Topic 1 - Question Set 1

Question #1 *Topic 1*

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

What should you include in the recommendation?

A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

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

Community vote distribution

C (100%)

Question #2 *Topic 1*

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

A. Azure Monitor webhooks

B. Azure Event Hubs

C. Azure Functions apps

D. Azure Logics Apps

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

Community vote distribution

D (100%)

Question #3 *Topic 1*

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

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

A. Azure Storage file shares

B. Azure Disk Storage

C. Azure Storage blob containers

D. Azure Data Lake Storage Gen2

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

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

Community vote distribution
CD (78%) AD (22%)

Question #4 *Topic 1*

HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To connect the Azure data sources to Microsoft Information Protection: [ ]
- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data: [ ]
- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

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

Correct Answer:

To triage security alerts related to resources that contain PII data: [ ]
- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Box 1: Azure Purview -

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

Microsoft Purview allows you to:

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

Enable data curators to manage and secure your data estate.

Empower data consumers to find valuable, trustworthy data.

Box 2: Microsoft Defender for Cloud

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

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

Question #5 *Topic 1*

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

A. notebooks

B. playbooks

C. workbooks

D. threat intelligence

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

Community vote distribution

C (100%)

Question #6 *Topic 1*

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

A. sensitivity labels

B. custom user tags

C. standalone sensors

D. honeytoken entity tags

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

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

Community vote distribution

D (100%)

Question #7 *Topic 1*

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

A. KQL

B. playbooks

C. data connectors

D. workbooks

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

Community vote distribution

B (89%) 11%

Question #8 *Topic 1*

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

A. Enable soft delete for backups.

B. Require PINs for critical operations.

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

D. Perform offline backups to Azure Data Box.

E. Use Azure Monitor notifications when backup configurations change.

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

Community vote distribution
AB (74%) 11% Other

Question #9 *Topic 1*

HOTSPOT -

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

- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

You need to recommend an access security architecture for App1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To enable Azure AD authentication for App1, use:	Azure AD application Azure AD Application Proxy Azure Application Gateway A managed identity in Azure AD Microsoft Defender for App
To implement access requests for App1, use:	An access package in Identity Governance An access policy in Microsoft Defender for Cloud Apps An access review in Identity Governance Azure AD Conditional Access App Control An OAuth app policy in Microsoft Defender for Cloud Apps

Correct Answer:

Answer Area

To enable Azure AD authentication for App1, use:	Azure AD application Azure AD Application Proxy Azure Application Gateway **A managed identity in Azure AD** Microsoft Defender for App
To implement access requests for App1, use:	An access package in Identity Governance An access policy in Microsoft Defender for Cloud Apps **An access review in Identity Governance** Azure AD Conditional Access App Control An OAuth app policy in Microsoft Defender for Cloud Apps

Box 1: A managed identity in Azure AD

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

Box 2: An access review in Identity Governance

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

Reference:

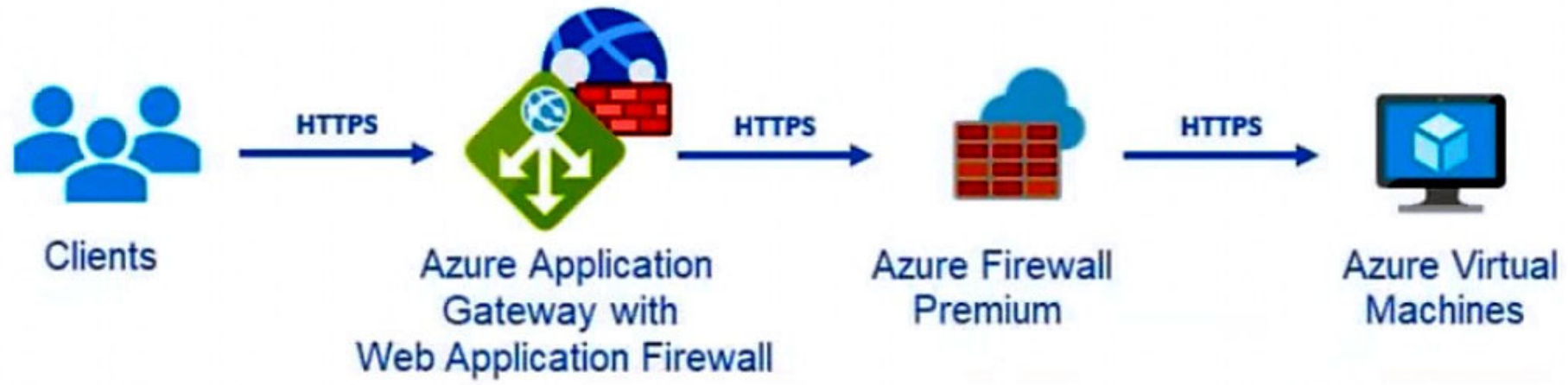
https://docs.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question #10 *Topic 1*

HOTSPOT -

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel.

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



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

- Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
- Use Defender for Cloud to review alerts from the virtual machines.

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

NOTE: Each correct selection is worth one point.

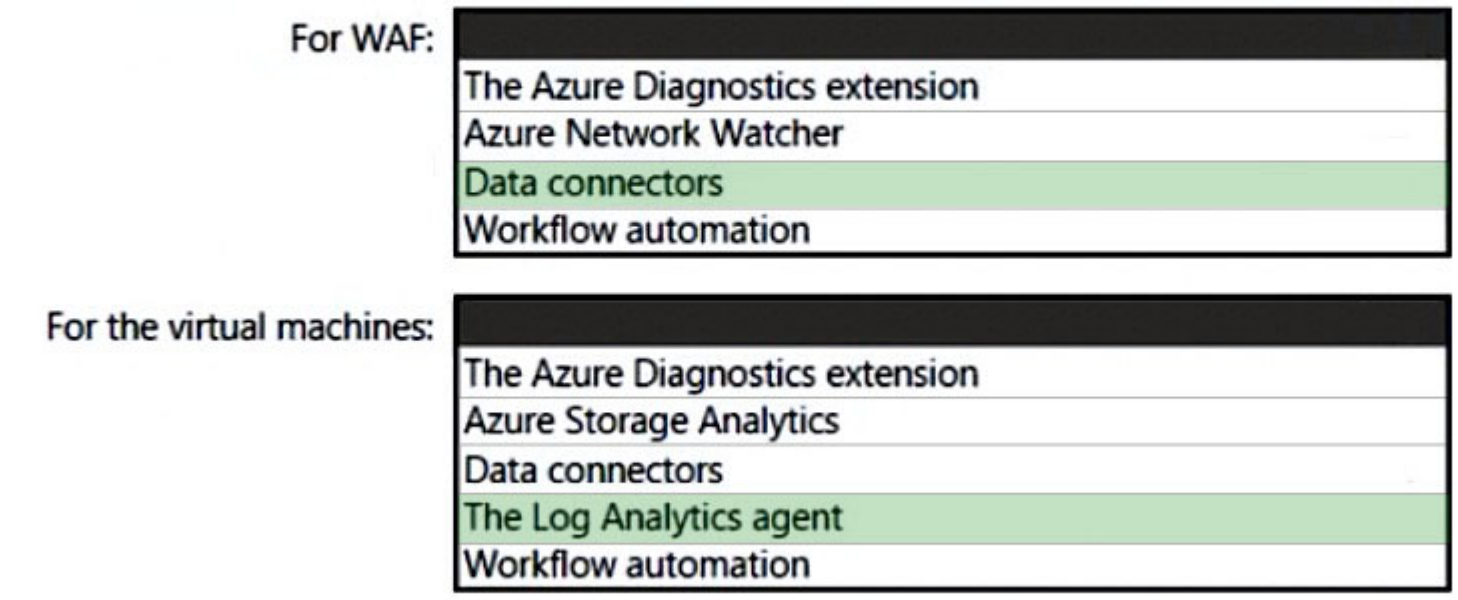
Hot Area:

Answer Area

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

Correct Answer:

Answer Area



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

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

Windows agents

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

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

Azure Log Analytics agent -
Use Defender for Cloud to review alerts from the virtual machines.
The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System
Center Operations Manager and sends collected data to your Log Analytics workspace in Azure Monitor.
Incorrect:
The Azure Diagnostics extension does not integrate with Microsoft Defender for Cloud.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

Question #11 *Topic 1*

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

A. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

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

Community vote distribution

B (88%) 12%

Question #12 *Topic 1*

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

A. The client access tokens are refreshed.

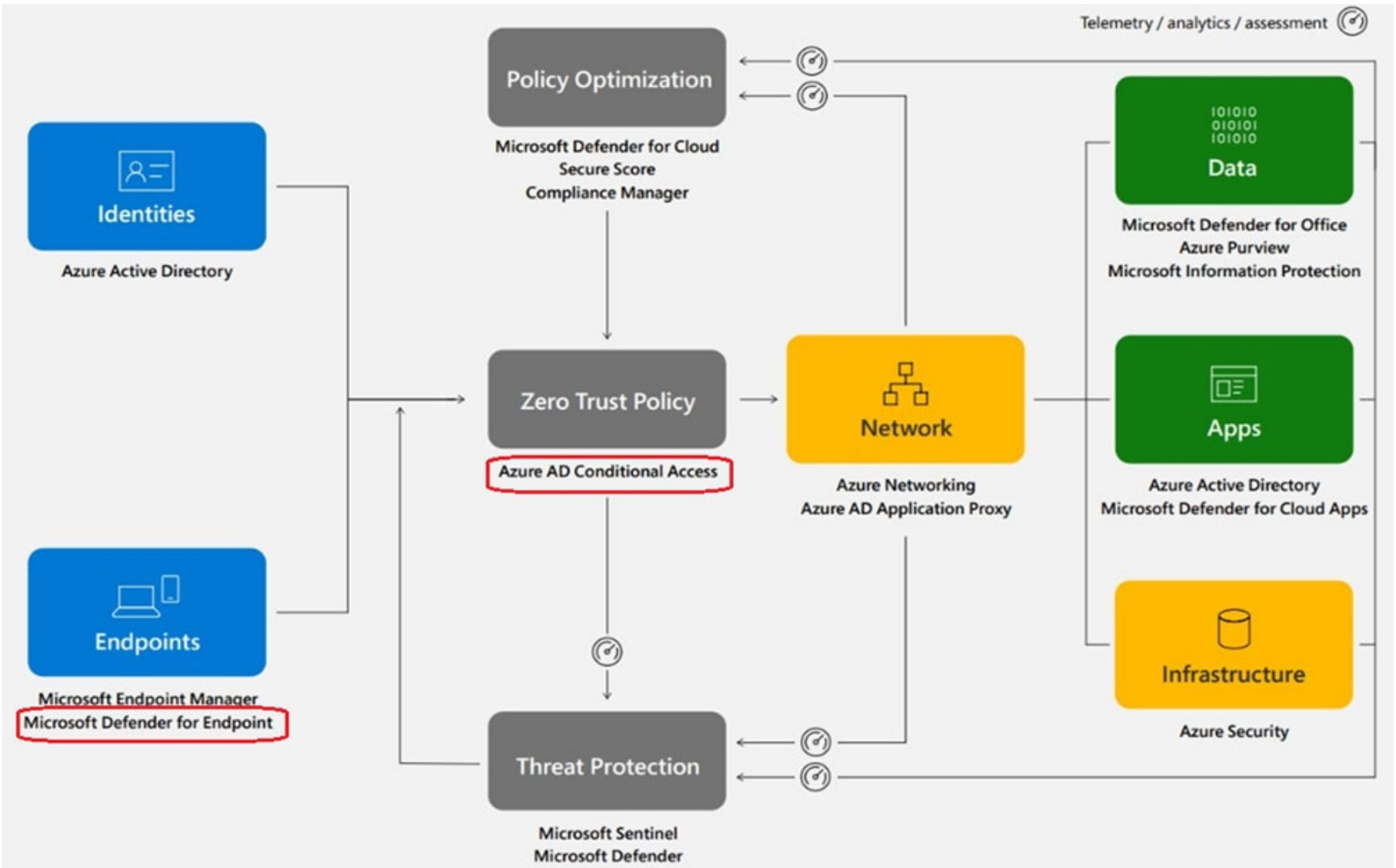
B. Microsoft Intune reports the endpoints as compliant.

