microsoft's SC-100
Question #: 23
Topic #: 1
[All SC-100 Questions]

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.



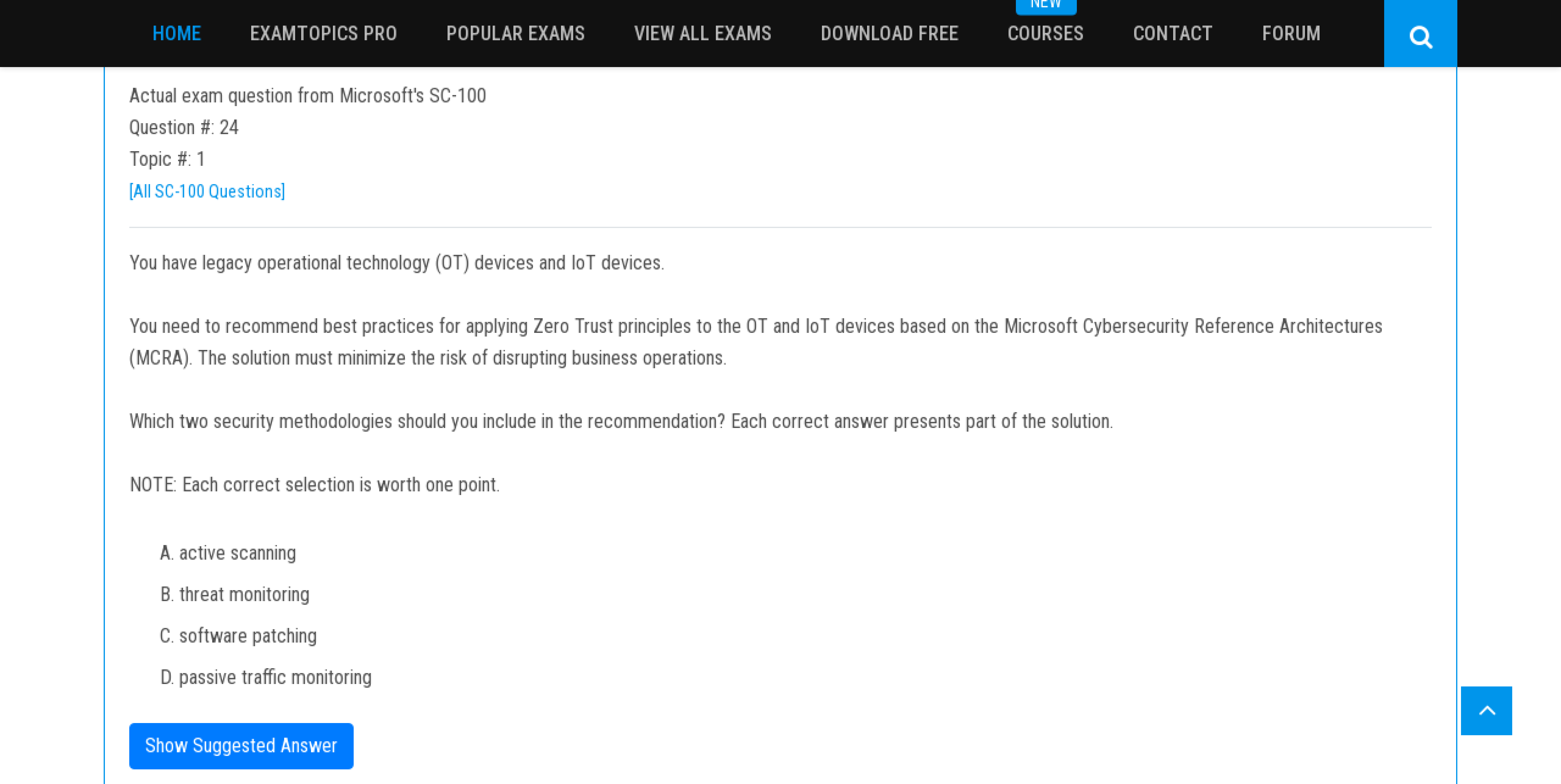
Methodology

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

Answer Area

Assume breach
Verify explicitly
Use least privilege access

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 24
Topic #: 1
[All SC-100 Questions]

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.

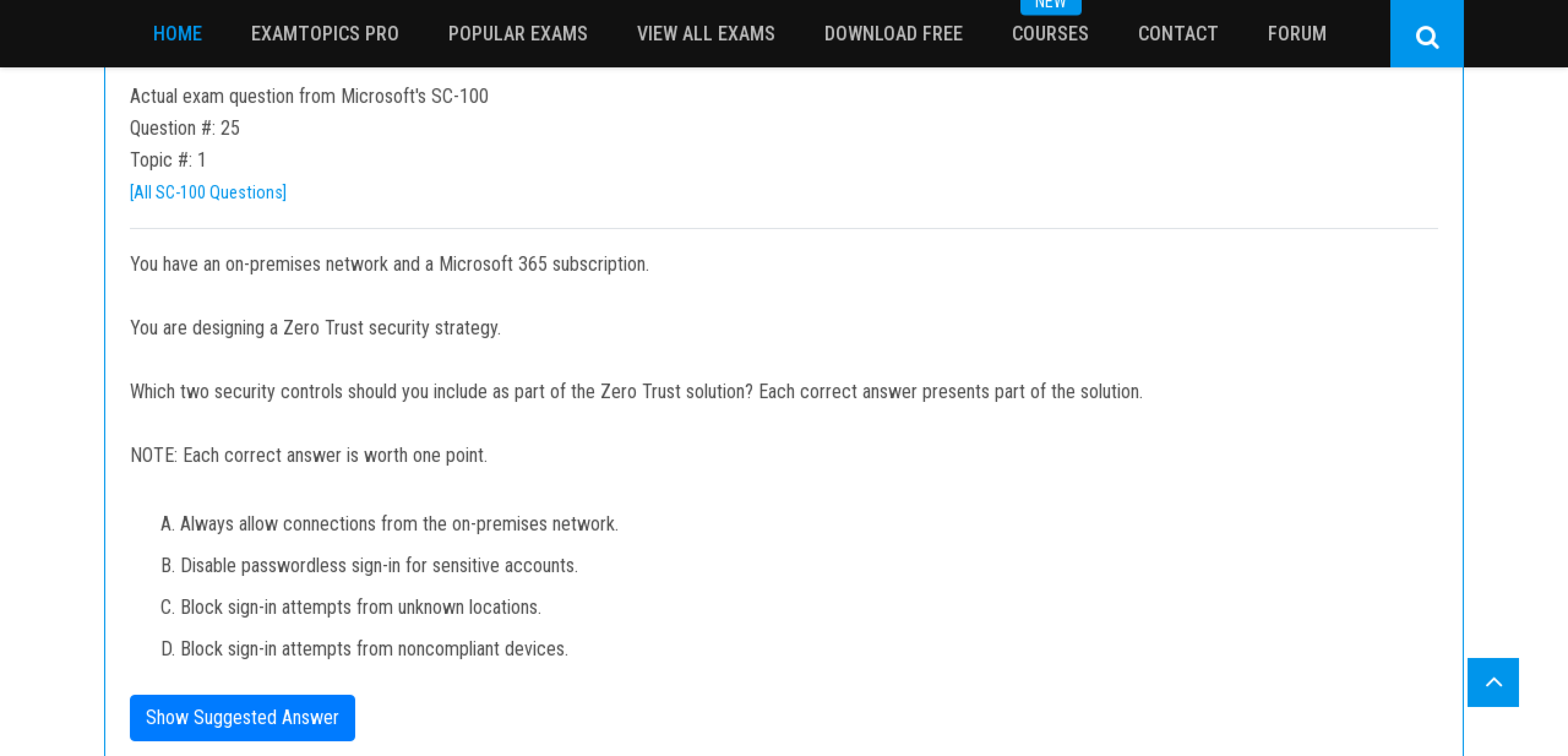
A. active scanning

B. threat monitoring

C. software patching

D. passive traffic monitoring

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 25
Topic #: 1
[All SC-100 Questions]

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.

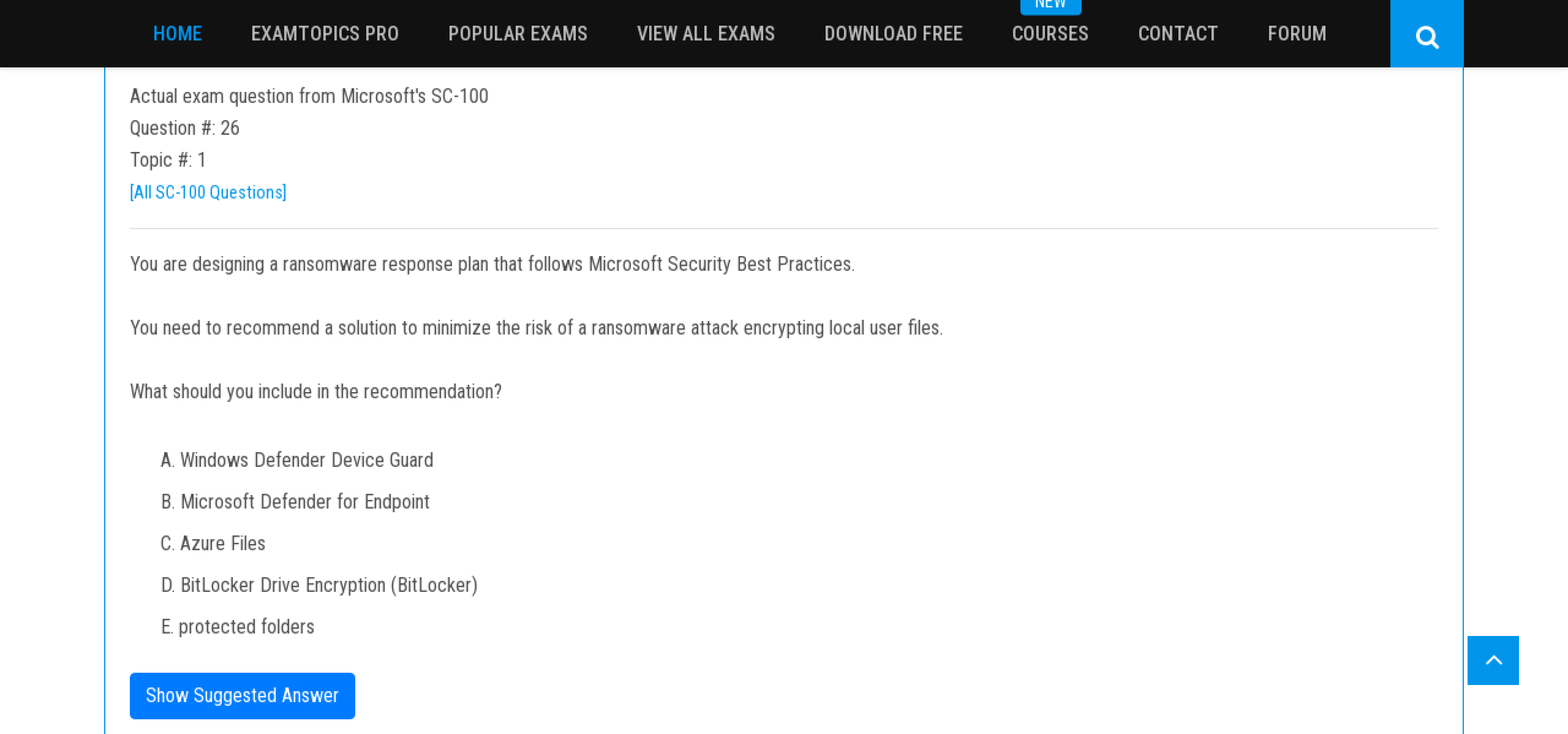
NOTE: Each correct answer is worth one point.

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.



Actual exam question from Microsoft's SC-100
Question #: 26
Topic #: 1
[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100
Question #: 27
Topic #: 1
[All SC-100 Questions]

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?

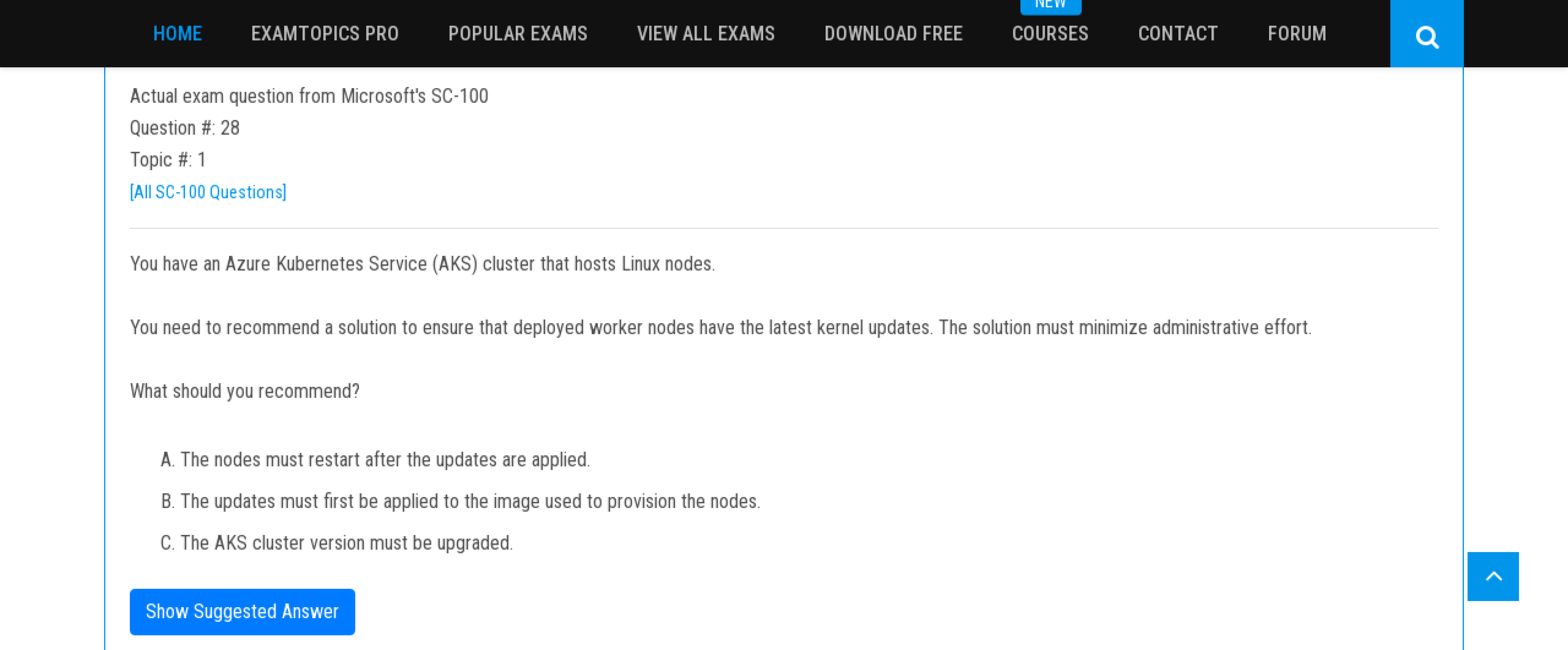
A. a managed identity in Azure

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

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 28

Topic #: 1

[All SC-100 Questions]

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

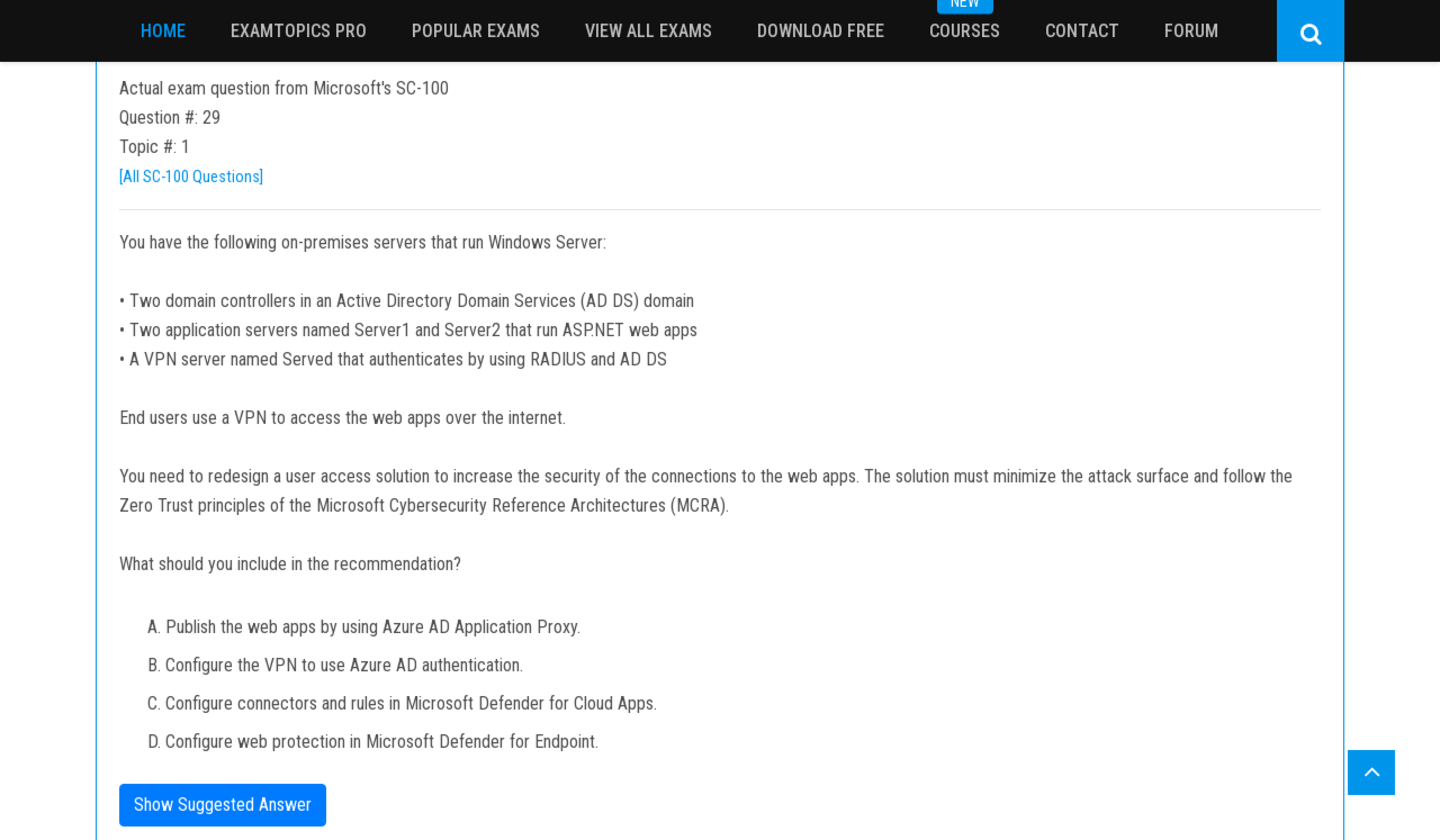
You need to recommend a solution to ensure that deployed worker nodes have the latest kernel updates. The solution must minimize administrative effort.

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.



Actual exam question from Microsoft's SC-100

Question #: 29

Topic #: 1

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 30

Topic #: 1

[All SC-100 Questions]

HOTSPOT

-

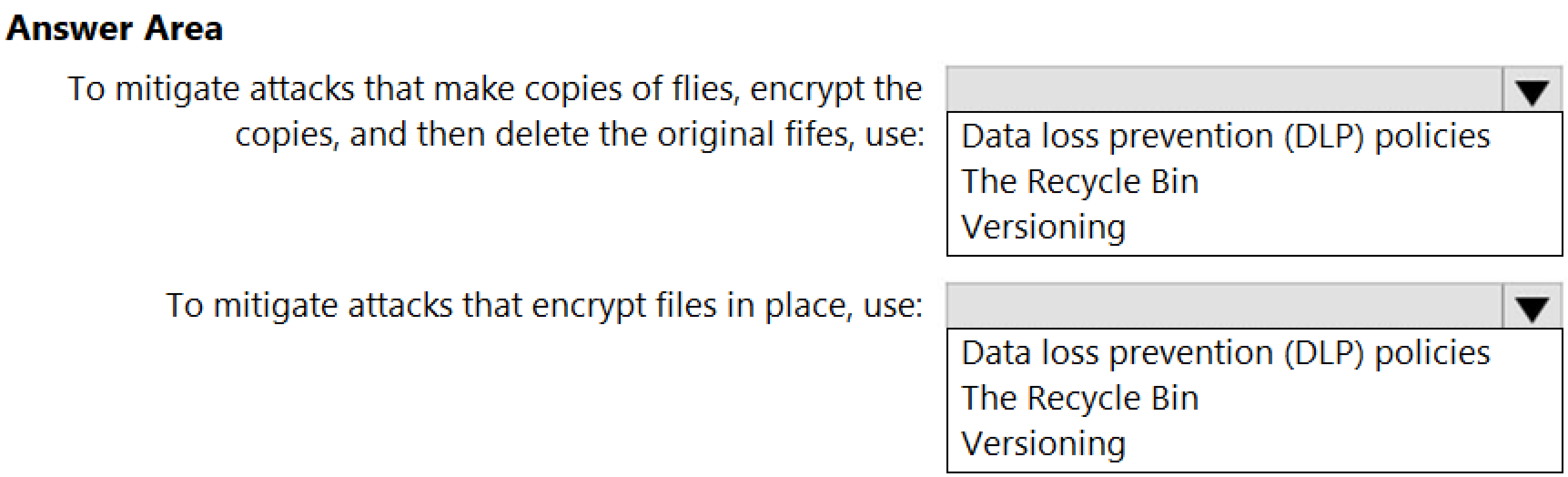
You have a Microsoft 365 E5 subscription that uses Microsoft Purview, SharePoint Online, and OneDrive for Business.

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

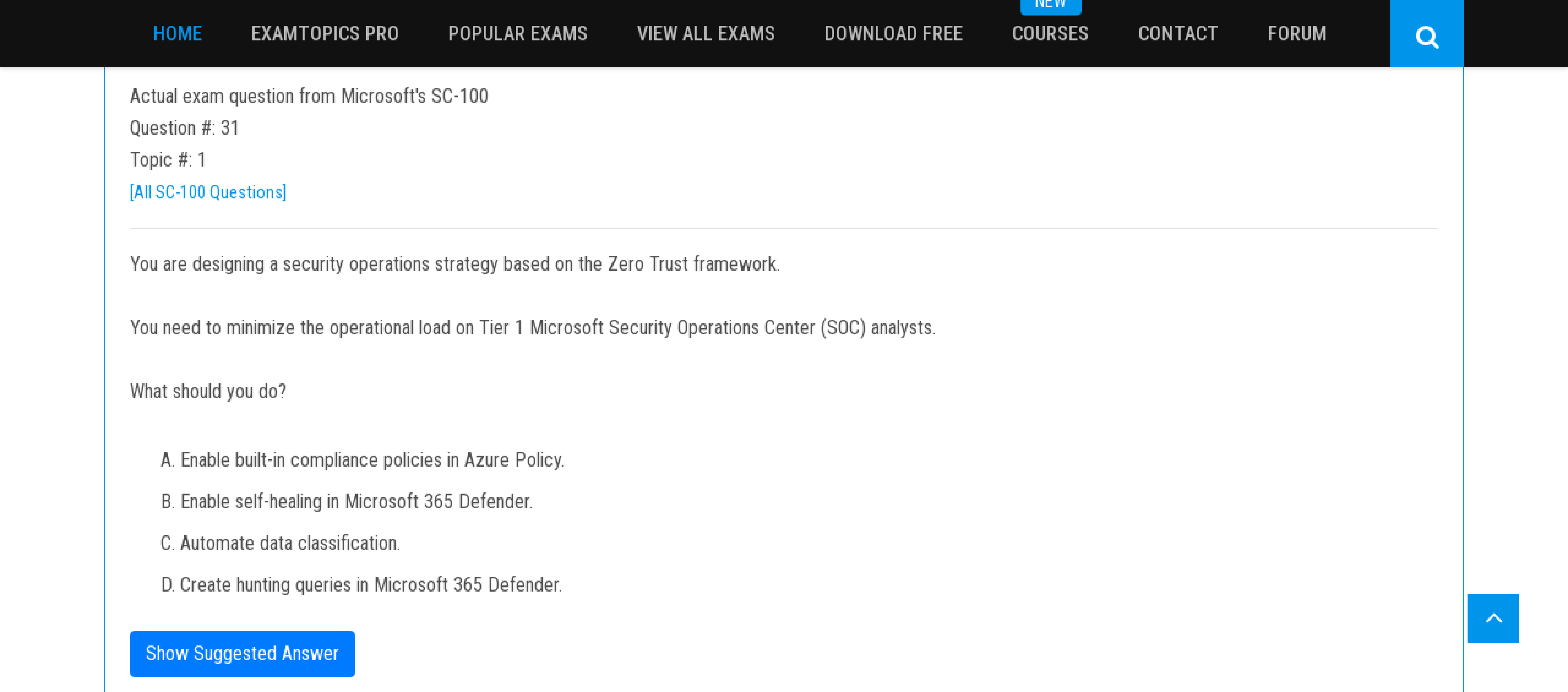
To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use:

- 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

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 31
Topic #: 1
[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 32

Topic #: 1

[All SC-100 Questions]

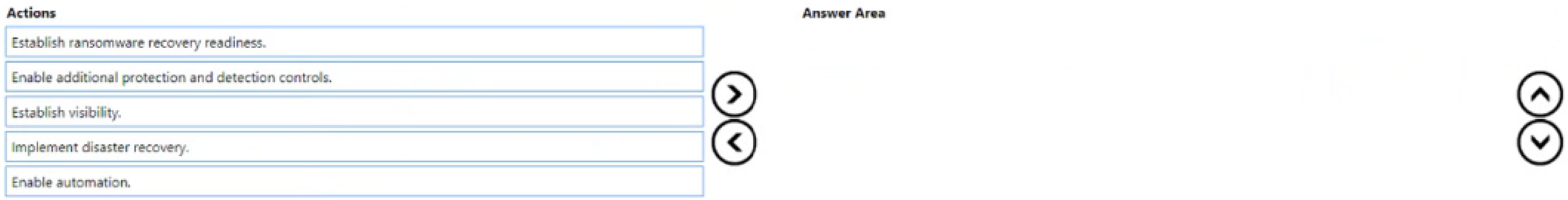
DRAG DROP

-

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.

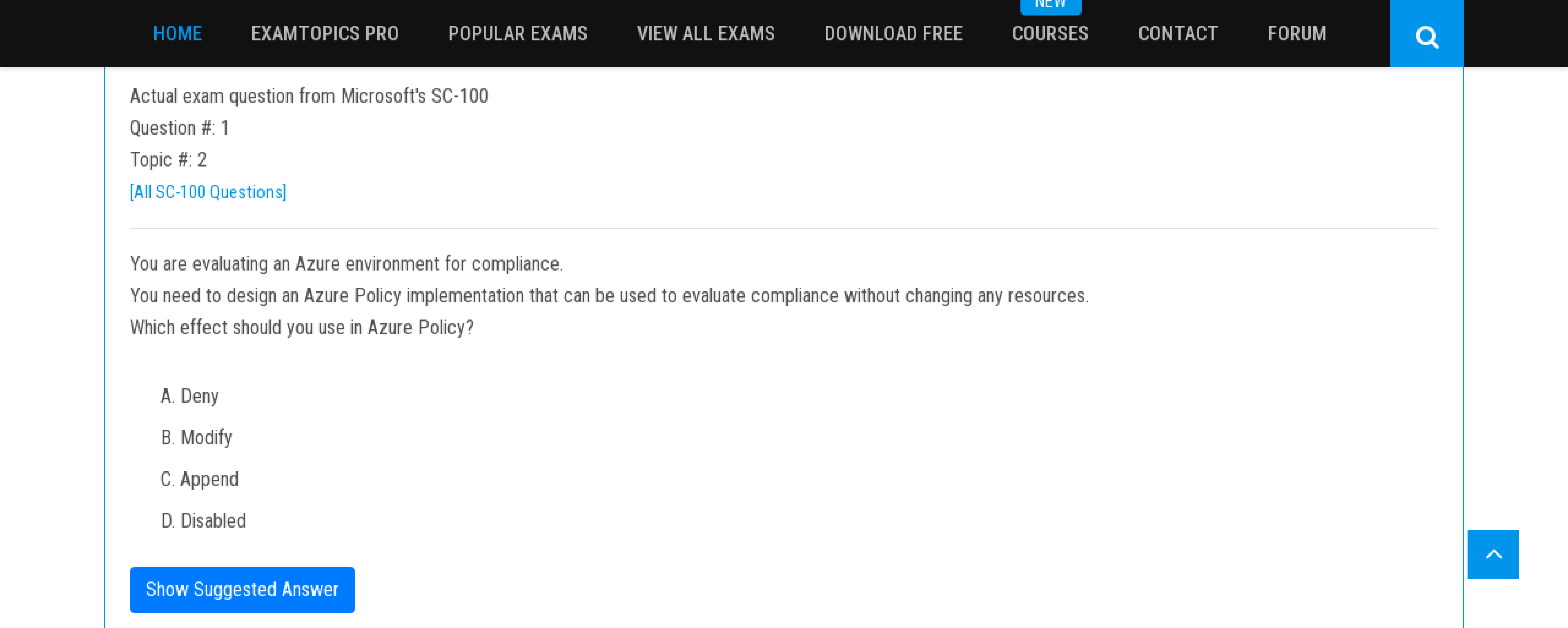
Establish visibility.

Implement disaster recovery.

Enable automation.

Answer Area

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 1

Topic #: 2

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

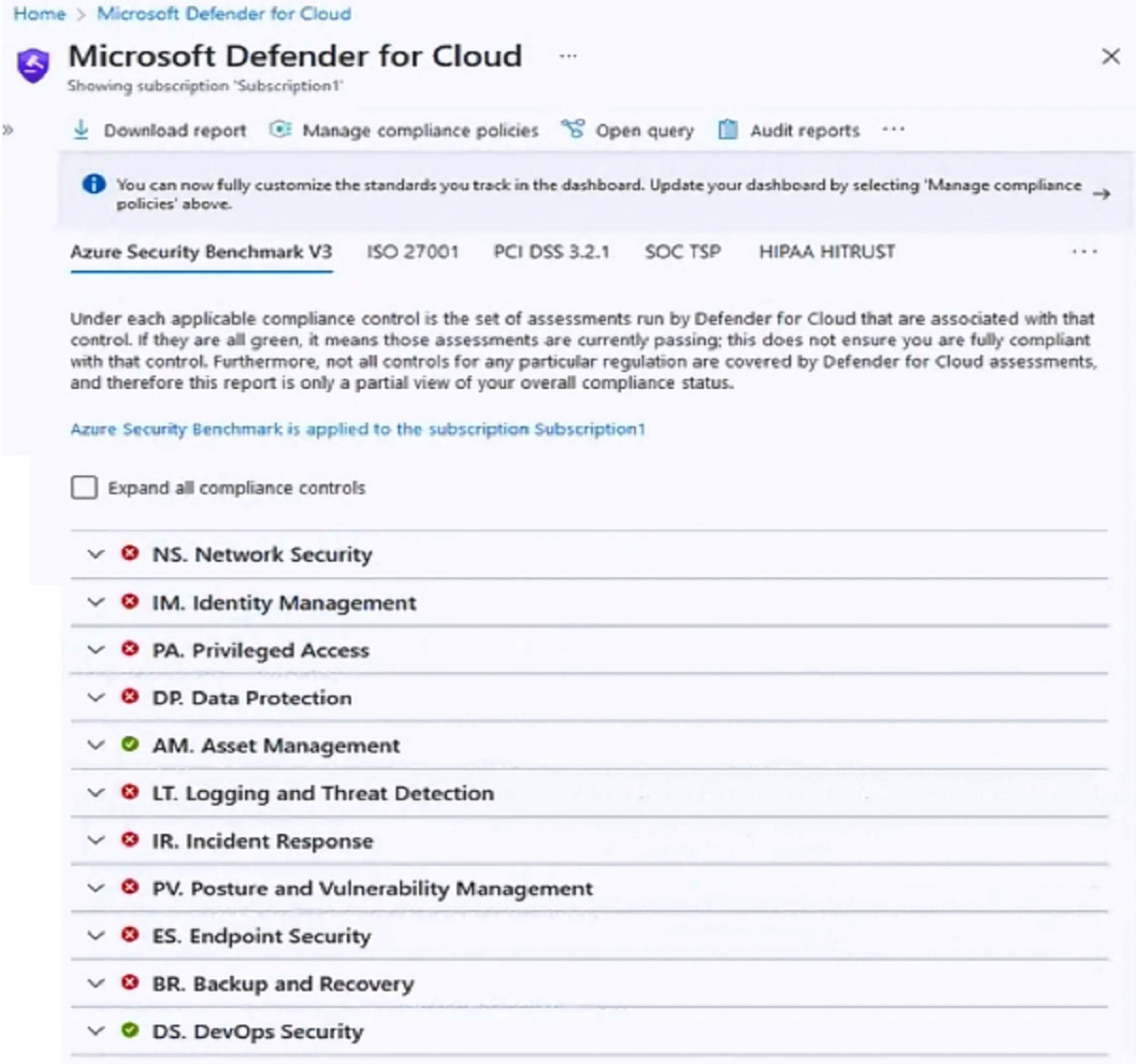
Question #: 2

Topic #: 2

[All SC-100 Questions]

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
Microsoft Defender for Cloud ...
Showing subscription 'Subscription1'
Download report
Manage compliance policies
Open query
Audit reports
...

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Azure Security Benchmark V3
ISO 27001
PCI DSS 3.2.1
SOC TSP
HIPAA HITRUST

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 3

Topic #: 2

[All SC-100 Questions]

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

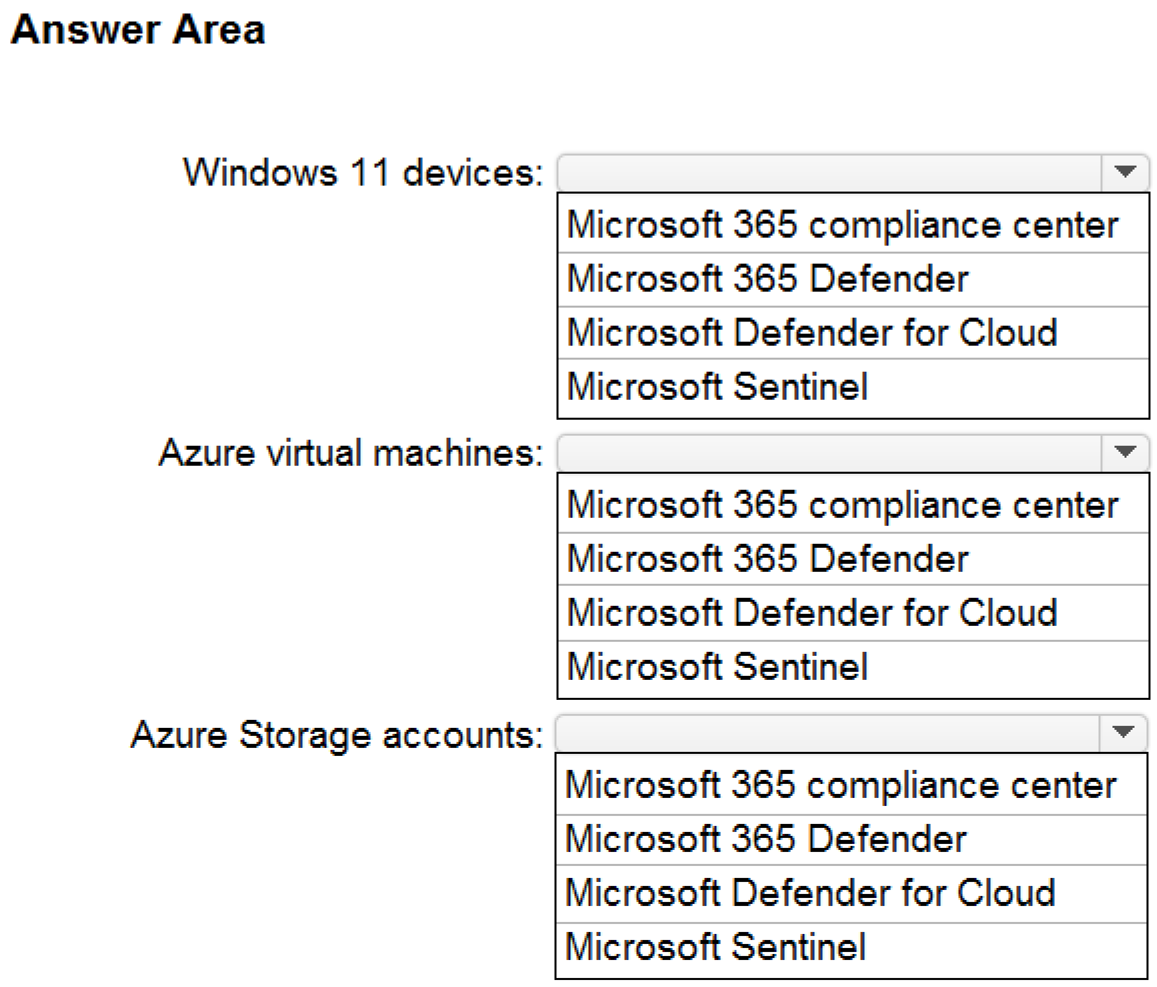
✑ Azure Storage accounts

✑ 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:

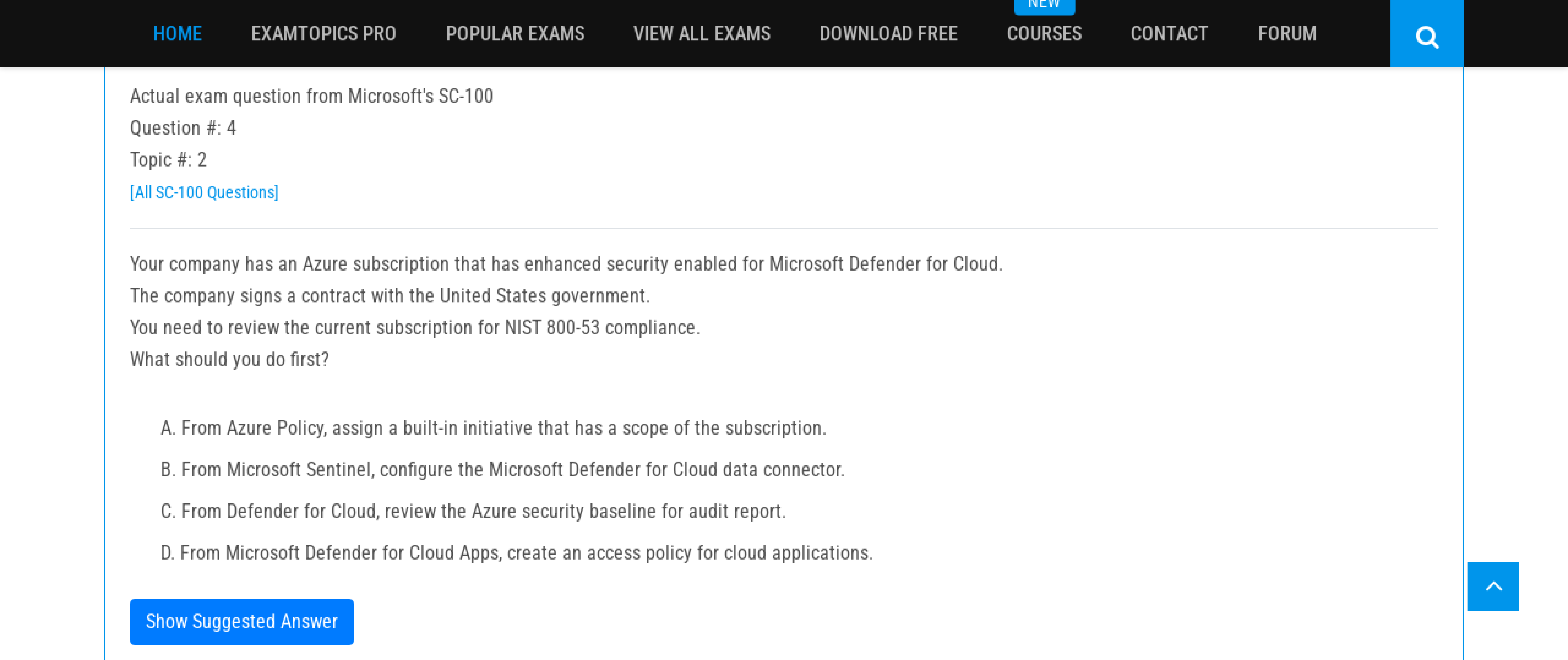


Answer Area

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



HOME EXAMTOPICS PRO POPULAR EXAMS VIEW ALL EXAMS DOWNLOAD FREE NEW COURSES CONTACT FORUM

Actual exam question from Microsoft's SC-100

Question #: 4

Topic #: 2

[All SC-100 Questions]

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.