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

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

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

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



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

and the core of your user-centric policies to guarantee least-privileged access. Azure AD's Conditional Access capabilities are the policy decision point for access to resource

Reference:

https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/

https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

Community vote distribution

AB (57%) BD (17%) AC (16%) 8%

Question #13 *Topic 1*

HOTSPOT -

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

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

Defender for Cloud, and Azure.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

EDR:	Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD). Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps. Onboard the servers to Azure Arc. Onboard the servers to Defender for Cloud.
SOAR:	Configure Microsoft Sentinel analytics rules. Configure Microsoft Sentinel playbooks. Configure regulatory compliance standards in Defender for Cloud. Configure workflow automation in Defender for Cloud.

Correct Answer:

Answer Area

EDR:	Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD). Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps. Onboard the servers to Azure Arc. Onboard the servers to Defender for Cloud.
SOAR:	Configure Microsoft Sentinel analytics rules. Configure Microsoft Sentinel playbooks. Configure regulatory compliance standards in Defender for Cloud. Configure workflow automation in Defender for Cloud.

Box 1: Onboard the servers to Defender for Cloud.

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

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

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

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

Question #14 *Topic 1*

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

A. Azure AD Privileged Identity Management (PIM)

B. role-based authorization

C. resource-based authorization

D. Azure AD Multi-Factor Authentication

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

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

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

Community vote distribution
A (93%) 7%

Question #15 *Topic 1*

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

A. Microsoft Security Development Lifecycle (SDL)

B. Enhanced Security Admin Environment (ESAE)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)

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

Identities -
Endpoints (devices)

Apps -

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

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

Community vote distribution

C (84%) B (16%)

Question #16 *Topic 1*

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

A. a custom collector that uses the Log Analytics agent

B. the Azure Monitor agent

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

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

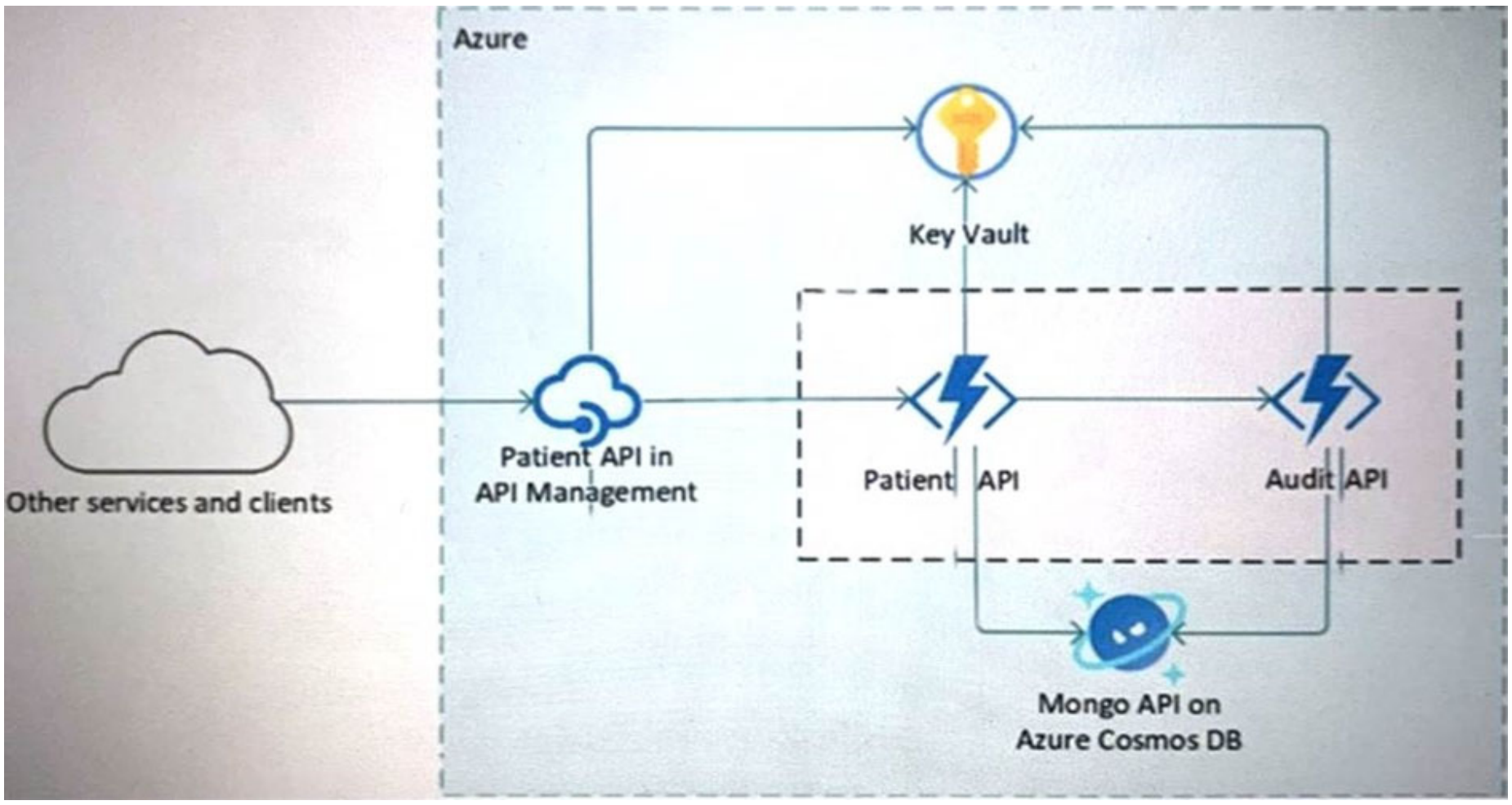
Correct Answer: *BC*
A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.
Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into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

Community vote distribution

BC (77%) AC (23%)

Question #17 *Topic 1*

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

Correct Answer: *B*

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

Windows web apps -

Linux web apps -

Docker containers -

Mobile apps -

Functions -

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

Very high scale.

Isolation and secure network access.

High memory utilization.

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

Reference:

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

Community vote distribution

B (92%) 8%

Question #18 *Topic 1*

HOTSPOT
-

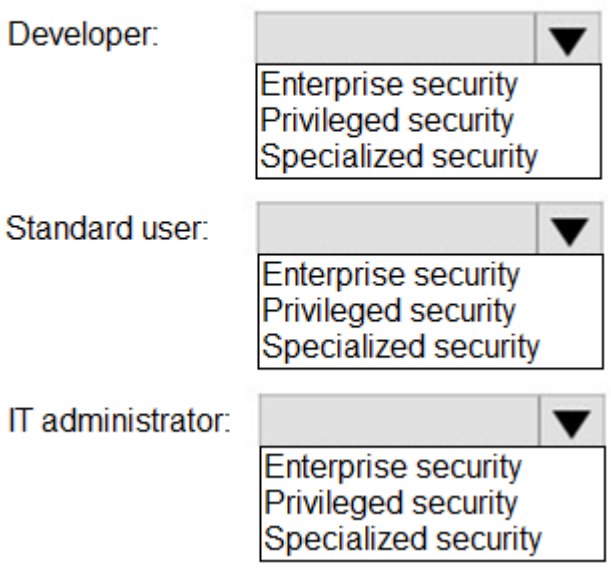
You are planning the security levels for a security access strategy.

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

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

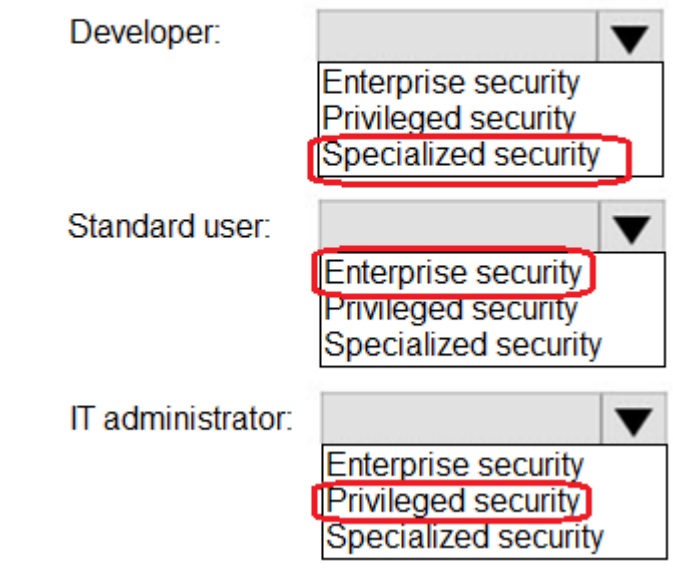
NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Correct Answer:



Question #19 *Topic 1*

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

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

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

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Correct Answer: *ACE*

Community vote distribution

ACE (85%) BCE (15%)

Question #20 *Topic 1*

HOTSPOT

-

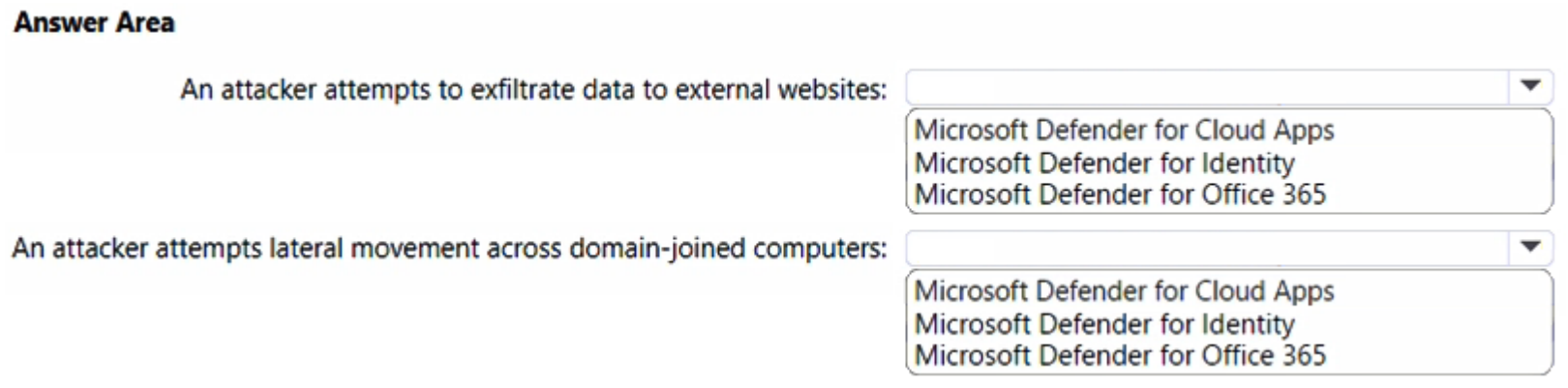
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA).

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

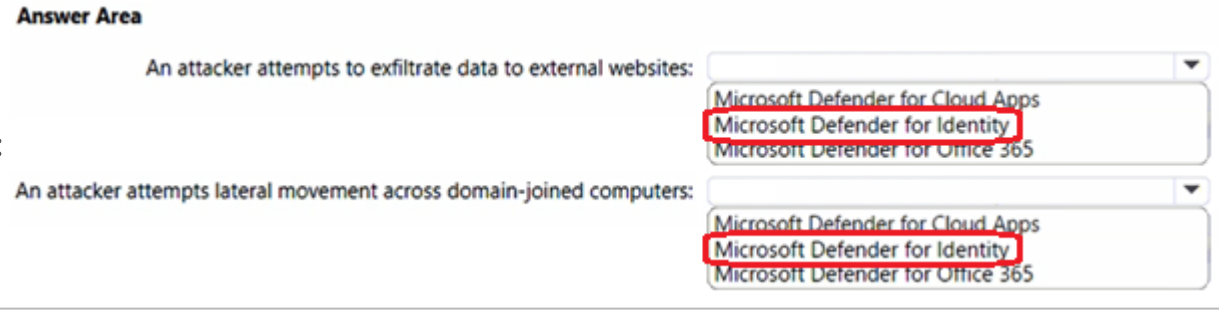
• An attacker attempts to exfiltrate data to external websites.
• An attacker attempts lateral movement across domain-joined computers.

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

NOTE: Each correct selection is worth one point.



Correct Answer:



Question #21 *Topic 1*

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

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

What should you include in the recommendation?

A. application registrations in Azure AD

B. managed identities in Azure

C. Azure service principals with usernames and passwords

D. device registrations in Azure AD

E. Azure service principals with certificate credentials

Correct Answer: *B*

Community vote distribution

B (69%) A (26%) 5%

Question #22 *Topic 1*

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

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

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

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

What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

Correct Answer: *A*

Community vote distribution

A (100%)

Question #23 *Topic 1*

29 DRAG DROP

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

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

NOTE: Each correct selection is worth one point.

Methodology

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

Answer Area

Assume breach	
Verify explicitly	
Use least privilege access	

Correct Answer:

Answer Area

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

Question #24 *Topic 1*

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

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

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

NOTE: Each correct selection is worth one point.

A. active scanning

B. threat monitoring

C. software patching

D. passive traffic monitoring

Correct Answer: *BC*

Community vote distribution

BD (78%) BC (22%)

Question #25 *Topic 1*

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

You are designing a Zero Trust security strategy.

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

NOTE: Each correct answer is worth one point.

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

B. Disable passwordless sign-in for sensitive accounts.

C. Block sign-in attempts from unknown locations.

D. Block sign-in attempts from noncompliant devices.

Correct Answer: *CD*

Community vote distribution

CD (86%) 14%

Question #26 *Topic 1*

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

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

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

Correct Answer: *B*

Community vote distribution

E (100%)

Question #27 *Topic 1*

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

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

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

What should you recommend?

A. a managed identity in Azure

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

C. a group managed service account (gMSA)

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

Correct Answer: *D*

Community vote distribution

A (82%) D (18%)

Question #28 *Topic 1*

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

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

What should you recommend?

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

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

C. The AKS cluster version must be upgraded.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #29 *Topic 1*

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

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

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

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

What should you include in the recommendation?

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

B. Configure the VPN to use Azure AD authentication.

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

D. Configure web protection in Microsoft Defender for Endpoint.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #30 *Topic 1*

HOTSPOT
-

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use: [▼]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use: [▼]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

Correct Answer:

Answer Area

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use: [Data loss prevention (DLP) policies ▼]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use: [Versioning ▼]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

Question #31 *Topic 1*

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

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

What should you do?

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

B. Enable self-healing in Microsoft 365 Defender.

C. Automate data classification.

D. Create hunting queries in Microsoft 365 Defender.

Correct Answer: *A*

Community vote distribution

B (100%)

Question #32 *Topic 1*

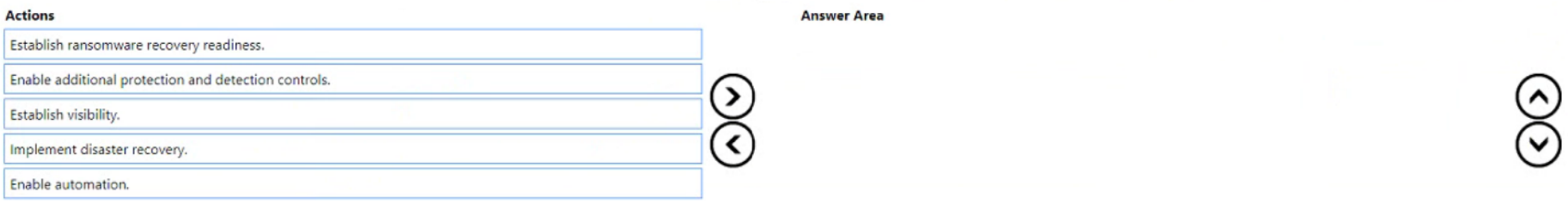
DRAG DROP

-

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

You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).

Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.



Correct Answer:

Answer Area
Establish visibility.
Enable automation.
Enable additional protection and detection controls.

Topic 2 - Question Set 2

Question #1 *Topic 2*

You are evaluating an Azure environment for compliance.
You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.
Which effect should you use in Azure Policy?

A. Deny

B. Modify

C. Append

D. Disabled

Correct Answer: *D*
This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disable a single assignment instead of disabling all of that policy's assignments.
An alternative to the Disabled effect is enforcementMode, which is set on the policy assignment. When enforcementMode is Disabled, resources are still evaluated.
Incorrect:
Not A: Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
Not B: Modify evaluates before the request gets processed by a Resource Provider during the creation or updating of a resource. The Modify operations are applied to the request content when the if condition of the policy rule is met. Each Modify operation can specify a condition that determines when it's applied.
Operations with conditions that are evaluated to false are skipped.
Not C: Append is used to add additional fields to the requested resource during creation or update.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

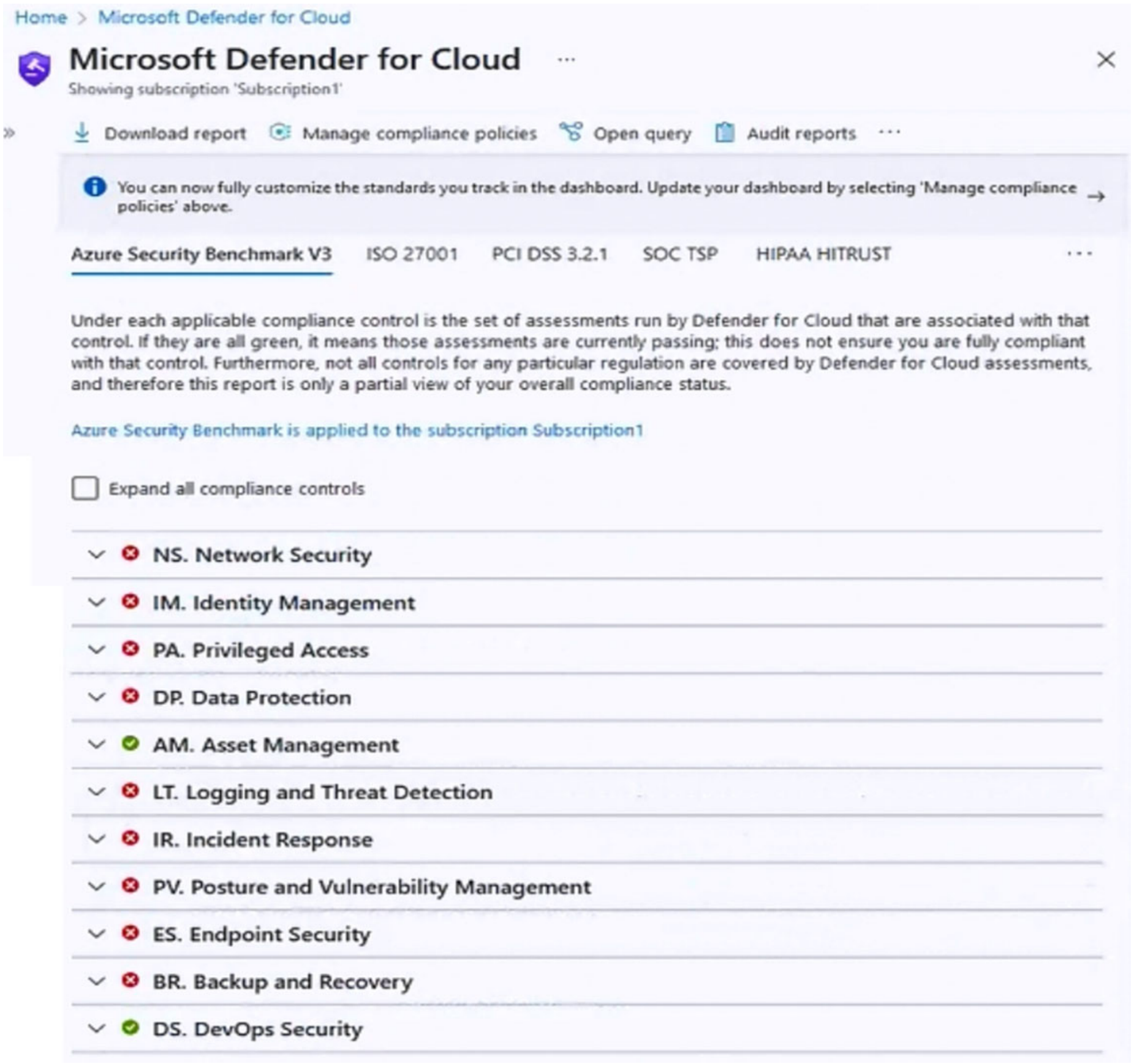
Community vote distribution

D (82%) A (18%)

Question #2 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.