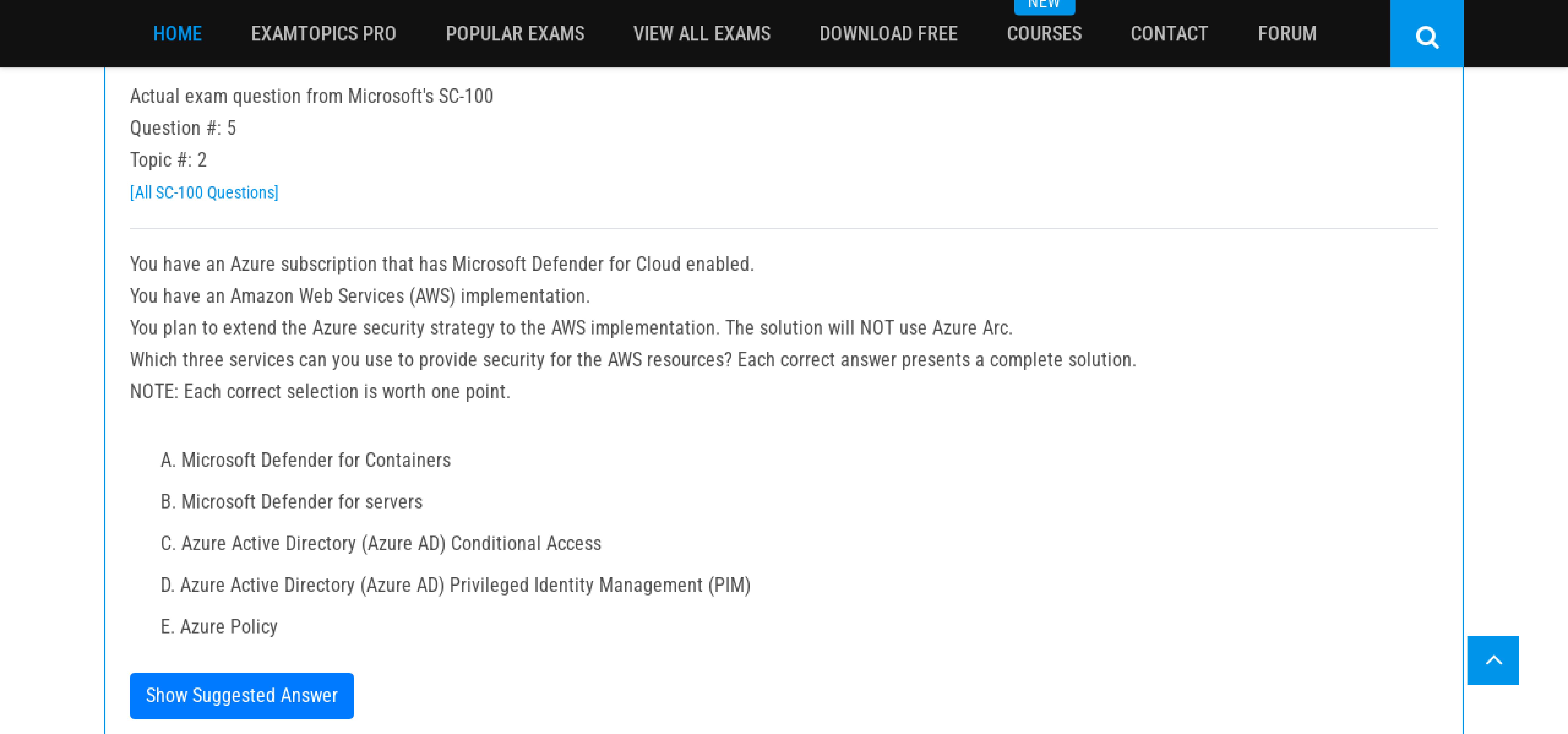
What should you do first?

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.



Actual exam question from Microsoft's SC-100

Question #: 5

Topic #: 2

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

Question #: 6

Topic #: 2

[All SC-100 Questions]

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.

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 7

Topic #: 2

[All SC-100 Questions]

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

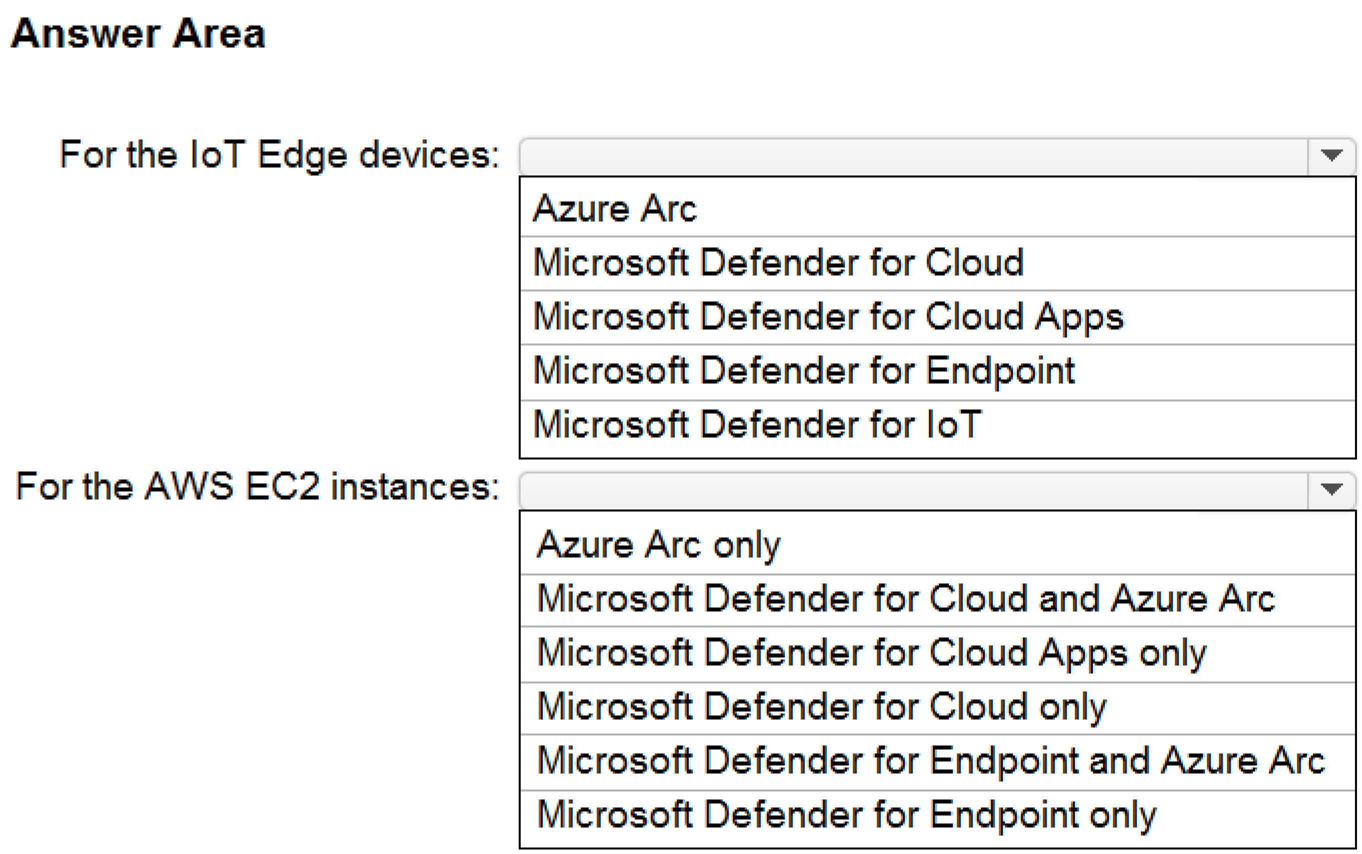
AWS EC2 instances -

.

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 8

Topic #: 2

[All SC-100 Questions]

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?

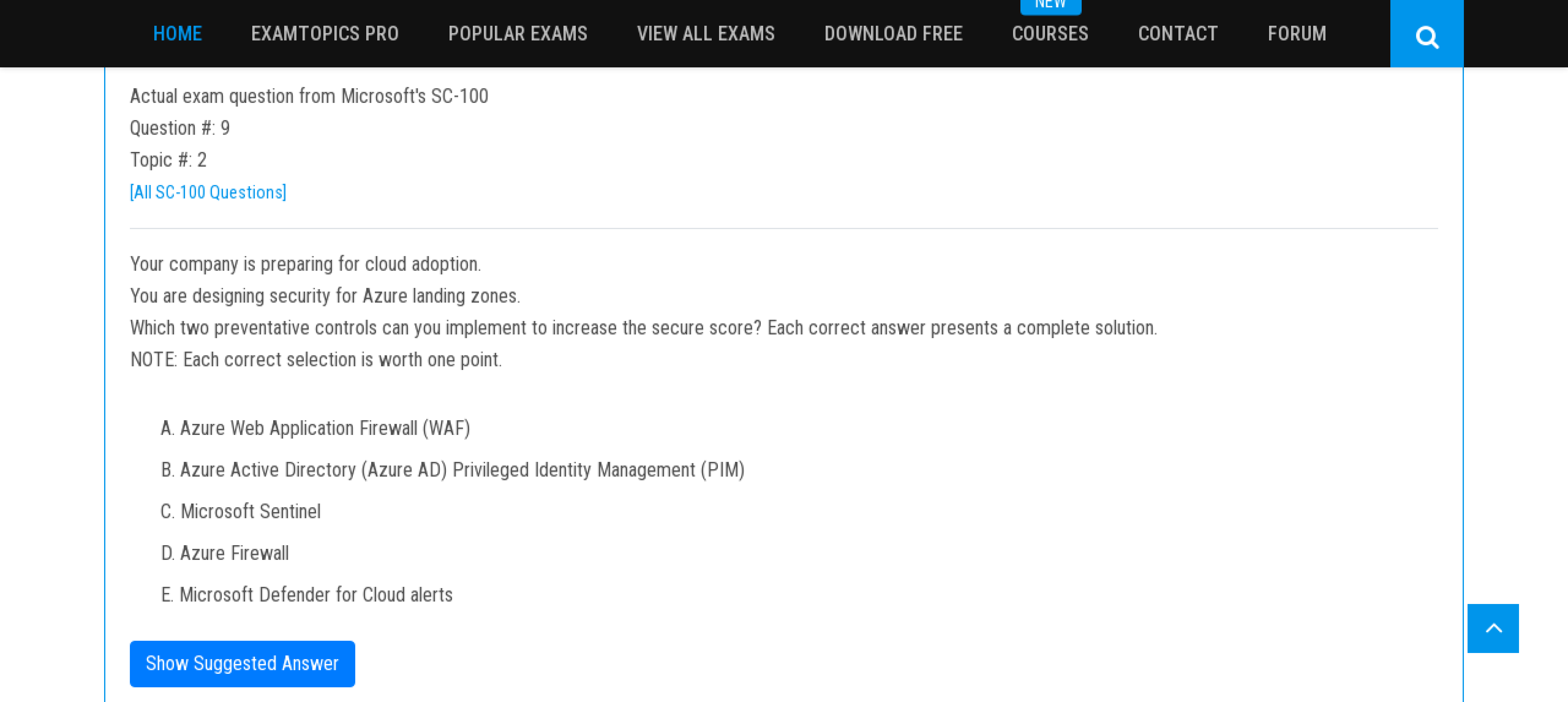
A. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

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.

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 9
Topic #: 2
[All SC-100 Questions]

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)

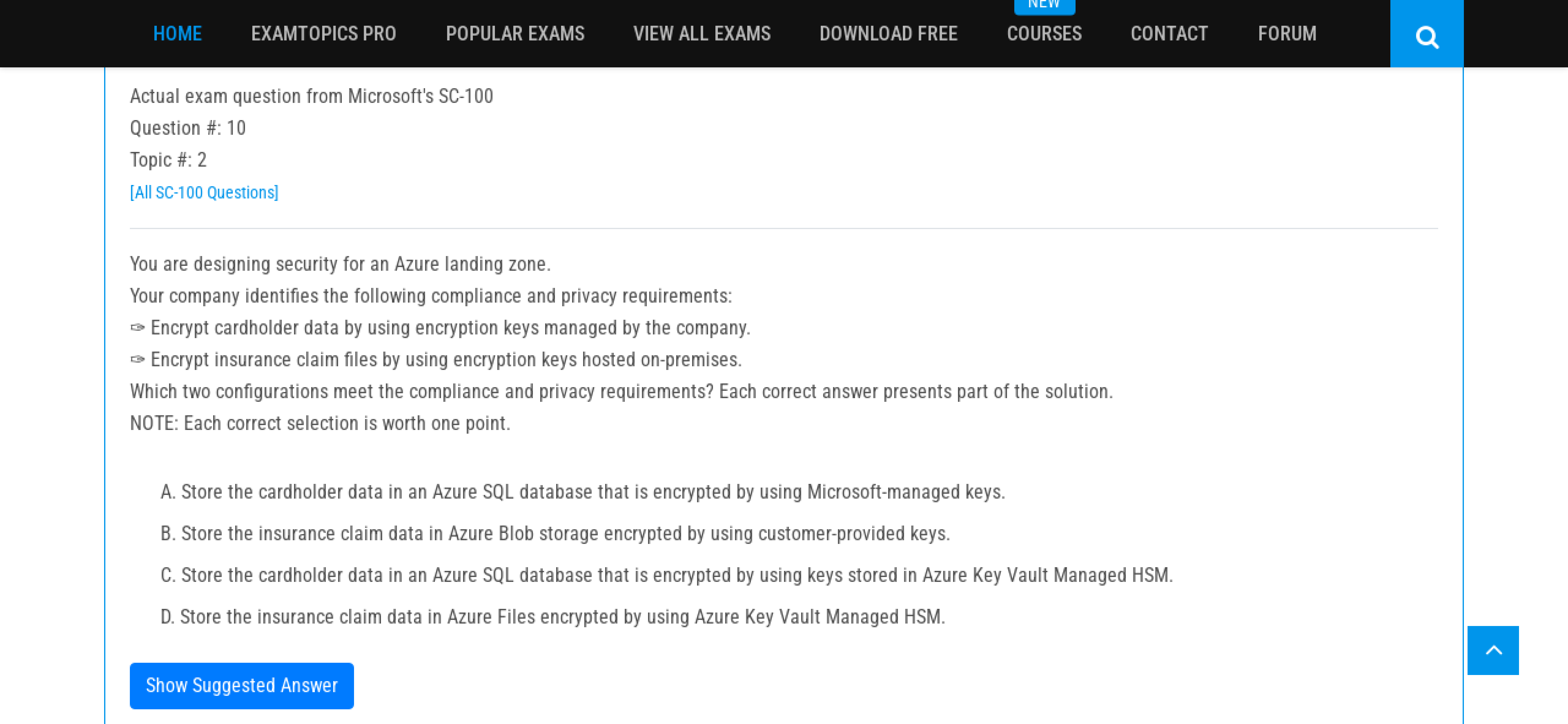
B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 10

Topic #: 2

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 11

Topic #: 2

[All SC-100 Questions]

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)

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 12

Topic #: 2

[All SC-100 Questions]

DRAG DROP -

You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

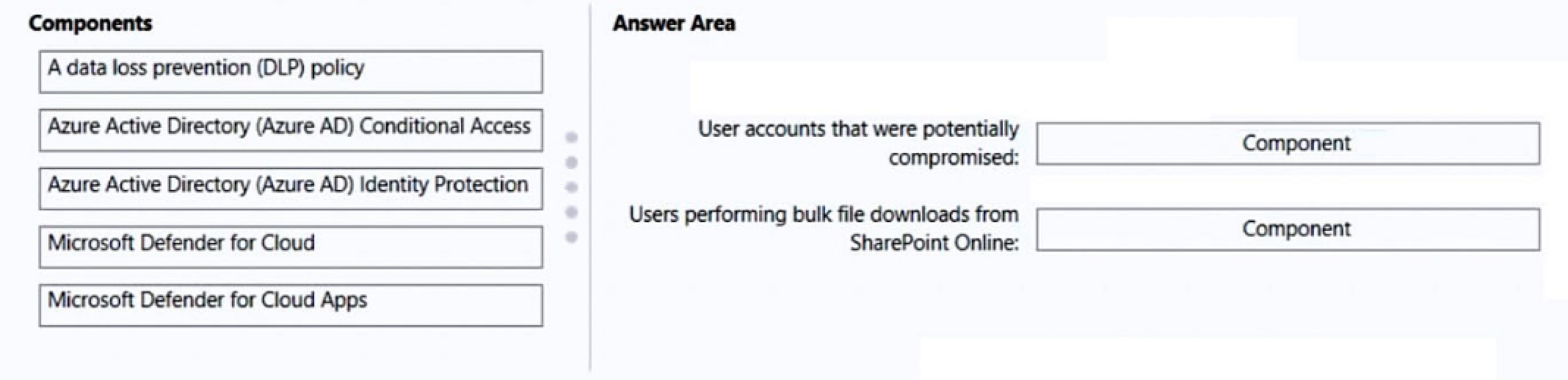
✑ User accounts that were potentially compromised

✑ 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:



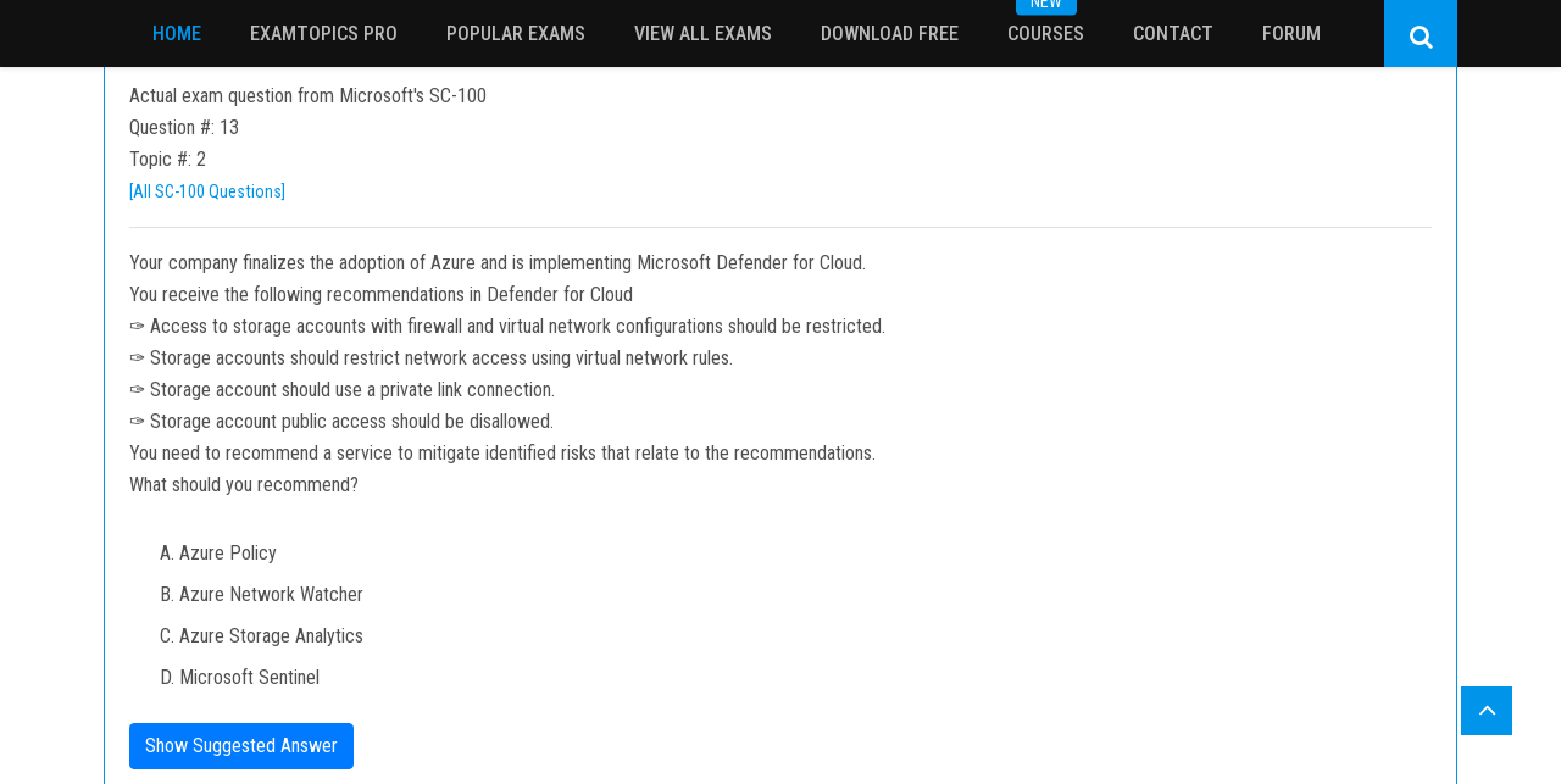
Components

- 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

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 13

Topic #: 2

[All SC-100 Questions]

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

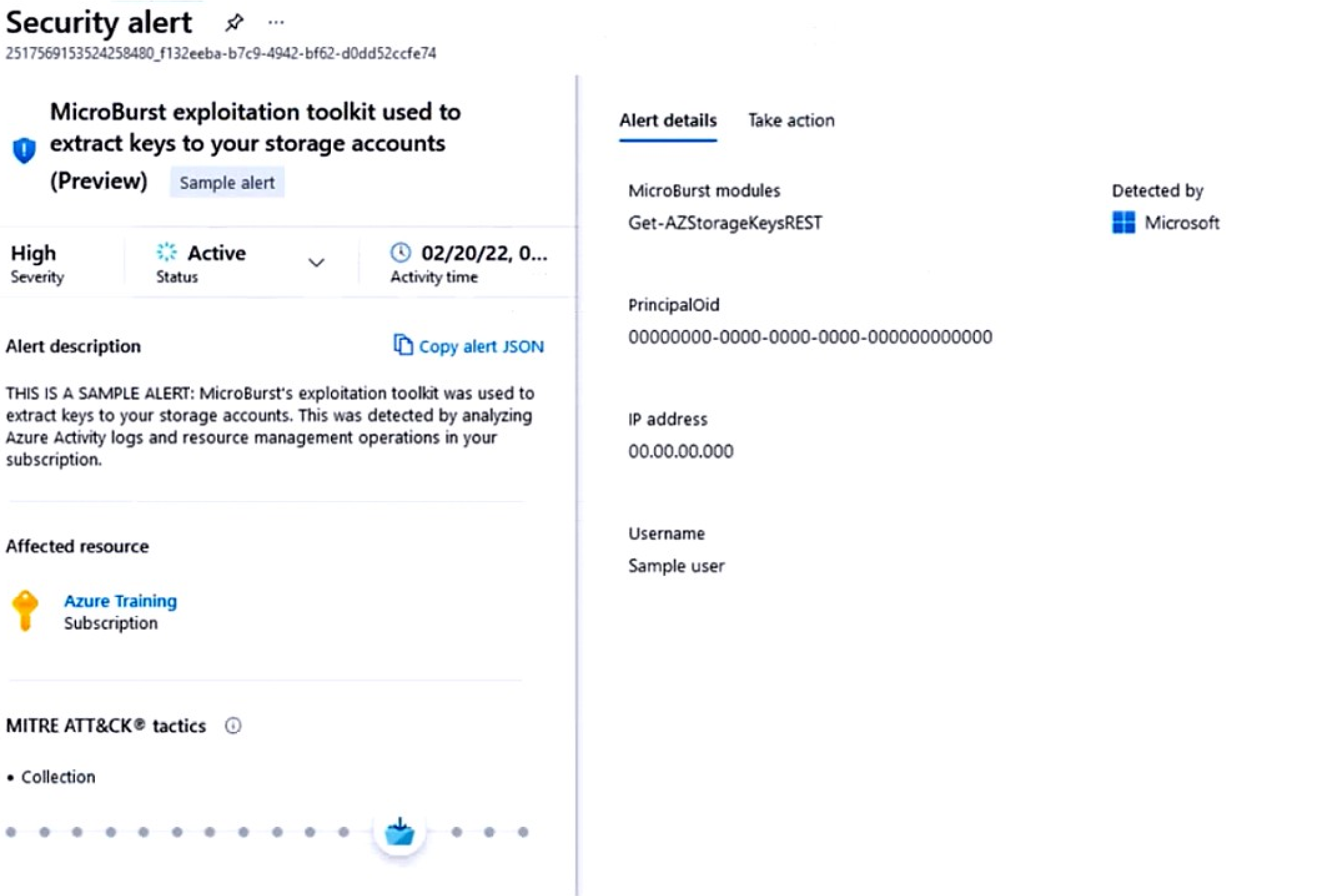
Actual exam question from Microsoft's SC-100

Question #: 14

Topic #: 2

[All SC-100 Questions]

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	Active	02/20/22, 0...
Severity	Status	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?

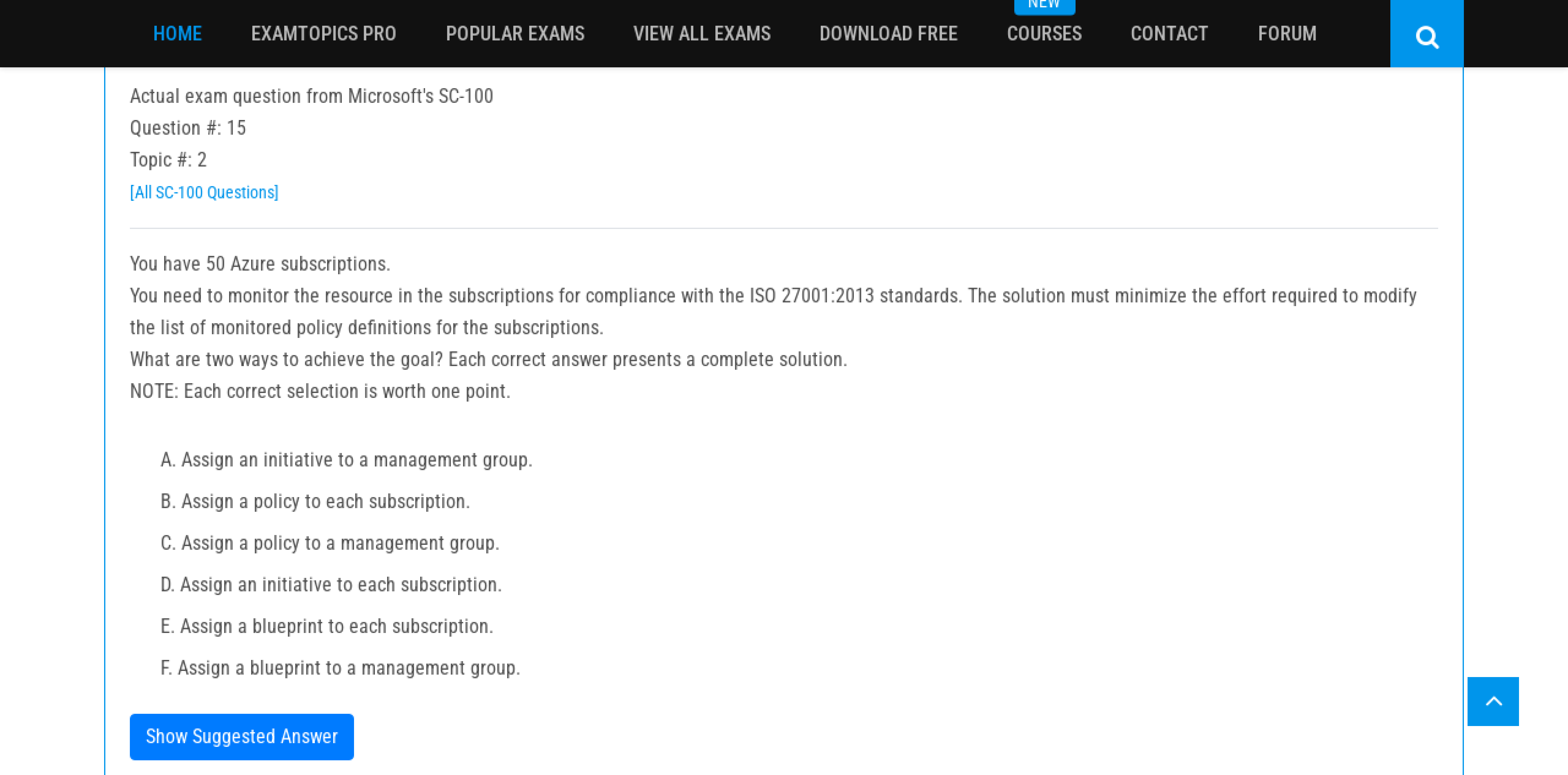
A. Storage account public access should be disallowed

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

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 15

Topic #: 2

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

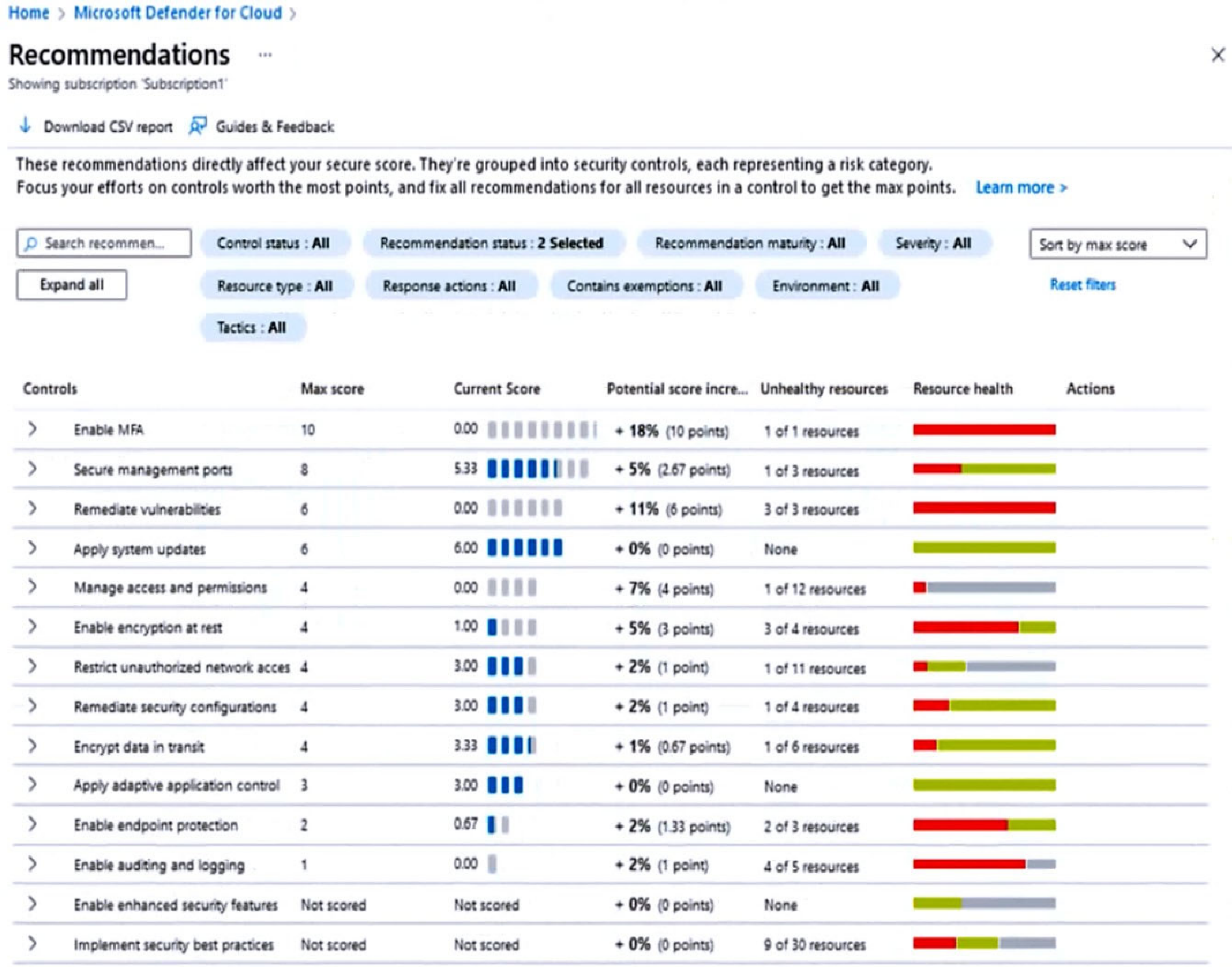
Question #: 16

Topic #: 2

[All SC-100 Questions]

HOTSPOT -

You open Microsoft Defender for Cloud as shown in the following exhibit.



Home > Microsoft Defender for Cloud >

Recommendations

Showing subscription 'Subscription1'

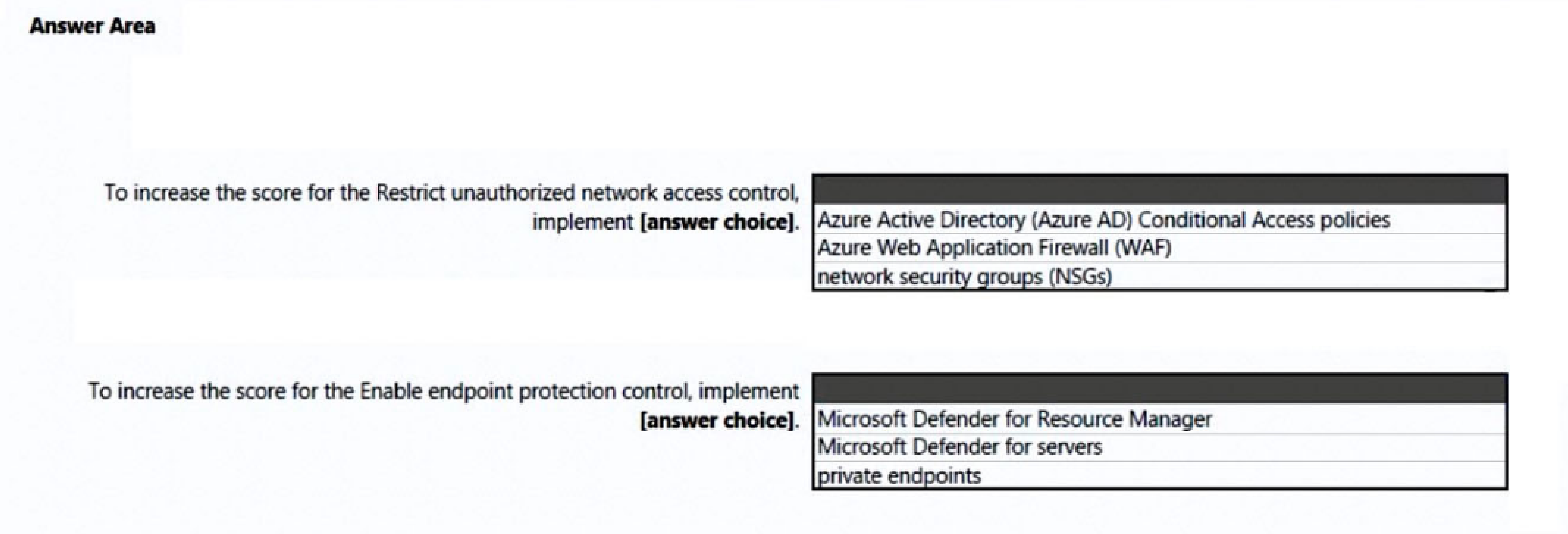
These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category. Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points. Learn more >

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

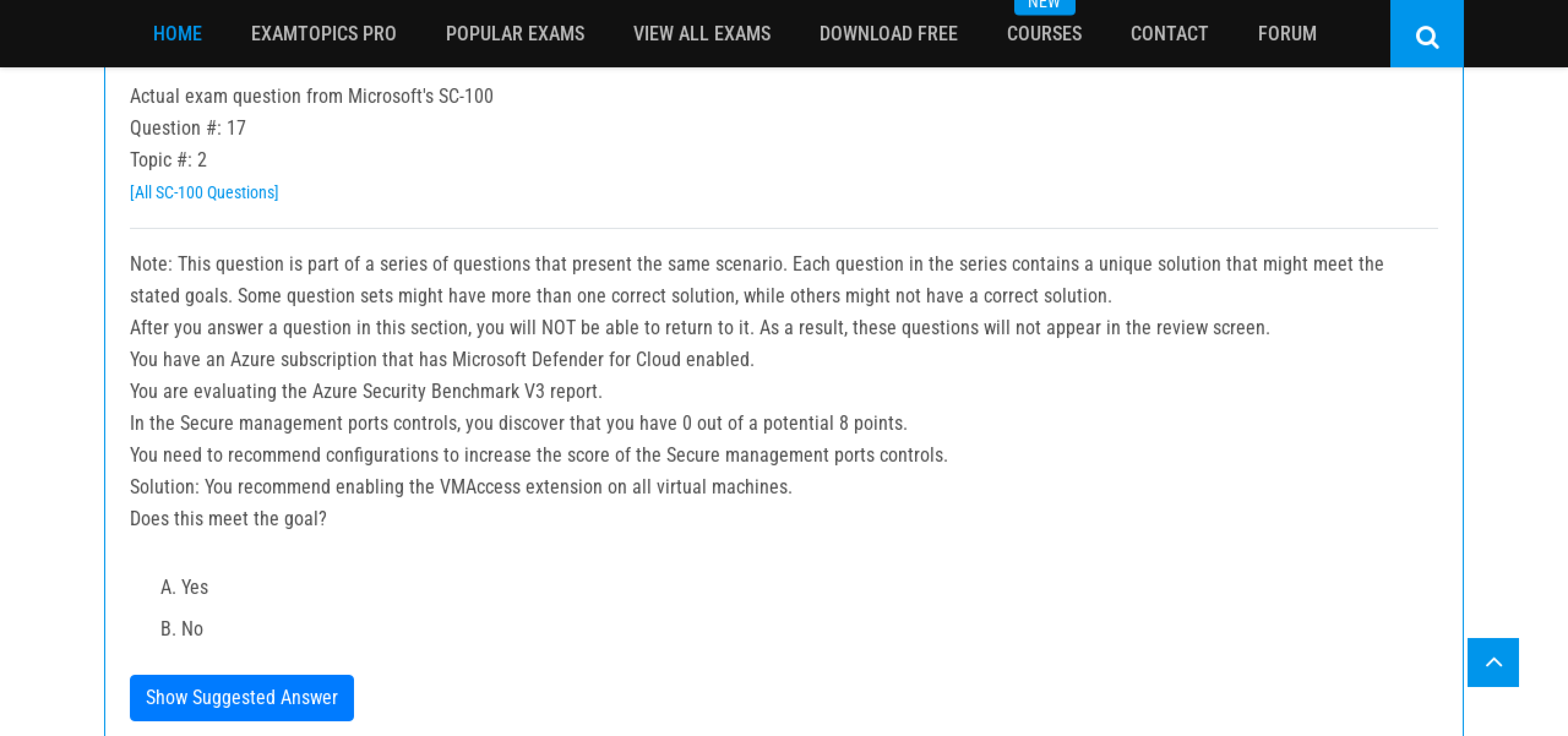
To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

- 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

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 17

Topic #: 2

[All SC-100 Questions]

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.