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

Correct Answer: *D*

Microsoft Defender for servers compliance control installed on Windows

Defender for clout "Endpoint Security" azure security benchmark v3

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.

Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.

Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.

Incorrect:

Not A: Asset Management covers controls to ensure security visibility and governance over Azure resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for services and resources (inventory, track, and correct).

Not B: Posture and Vulnerability Management focuses on controls for assessing and improving Azure security posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting, and correction in Azure resources.

Not C: Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key and certificate management in Azure.

Not E: Incident Response covers controls in incident response life cycle - preparation, detection and analysis, containment, and post-incident activities, including using Azure services such as Microsoft Defender for Cloud and Sentinel to automate the incident response process.

Reference:

https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

Community vote distribution

D (100%)

Question #3 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to evaluate the existing environment to increase the overall security posture for the following components:

- Windows 11 devices managed by Microsoft Intune
- Azure Storage accounts
- Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Windows 11 devices:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure virtual machines:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure Storage accounts:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

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

Correct Answer:

Box 1: Microsoft 365 Defender -

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes

Microsoft Defender for Endpoint.
Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.
Microsoft Defender for Endpoint works with devices that run:

Android -
iOS/iPadOS

Windows 10 -

Windows 11 -
Box 2: Microsoft Defender for Cloud
Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed Instance and Azure Virtual Machines.
Box 3: Microsoft 365 Compliance Center
Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.
Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.
Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender
?
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

Question #4 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

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

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: *A*
The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in NIST SP 800-53 Rev. 5.
The following mappings are to the NIST SP 800-53 Rev. 5 controls. Use the navigation on the right to jump directly to a specific compliance domain. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open Policy in the Azure portal and select the
Definitions page. Then, find and select the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

Community vote distribution
A (100%)

Question #5 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have an Amazon Web Services (AWS) implementation.
You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc.
Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Containers

B. Microsoft Defender for servers

C. Azure Active Directory (Azure AD) Conditional Access

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

E. Azure Policy

Correct Answer: *ACE*
Environment settings page (in preview) (recommended) - This preview page provides a greatly improved, simpler, onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud's enhanced security features to your AWS resources:
*(A) Microsoft Defender for Containers brings threat detection and advanced defenses to your Amazon EKS clusters. This plan includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control recommendations and more.
* Microsoft Defender for Servers, though it requires Arc.
C: AWS installations can benefit from Conditional Access. Defender for Cloud Apps integrates with Azure AD Conditional Access to enforce additional restrictions, and monitors and protects sessions after sign-in. Defender for Cloud Apps uses user behavior analytics (UBA) and other AWS APIs to monitor sessions and users and to support information protection.
E: Kubernetes data plane hardening.
For a bundle of recommendations to protect the workloads of your Kubernetes containers, install the Azure Policy for Kubernetes. You can also auto deploy this component as explained in enable auto provisioning of agents and extensions.
With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure to enforce the best practices and mandate them for future workloads.
Incorrect:
Not B: To enable the Defender for Servers plan you need Azure Arc for servers installed on your EC2 instances.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-security-solutions

Community vote distribution
ACE (48%) ACD (40%) 8%

Question #6 *Topic 2*

Your company has on-premises network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency for developers.
Which three actions should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.

B. Deploy a Remote Desktop server to an Azure region located in France.

C. Migrate from the Remote Desktop server to Azure Virtual Desktop.

D. Implement Azure Firewall to restrict host pool outbound access.

E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

Correct Answer: *CDE*
E: Organizations can use this location for common tasks like:
Requiring multi-factor authentication for users accessing a service when they're off the corporate network.
Blocking access for users accessing a service from specific countries or regions.
The location is determined by the public IP address a client provides to Azure Active Directory or GPS coordinates provided by the Microsoft Authenticator app.
Conditional Access policies by default apply to all IPv4 and IPv6 addresses.
CD: Use Azure Firewall to protect Azure Virtual Desktop deployments.
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
Reference:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

Community vote distribution

CDE (86%) 10%

Question #7 *Topic 2*

HOTSPOT -

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation.

You need to recommend a security posture management solution for the following components:

☞ Azure IoT Edge devices

AWS EC2 instances -

▪

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

For the IoT Edge devices:
- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:
- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

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

Correct Answer:

For the AWS EC2 instances:
- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Box 1: Microsoft Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Azure IoT Edge provides powerful capabilities to manage and perform business workflows at the edge. The key part that IoT Edge plays in IoT environments make it particularly attractive for malicious actors.

Defender for IoT azureiotsecurity provides a comprehensive security solution for your IoT Edge devices. Defender for IoT module collects, aggregates and analyzes raw security data from your Operating System and container system into actionable security recommendations and

alerts.

Box 2: Microsoft Defender for Cloud and Azure Arc

Microsoft Defender for Cloud provides the following features in the CSPM (Cloud Security Posture Management) category in the multi-cloud scenario for AWS.

Take into account that some of them require Defender plan to be enabled (such as Regulatory Compliance):

* Detection of security misconfigurations
* Single view showing Security Center recommendations and AWS Security Hub findings
* Incorporation of AWS resources into Security Center's secure score calculations
* Regulatory compliance assessments of AWS resources

Security Center uses Azure Arc to deploy the Log Analytics agent to AWS instances.

Incorrect:

AWS EC2 Microsoft Defender for Cloud Apps

Amazon Web Services is an IaaS provider that enables your organization to host and manage their entire workloads in the cloud. Along with the benefits of leveraging infrastructure in the cloud, your organization's most critical assets may be exposed to threats. Exposed assets include storage instances with potentially sensitive information, compute resources that operate some of your most critical applications, ports, and virtual private networks that enable access to your organization.

Connecting AWS to Defender for Cloud Apps helps you secure your assets and detect potential threats by monitoring administrative and sign-in activities, notifying on possible brute force attacks, malicious use of a privileged user account, unusual deletions of VMs, and publicly exposed storage buckets.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/security-edge-architecture

https://samilamppu.com/2021/11/04/multi-cloud-security-posture-management-in-microsoft-defender-for-cloud/

Question #8 *Topic 2*

Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company's on-premises network.
The company's secutity policy prevents the use of personal devices for accessing company data and applications.
You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.
What should you include in the recommendation?

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

B. Redesign the VPN infrastructure by adopting a split tunnel configuration.

C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.

D. Migrate the on-premises applications to cloud-based applications.

Correct Answer: *A*
You can connect an Azure Virtual Desktop to an on-premises network using a virtual private network (VPN), or use Azure ExpressRoute to extend the on- premises network into the Azure cloud over a private connection.
* Azure AD: Azure Virtual Desktop uses Azure AD for identity and access management. Azure AD integration applies Azure AD security features like conditional access, multi-factor authentication, and the Intelligent Security Graph, and helps maintain app compatibility in domain-joined VMs.
* Azure Virtual Desktop, enable Microsoft Defender for Cloud.
We recommend enabling Microsoft Defender for Cloud's enhanced security features to:
Manage vulnerabilities.
Assess compliance with common frameworks like PCI.
* Microsoft Defender for Cloud Apps, formerly known as Microsoft Cloud App Security, is a comprehensive solution for security and compliance teams enabling users in the organization, local and remote, to safely adopt business applications without compromising productivity.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cloud-apps/ba-p/2835842

Community vote distribution

A (100%)

Question #9 *Topic 2*

Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Web Application Firewall (WAF)

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

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

Correct Answer: *BC*
B: Azure identity and access for landing zones, Privileged Identity Management (PIM)
Use Azure AD Privileged Identity Management (PIM) to establish zero-trust and least privilege access. Map your organization's roles to the minimum access levels needed. Azure AD PIM can use Azure native tools, extend current tools and processes, or use both current and native tools as needed.
Azure identity and access for landing zones, Design recommendations include:
* (B) Use Azure AD managed identities for Azure resources to avoid credential-based authentication. Many security breaches of public cloud resources originate with credential theft embedded in code or other text. Enforcing managed identities for programmatic access greatly reduces the risk of credential theft.
* Etc.
C: Improve landing zone security, onboard Microsoft Sentinel
You can enable Microsoft Sentinel, and then set up data connectors to monitor and protect your environment. After you connect your data sources using data connectors, you choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.
Note: Landing zone security best practices
The following list of reference architectures and best practices provides examples of ways to improve landing zone security:
Microsoft Defender for Cloud: Onboard a subscription to Defender for Cloud.
Microsoft Sentinel: Onboard to Microsoft Sentinel to provide a security information event management (SIEM) and security orchestration automated response
(SOAR) solution.
Secure network architecture: Reference architecture for implementing a perimeter network and secure network architecture.
Identity management and access control: Series of best practices for implementing identity and access to secure a landing zone in Azure.
Network security practices: Provides additional best practices for securing the network.
Operational security provides best practices for increasing operational security in Azure.
The Security Baseline discipline: Example of developing a governance-driven security baseline to enforce security requirements.
Incorrect:
Not E: Implementing alerts is not a preventive measure.
Reference:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones
https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

Community vote distribution

AD (81%) Other

Question #10 *Topic 2*

You are designing security for an Azure landing zone.

Your company identifies the following compliance and privacy requirements:

- Encrypt cardholder data by using encryption keys managed by the company.
- Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed keys.

B. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.

C. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM.

D. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.

Correct Answer: *CD*

C: Azure Key Vault Managed HSM (Hardware Security Module) is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguard cryptographic keys for your cloud applications, using FIPS 140-2 Level 3 validated HSMs.

D: You can generate HSM-protected keys in your on-premise HSM and import them securely into Managed HSM.

Incorrect:

Not A: The company must manage the keys, not Microsoft.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

Community vote distribution

BC (67%) CD (32%)

Question #11 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You need to enforce ISO 27001:2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically.
What should you use?

A. Azure Policy

B. Azure Blueprints

C. the regulatory compliance dashboard in Defender for Cloud

D. Azure role-based access control (Azure RBAC)

Correct Answer: *A*
Control mapping of the ISO 27001 Shared Services blueprint sample
The following mappings are to the ISO 27001:2013 controls. Use the navigation on the right to jump directly to a specific control mapping.
Many of the mapped controls are implemented with an Azure Policy initiative.
Open Policy in the Azure portal and select the Definitions page. Then, find and select the [Preview] Audit ISO 27001:2013 controls and deploy specific VM
Extensions to support audit requirements built-in policy initiative.
Note: Security Center can now auto provision the Azure Policy's Guest Configuration extension (in preview)
Azure Policy can audit settings inside a machine, both for machines running in Azure and Arc connected machines. The validation is performed by the Guest
Configuration extension and client.
With this update, you can now set Security Center to automatically provision this extension to all supported machines.
Enforcing a secure configuration, based on a specific recommendation, is offered in two modes:
Using the Deny effect of Azure Policy, you can stop unhealthy resources from being created
Using the Enforce option, you can take advantage of Azure Policy's DeployIfNotExist effect and automatically remediate non-compliant resources upon creation
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive https://docs.microsoft.com/en-us/azure/defender-for-cloud/prevent-misconfigurations

Community vote distribution

A (90%) 10%

Question #12 *Topic 2*

DRAG DROP -

You have a Microsoft 365 subscription.

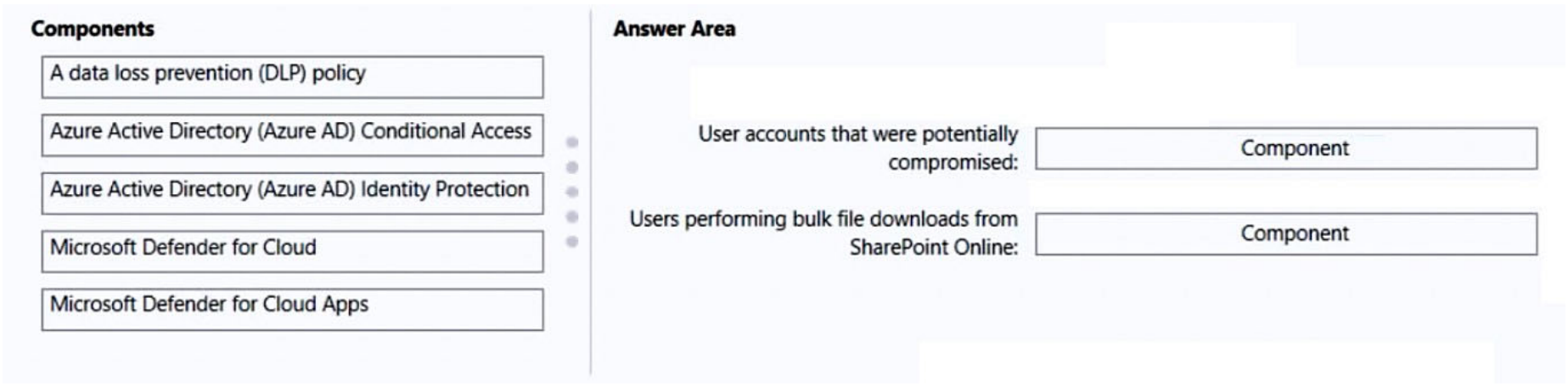
You need to recommend a security solution to monitor the following activities:

- User accounts that were potentially compromised
- Users performing bulk file downloads from Microsoft SharePoint Online

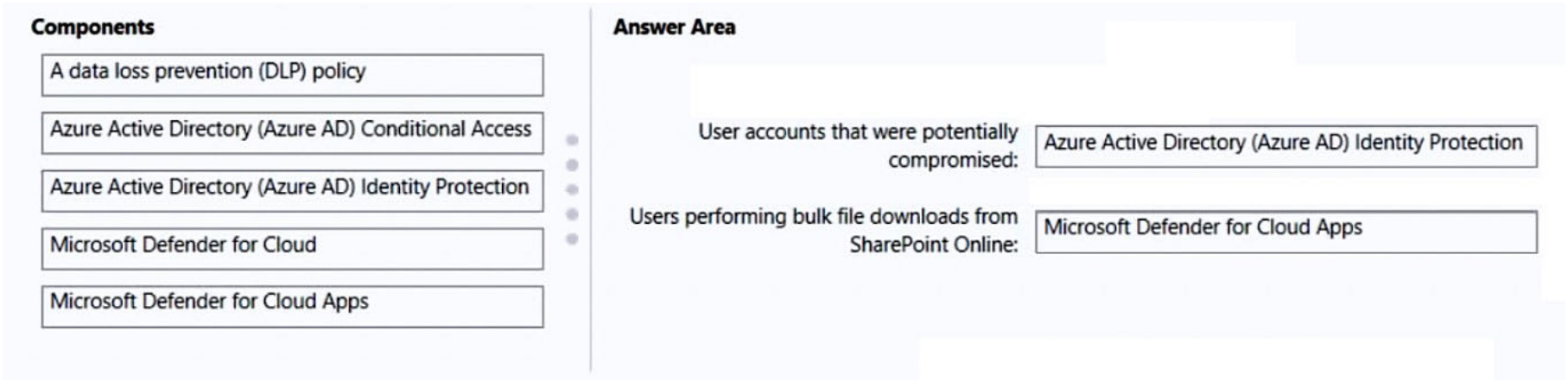
What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

Premium sign-in risk detections include:

* Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.
* Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This detection may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.
* Etc.

Incorrect:

Not: Microsoft 365 Defender for Cloud

Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365

Defender portal from Incidents & alerts > incident > Users.

Box 2: Microsoft 365 Defender for App

Defender for Cloud apps detect mass download (data exfiltration) policy

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

Question #13 *Topic 2*

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

- Access to storage accounts with firewall and virtual network configurations should be restricted.
- Storage accounts should restrict network access using virtual network rules.
- Storage account should use a private link connection.
- Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations.

What should you recommend?

A. Azure Policy

B. Azure Network Watcher

C. Azure Storage Analytics

D. Microsoft Sentinel

Correct Answer: *A*

An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled. Built in definitions include things like controlling what type of resources can be deployed or enforcing the use of tags on all resources. You can also create your own custom policy definitions.

Note: Azure security baseline for Azure Storage

This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Azure Storage. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Azure Security

Benchmark and the related guidance applicable to Azure Storage.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory

Compliance section of the Microsoft Defender for Cloud dashboard.

For example:

* 1.1: Protect Azure resources within virtual networks

Guidance: Configure your storage account's firewall by restricting access to clients from specific public IP address ranges, select virtual networks, or specific

Azure resources. You can also configure Private Endpoints so traffic to the storage service from your enterprise travels exclusively over private networks.

* 1.8: Minimize complexity and administrative overhead of network security rules

Guidance: For resource in Virtual Networks that need access to your Storage account, use Virtual Network Service tags for the configured Virtual Network to define network access controls on network security groups or Azure Firewall. You can use service tags in place of specific IP addresses when creating security rules.

Reference:

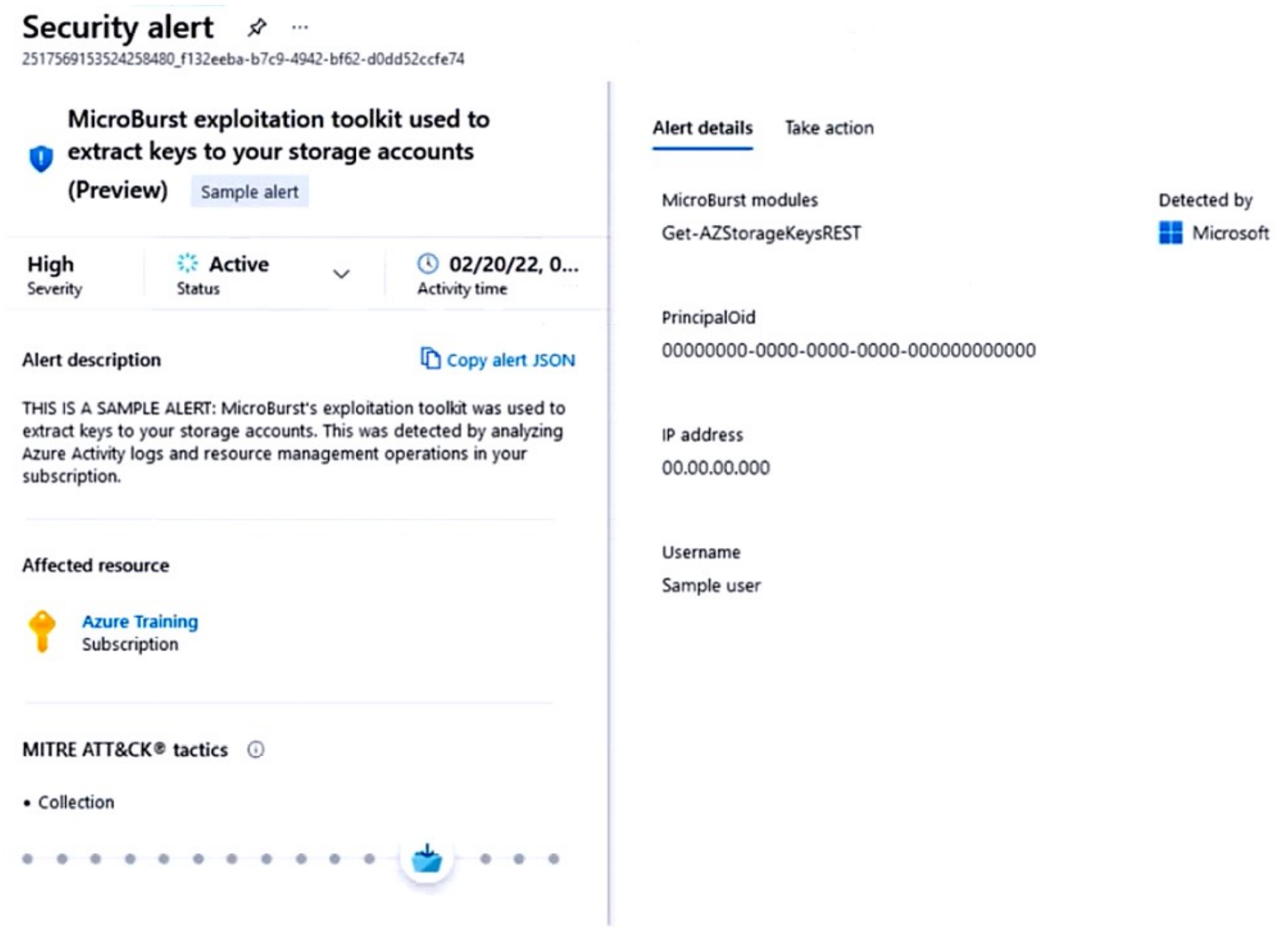
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

Community vote distribution

A (100%)

Question #14 *Topic 2*

You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



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

Correct Answer: *A*

Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but may also present a security risk. It's important to manage anonymous access judiciously and to understand how to evaluate anonymous access to your data. Operational complexity, human error, or malicious attack against data that is publicly accessible can result in costly data breaches. Microsoft recommends that you enable anonymous access only when necessary for your application scenario.