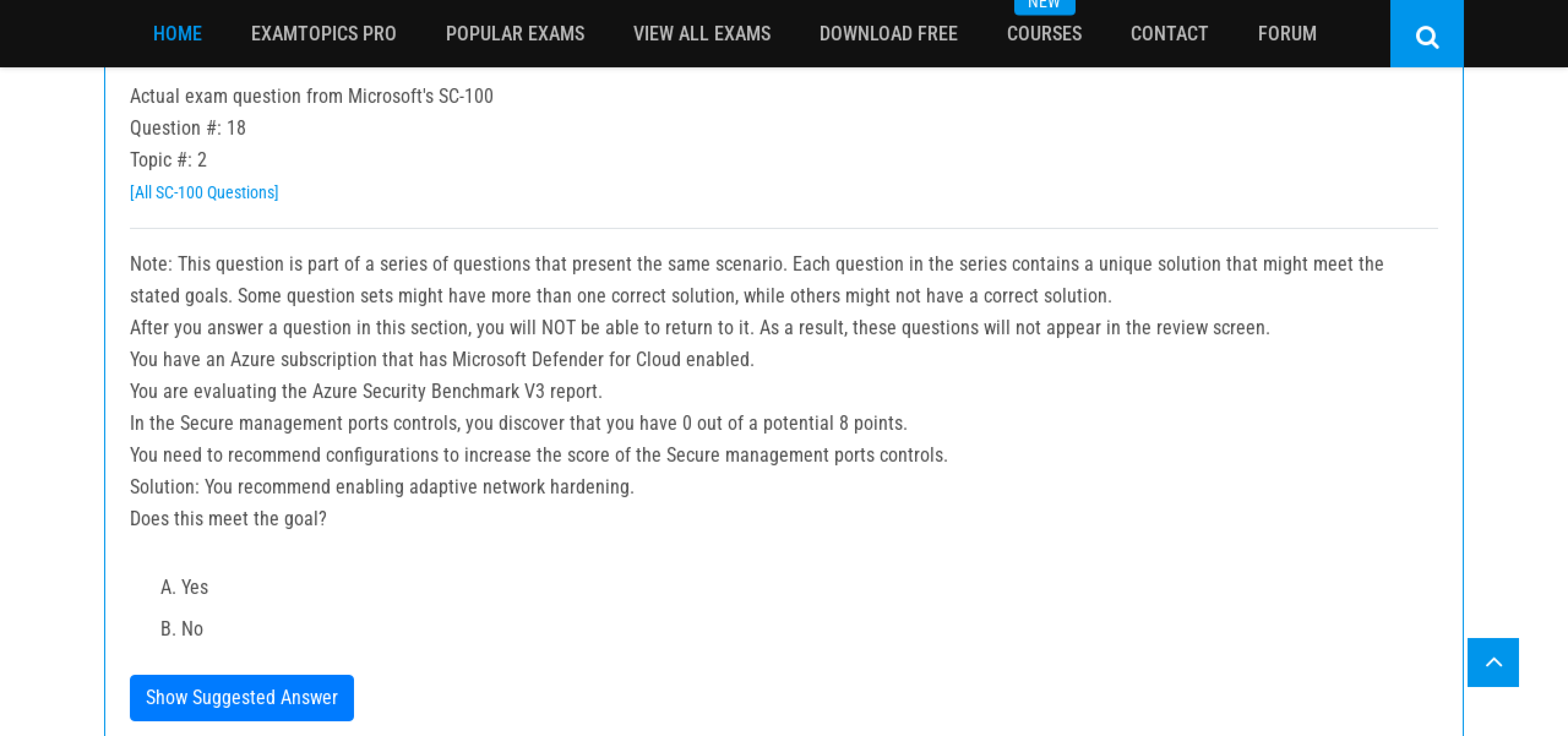
You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling the VMAccess extension on all virtual machines.

Does this meet the goal?

A. Yes

B. No



Actual exam question from Microsoft's SC-100

Question #: 18

Topic #: 2

[All SC-100 Questions]

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.

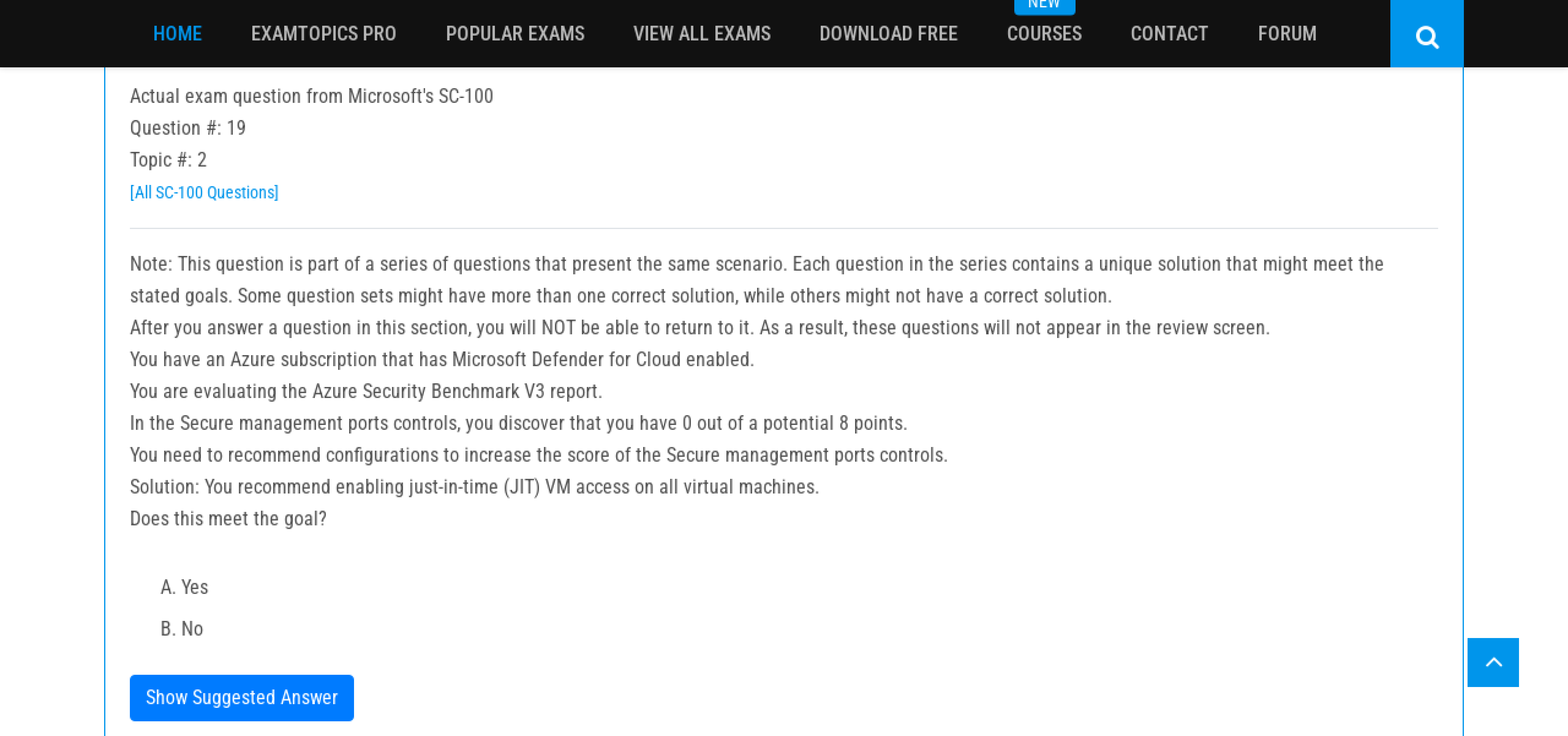
Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

A. Yes

B. No

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 19

Topic #: 2

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

Question #: 20

Topic #: 2

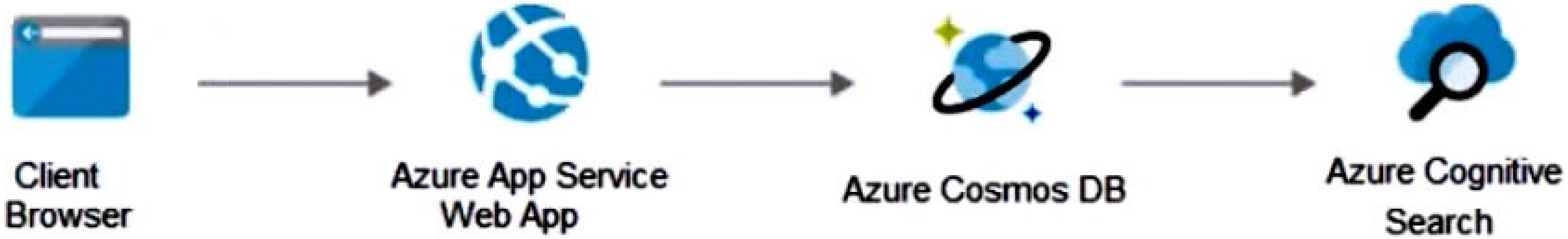
[All SC-100 Questions]

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 21

Topic #: 2

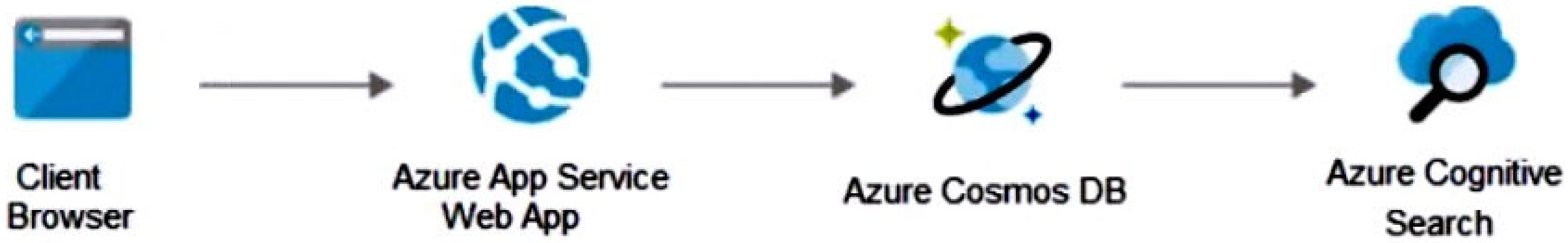
[All SC-100 Questions]

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 22

Topic #: 2

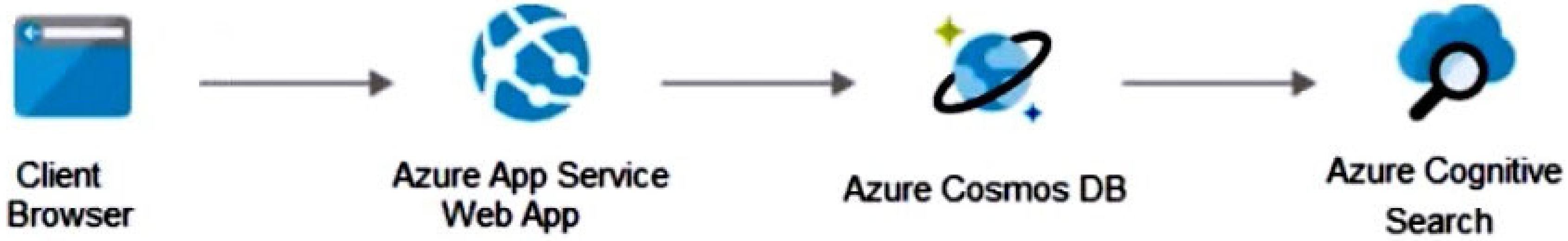
[All SC-100 Questions]

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.

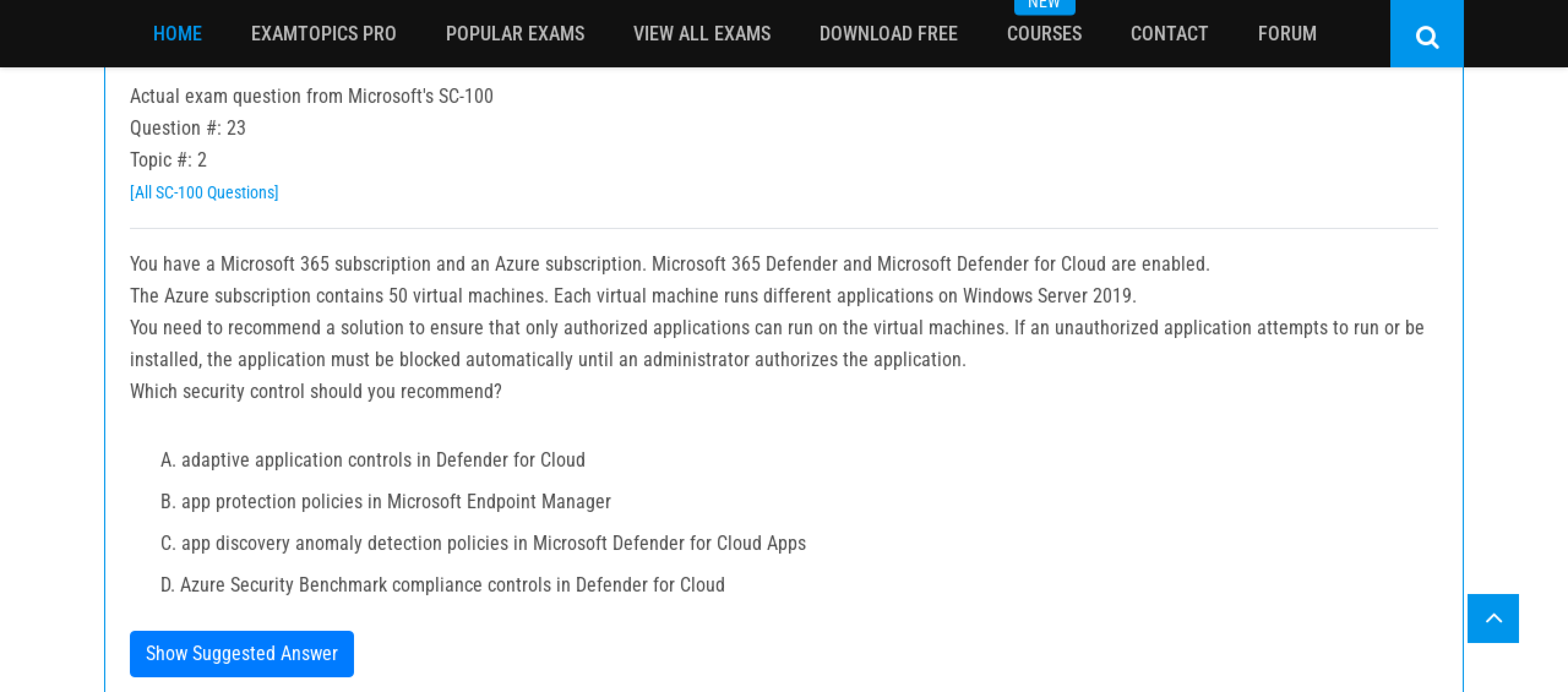
Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

A. Yes

B. No

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 23

Topic #: 2

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

Question #: 24

Topic #: 2

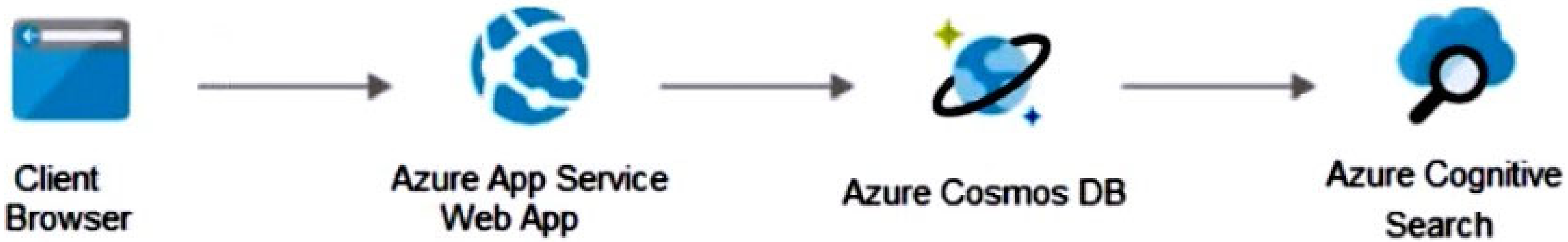
[All SC-100 Questions]

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.

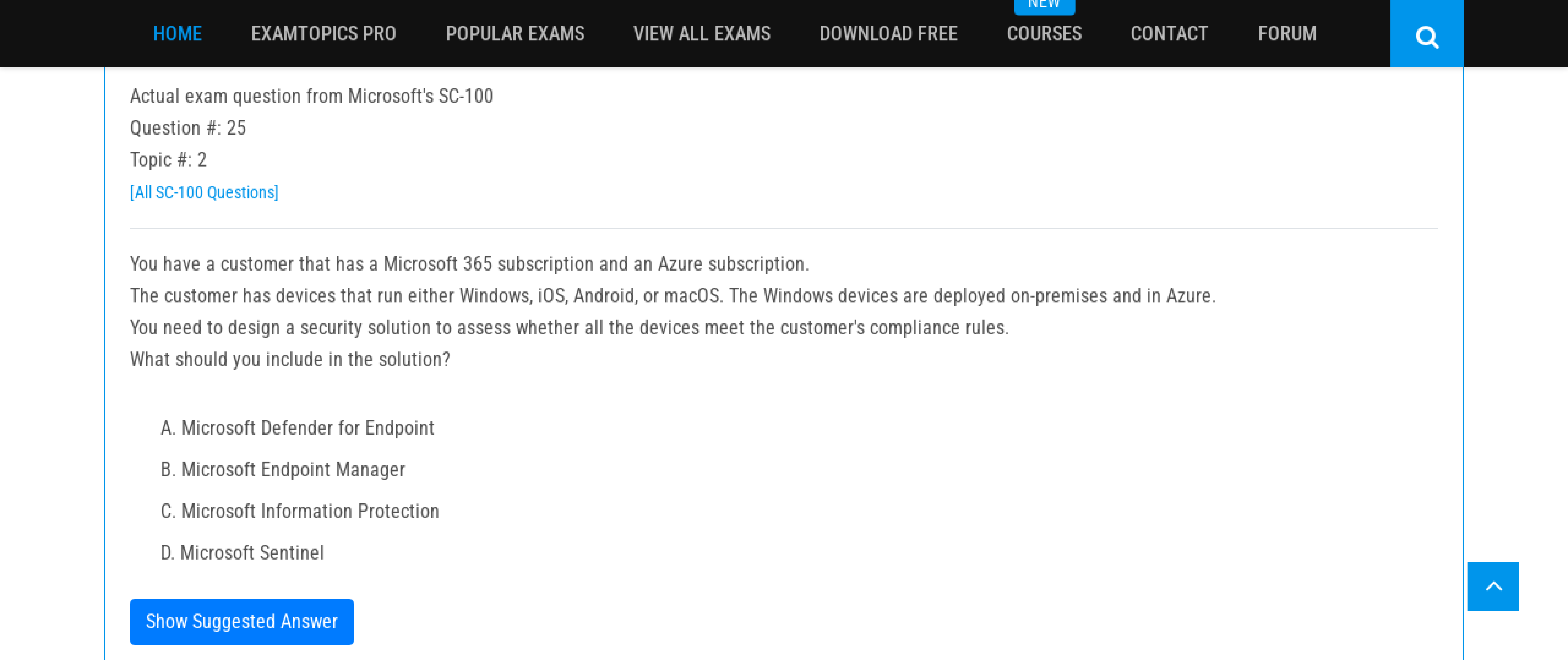
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).

Does this meet the goal?

A. Yes

B. No

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 25

Topic #: 2

[All SC-100 Questions]

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?

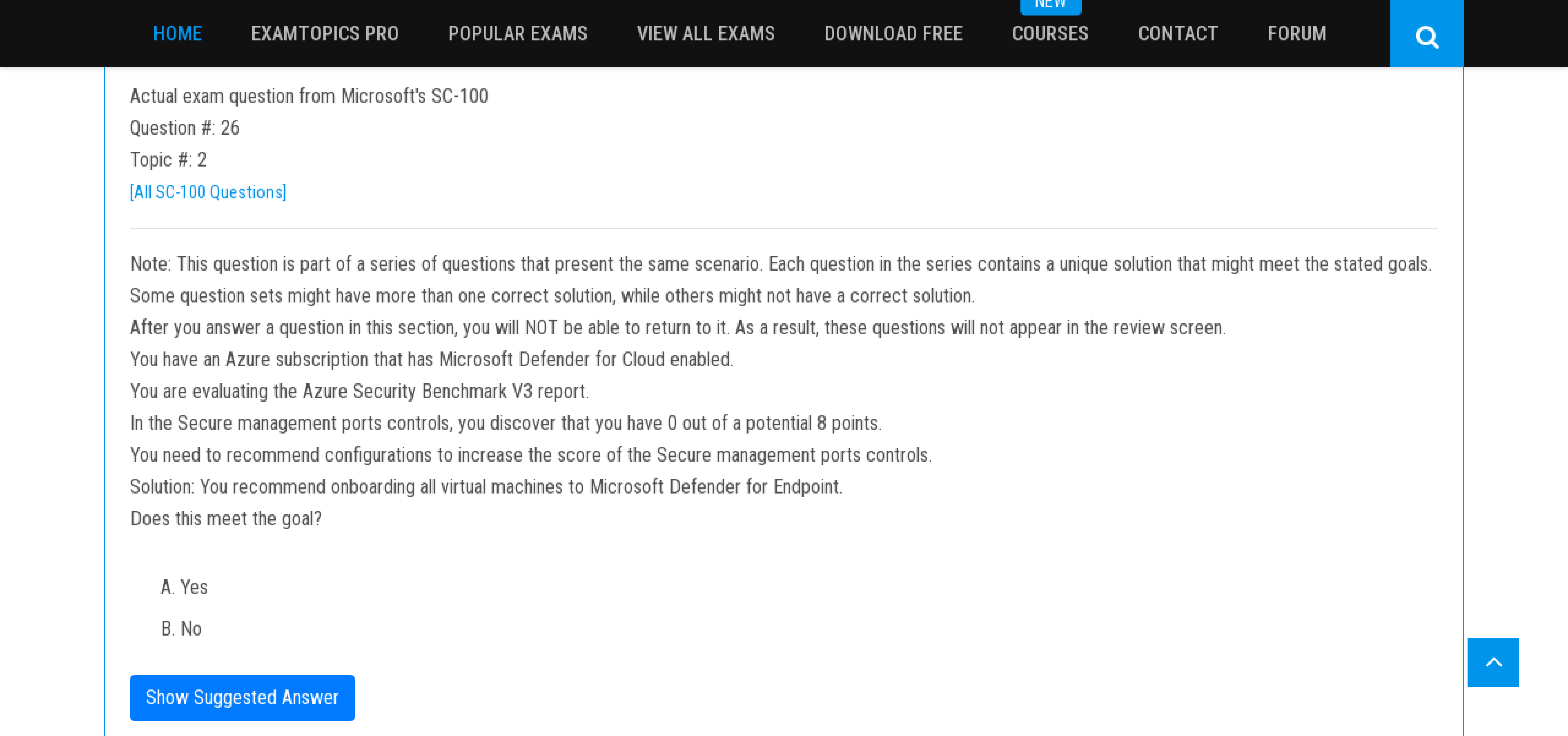
A. Microsoft Defender for Endpoint

B. Microsoft Endpoint Manager

C. Microsoft Information Protection

D. Microsoft Sentinel

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 26

Topic #: 2

[All SC-100 Questions]

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.

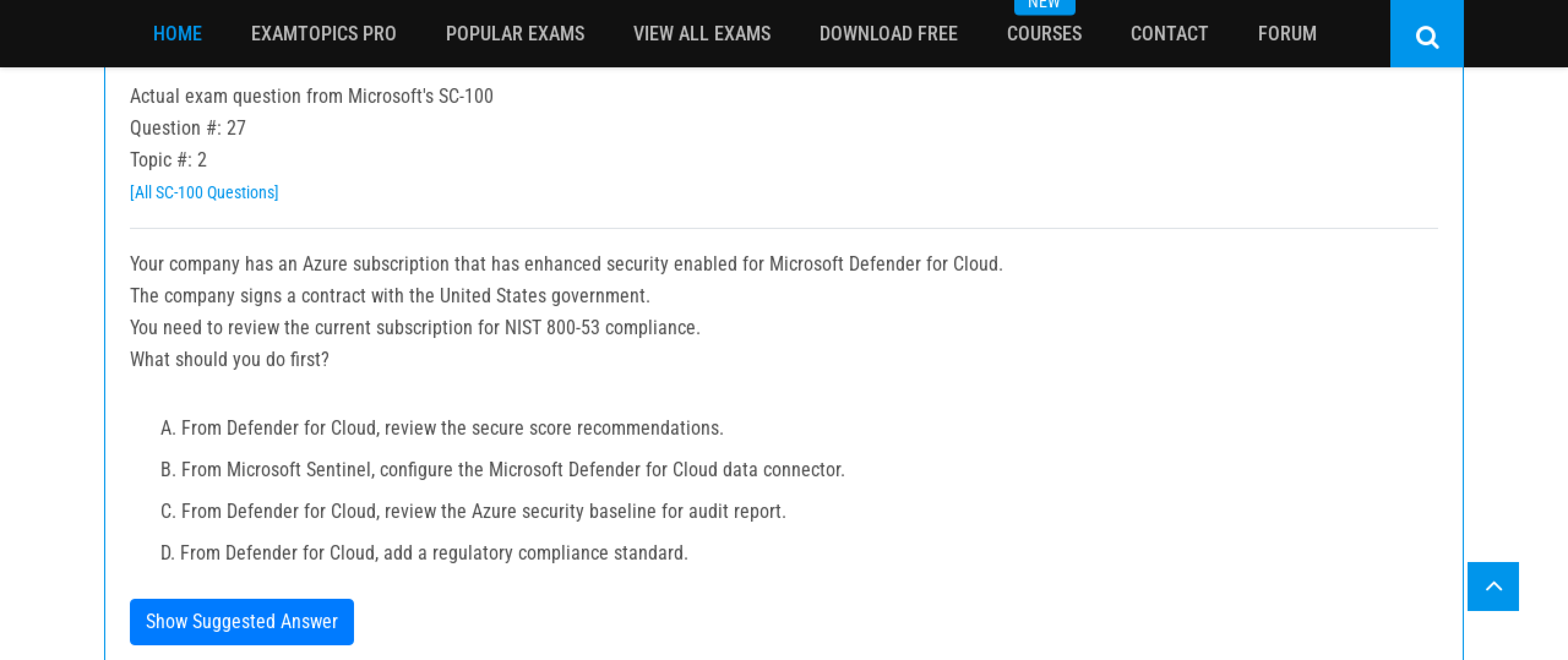
You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint.

Does this meet the goal?

A. Yes

B. No



Actual exam question from Microsoft's SC-100

Question #: 27

Topic #: 2

[All SC-100 Questions]

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.

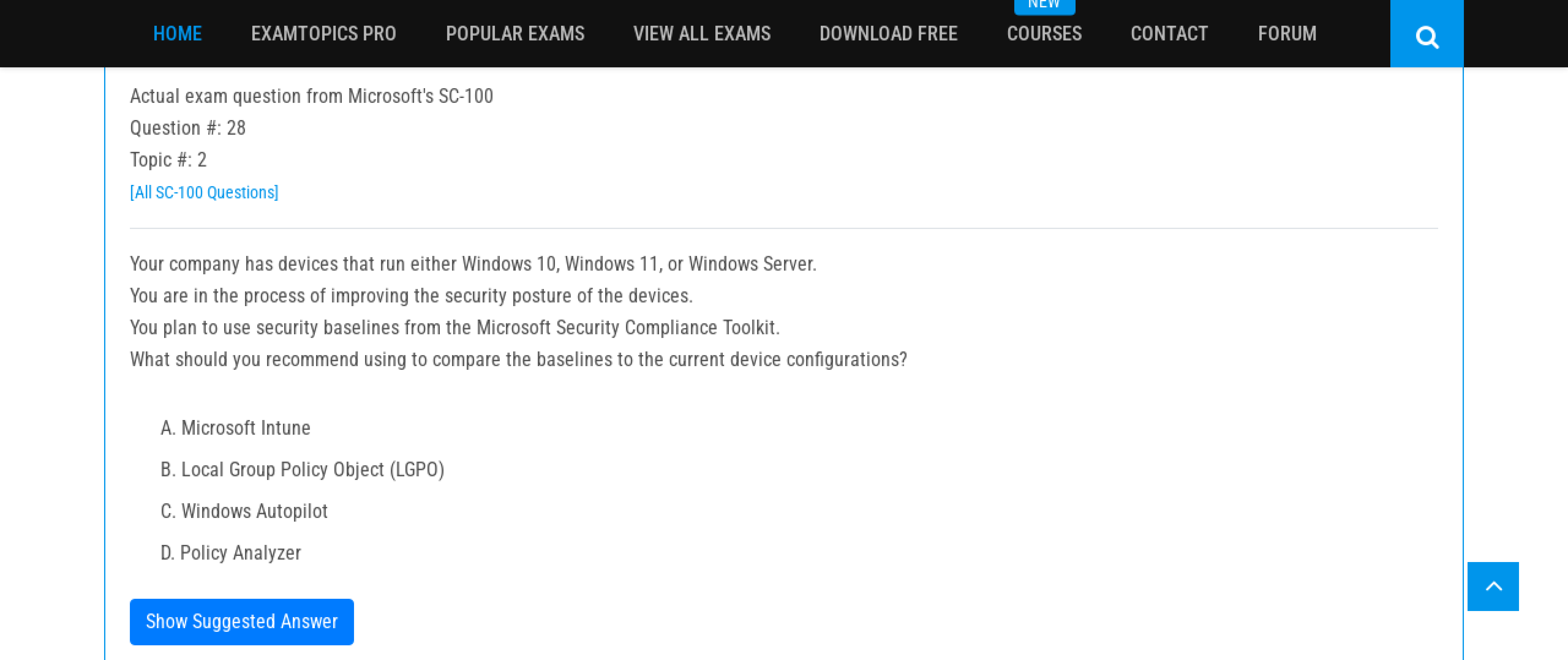
What should you do first?

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.



Actual exam question from Microsoft's SC-100

Question #: 28

Topic #: 2

[All SC-100 Questions]

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.

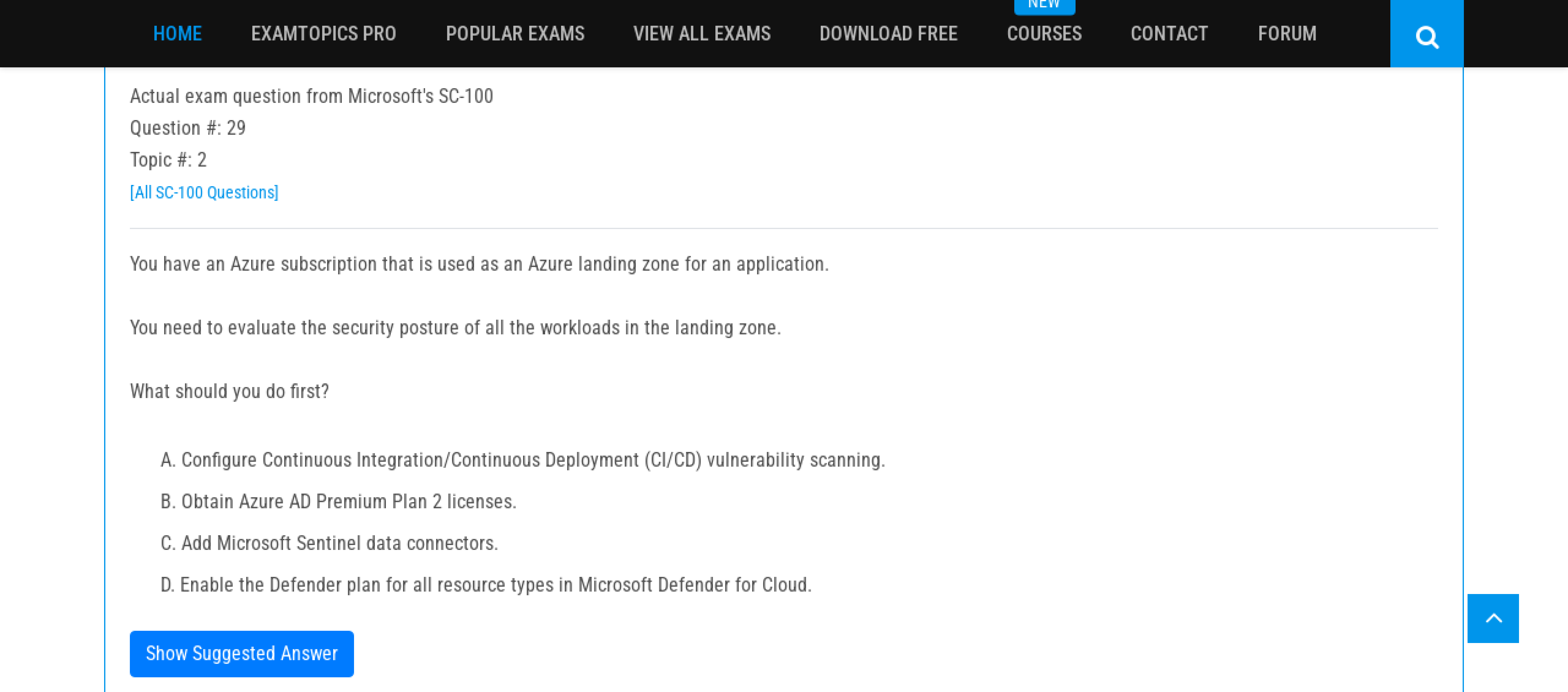
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune

B. Local Group Policy Object (LGPO)

C. Windows Autopilot

D. Policy Analyzer



Actual exam question from Microsoft's SC-100

Question #: 29

Topic #: 2

[All SC-100 Questions]

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.

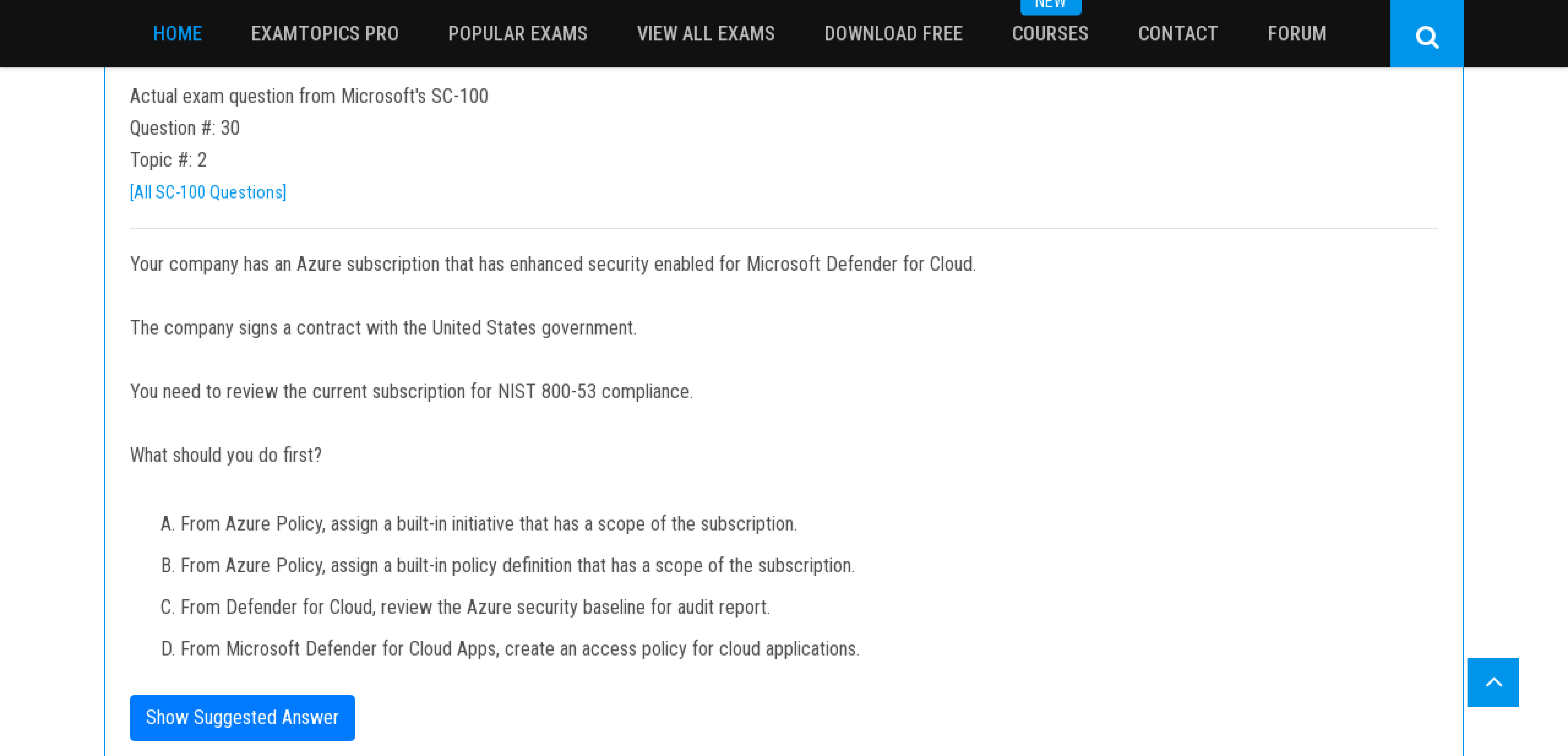
What should you do first?