Note: Attackers have been crawling for public containers using tools such as MicroBurst.

Exploiting Anonymous Blob Access

Now, there are thousands of articles explaining how this can be abused and how to search for insecure storage in Azure. One of the easiest way is to use

MicroBurst, provide the storage account name to search for, and it'll check if the containers exists based on a wordlist saved in the Misc/permutations.txt

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent https://hackingthe.cloud/azure/anonymous-blob-access/

Community vote distribution

C (79%) A (21%)

Question #15 *Topic 2*

You have 50 Azure subscriptions.
You need to monitor the resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
What are two ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.

B. Assign a policy to each subscription.

C. Assign a policy to a management group.

D. Assign an initiative to each subscription.

E. Assign a blueprint to each subscription.

F. Assign a blueprint to a management group.

Correct Answer: *AF*
An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions en masse.
If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions.
Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.
F: Blueprint definition locations
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have
Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.
A: Create and assign an initiative definition
With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.
Note: The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in ISO 27001:2013.
The Azure Policy control mapping provides details on policy definitions included within this blueprint and how these policy definitions map to the compliance domains and controls in ISO 27001. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions.
Incorrect:
Not B, D, E: If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

Community vote distribution

AF (80%) AC (17%)

Question #16 *Topic 2*

HOTSPOT -

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

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

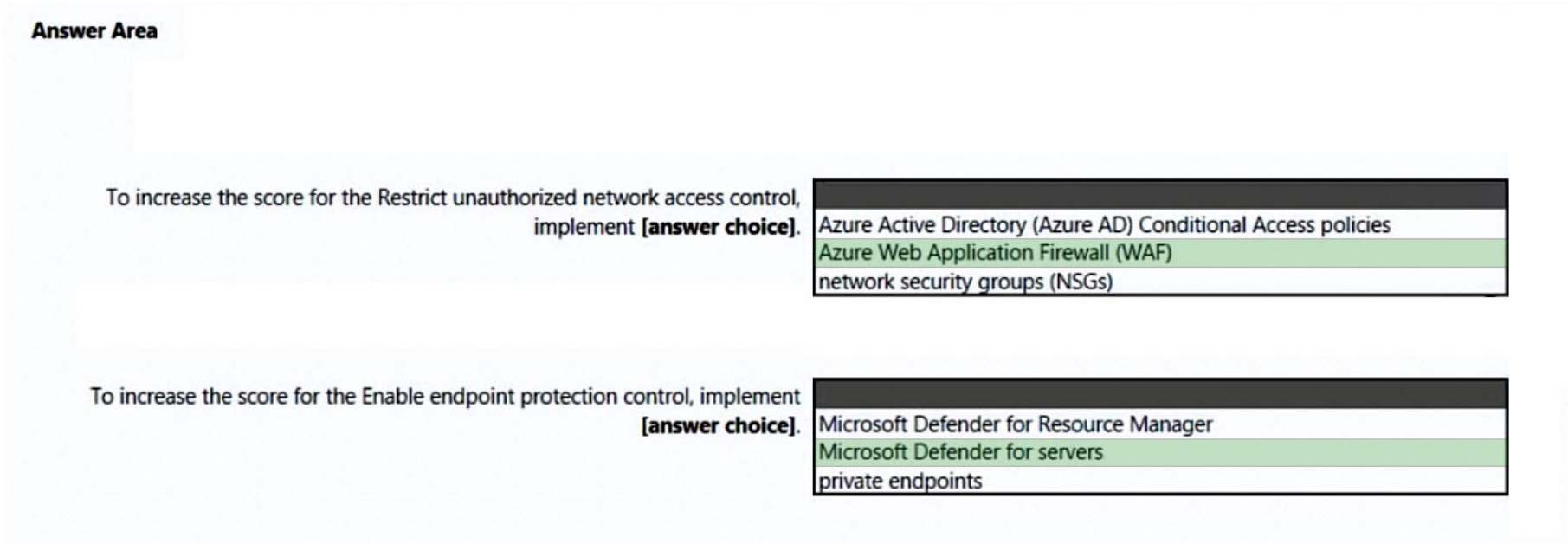
To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

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

Correct Answer:



Box 1: Azure Web Application Firewall (WAF)

Restrict unauthorized network access control: 1 resource out of 11 needs to be addresses.

Restrict unauthorized network access - Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.

Use these recommendations to manage Defender for Cloud's adaptive network hardening settings, ensure you've configured Azure Private Link for all relevant

PaaS services, enable Azure Firewall on your virtual networks, and more.

Note: Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway.

Azure WAF protects inbound traffic to the web workloads, and the Azure Firewall inspects inbound traffic for the other applications. The Azure Firewall will cover outbound flows from both workload types.

Incorrect:

Not network security groups (NSGs).

Box 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft

Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Question #17 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling the VMAccess extension on all virtual machines.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Note:
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution

B (100%)

Question #18 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling adaptive network hardening.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Note:
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution

B (77%) A (23%)

Question #19 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Does this meet the goal?

A. Yes

B. No

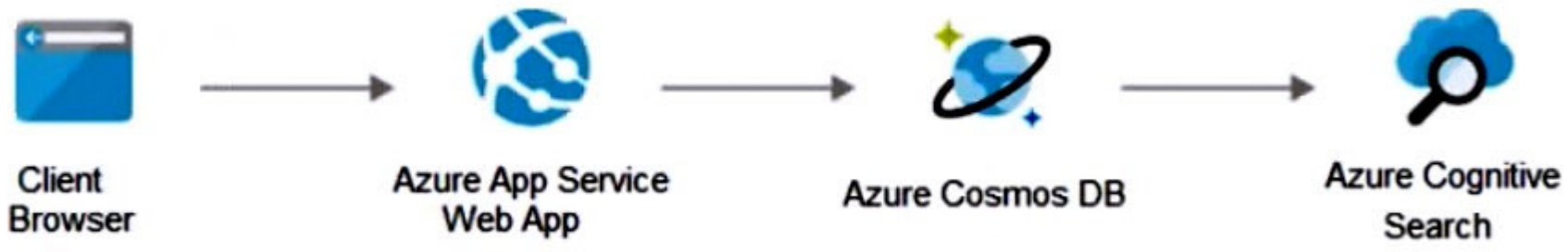
Correct Answer: *A*
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution

A (100%)

Question #20 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend creating private endpoints for the web app and the database layer.
Does this meet the goal?

A. Yes

B. No

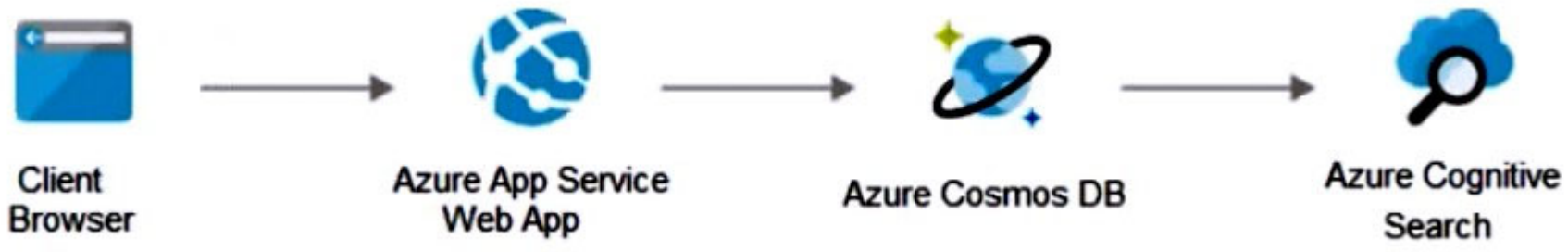
Correct Answer: *A*
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

A (89%) 11%

Question #21 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Key Vault to store credentials.
Does this meet the goal?

A. Yes

B. No

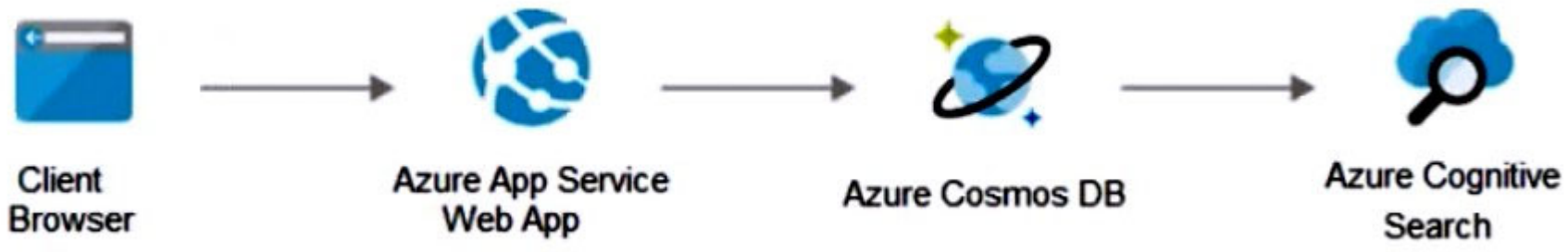
Correct Answer: *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

B (52%) A (48%)

Question #22 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

B (75%) A (25%)

Question #23 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

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

D. Azure Security Benchmark compliance controls in Defender for Cloud

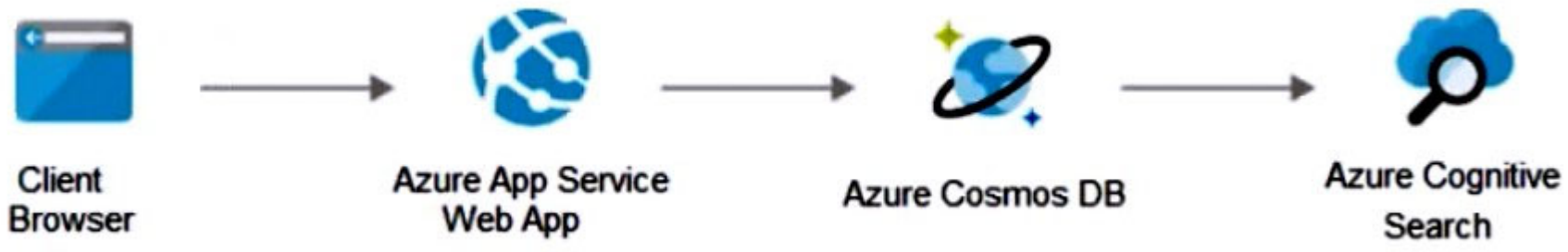
Correct Answer: *A*
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
Incorrect:
Not B: App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.
Not C: Cloud Discovery anomaly detection policy reference. A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are considered for each cloud application.
Not D: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy https://docs.microsoft.com/en-us/security/benchmark/azure/overview

Community vote distribution

A (96%) 4%

Question #24 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

Community vote distribution

B (91%) 9%

Question #25 *Topic 2*

You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules.
What should you include in the solution?

A. Microsoft Defender for Endpoint

B. Microsoft Endpoint Manager

C. Microsoft Information Protection

D. Microsoft Sentinel

Correct Answer: *B*
Microsoft Endpoint Manager includes Microsoft Intune.
Device compliance policies are a key feature when using Intune to protect your organization's resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version.
Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint
Manager includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.
Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co- management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk.
Note: Microsoft Defender for Endpoint Plan 2 protects your Windows and Linux machines whether they're hosted in Azure, hybrid clouds (on-premises), or multicloud.
Microsoft Defender for Endpoint on iOS offers protection against phishing and unsafe network connections from websites, emails, and apps.
Microsoft Defender for Endpoint on Android supports installation on both modes of enrolled devices - the legacy Device Administrator and Android Enterprise modes. Currently, Personally-owned devices with work profile and Corporate-owned fully managed user device enrollments are supported in Android Enterprise.
Reference:
https://docs.microsoft.com/en-us/mem/endpoint-manager-overview https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint

Community vote distribution

B (100%)

Question #26 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Note: Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in- time VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Community vote distribution

B (100%)

Question #27 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

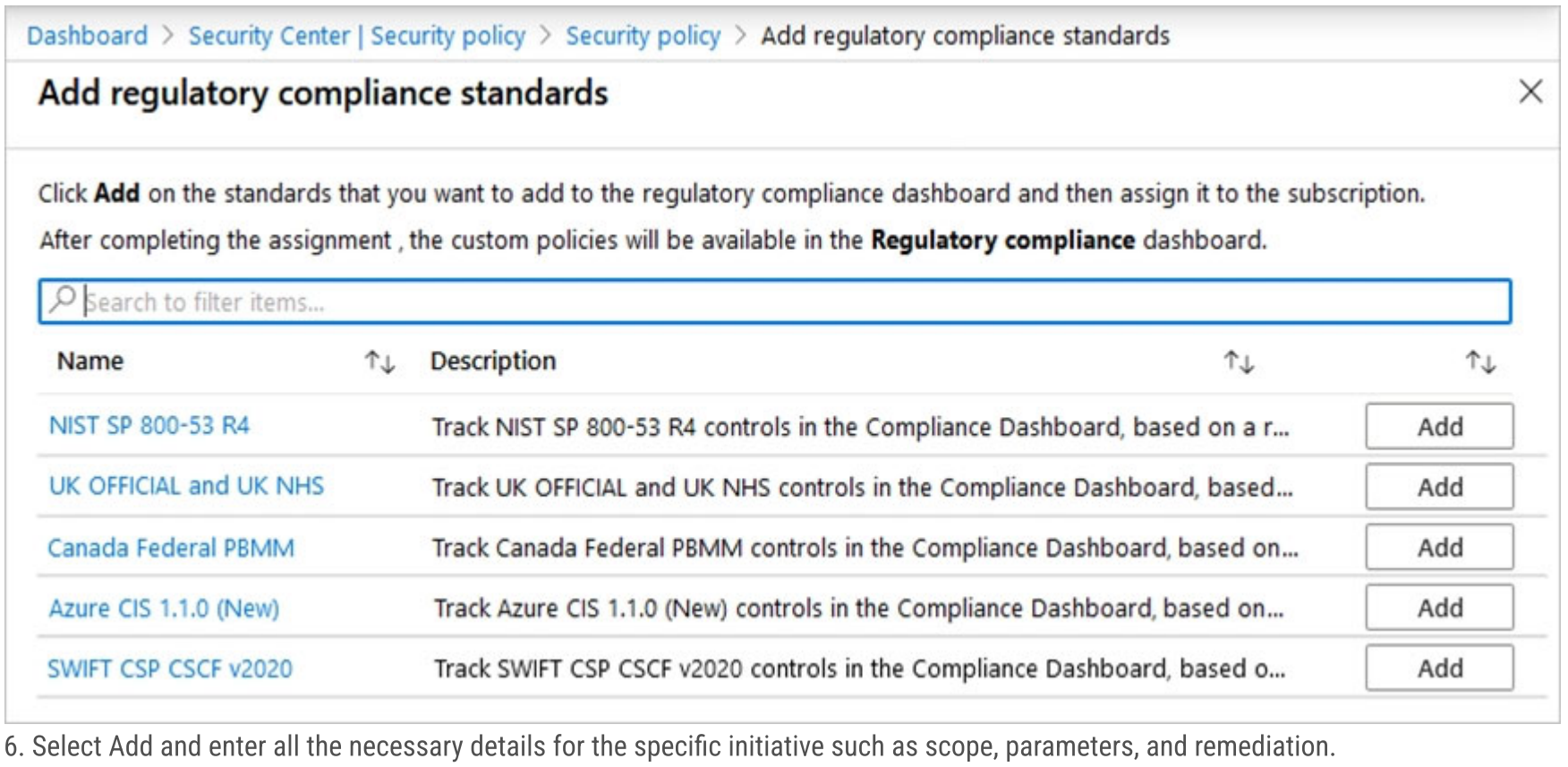
A. From Defender for Cloud, review the secure score recommendations.

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

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Defender for Cloud, add a regulatory compliance standard.

Correct Answer: *D*
Add a regulatory standard to your dashboard
The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.
Add a standard to your Azure resources
1. From Defender for Cloud's menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.
2. From the top of the page, select Manage compliance policies. The Policy Management page appears.
3. Select the subscription or management group for which you want to manage the regulatory compliance posture.
4. To add the standards relevant to your organization, expand the Industry & regulatory standards section and select Add more standards.
5. From the Add regulatory compliance standards page, you can search for any of the available standards:



6. Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.
7. From Defender for Cloud's menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.
Your new standard appears in your list of Industry & regulatory standards.
Note: Customize the set of standards in your regulatory compliance dashboard.
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

Community vote distribution
D (100%)

Question #28 *Topic 2*

Your company has devices that run either Windows 10, Windows 11, or Windows Server.
You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune

B. Local Group Policy Object (LGPO)

C. Windows Autopilot

D. Policy Analyzer

Correct Answer: *D*
Microsoft Security Compliance Toolkit 1.0, Policy Analyzer.
The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:
Highlight when a set of Group Policies has redundant settings or internal inconsistencies.
Highlight the differences between versions or sets of Group Policies.
Compare GPOs against current local policy and local registry settings
Export results to a Microsoft Excel spreadsheet
Policy Analyzer lets you treat a set of GPOs as a single unit. This treatment makes it easy to determine whether particular settings are duplicated across the
GPOs or are set to conflicting values. Policy Analyzer also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.
Note: The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft- recommended security configuration baselines for Windows and other Microsoft products.
The SCT enables administrators to effectively manage their enterprise's Group Policy Objects (GPOs). Using the toolkit, administrators can compare their current
GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active
Directory or individually through local policy.
Security Compliance Toolkit Tools:

Policy Analyzer -
Local Group Policy Object (LGPO)

Set Object Security -

GPO to Policy Rules -
Incorrect:
Not B: Local Group Policy Object (LGPO)
What is the Local Group Policy Object (LGPO) tool?
LGPO.exe is a command-line utility that is designed to help automate management of Local Group Policy. Using local policy gives administrators a simple way to verify the effects of Group Policy settings, and is also useful for managing non-domain-joined systems.
LGPO.exe can import and apply settings from Registry
Policy (Registry.pol) files, security templates, Advanced Auditing backup files, as well as from formatted ג€LGPO textג€ files. It can export local policy to a GPO backup. It can export the contents of a Registry Policy file to the ג€LGPO textג€ format that can then be edited, and can build a Registry Policy file from an LGPO text file.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

Community vote distribution

D (100%)

Question #29 *Topic 2*

You have an Azure subscription that is used as an Azure landing zone for an application.

You need to evaluate the security posture of all the workloads in the landing zone.

What should you do first?

A. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.

B. Obtain Azure AD Premium Plan 2 licenses.

C. Add Microsoft Sentinel data connectors.

D. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #30 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: *A*

Community vote distribution

A (70%) B (30%)

Question #31 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #32 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

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

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Defender for Cloud, add a regulatory compliance standard.

Correct Answer: *D*

Community vote distribution

D (75%) C (25%)

Question #33 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Defender for Cloud, review the Azure security baseline for audit report.

C. From Defender for Cloud, add a regulatory compliance standard.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #34 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

C. From Defender for Cloud, review the secure score recommendations.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #35 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

C. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

D. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

Correct Answer: *B*

Community vote distribution

B (67%) D (33%)

Question #36 *Topic 2*

You have an Azure subscription.

Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.

What should you recommend using to enforce the governance requirement?