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.



Actual exam question from Microsoft's SC-100
Question #: 30
Topic #: 2
[All SC-100 Questions]

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.

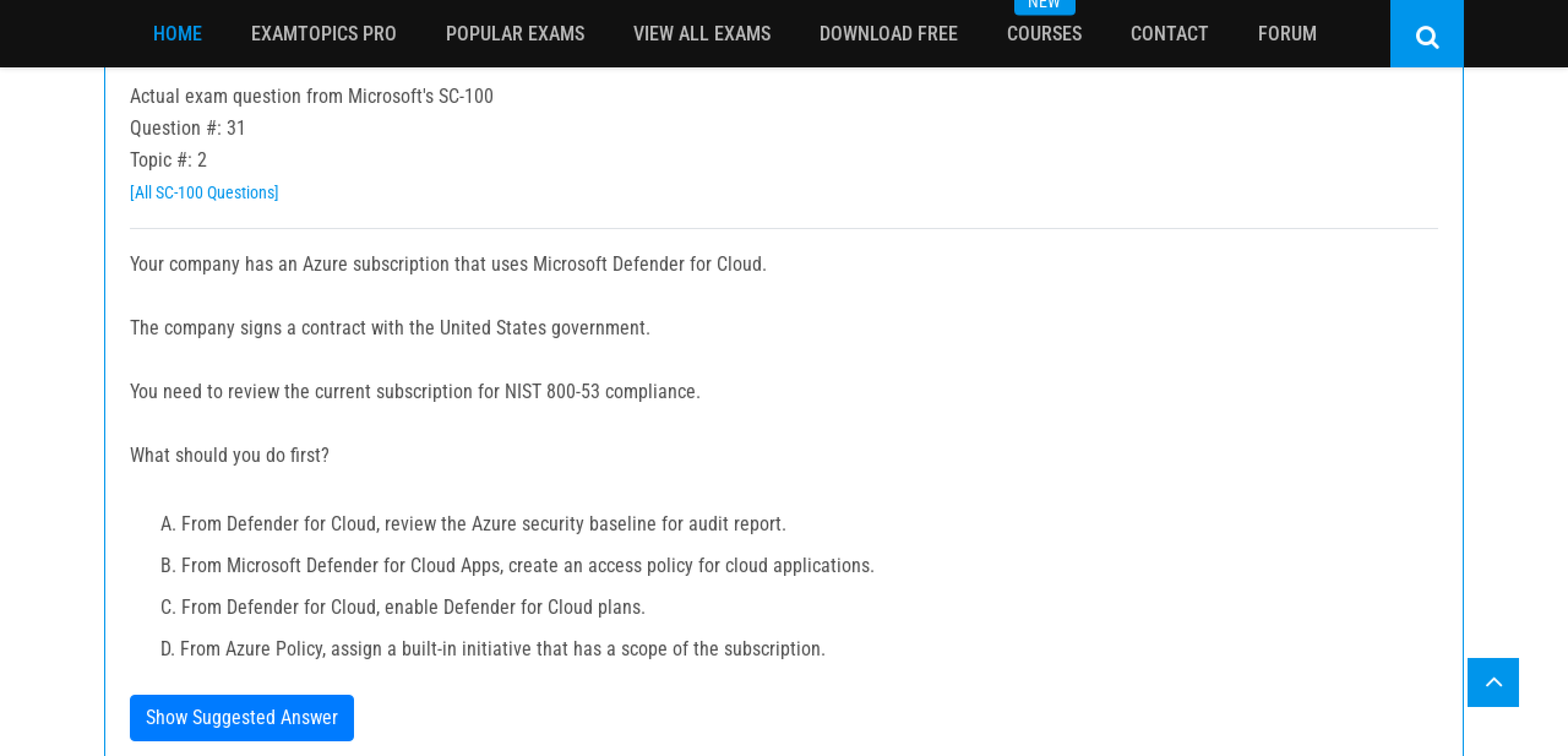
What should you do first?

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.



Actual exam question from Microsoft's SC-100

Question #: 31

Topic #: 2

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 32

Topic #: 2

[All SC-100 Questions]

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?

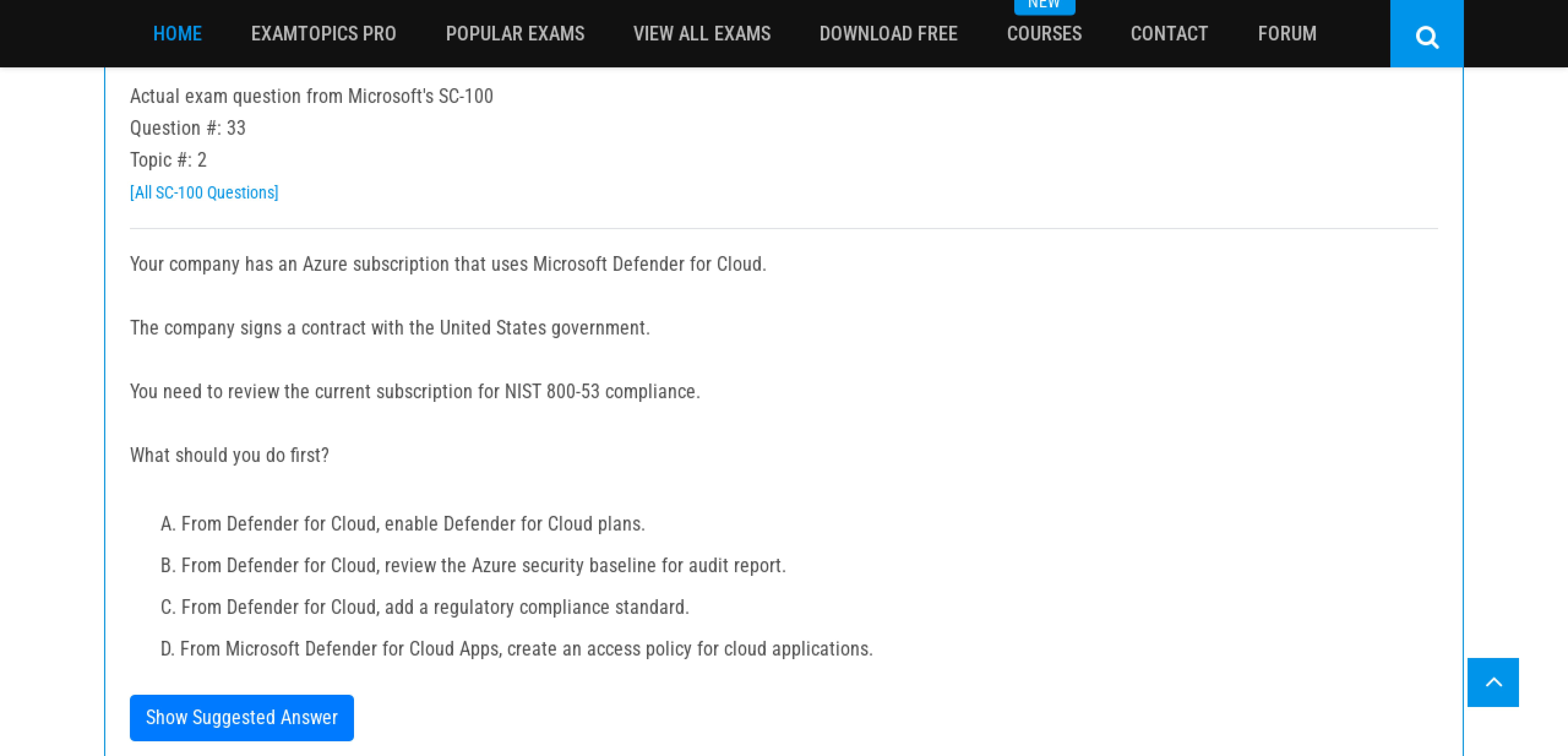
A. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

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.

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 33

Topic #: 2

[All SC-100 Questions]

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.

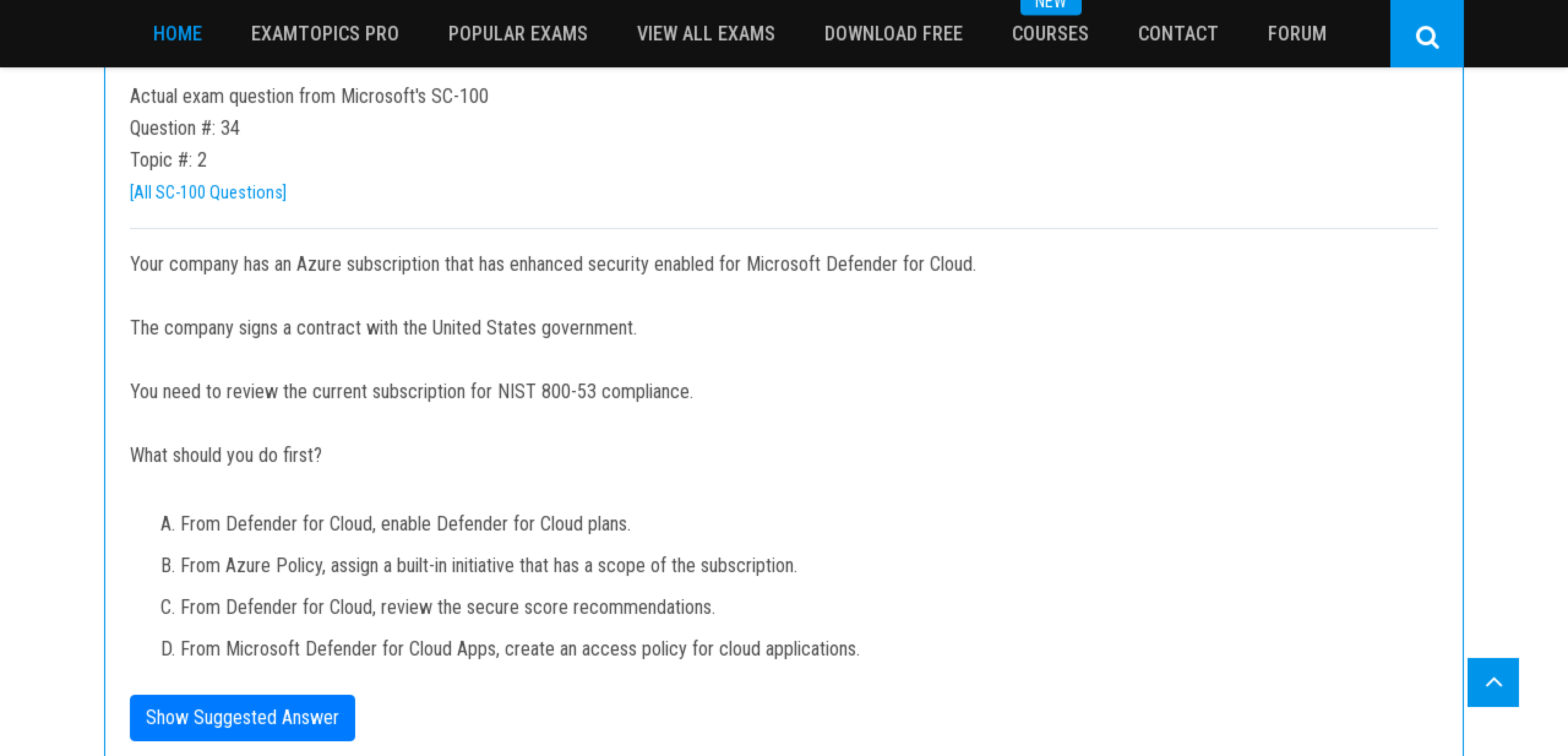
What should you do first?

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.



Actual exam question from Microsoft's SC-100
Question #: 34
Topic #: 2
[All SC-100 Questions]

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.

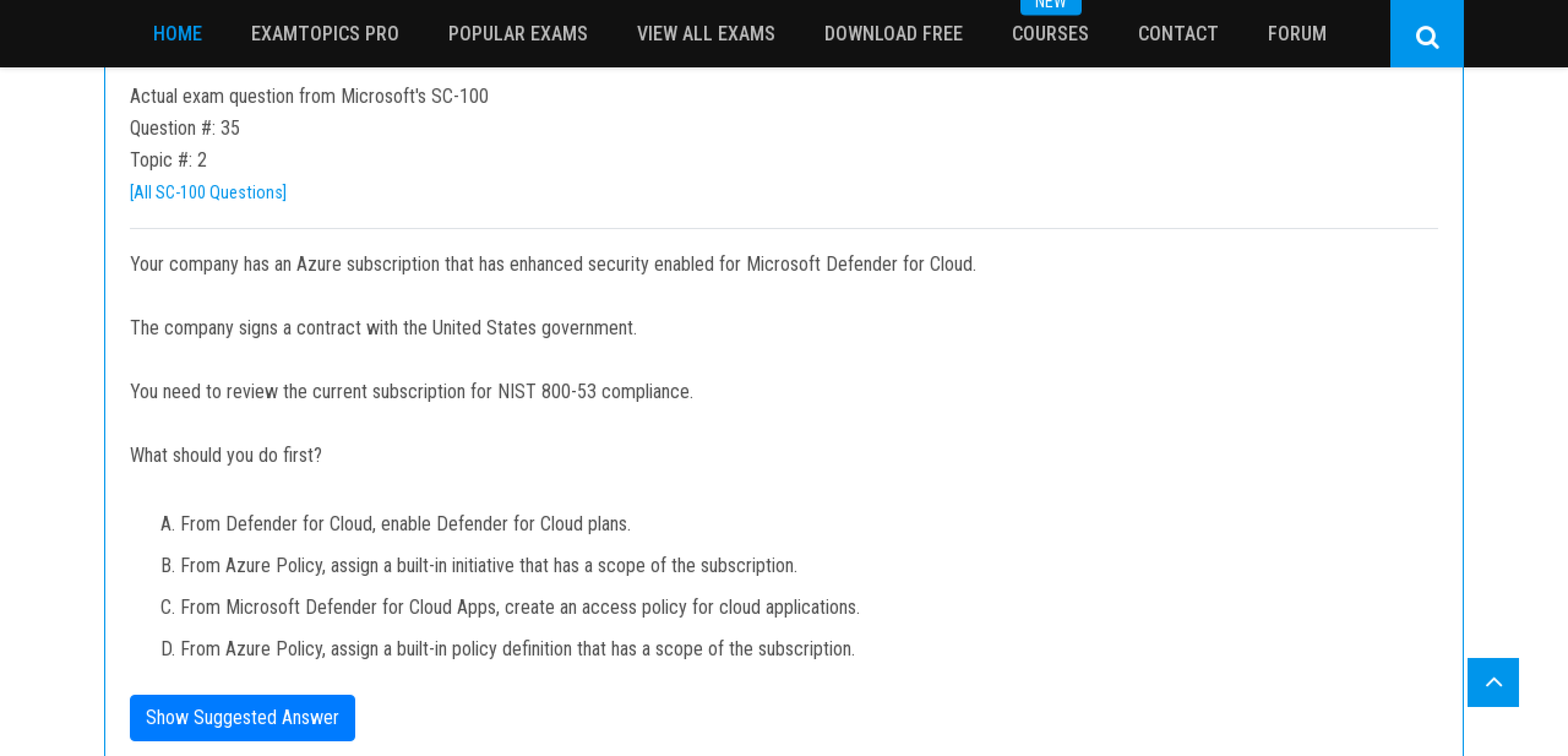
What should you do first?

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.



Actual exam question from Microsoft's SC-100
Question #: 35
Topic #: 2
[All SC-100 Questions]

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.

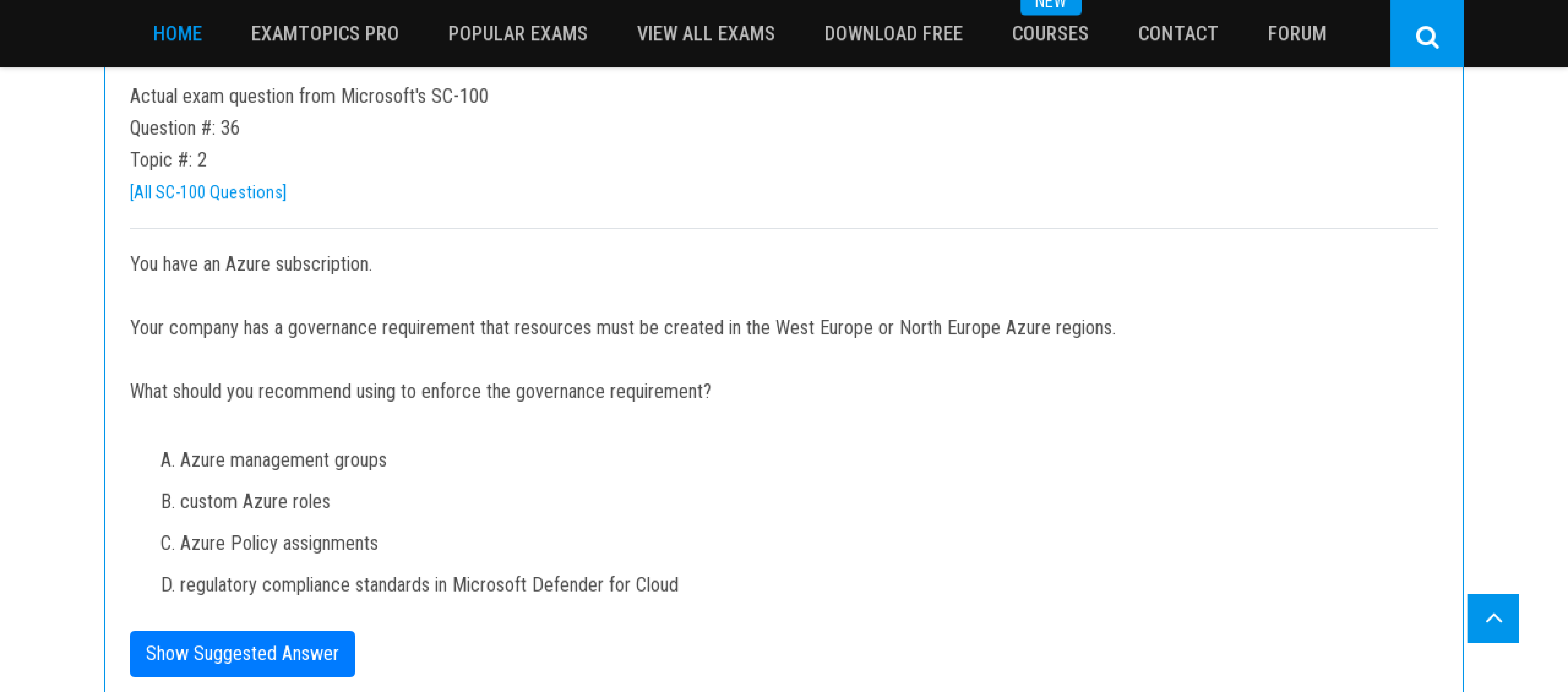
What should you do first?

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.



Actual exam question from Microsoft's SC-100

Question #: 36

Topic #: 2

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100
Question #: 37
Topic #: 2
[All SC-100 Questions]

HOTSPOT
-

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender.

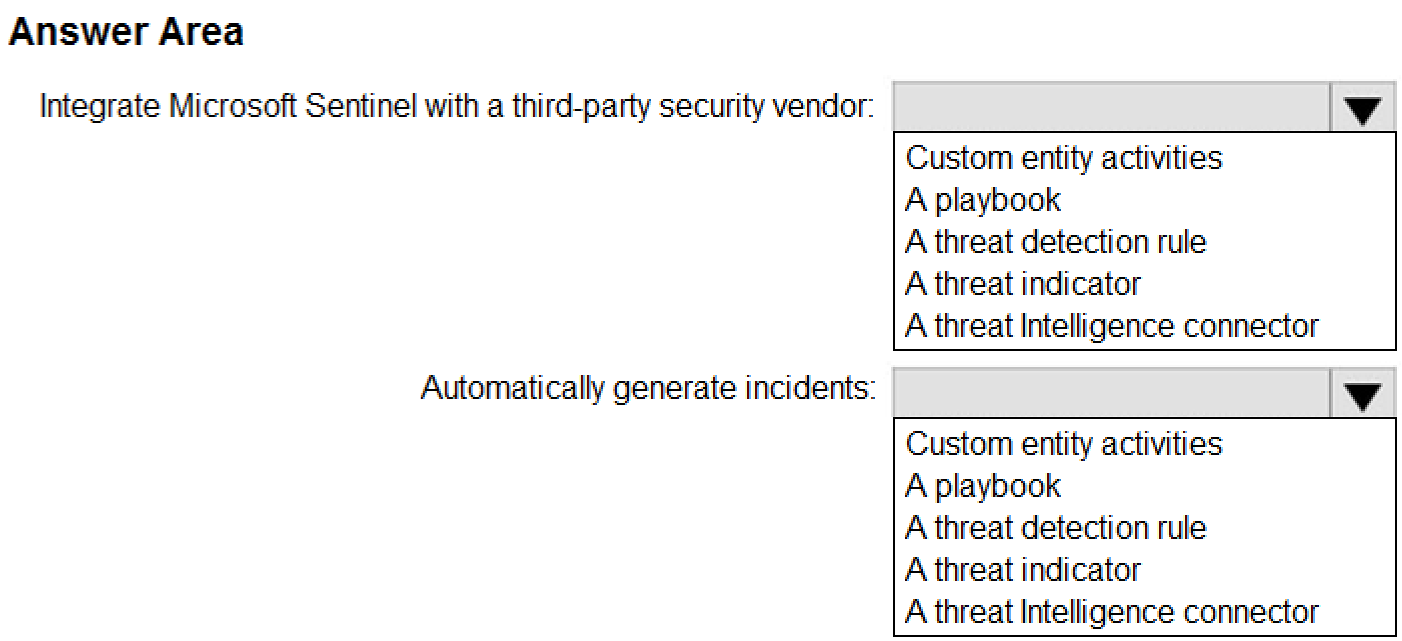
You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender.

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.

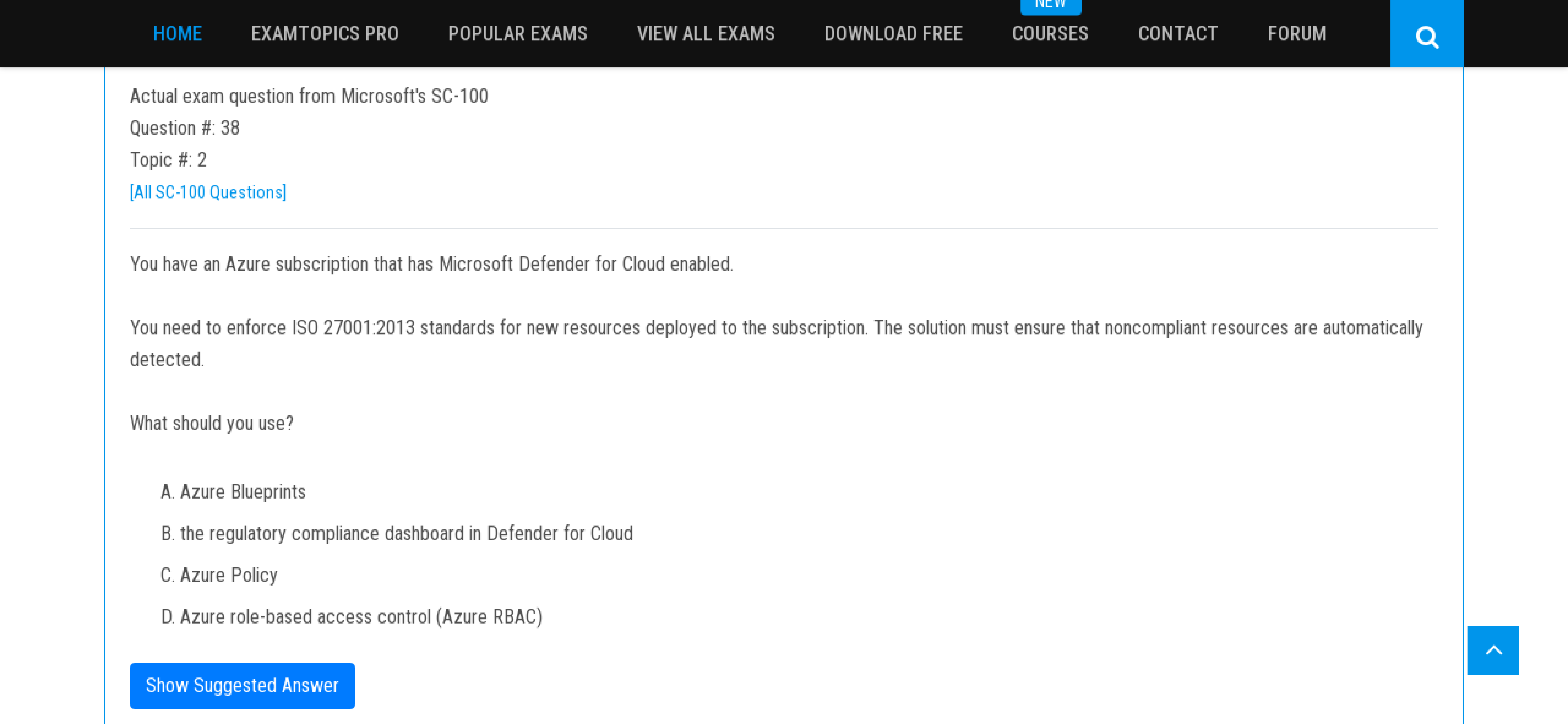


Answer Area

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

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 38
Topic #: 2
[All SC-100 Questions]

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)

Actual exam question from Microsoft's SC-100
Question #: 39
Topic #: 2
[All SC-100 Questions]

DRAG DROP

-

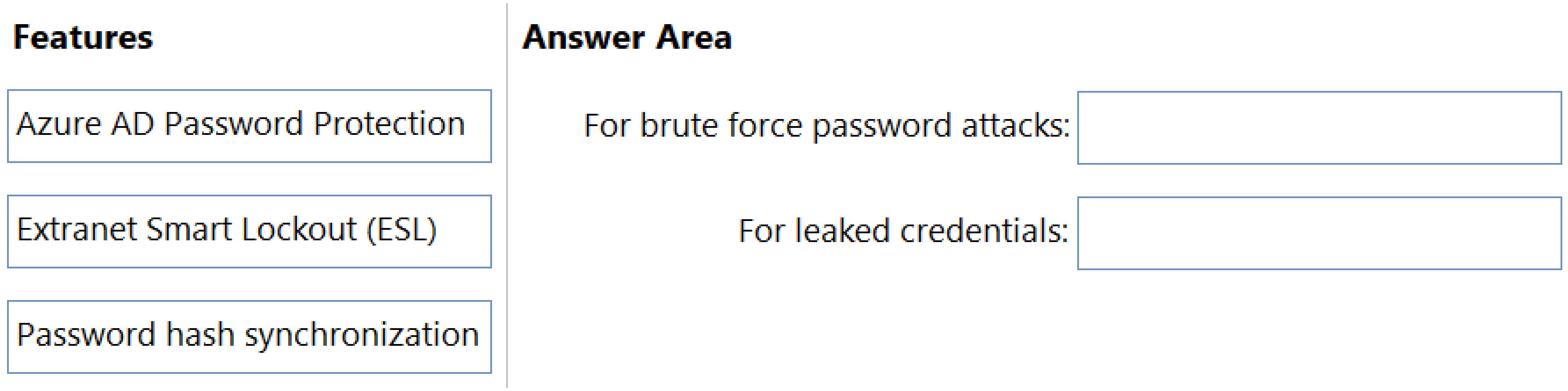
You have a hybrid Azure AD tenant that has pass-through authentication enabled.

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:

Show Suggested Answer

Actual exam question from Microsoft's SC-100
Question #: 40
Topic #: 2
[All SC-100 Questions]

HOTSPOT
-

You are designing the security architecture for a cloud-only environment.

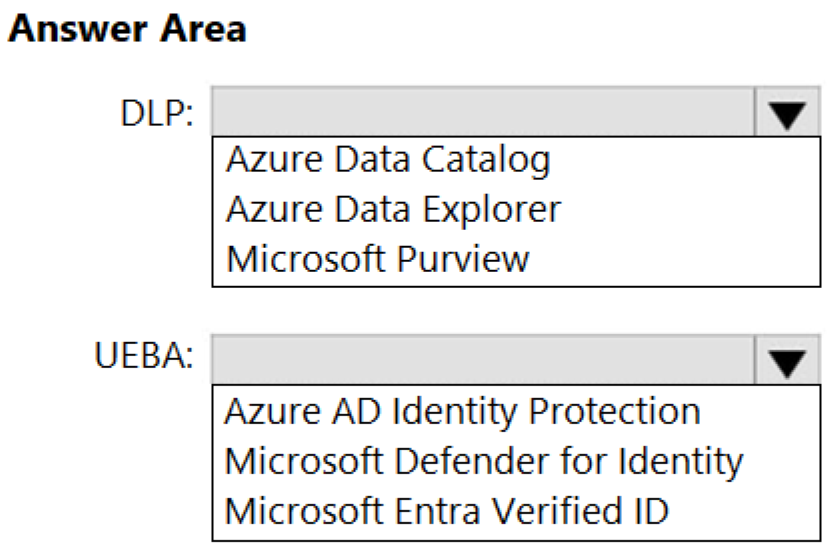
You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 41

Topic #: 2

[All SC-100 Questions]

HOTSPOT

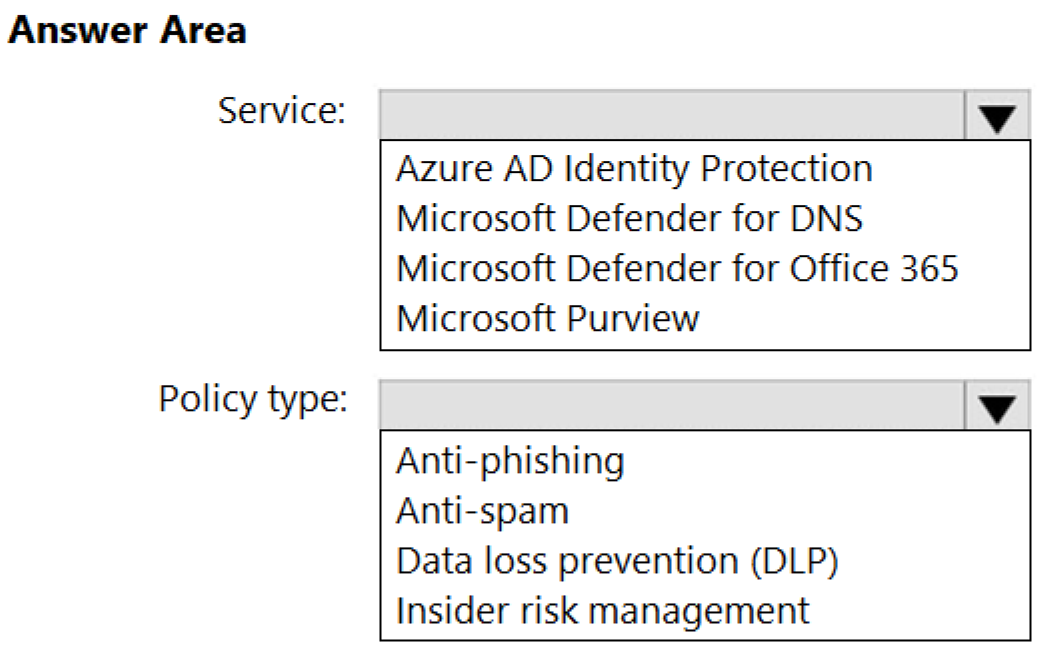
-

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

Show Suggested Answer

Actual exam question from Microsoft's SC-100
Question #: 42
Topic #: 2
[All SC-100 Questions]

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.

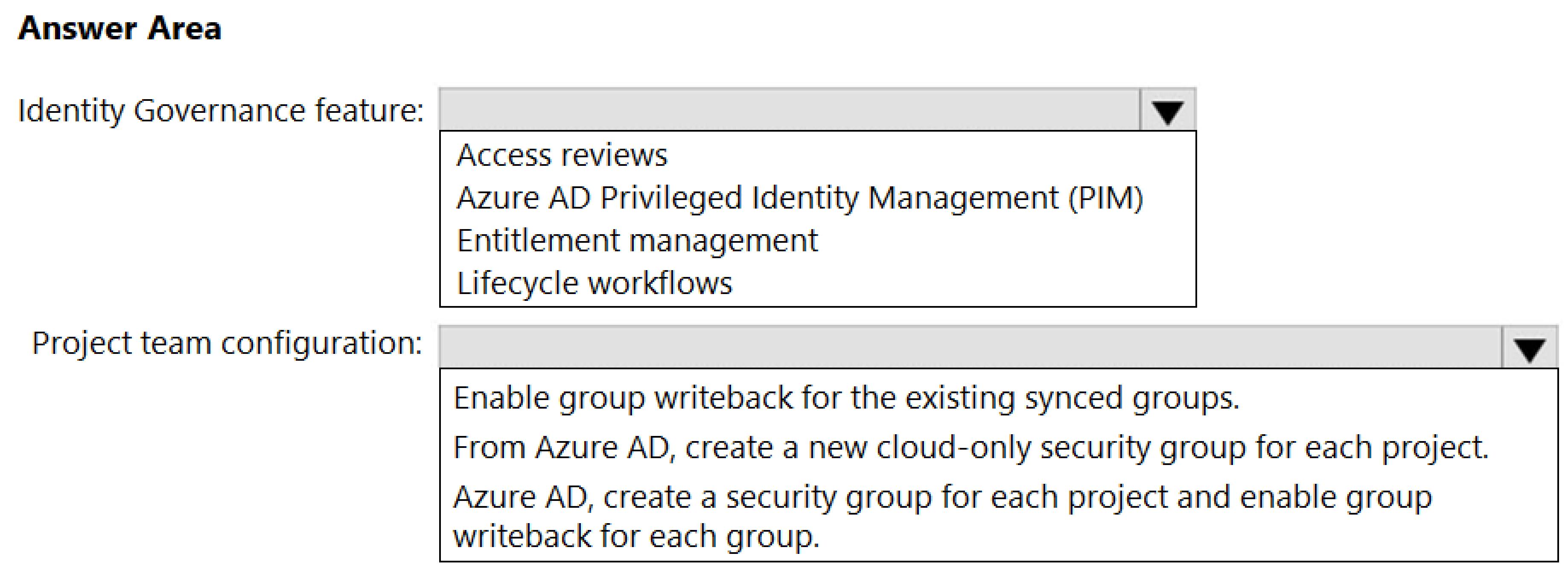
Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

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.

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 43

Topic #: 2

[All SC-100 Questions]

HOTSPOT

-

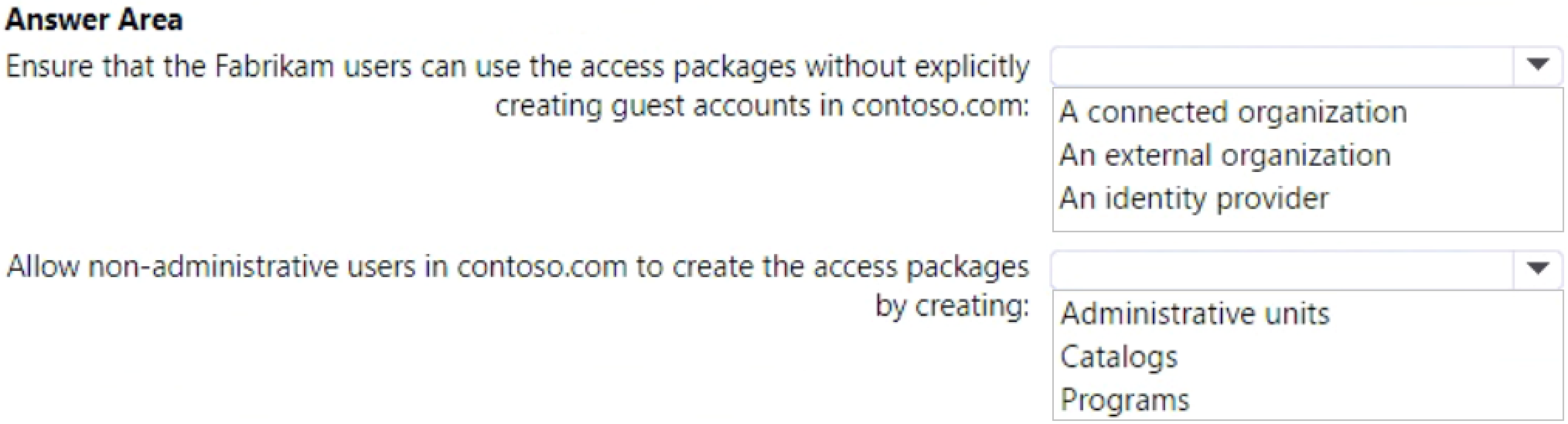
You are designing a privileged access strategy for a company named Contoso, Ltd. and its partner company named Fabrikam, Inc. Contoso has an Azure AD tenant named contoso.com. Fabrikam has an Azure AD tenant named fabrikam.com. Users at Fabrikam must access the resources in contoso.com.

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.

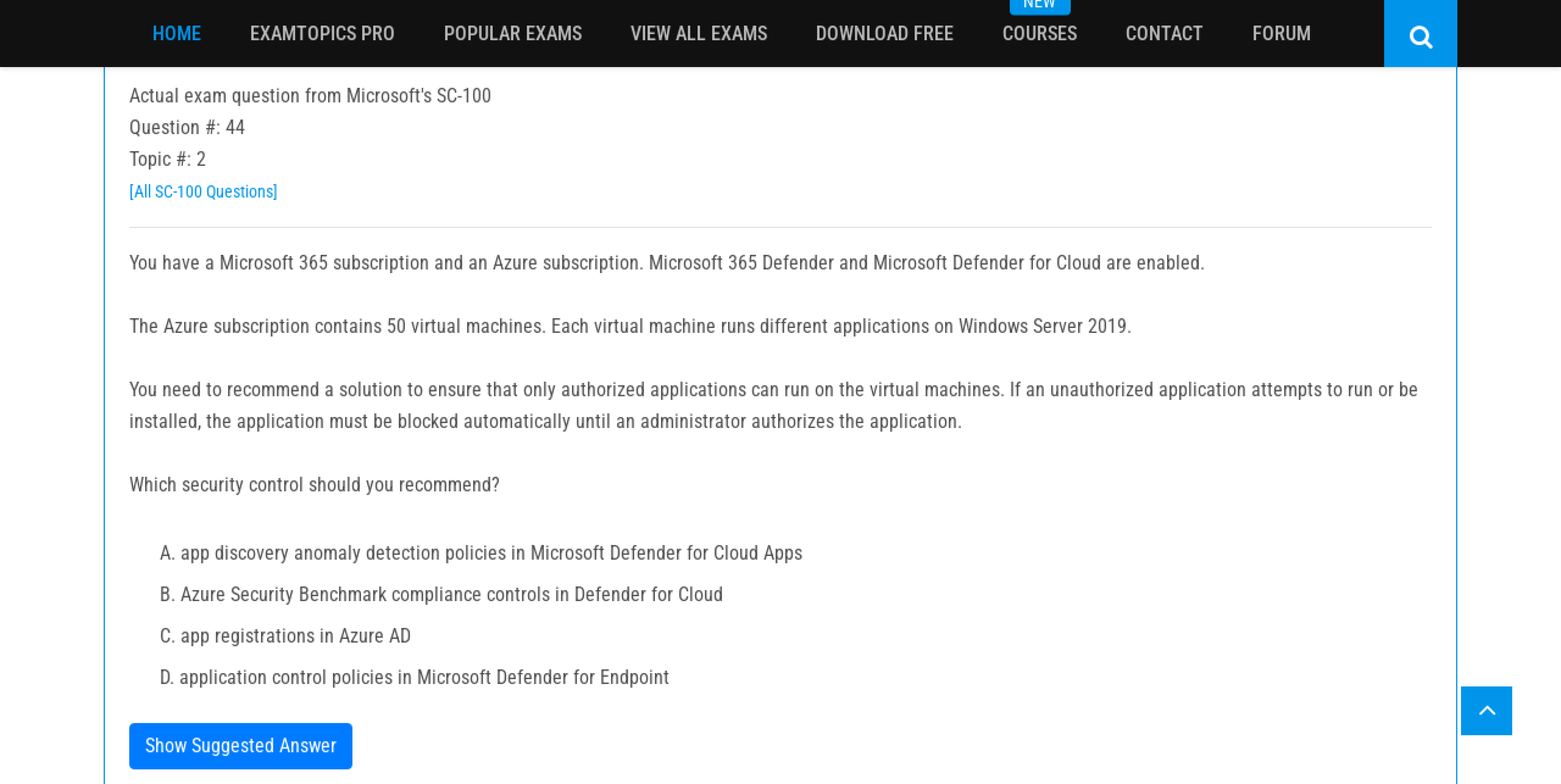


Answer Area

Ensure that the Fabrikam users can use the access packages without explicitly creating guest accounts in contoso.com:

Allow non-administrative users in contoso.com to create the access packages by creating:

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 44

Topic #: 2

[All SC-100 Questions]

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?

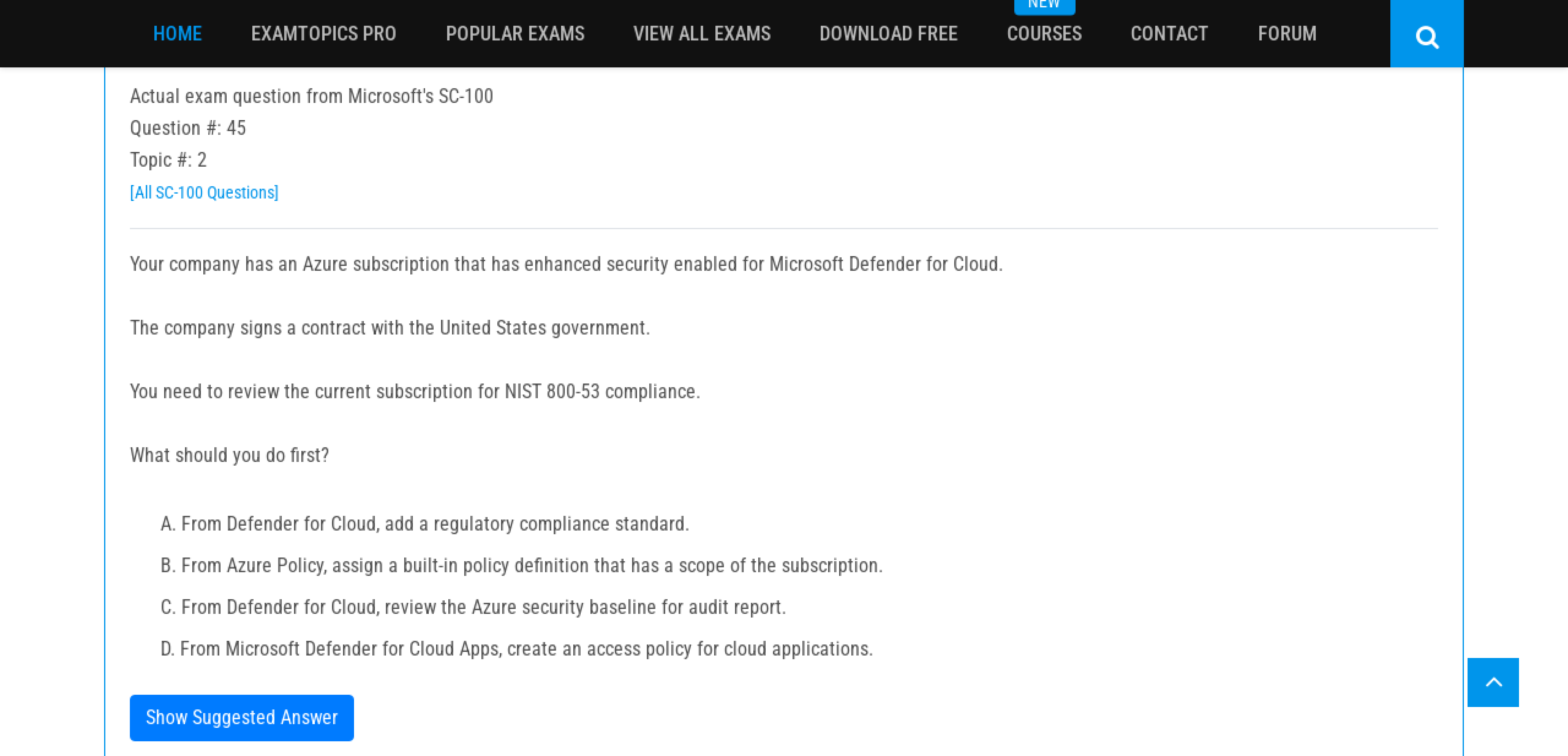
A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

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

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 45

Topic #: 2

[All SC-100 Questions]

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.

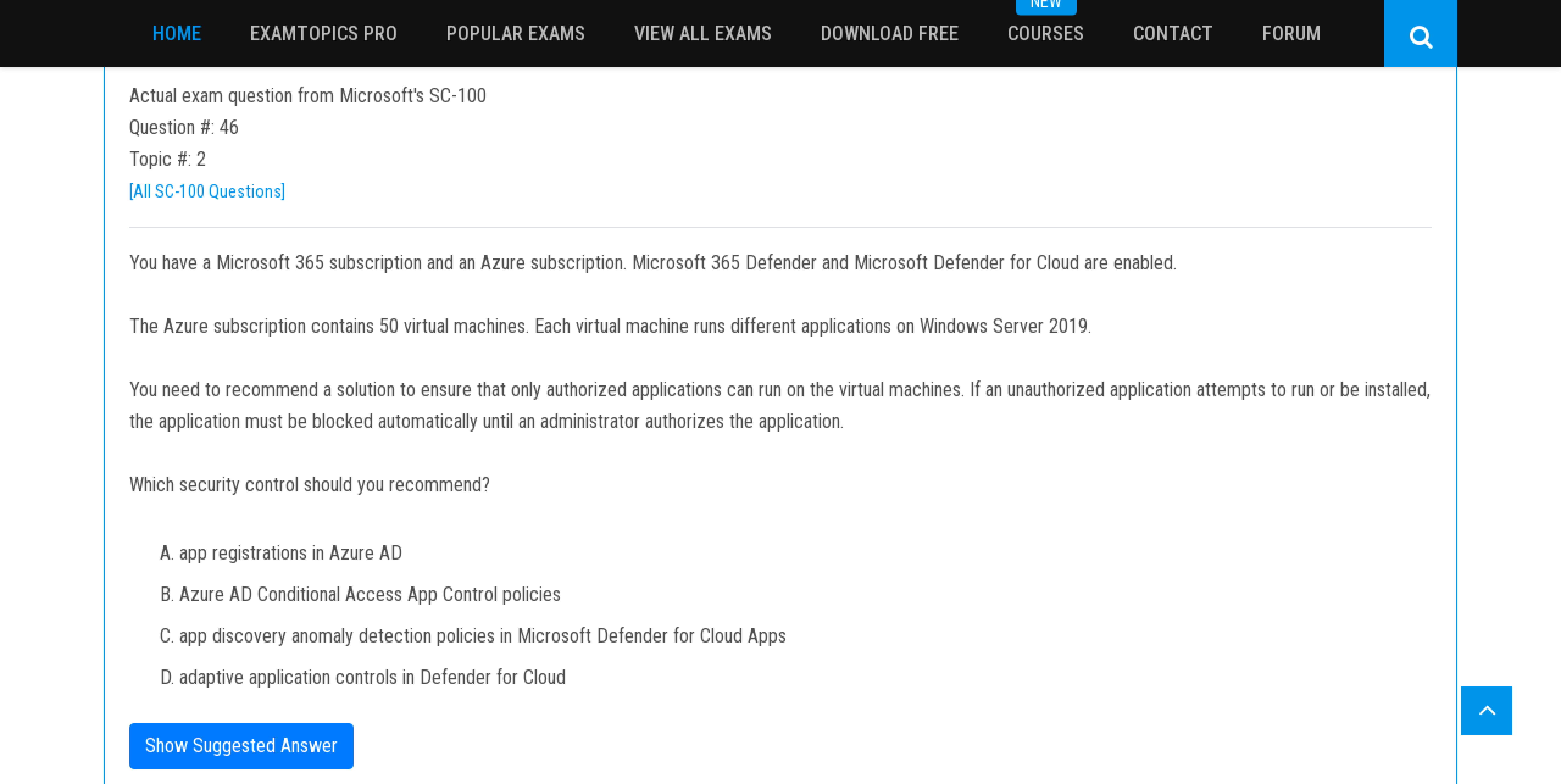
What should you do first?

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.



Actual exam question from Microsoft's SC-100
Question #: 46
Topic #: 2
[All SC-100 Questions]

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.

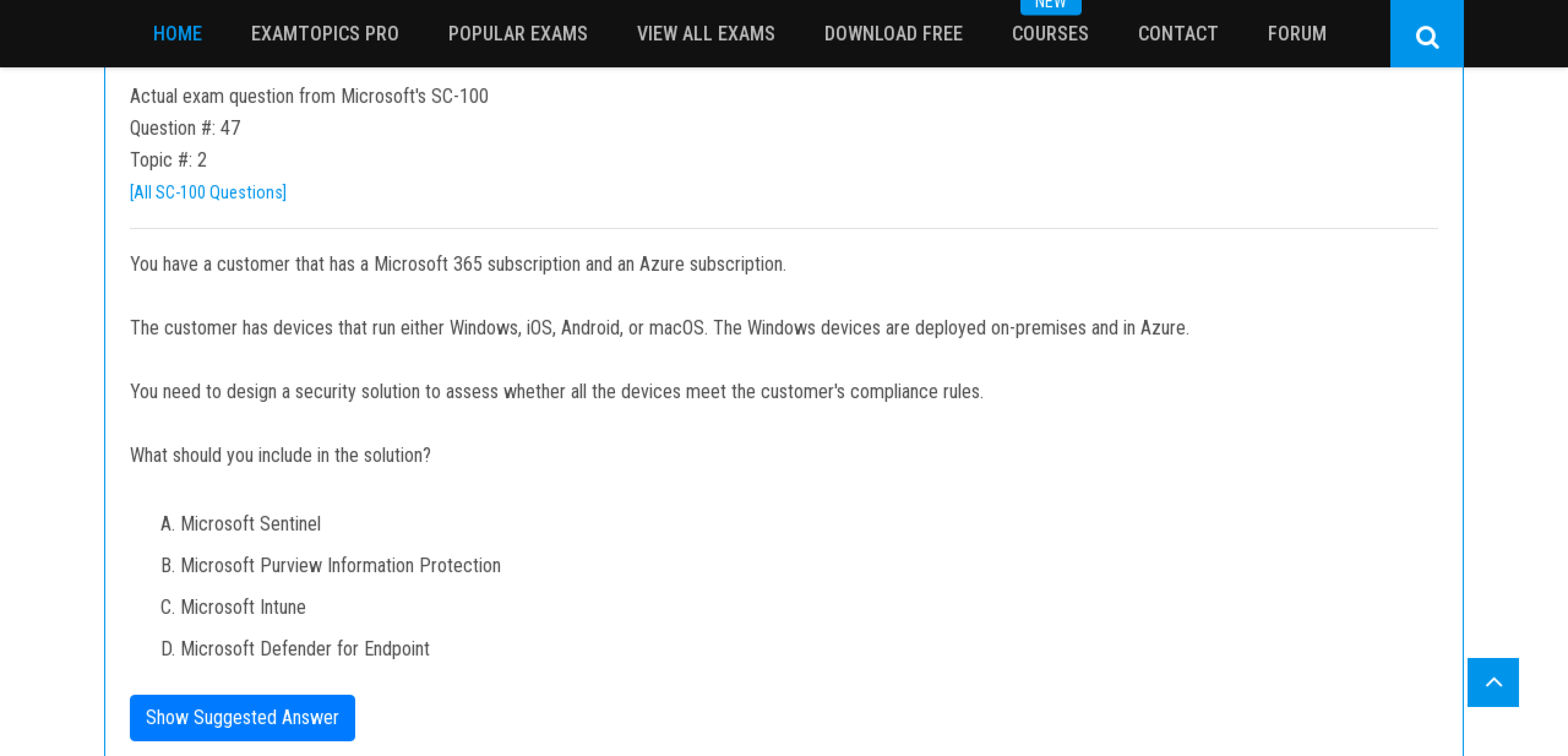
Which security control should you recommend?

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



Actual exam question from Microsoft's SC-100

Question #: 47

Topic #: 2

[All SC-100 Questions]

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.

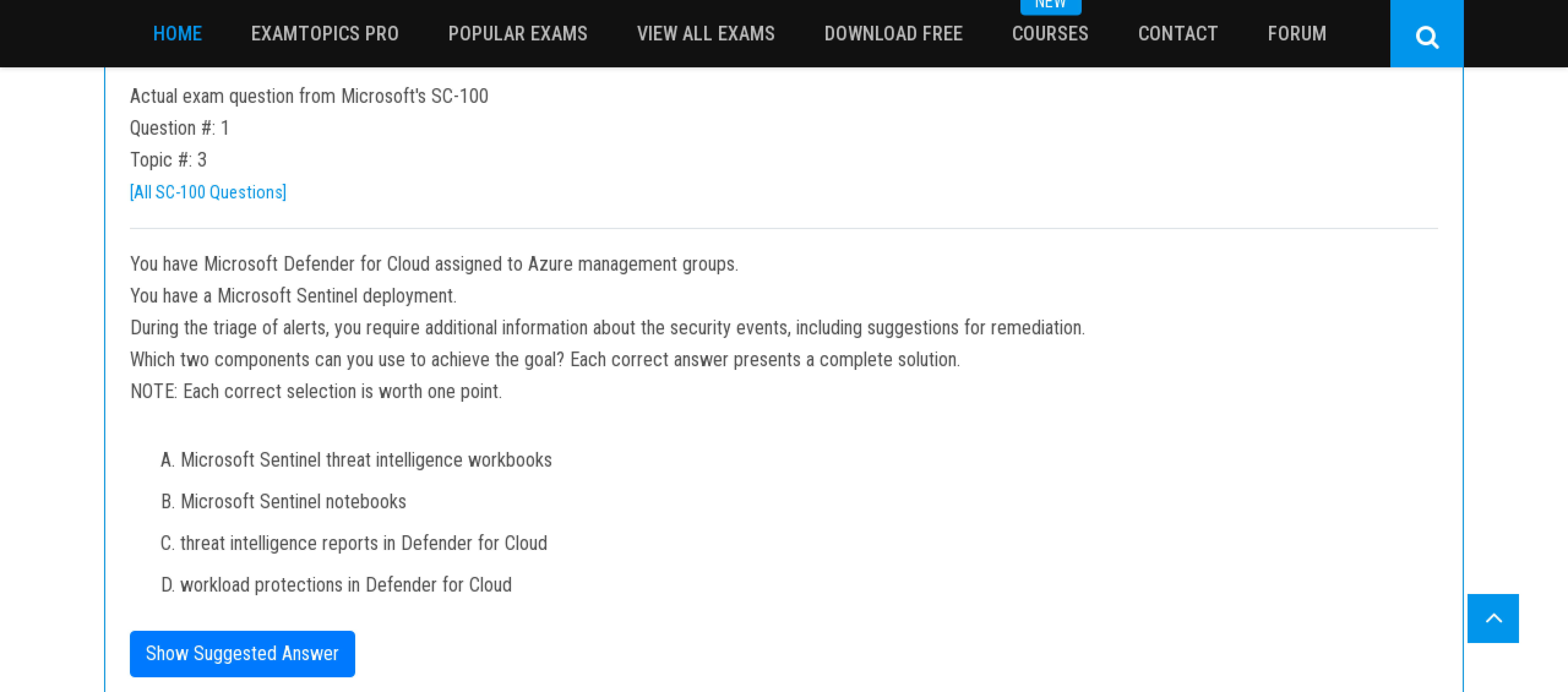
What should you include in the solution?

A. Microsoft Sentinel

B. Microsoft Purview Information Protection

C. Microsoft Intune

D. Microsoft Defender for Endpoint



Actual exam question from Microsoft's SC-100

Question #: 1

Topic #: 3

[All SC-100 Questions]

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.

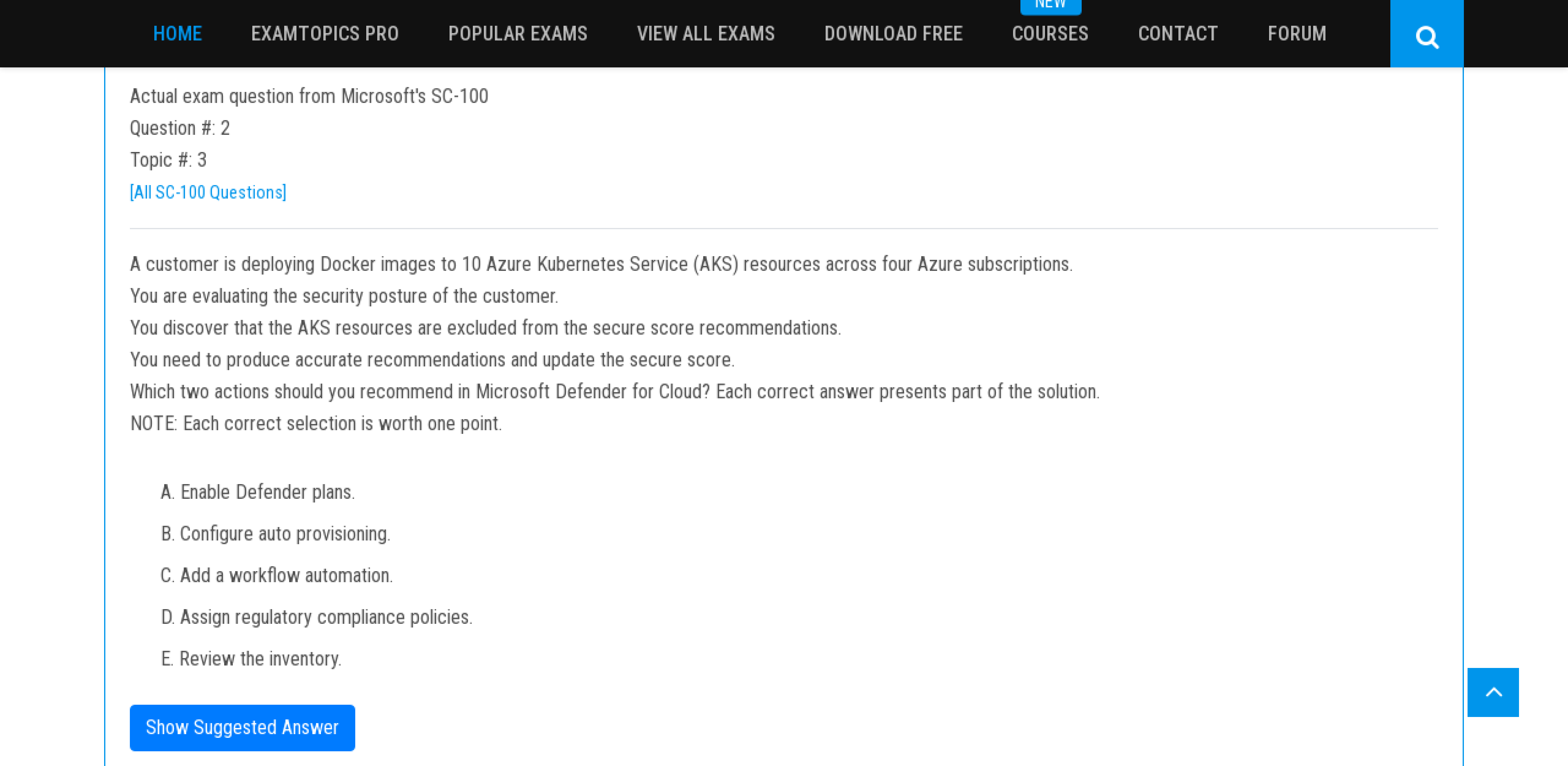
NOTE: Each correct selection is worth one point.

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



Actual exam question from Microsoft's SC-100

Question #: 2

Topic #: 3

[All SC-100 Questions]

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.

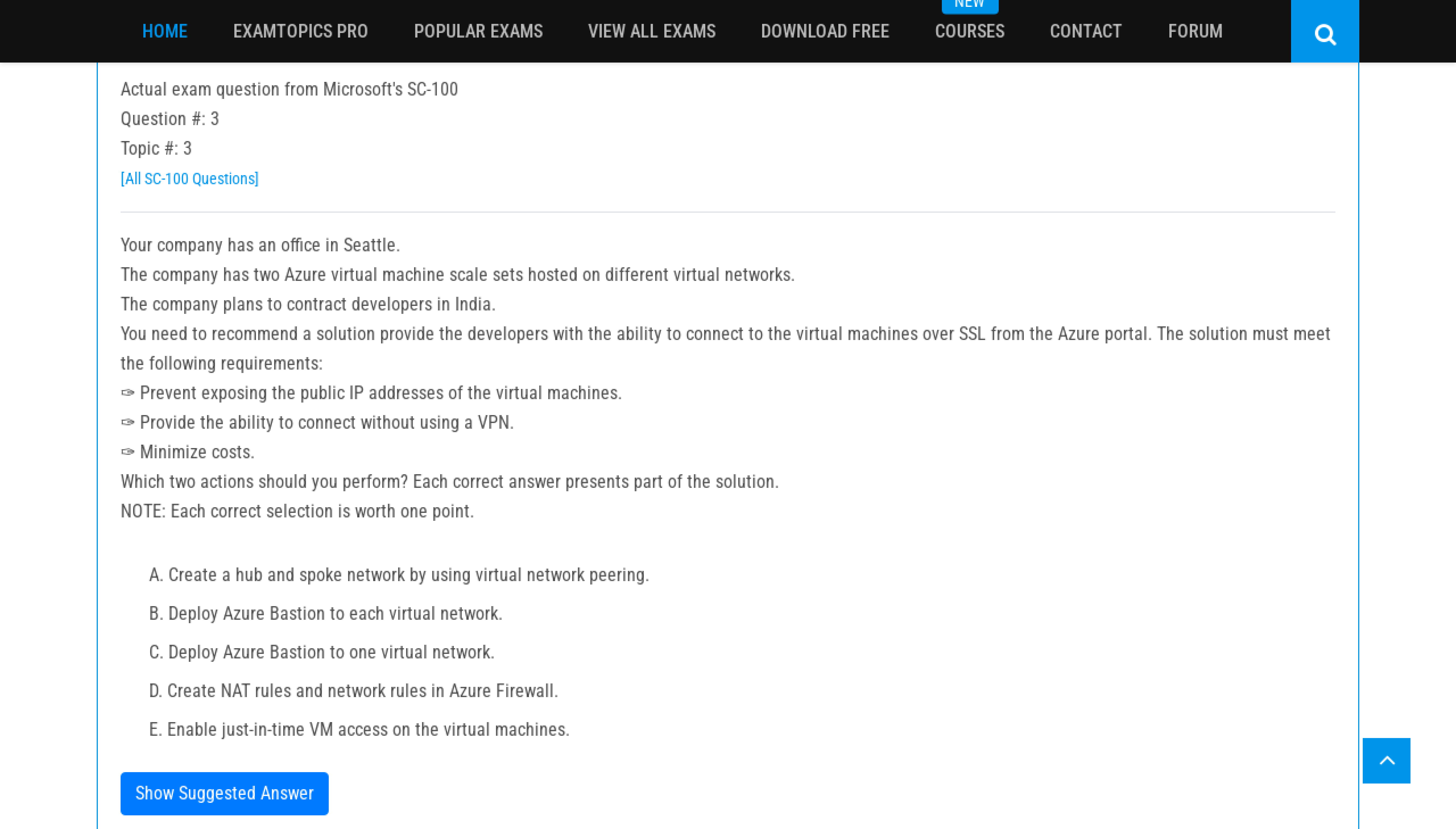
A. Enable Defender plans.

B. Configure auto provisioning.

C. Add a workflow automation.

D. Assign regulatory compliance policies.

E. Review the inventory.



Actual exam question from Microsoft's SC-100

Question #: 3

Topic #: 3

[All SC-100 Questions]

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.

Actual exam question from Microsoft's SC-100

Question #: 4

Topic #: 3

[All SC-100 Questions]

HOTSPOT -

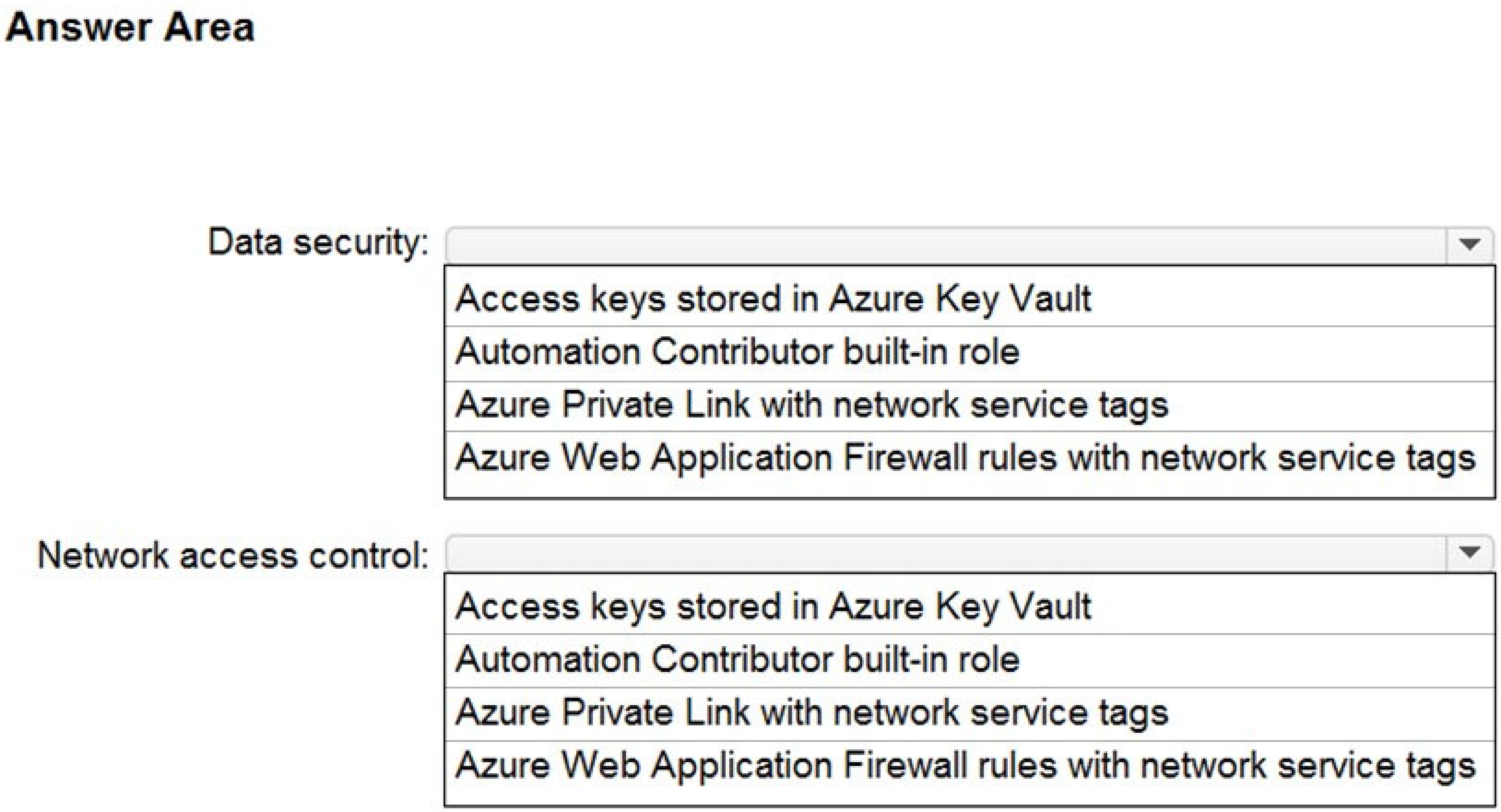
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

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

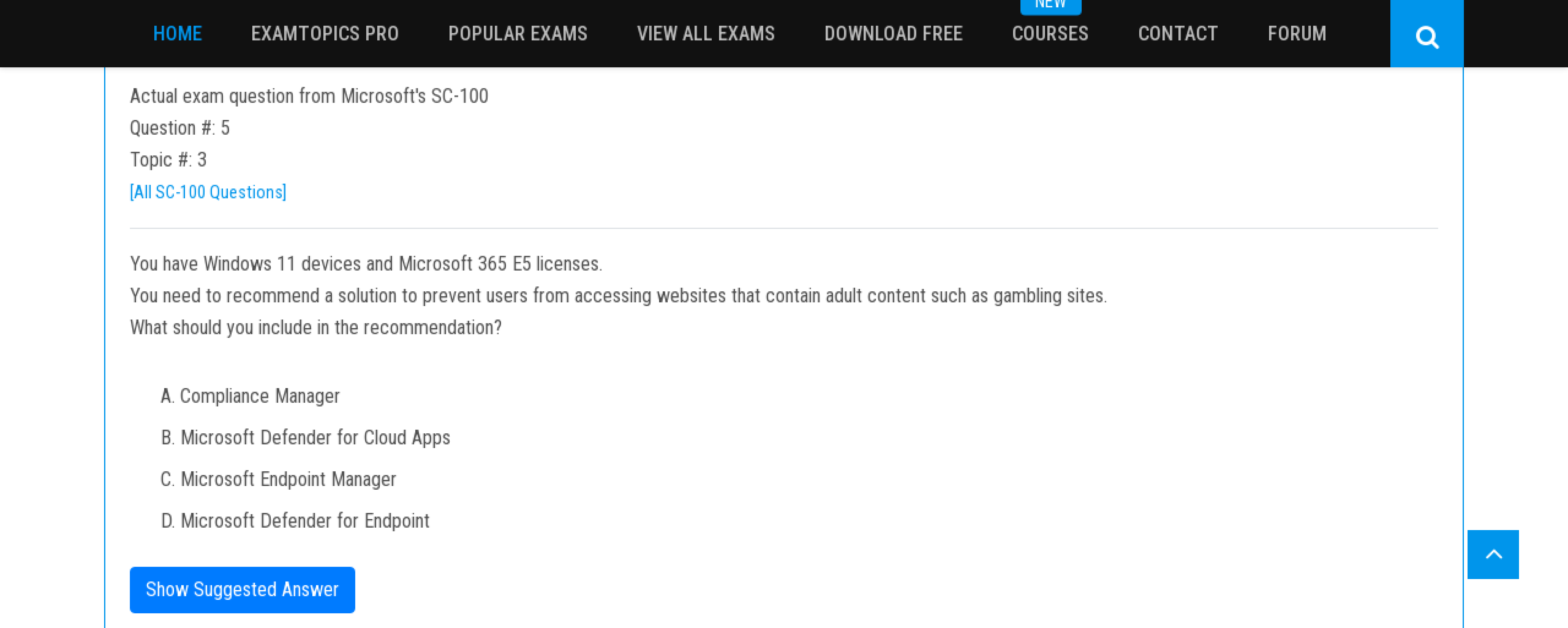
Data security:

- 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

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 5

Topic #: 3

[All SC-100 Questions]

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.

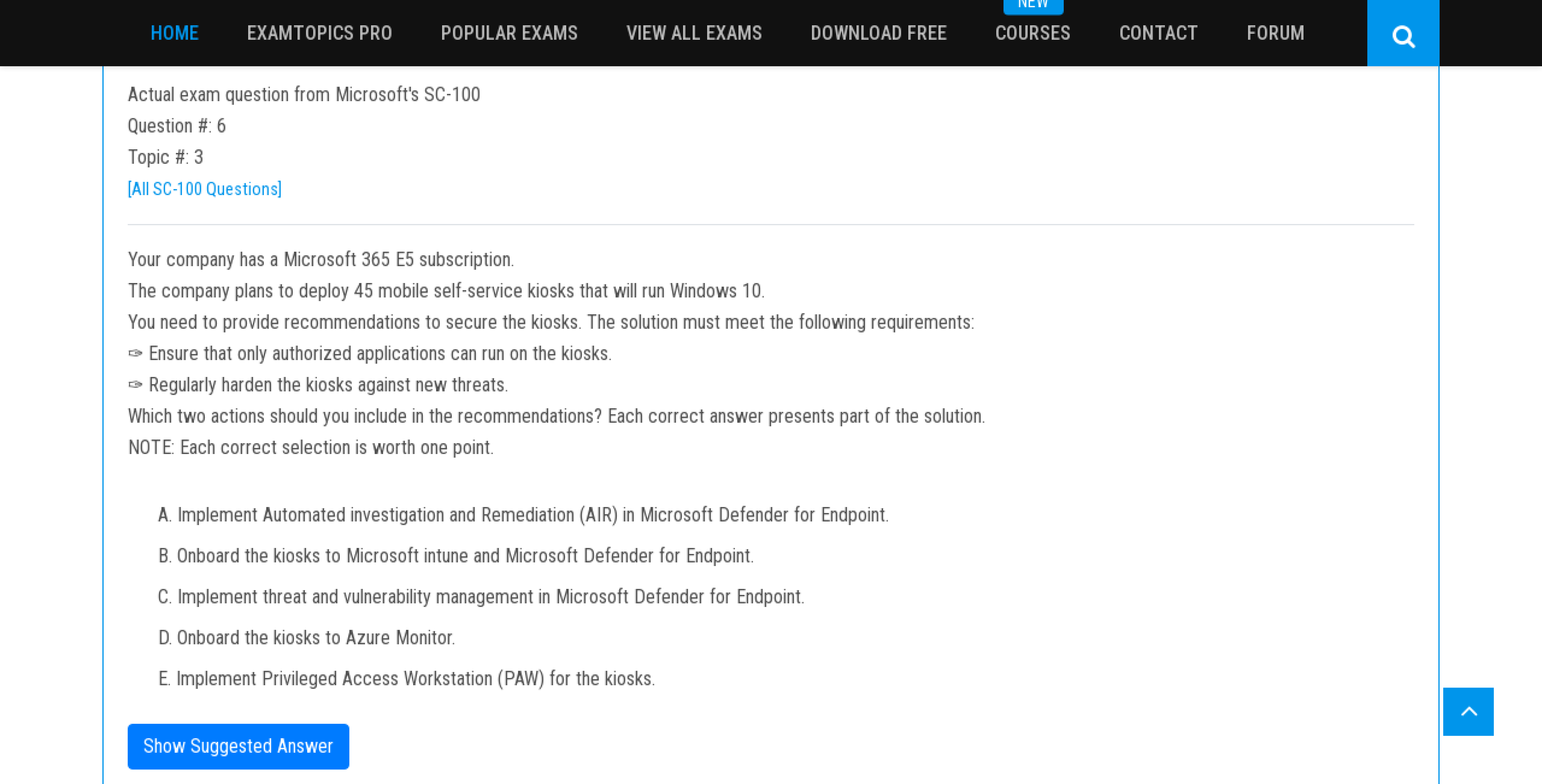
What should you include in the recommendation?

A. Compliance Manager

B. Microsoft Defender for Cloud Apps

C. Microsoft Endpoint Manager

D. Microsoft Defender for Endpoint



Actual exam question from Microsoft's SC-100

Question #: 6

Topic #: 3

[All SC-100 Questions]

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.

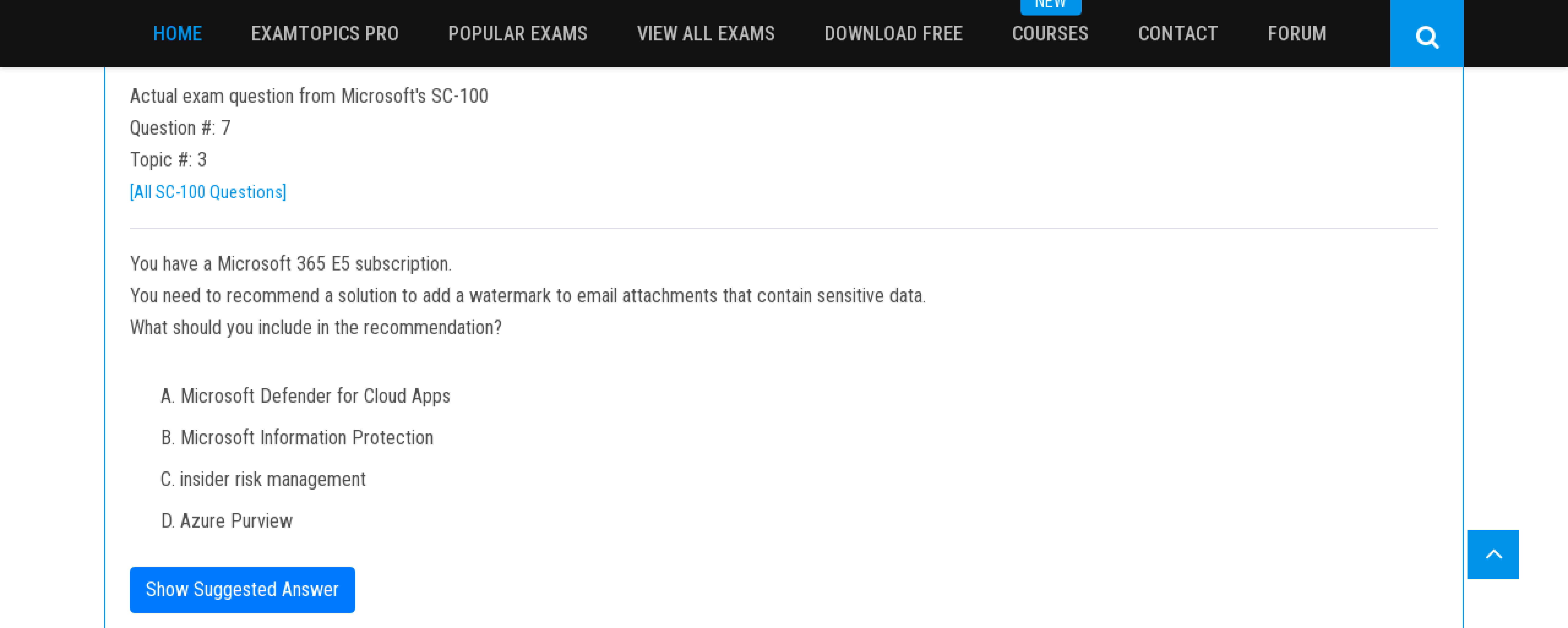
A. Implement Automated investigation and Remediation (AIR) in Microsoft Defender for Endpoint.

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.



Actual exam question from Microsoft's SC-100

Question #: 7

Topic #: 3

[All SC-100 Questions]

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?

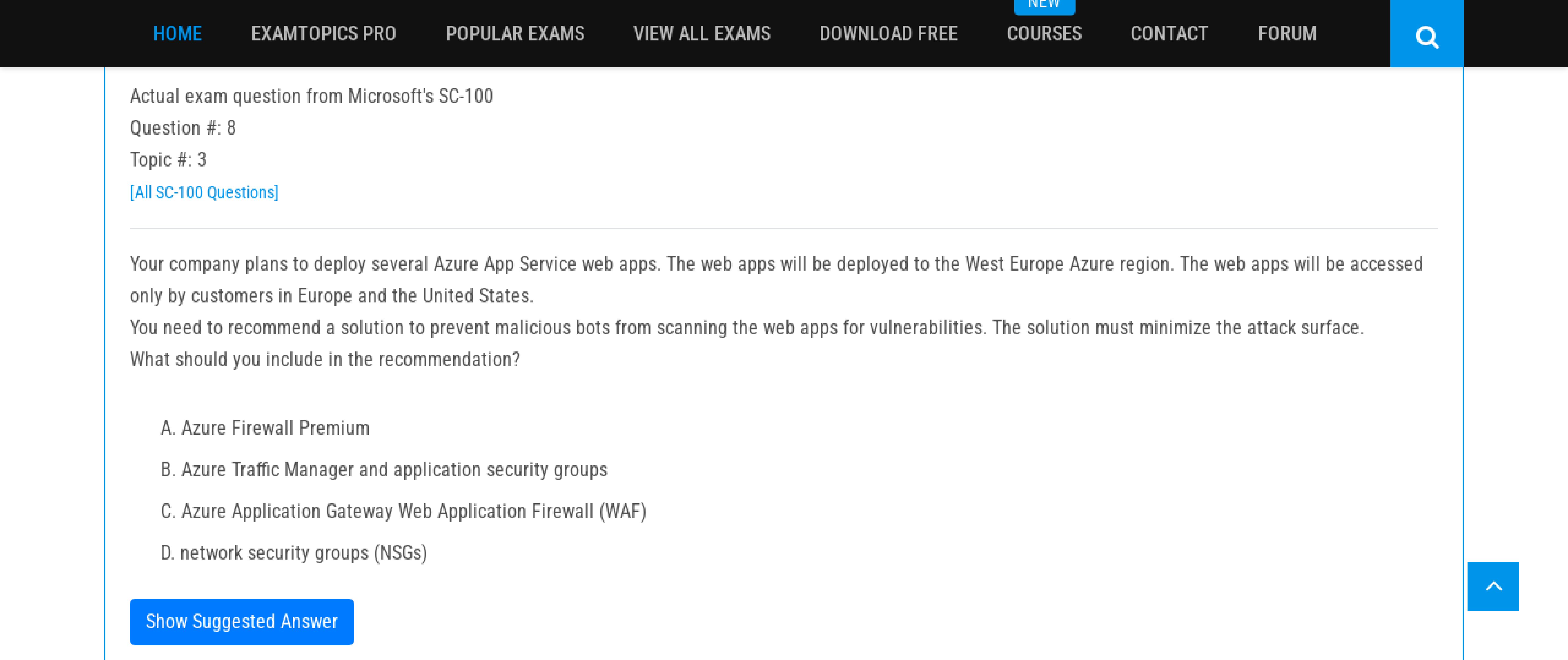
A. Microsoft Defender for Cloud Apps

B. Microsoft Information Protection

C. insider risk management

D. Azure Purview

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 8

Topic #: 3

[All SC-100 Questions]

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)

Actual exam question from Microsoft's SC-100

Question #: 9

Topic #: 3

[All SC-100 Questions]

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.

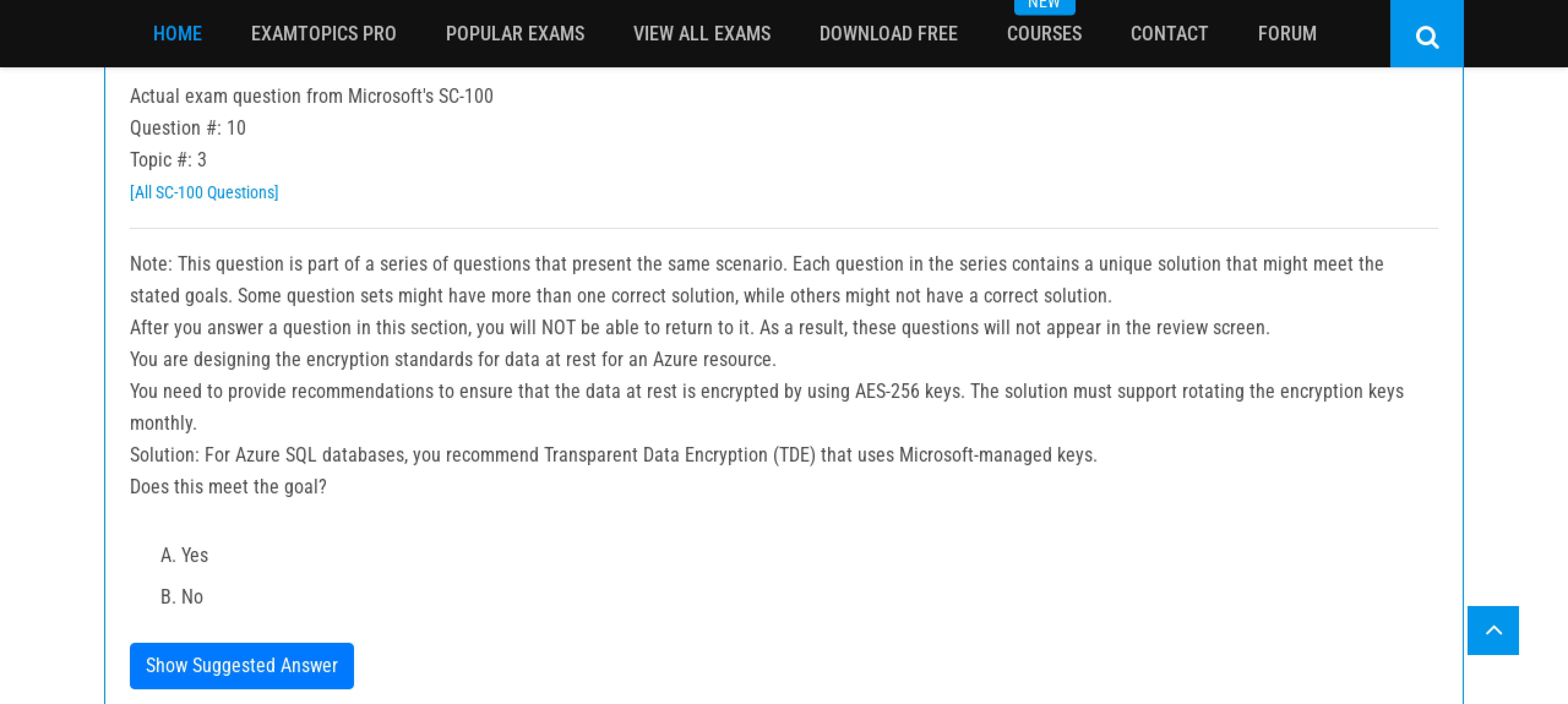
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.

Does this meet the goal?

A. Yes

B. No

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 10

Topic #: 3

[All SC-100 Questions]

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.

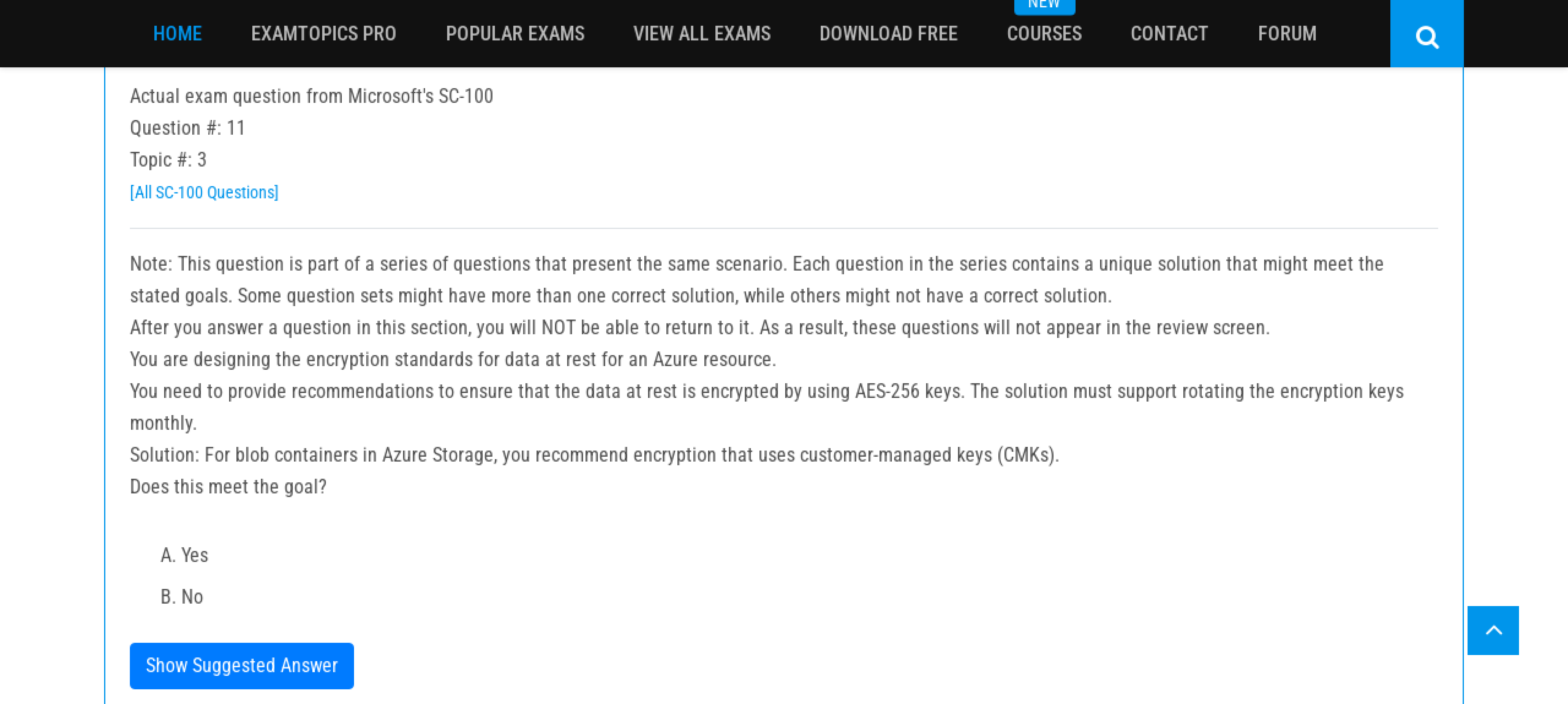
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

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



Actual exam question from Microsoft's SC-100

Question #: 11

Topic #: 3

[All SC-100 Questions]

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.

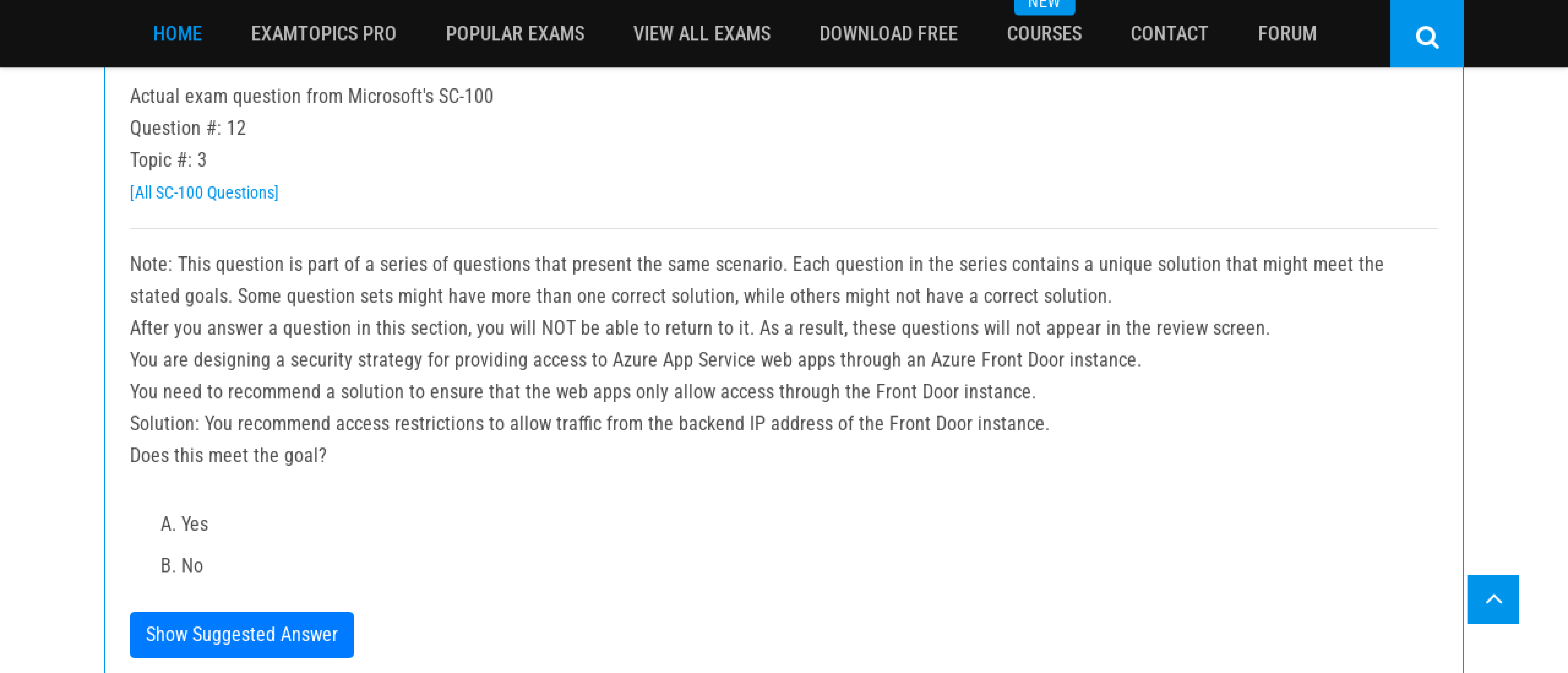
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

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



Actual exam question from Microsoft's SC-100

Question #: 12

Topic #: 3

[All SC-100 Questions]

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

Actual exam question from Microsoft's SC-100

Question #: 13

Topic #: 3

[All SC-100 Questions]

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.

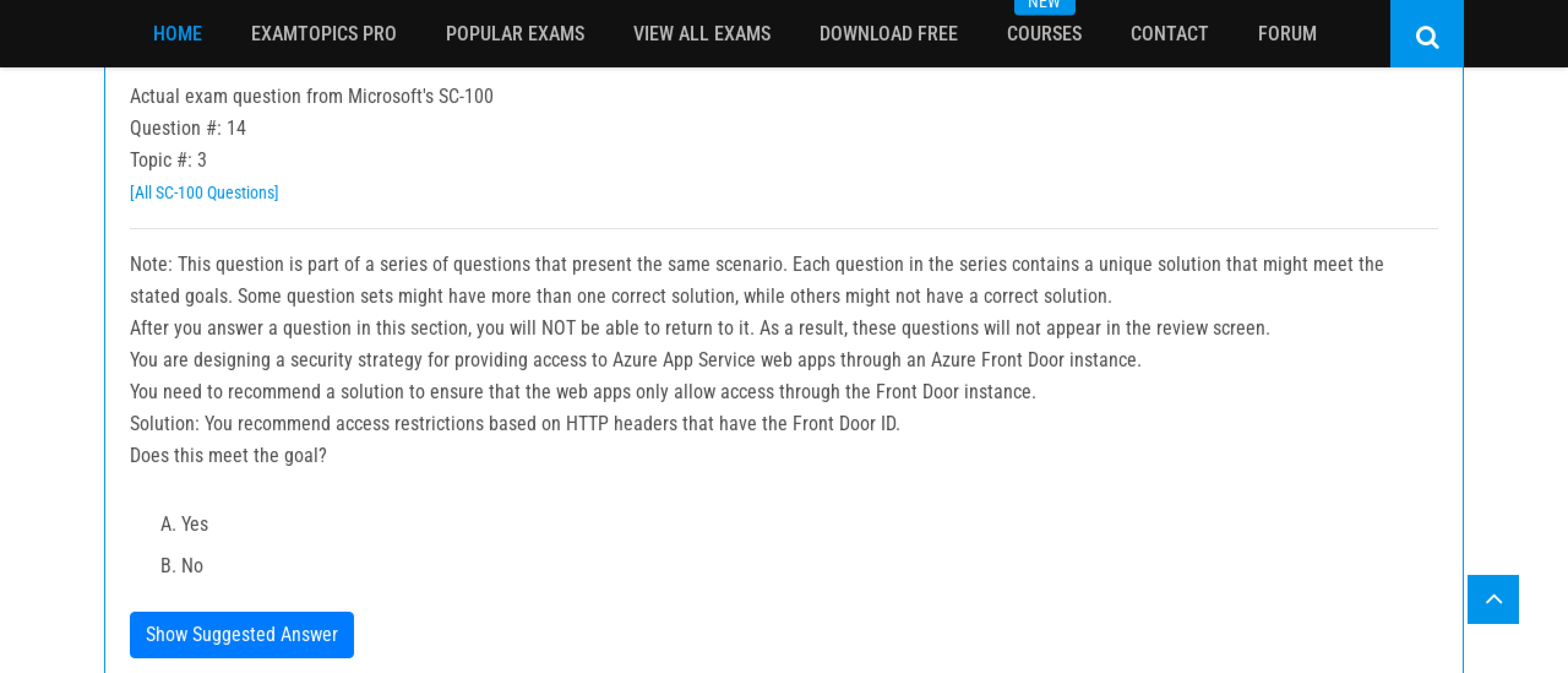
Solution: You recommend access restrictions that allow traffic from the Front Door service tags.

Does this meet the goal?

A. Yes

B. No

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 14

Topic #: 3

[All SC-100 Questions]

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 based on HTTP headers that have the Front Door ID.

Does this meet the goal?

A. Yes

B. No

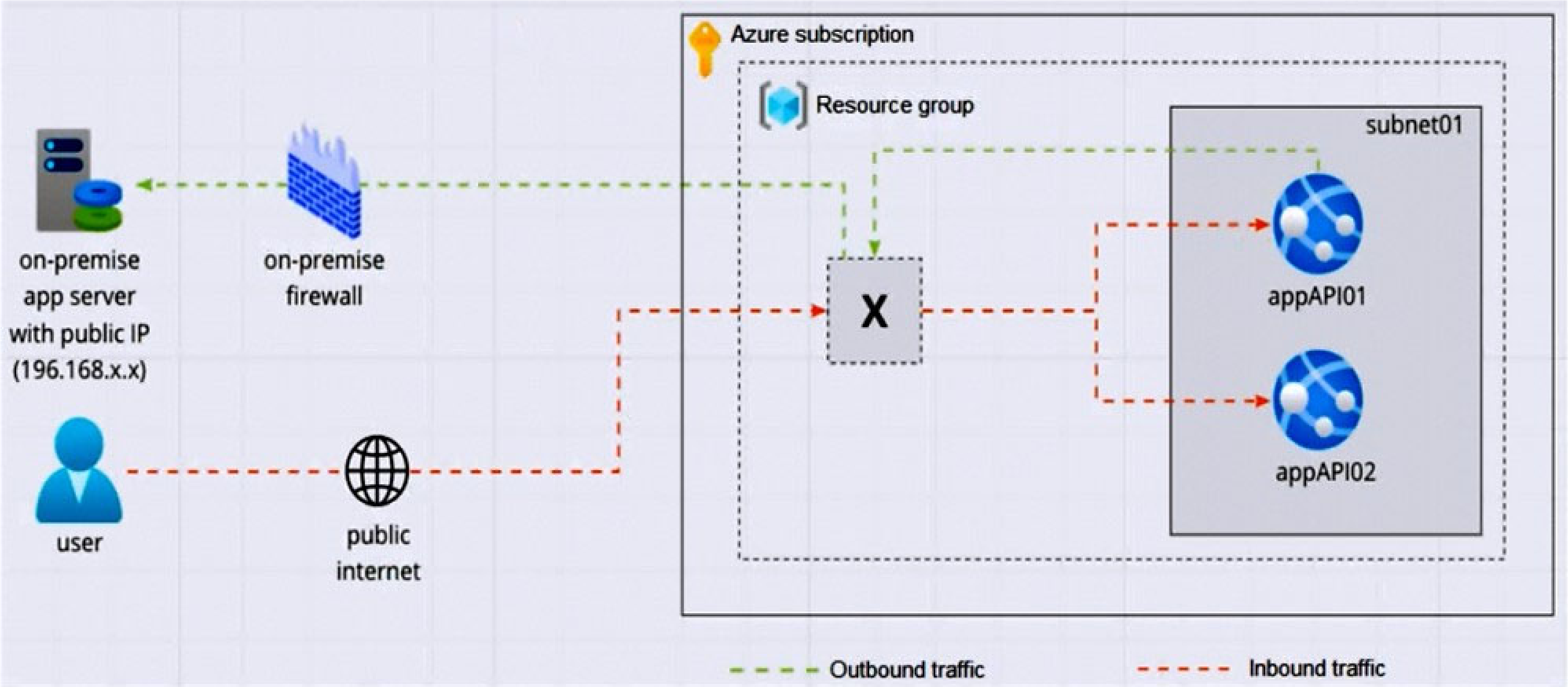
Actual exam question from Microsoft's SC-100

Question #: 15

Topic #: 3

[All SC-100 Questions]

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

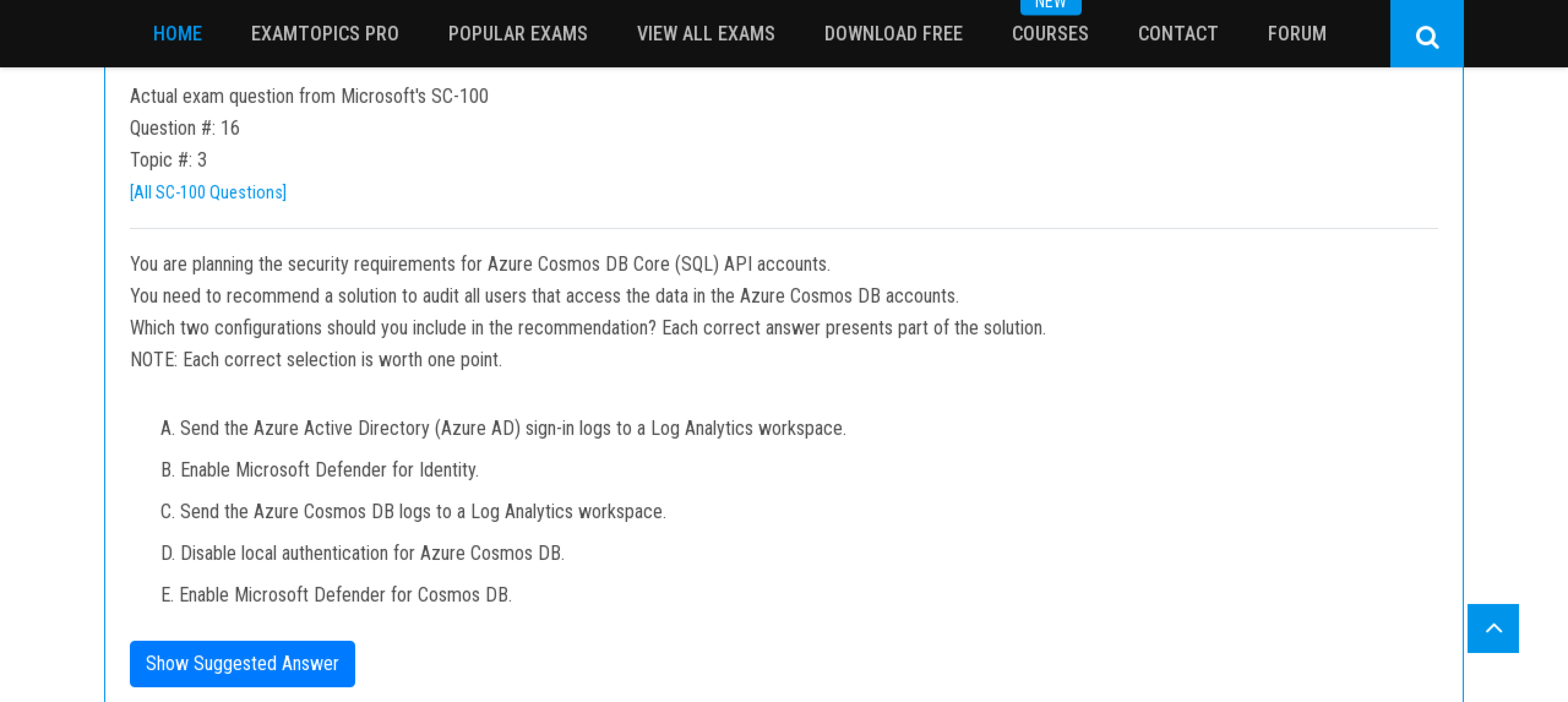
A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Firewall with policy rule sets

C. Azure Front Door with Azure Web Application Firewall (WAF)

D. Azure Application Gateway v2 with user-defined routes (UDRs)

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 16

Topic #: 3

[All SC-100 Questions]

You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts.

You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts.

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

NOTE: Each correct selection is worth one point.

A. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.

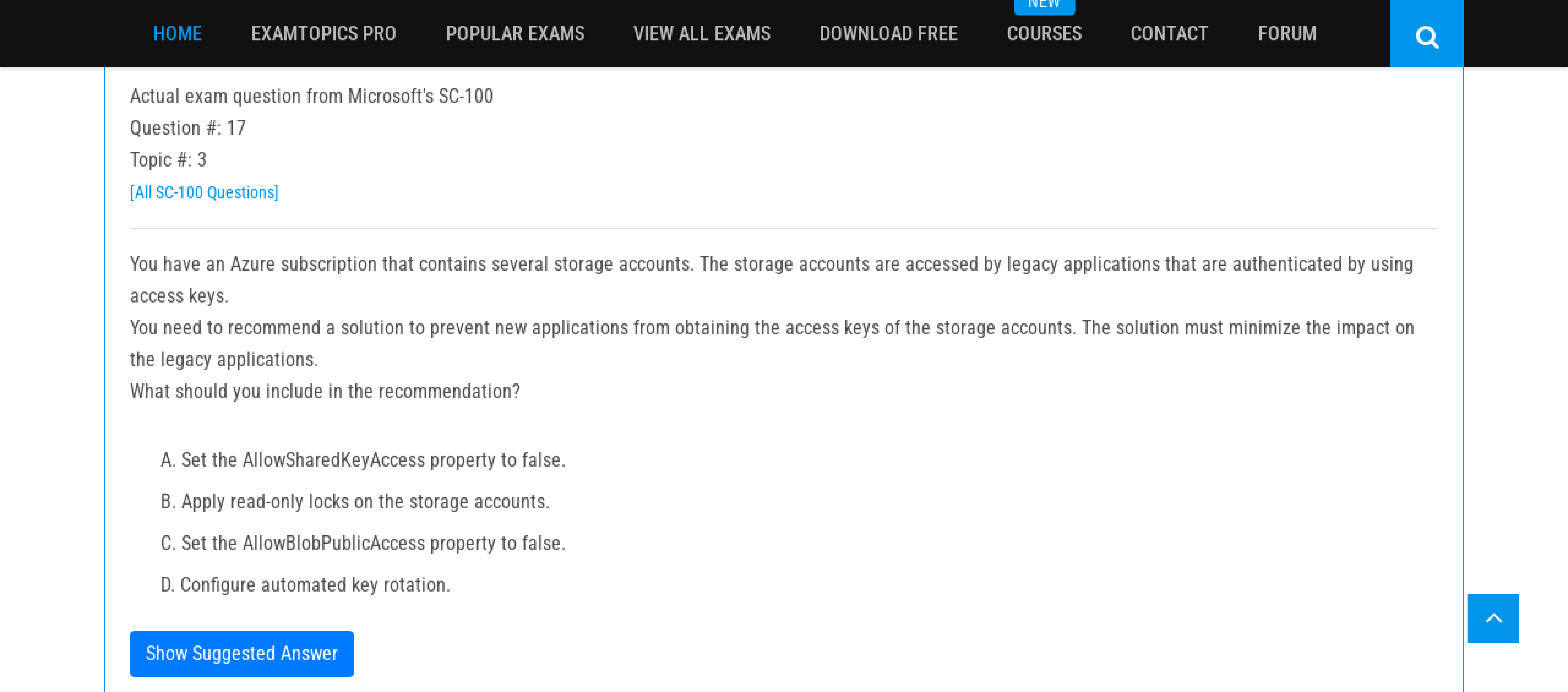
B. Enable Microsoft Defender for Identity.

C. Send the Azure Cosmos DB logs to a Log Analytics workspace.

D. Disable local authentication for Azure Cosmos DB.

E. Enable Microsoft Defender for Cosmos DB.

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 17

Topic #: 3

[All SC-100 Questions]

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

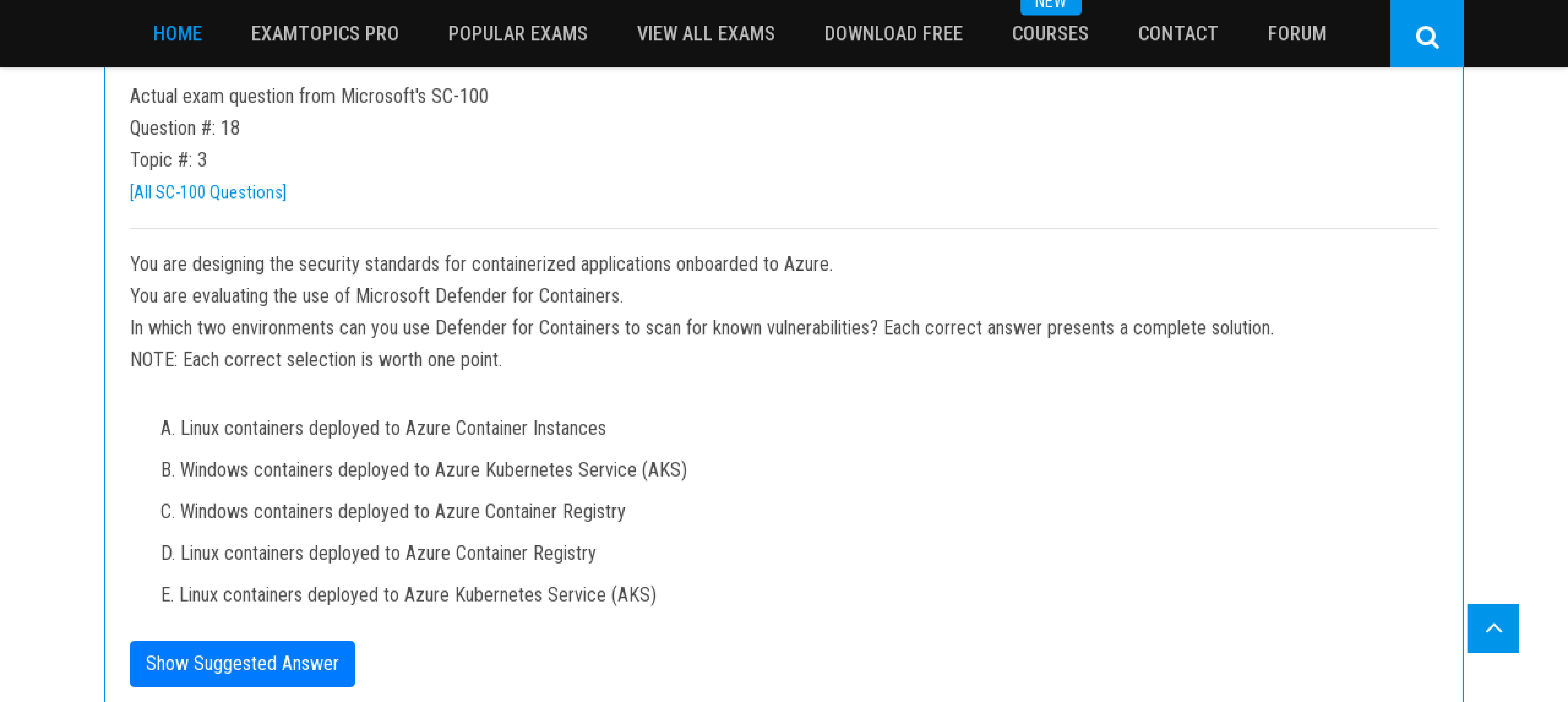
What should you include in the recommendation?

A. Set the AllowSharedKeyAccess property to false.

B. Apply read-only locks on the storage accounts.

C. Set the AllowBlobPublicAccess property to false.

D. Configure automated key rotation.



Actual exam question from Microsoft's SC-100

Question #: 18

Topic #: 3

[All SC-100 Questions]

You are designing the security standards for containerized applications onboarded to Azure.

You are evaluating the use of Microsoft Defender for Containers.

In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

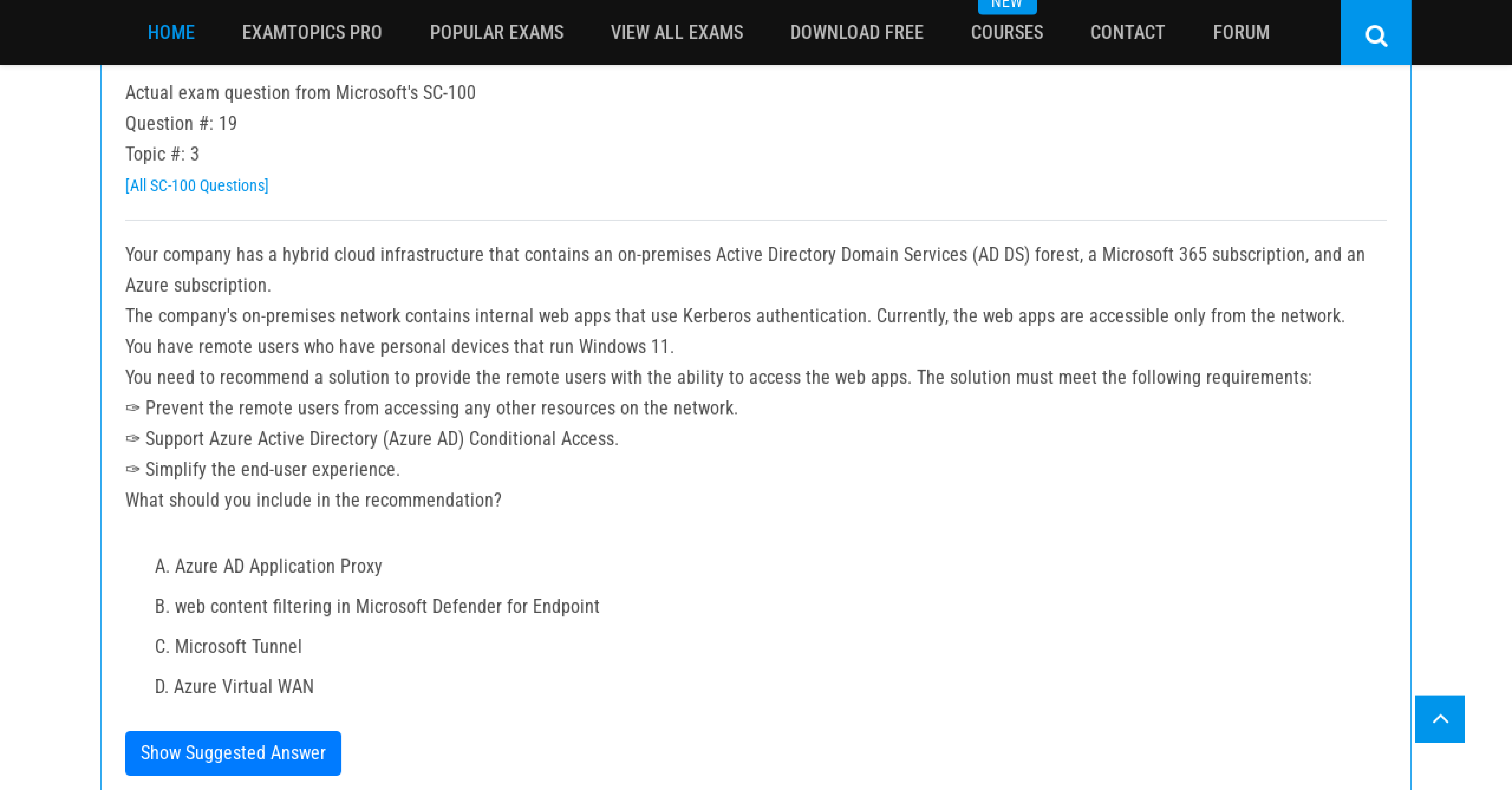
A. Linux containers deployed to Azure Container Instances

B. Windows containers deployed to Azure Kubernetes Service (AKS)

C. Windows containers deployed to Azure Container Registry

D. Linux containers deployed to Azure Container Registry

E. Linux containers deployed to Azure Kubernetes Service (AKS)



Actual exam question from Microsoft's SC-100

Question #: 19

Topic #: 3

[All SC-100 Questions]

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft 365 subscription, and an Azure subscription.

The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

✑ Prevent the remote users from accessing any other resources on the network.

✑ Support Azure Active Directory (Azure AD) Conditional Access.

✑ Simplify the end-user experience.

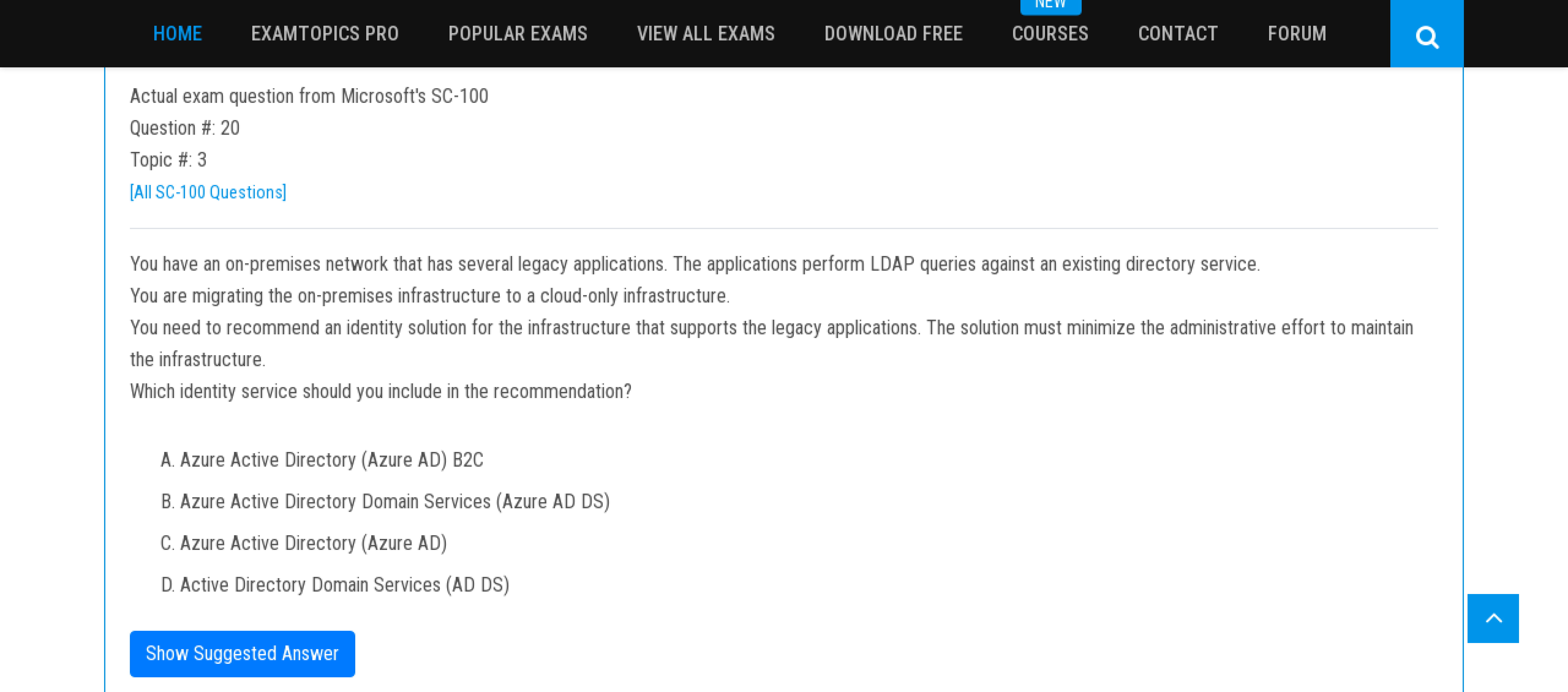
What should you include in the recommendation?

A. Azure AD Application Proxy

B. web content filtering in Microsoft Defender for Endpoint

C. Microsoft Tunnel

D. Azure Virtual WAN



Actual exam question from Microsoft's SC-100
Question #: 20
Topic #: 3
[All SC-100 Questions]

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service.

You are migrating the on-premises infrastructure to a cloud-only infrastructure.

You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.

Which identity service should you include in the recommendation?

A. Azure Active Directory (Azure AD) B2C

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD)

D. Active Directory Domain Services (AD DS)

Actual exam question from Microsoft's SC-100

Question #: 21

Topic #: 3

[All SC-100 Questions]

HOTSPOT -

Your company has a Microsoft 365 ES subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS).

You need to recommend an identity security strategy that meets the following requirements:

✑ Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

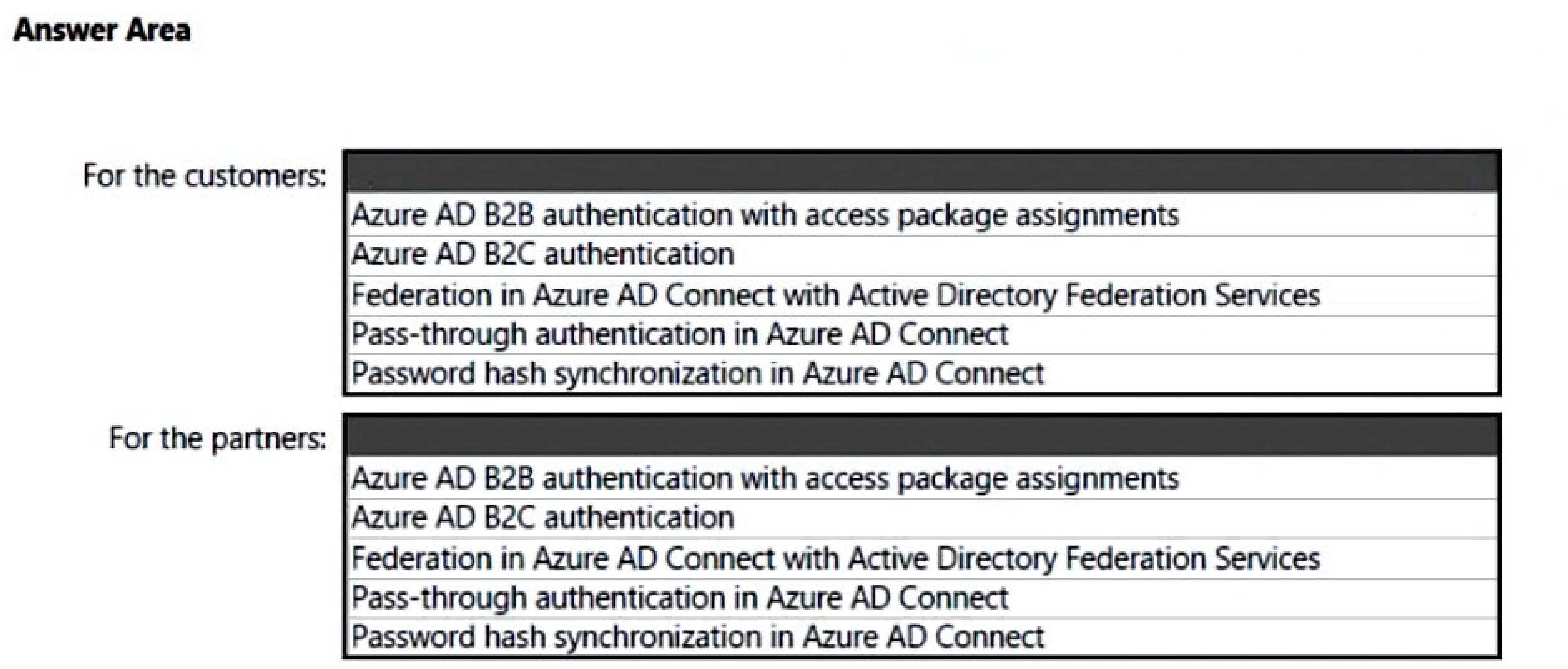
✑ Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components.

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

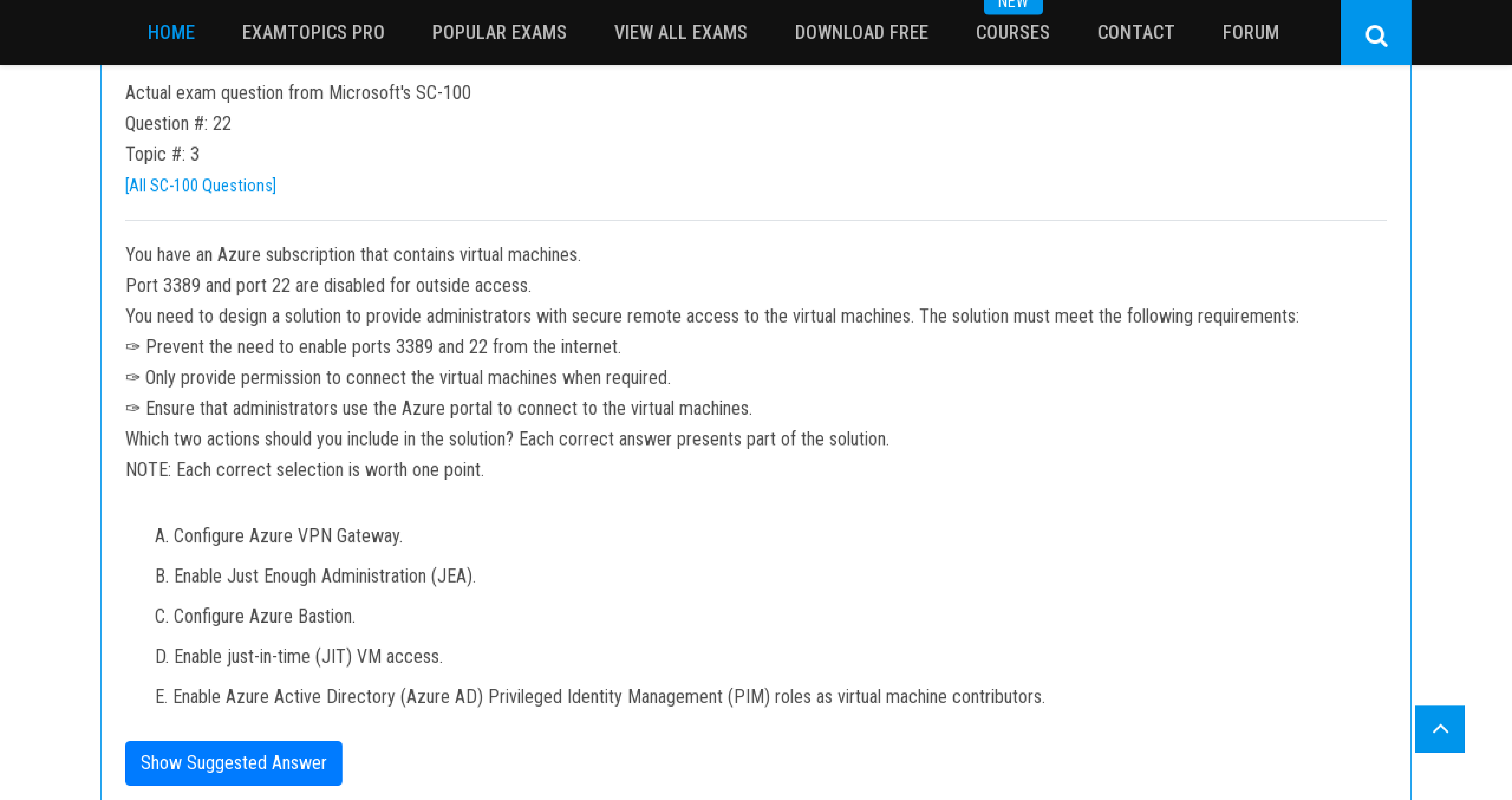
For the customers:

- Azure AD B2B authentication with access package assignments
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

For the partners:

- Azure AD B2B authentication with access package assignments
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 22
Topic #: 3
[All SC-100 Questions]

You have an Azure subscription that contains virtual machines.
Port 3389 and port 22 are disabled for outside access.
You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:
✑ Prevent the need to enable ports 3389 and 22 from the internet.
✑ Only provide permission to connect the virtual machines when required.
✑ Ensure that administrators use the Azure portal to connect to the virtual machines.
Which two actions should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

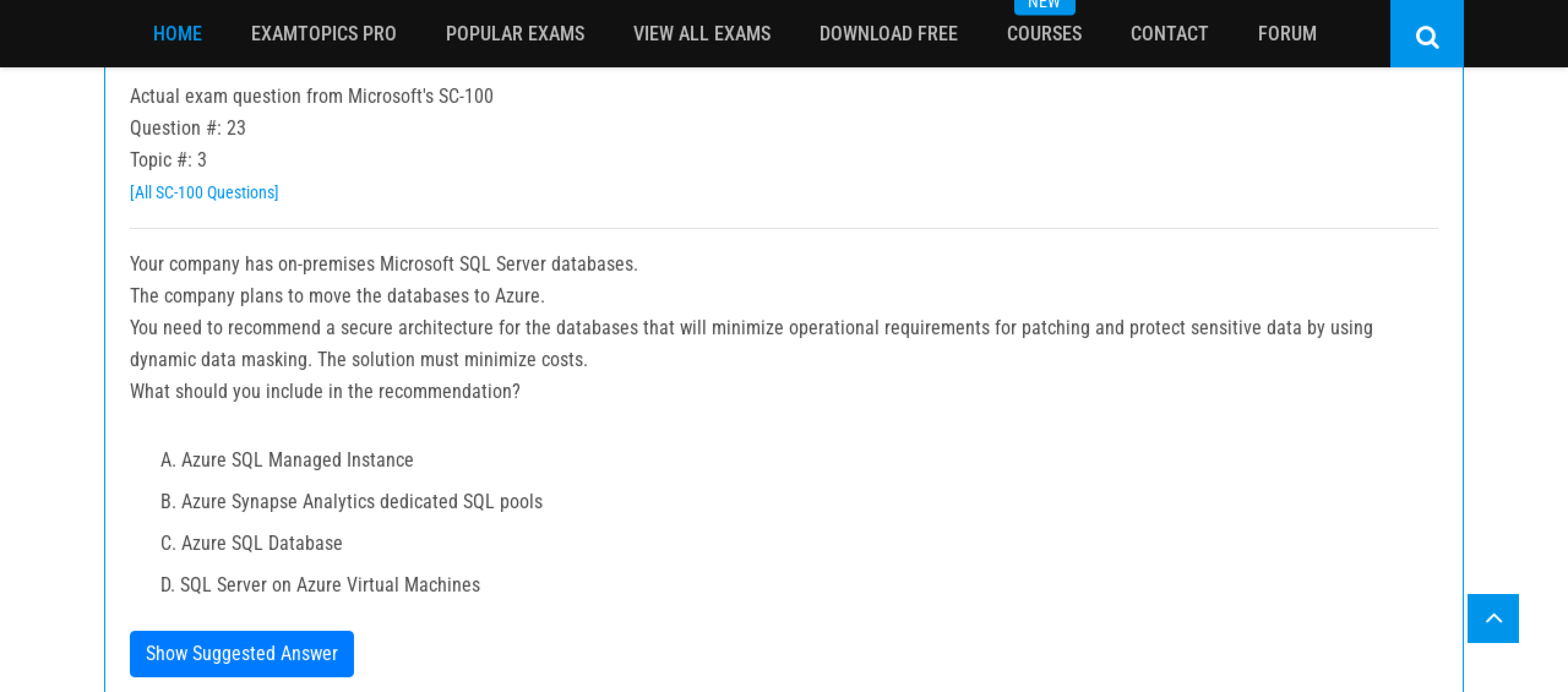
A. Configure Azure VPN Gateway.

B. Enable Just Enough Administration (JEA).

C. Configure Azure Bastion.

D. Enable just-in-time (JIT) VM access.

E. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.



Actual exam question from Microsoft's SC-100

Question #: 23

Topic #: 3

[All SC-100 Questions]

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. Azure SQL Managed Instance

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

D. SQL Server on Azure Virtual Machines

Actual exam question from Microsoft's SC-100

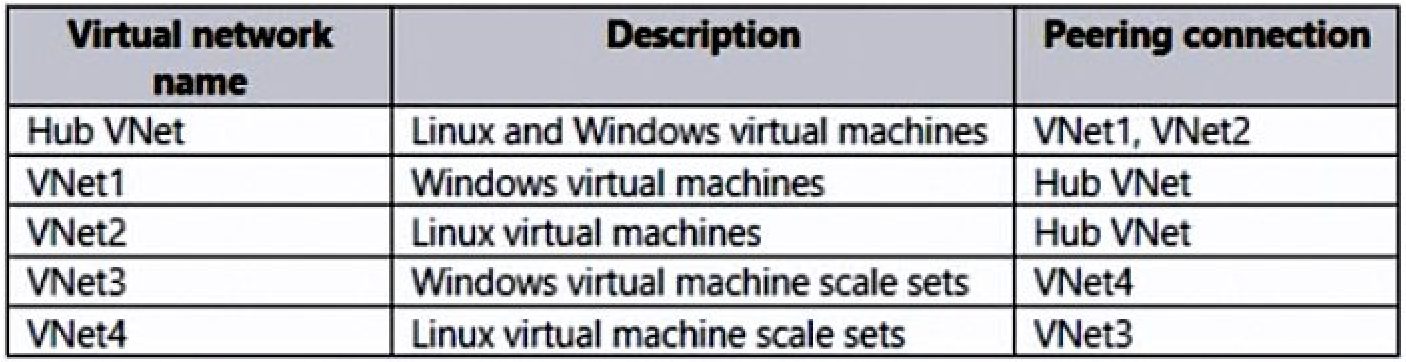
Question #: 24

Topic #: 3

[All SC-100 Questions]

Your company plans to move all on-premises virtual machines to Azure.

A network engineer proposes the Azure virtual network design shown in the following table.



Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines.

Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1

B. 2

C. 3

D. 4

E. 5

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 25

Topic #: 3

[All SC-100 Questions]

HOTSPOT -

Your company has an Azure App Service plan that is used to deploy containerized web apps.

You are designing a secure DevOps strategy for deploying the web apps to the App Service plan.

You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:

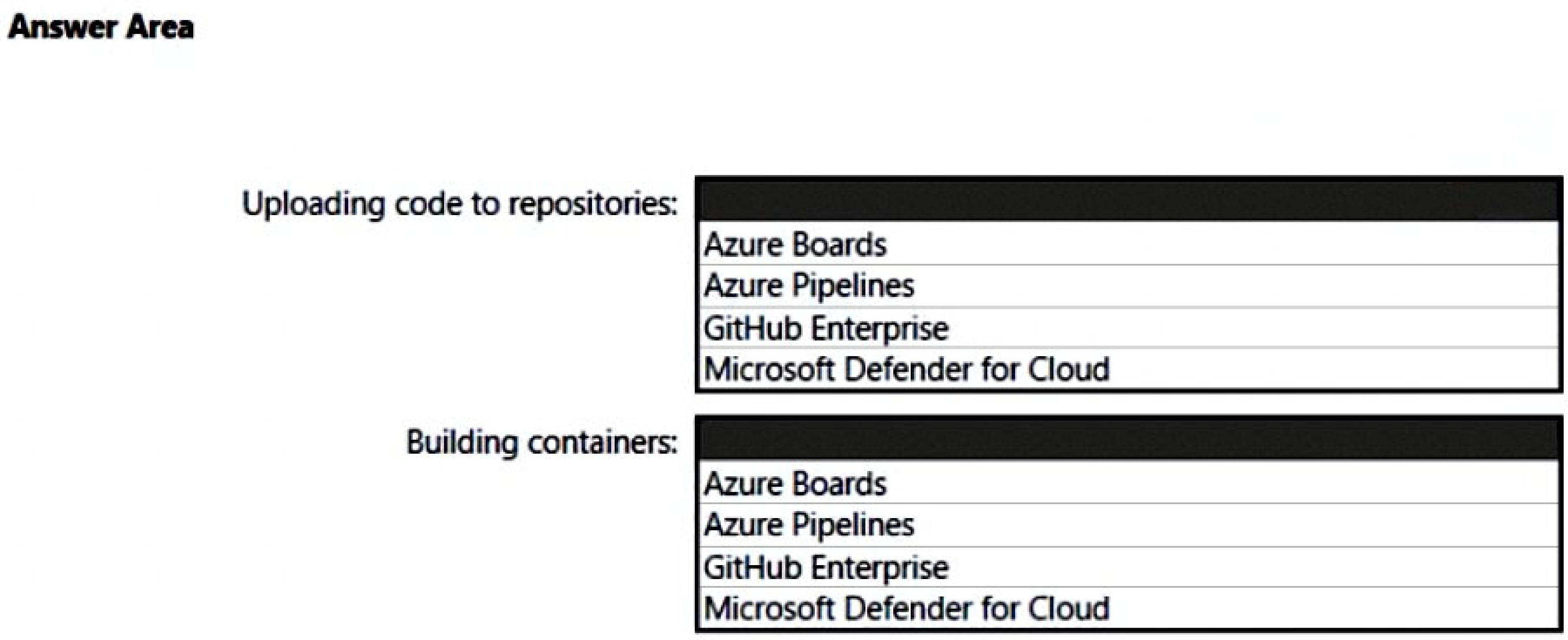
✑ Uploading the code to repositories

✑ Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

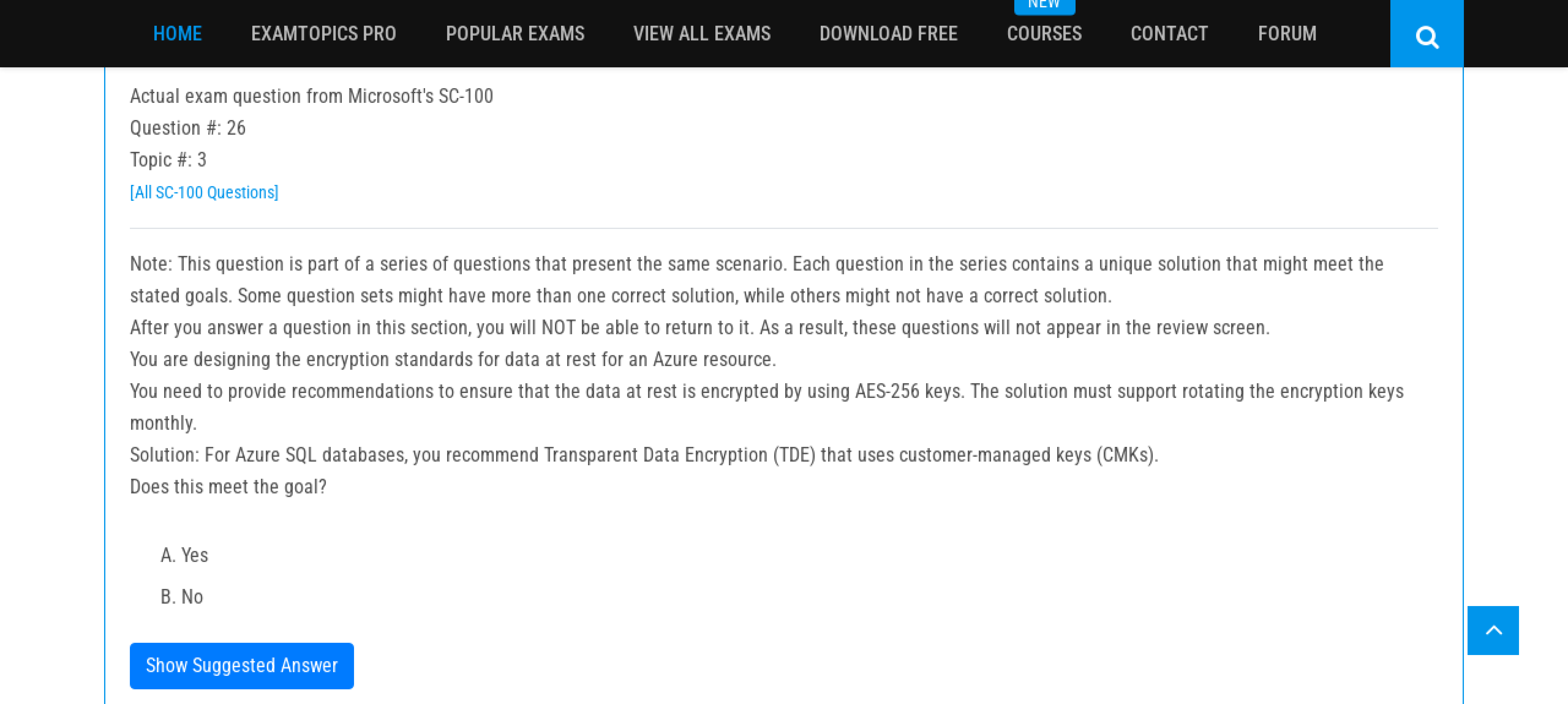
Uploading code to repositories:

Azure Boards
Azure Pipelines
GitHub Enterprise
Microsoft Defender for Cloud

Building containers:

Azure Boards
Azure Pipelines
GitHub Enterprise
Microsoft Defender for Cloud

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 26

Topic #: 3

[All SC-100 Questions]

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 customer-managed keys (CMKs).

Does this meet the goal?

A. Yes

B. No

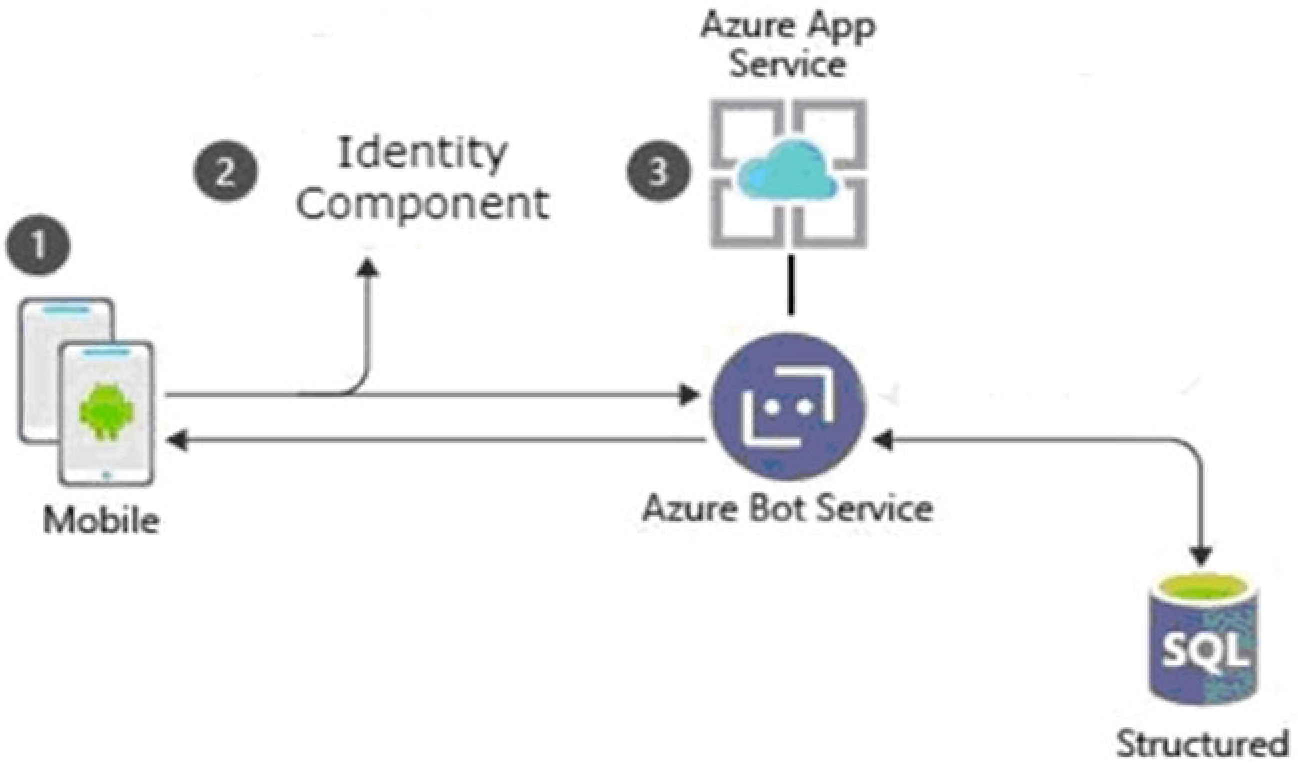
Actual exam question from Microsoft's SC-100

Question #: 27

Topic #: 3

[All SC-100 Questions]

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

✑ Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.

✑ Use a customer identity store.

✑ Support fully customizable branding for the app.

Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2B

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD) B2C

D. Azure AD Connect

Show Suggested Answer

Actual exam question from Microsoft's SC-100

Question #: 28

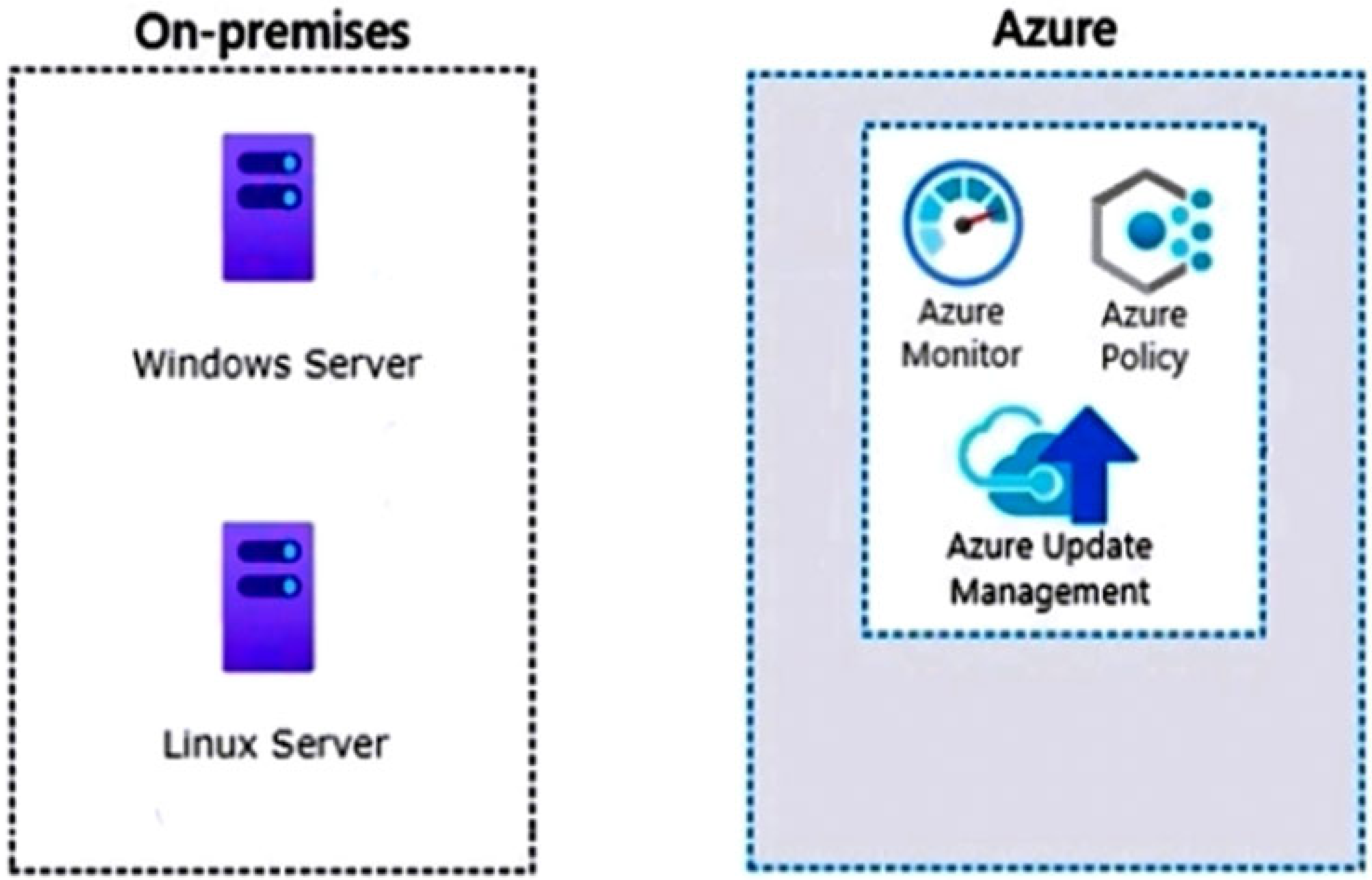
Topic #: 3

[All SC-100 Questions]

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:

✑ Govern virtual machines and servers across multiple environments.

✑ Enforce standards for all the resources across all the environments by using Azure Policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. on-premises data gateway

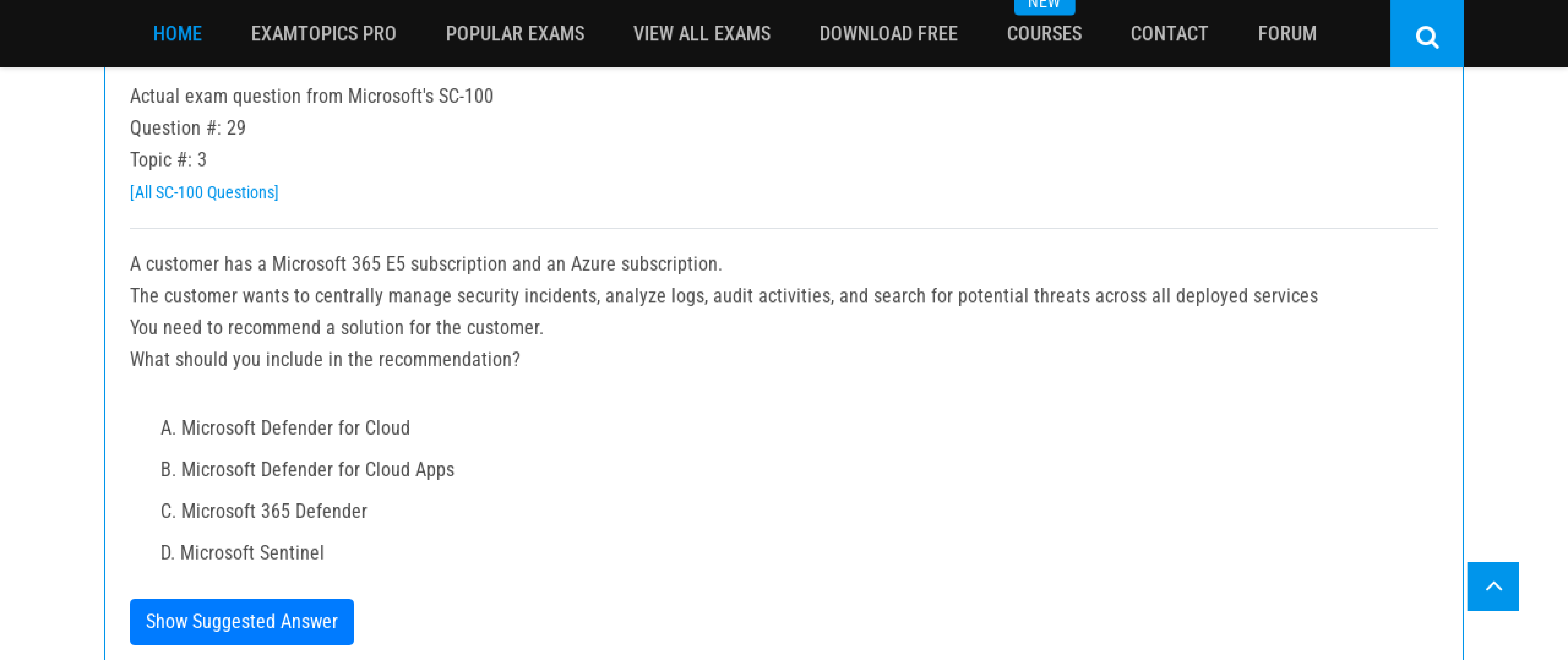
B. Azure VPN Gateway

C. guest configuration in Azure Policy

D. Azure Arc

E. Azure Bastion

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 29

Topic #: 3

[All SC-100 Questions]

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze logs, audit activities, and search for potential threats across all deployed services

You need to recommend a solution for the customer.

What should you include in the recommendation?

A. Microsoft Defender for Cloud

B. Microsoft Defender for Cloud Apps

C. Microsoft 365 Defender

D. Microsoft Sentinel

Actual exam question from Microsoft's SC-100
Question #: 30
Topic #: 3
[All SC-100 Questions]

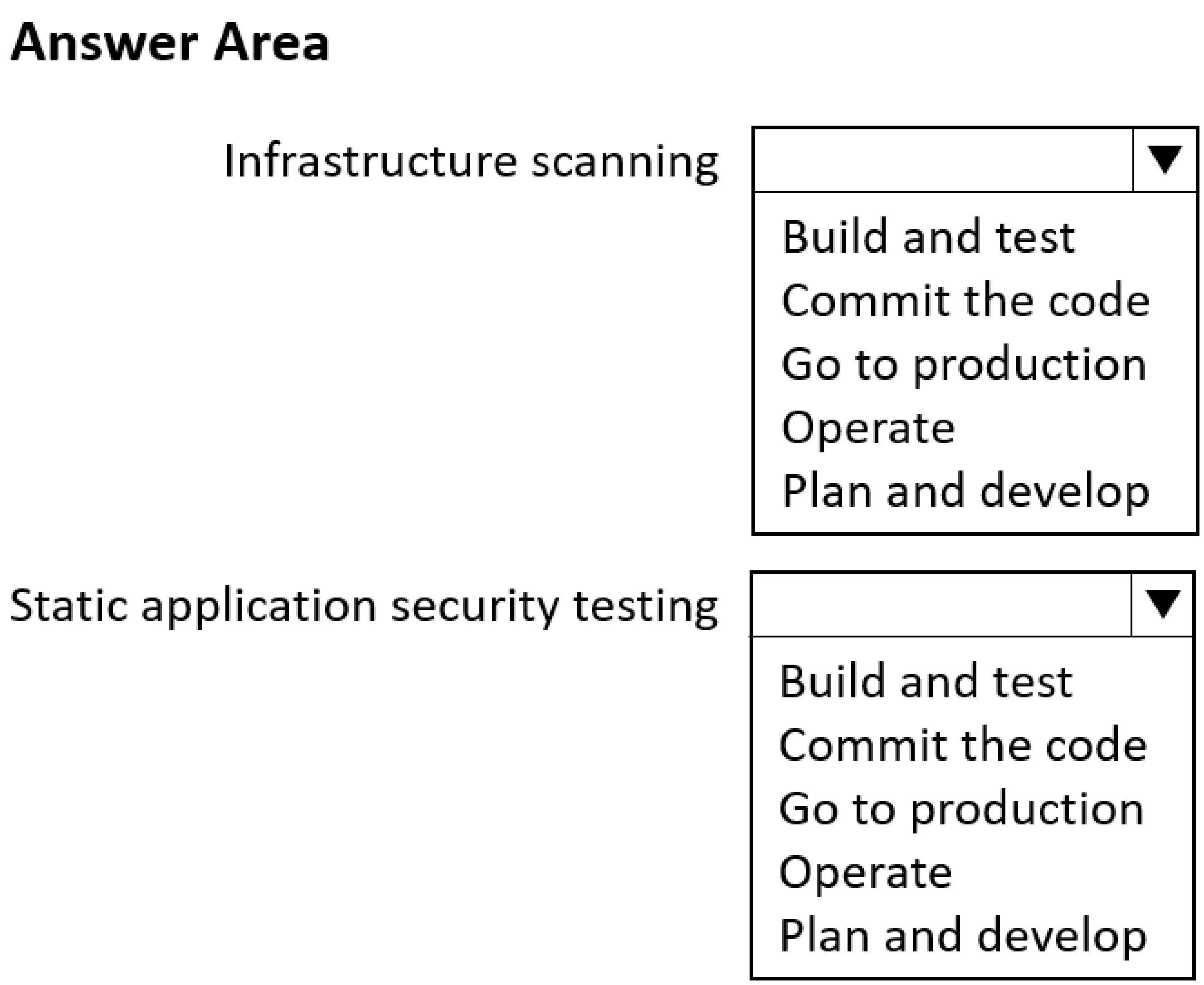
HOTSPOT
-

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines.

You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines.

What should recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

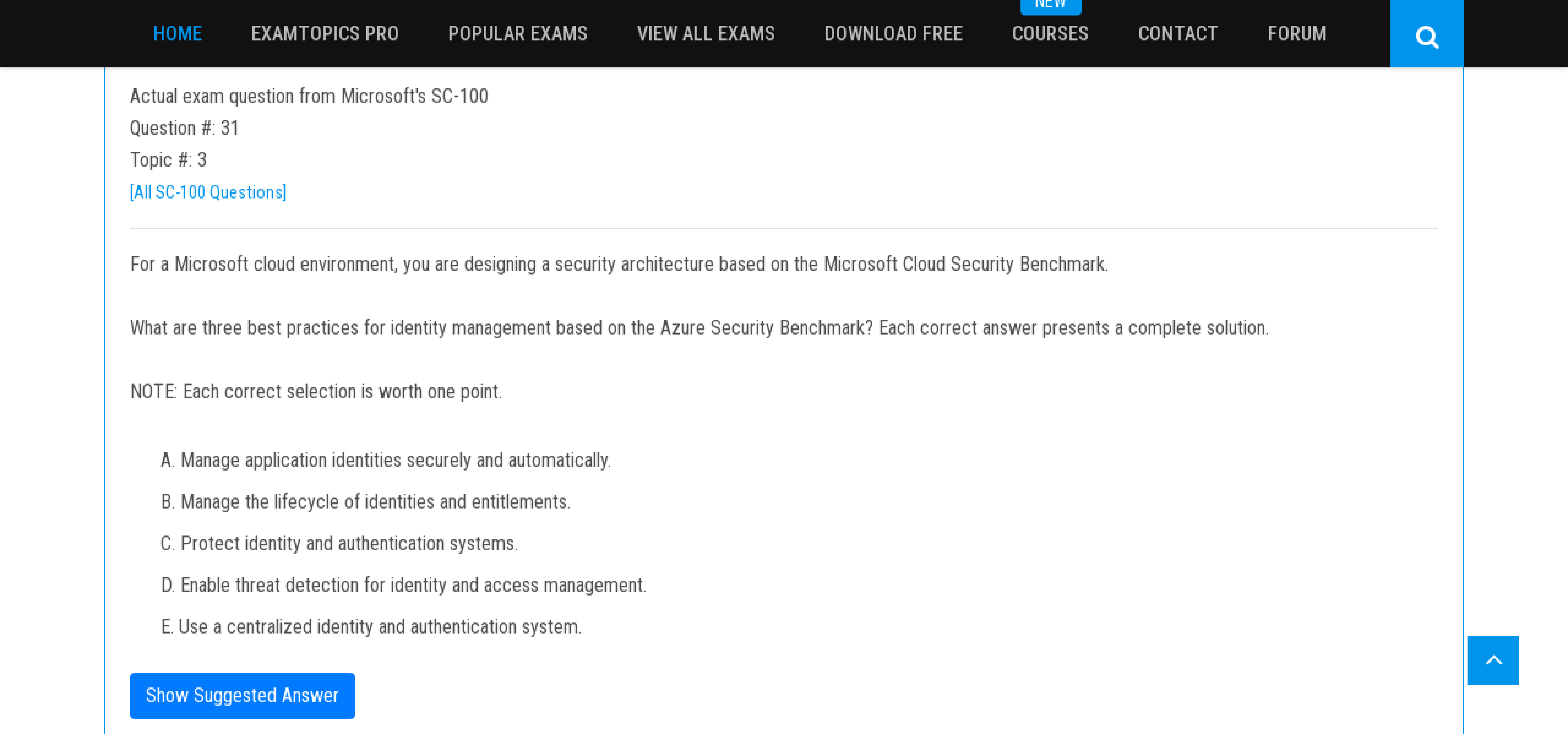


Answer Area

Infrastructure scanning ▼
- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Static application security testing ▼
- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 31
Topic #: 3
[All SC-100 Questions]

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

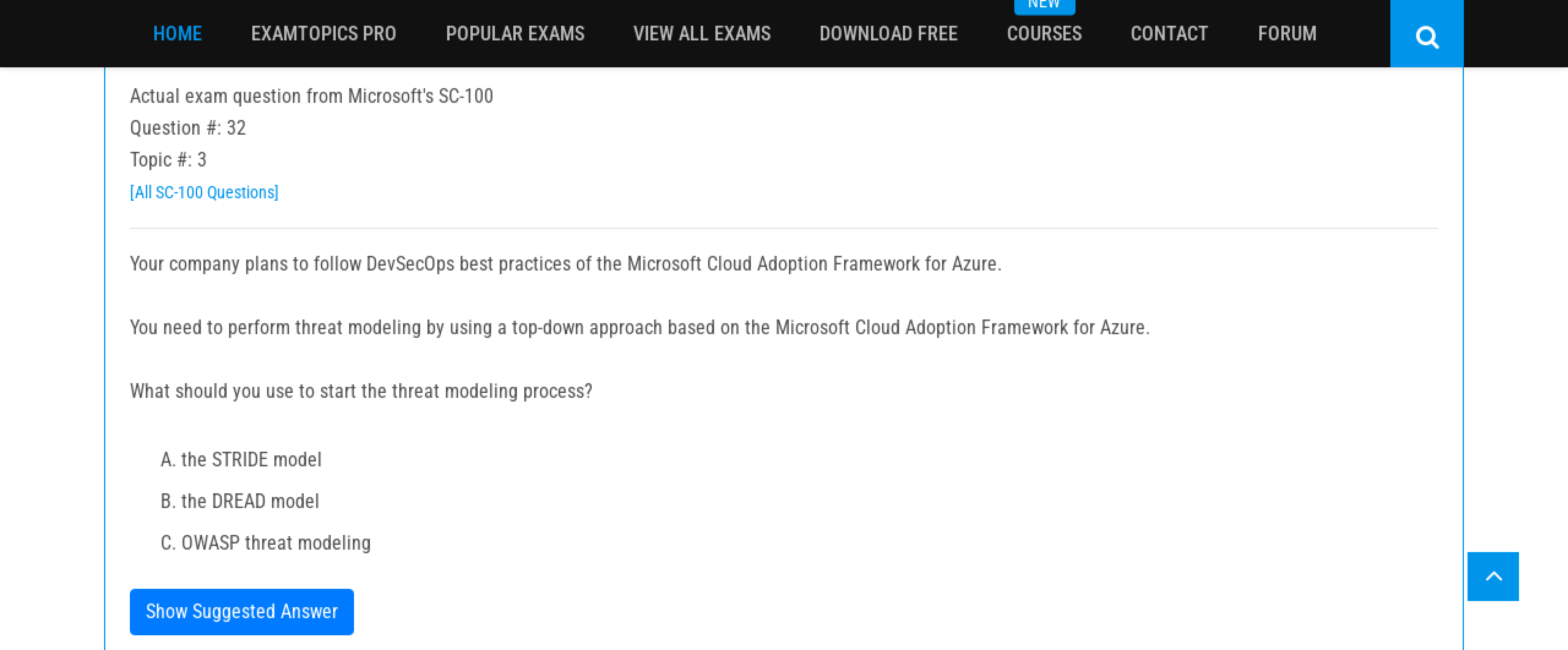
A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements.

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.



Actual exam question from Microsoft's SC-100

Question #: 32

Topic #: 3

[All SC-100 Questions]

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure.

You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure.

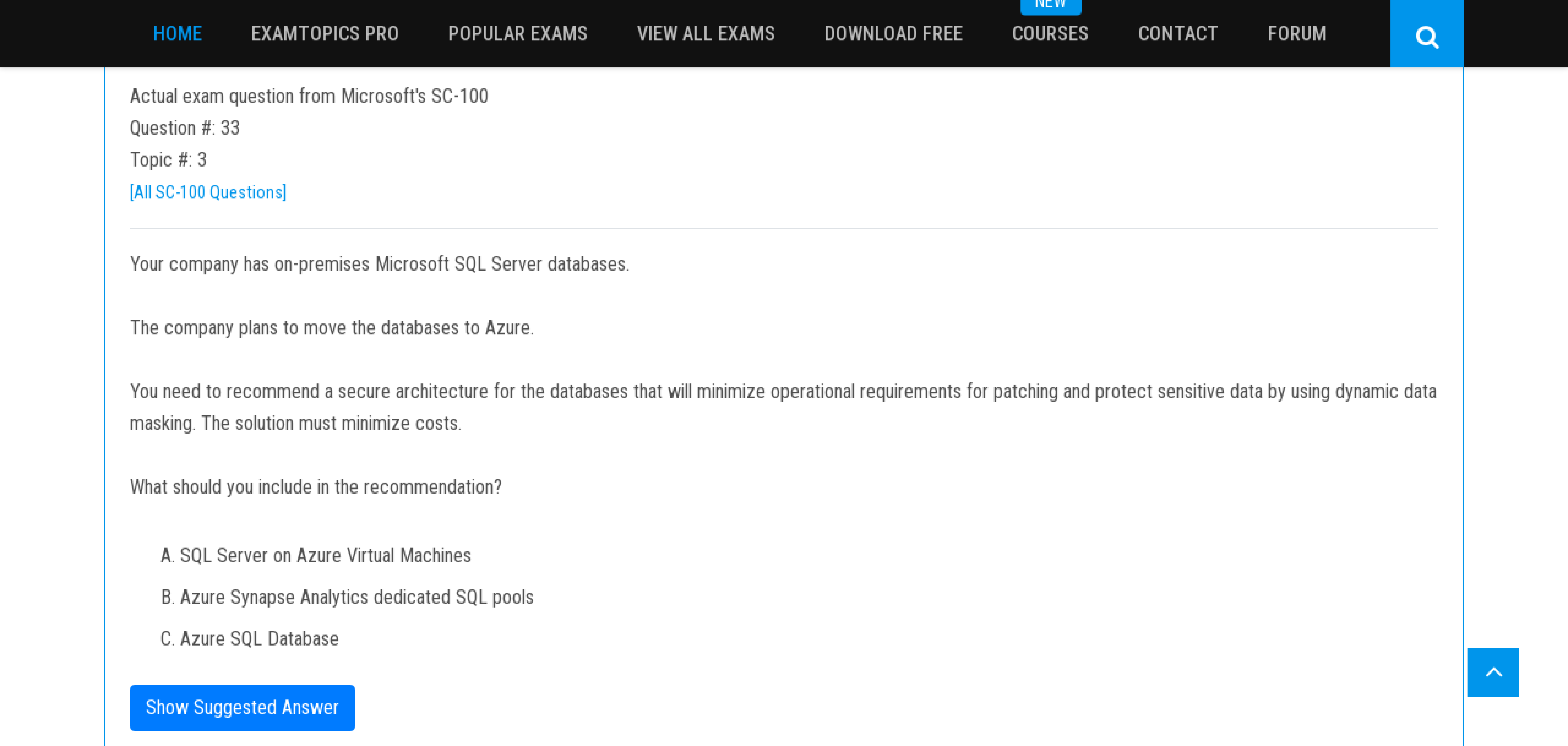
What should you use to start the threat modeling process?

A. the STRIDE model

B. the DREAD model

C. OWASP threat modeling

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 33
Topic #: 3
[All SC-100 Questions]

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

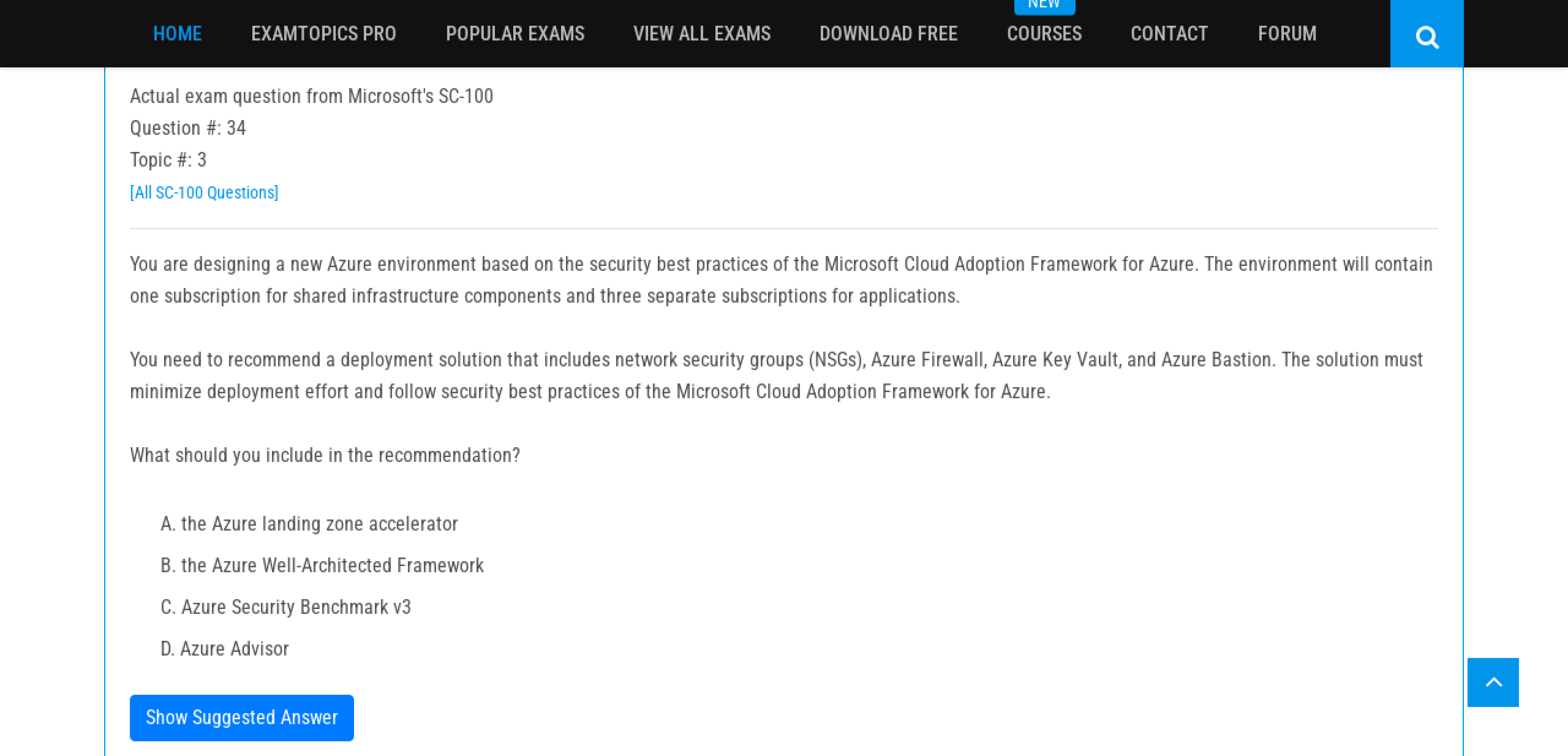
You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. SQL Server on Azure Virtual Machines

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database



Actual exam question from Microsoft's SC-100

Question #: 34

Topic #: 3

[All SC-100 Questions]

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs), Azure Firewall, Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure.

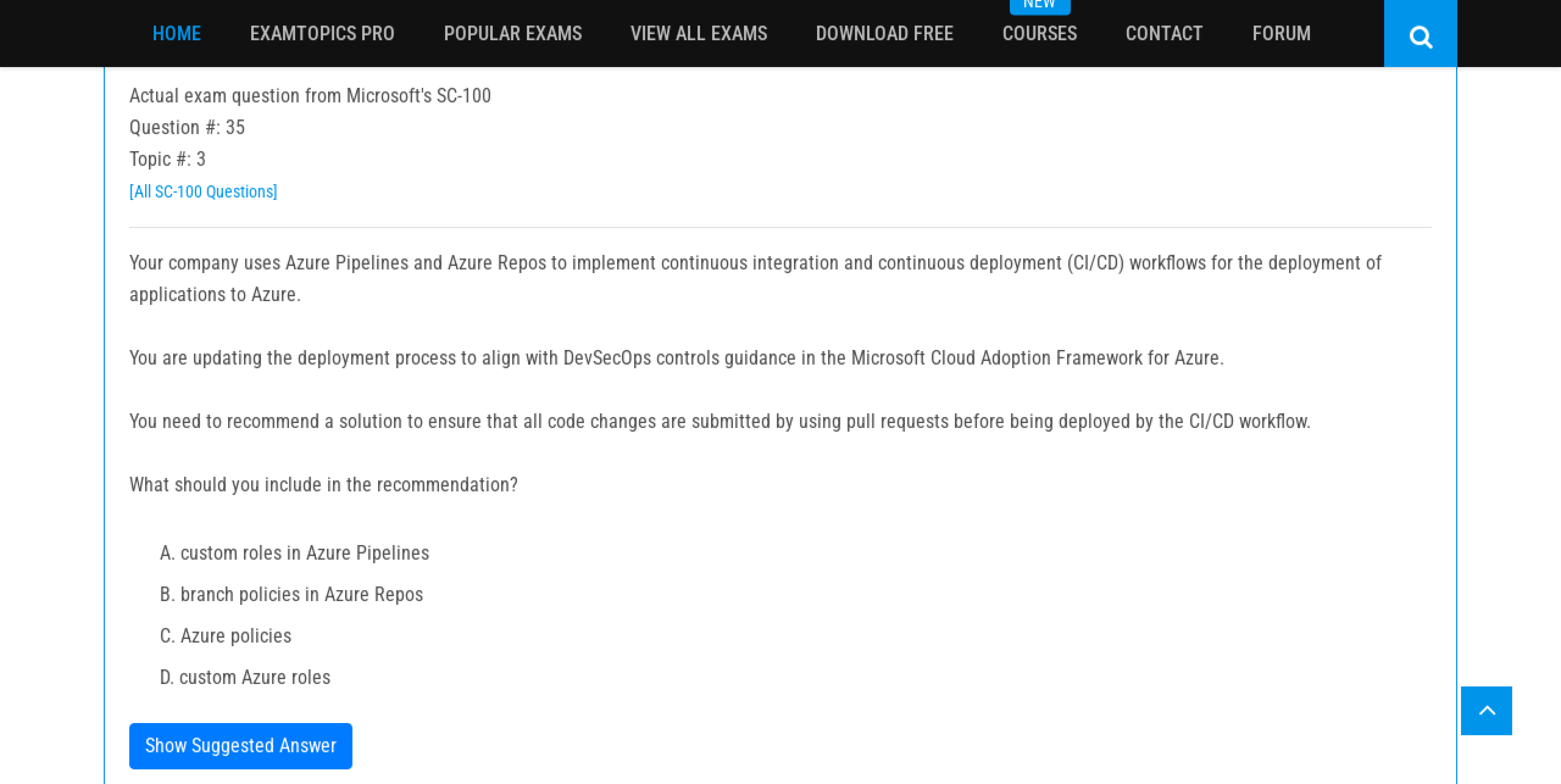
What should you include in the recommendation?

A. the Azure landing zone accelerator

B. the Azure Well-Architected Framework

C. Azure Security Benchmark v3

D. Azure Advisor



Actual exam question from Microsoft's SC-100

Question #: 35

Topic #: 3

[All SC-100 Questions]

Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.

What should you include in the recommendation?

A. custom roles in Azure Pipelines

B. branch policies in Azure Repos

C. Azure policies

D. custom Azure roles

Actual exam question from Microsoft's SC-100

Question #: 36

Topic #: 3

[All SC-100 Questions]

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Your on-premises network contains firewalls that support forwarding event logs in the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls.

You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel.

What should you include in the recommendation?

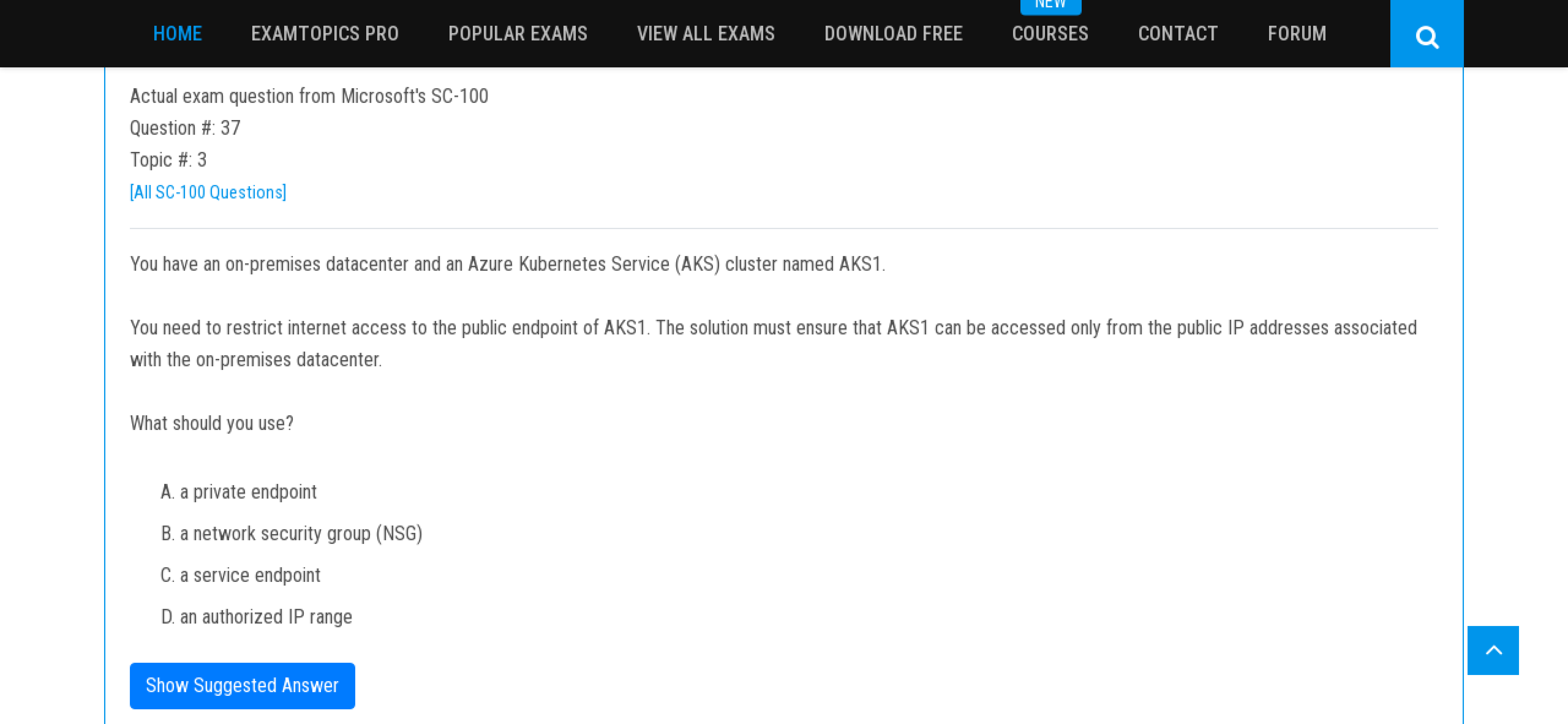
A. an Azure logic app

B. an on-premises Syslog server

C. an on-premises data gateway

D. Azure Data Factory

Show Suggested Answer



Actual exam question from Microsoft's SC-100

Question #: 37

Topic #: 3

[All SC-100 Questions]

You have an on-premises datacenter and an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to restrict internet access to the public endpoint of AKS1. The solution must ensure that AKS1 can be accessed only from the public IP addresses associated with the on-premises datacenter.

What should you use?

A. a private endpoint

B. a network security group (NSG)

C. a service endpoint

D. an authorized IP range

Actual exam question from Microsoft's SC-100

Question #: 38

Topic #: 3

[All SC-100 Questions]

HOTSPOT

-

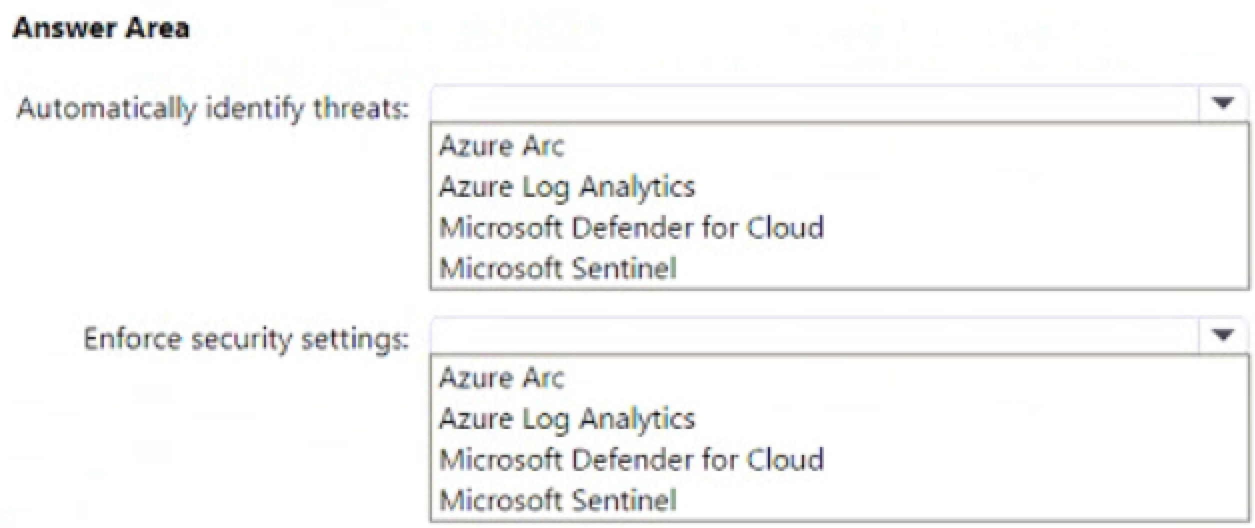
You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.

You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:

- Automatically identify threats found in AWS CloudTrail events.
- Enforce security settings on AWS virtual machines by using Azure policies.

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

NOTE: Each correct selection is worth one point.

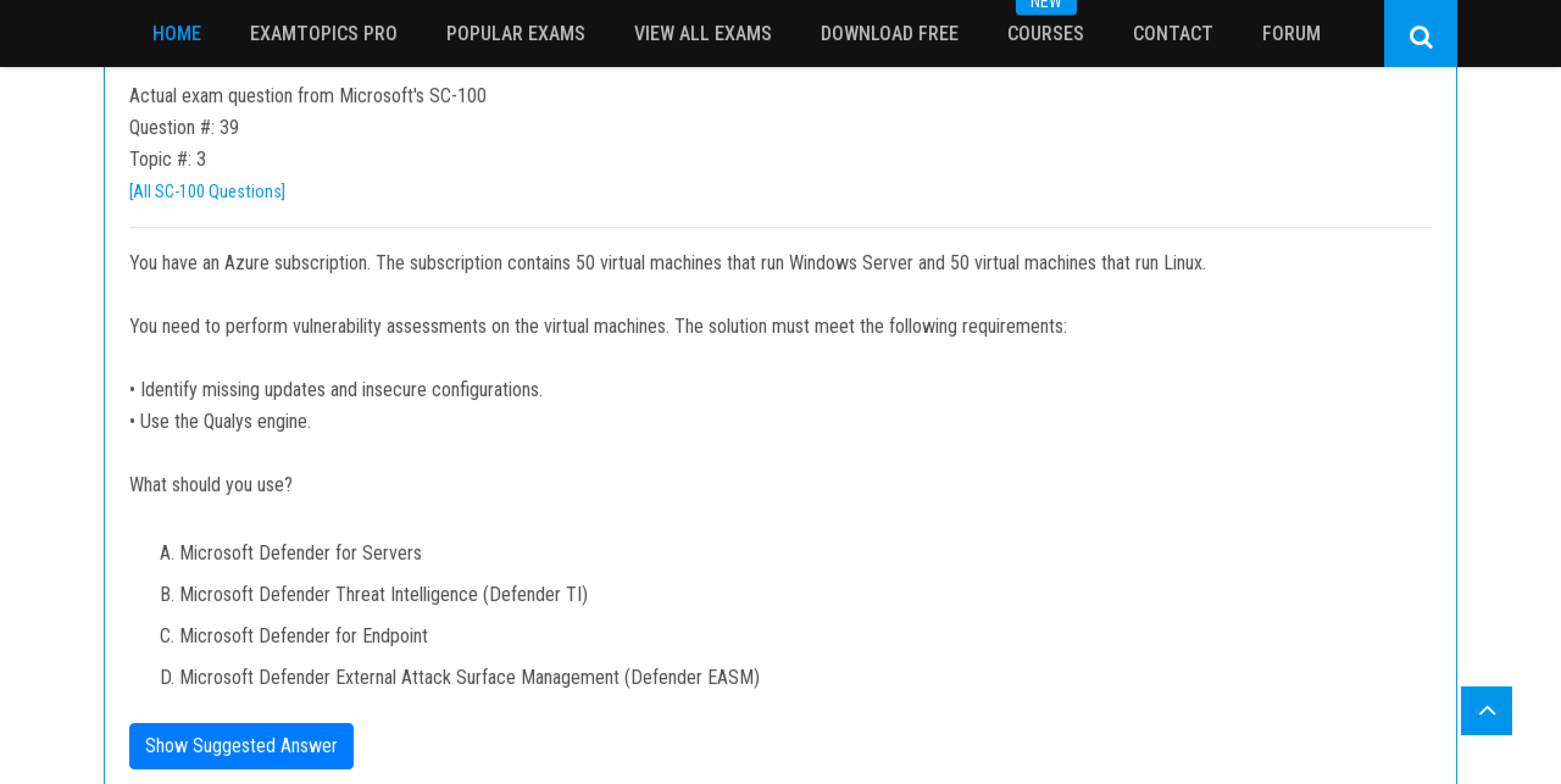


Answer Area

Automatically identify threats:
Azure Arc
Azure Log Analytics
Microsoft Defender for Cloud
Microsoft Sentinel

Enforce security settings:
Azure Arc
Azure Log Analytics
Microsoft Defender for Cloud
Microsoft Sentinel

Show Suggested Answer



Actual exam question from Microsoft's SC-100
Question #: 39
Topic #: 3
[All SC-100 Questions]

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux.

You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:

- Identify missing updates and insecure configurations.
- Use the Qualys engine.

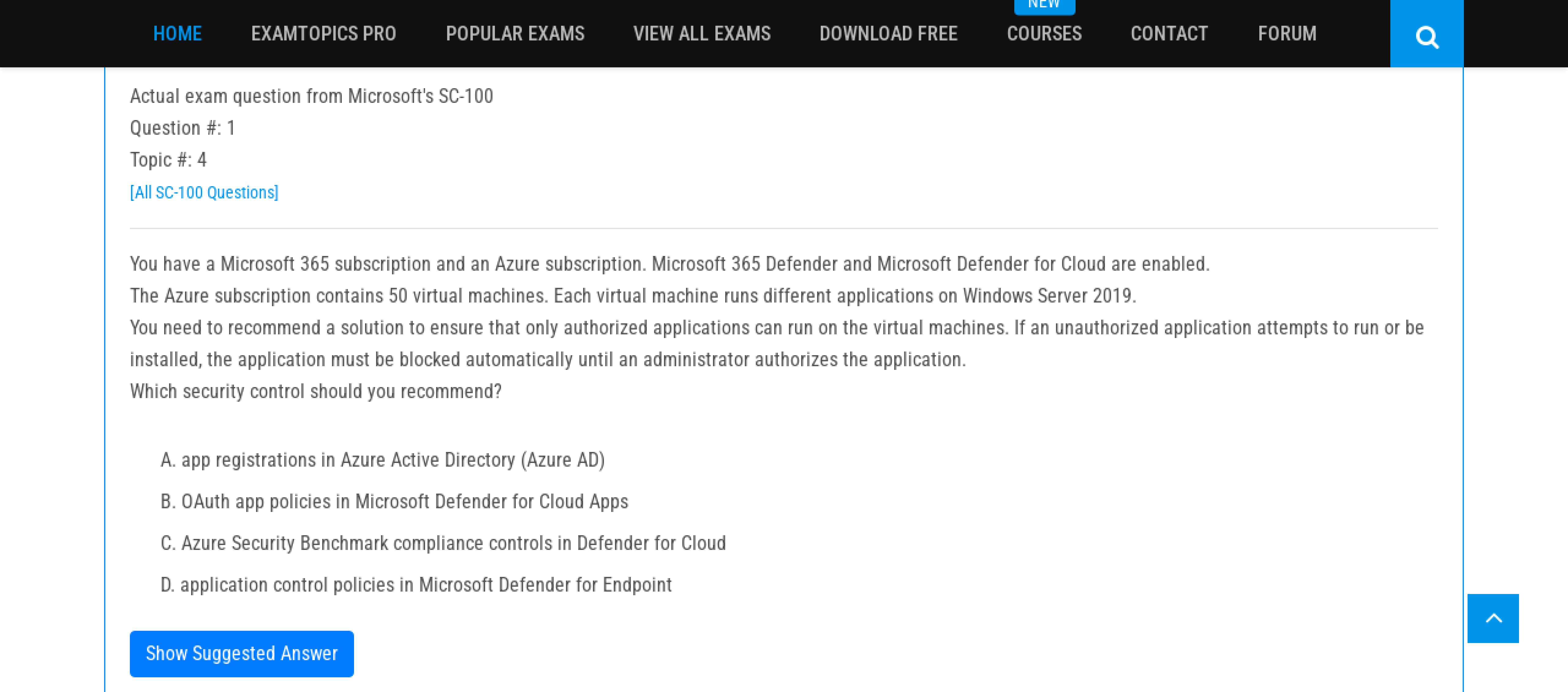
What should you use?

A. Microsoft Defender for Servers

B. Microsoft Defender Threat Intelligence (Defender TI)

C. Microsoft Defender for Endpoint

D. Microsoft Defender External Attack Surface Management (Defender EASM)



Actual exam question from Microsoft's SC-100

Question #: 1

Topic #: 4

[All SC-100 Questions]

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.

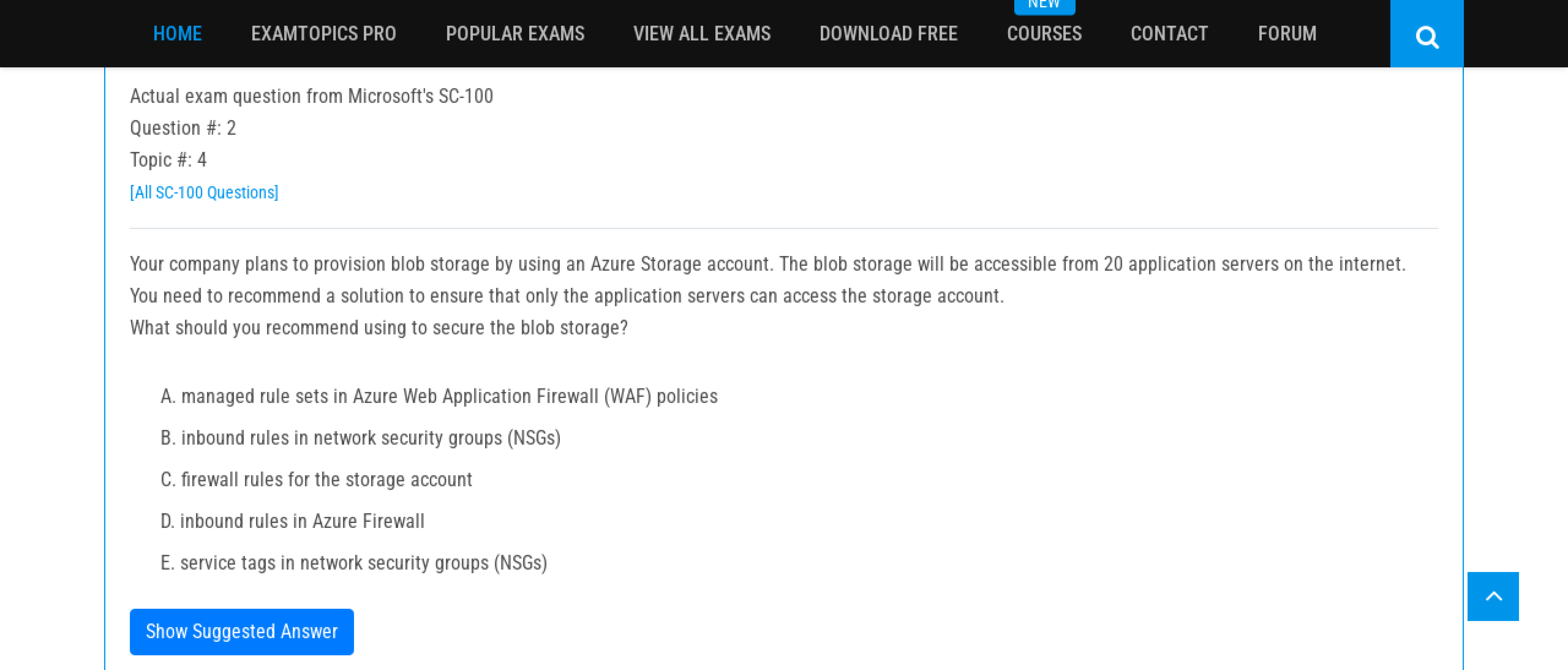
Which security control should you recommend?

A. app registrations in Azure Active Directory (Azure AD)

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. Azure Security Benchmark compliance controls in Defender for Cloud

D. application control policies in Microsoft Defender for Endpoint



Actual exam question from Microsoft's SC-100

Question #: 2

Topic #: 4

[All SC-100 Questions]

Your company plans to provision blob storage by using an Azure Storage account. The blob storage will be accessible from 20 application servers on the internet.

You need to recommend a solution to ensure that only the application servers can access the storage account.

What should you recommend using to secure the blob storage?

A. managed rule sets in Azure Web Application Firewall (WAF) policies

B. inbound rules in network security groups (NSGs)

C. firewall rules for the storage account

D. inbound rules in Azure Firewall

E. service tags in network security groups (NSGs)