A. Azure management groups

B. custom Azure roles

C. Azure Policy assignments

D. regulatory compliance standards in Microsoft Defender for Cloud

Correct Answer: *C*

Community vote distribution

C (100%)

Question #37 *Topic 2*

HOTSPOT
-

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

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

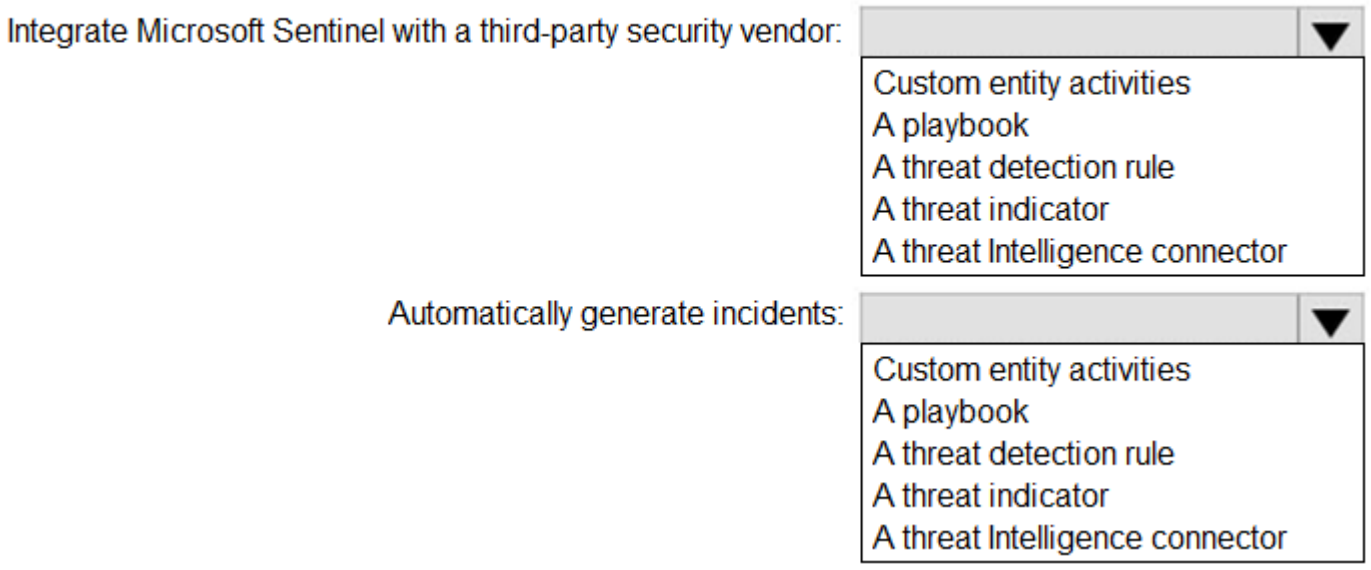
You need to recommend a solution to meet the following requirements:

• Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware.
• Automatically generate incidents when the IP address of a command-and-control server is detected in the events.

What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

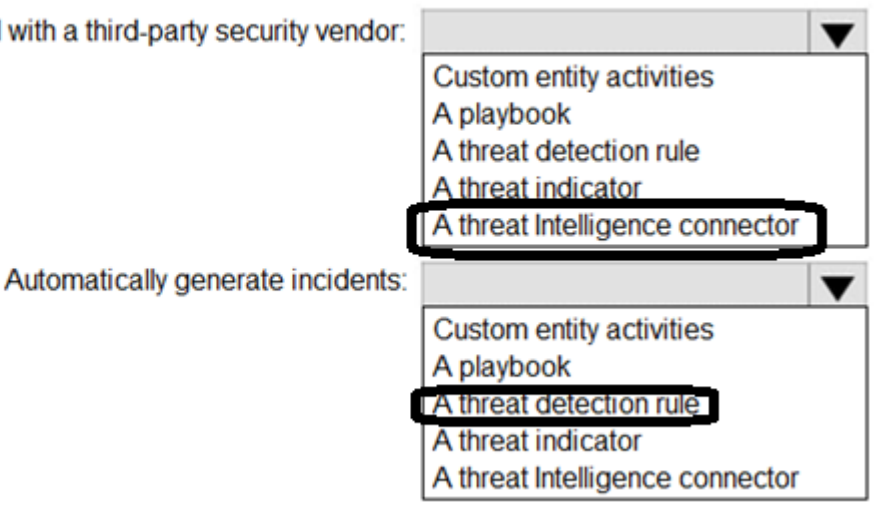
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Question #38 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You need to enforce ISO 27001:2013 standards for new resources deployed to the subscription. The solution must ensure that noncompliant resources are automatically detected.

What should you use?

A. Azure Blueprints

B. the regulatory compliance dashboard in Defender for Cloud

C. Azure Policy

D. Azure role-based access control (Azure RBAC)

Correct Answer: *C*

Community vote distribution

C (67%) B (33%)

Question #39 *Topic 2*

DRAG DROP

-

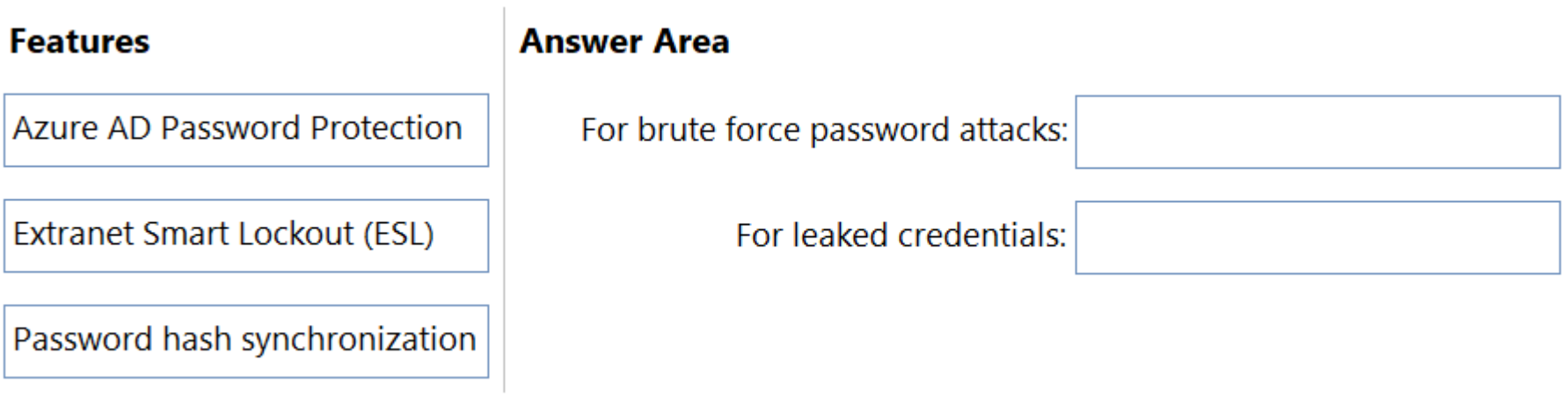
You have a hybrid Azure AD tenant that has pass-through authentication enabled.

You are designing an identity security strategy.

You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.

What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Correct Answer:

Answer Area

For brute force password attacks: Azure AD Password Protection

For leaked credentials: Password hash synchronization

Question #40 *Topic 2*

HOTSPOT
-

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

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

You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

• Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
• Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

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

NOTE: Each correct selection is worth one point.

Answer Area

DLP:
- Azure Data Catalog
- Azure Data Explorer
- Microsoft Purview

UEBA:
- Azure AD Identity Protection
- Microsoft Defender for Identity
- Microsoft Entra Verified ID

Correct Answer:

Answer Area

DLP:
- Azure Data Catalog
- Azure Data Explorer
- Microsoft Purview

UEBA:
- Azure AD Identity Protection
- Microsoft Defender for Identity
- Microsoft Entra Verified ID

Question #41 *Topic 2*

HOTSPOT

-

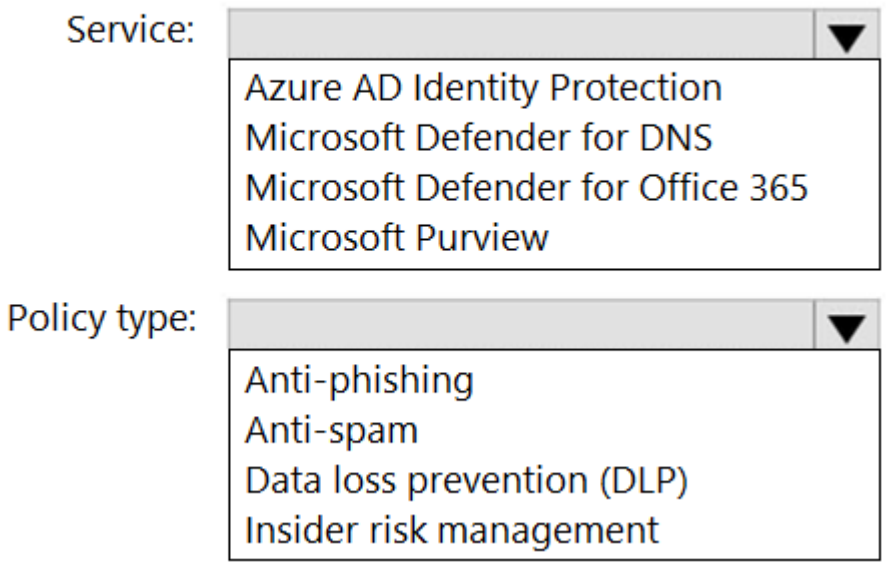
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

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

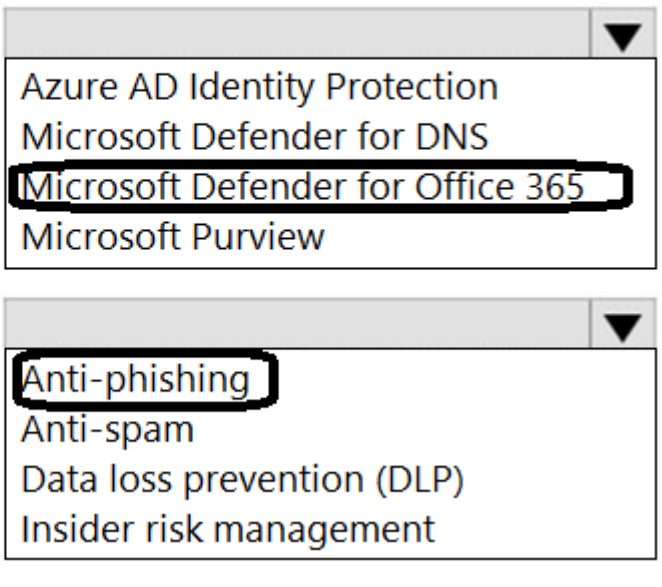
NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Correct Answer:



Question #42 *Topic 2*

HOTSPOT
-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

You have multiple project teams. Each team has an AD DS group that syncs with Azure AD.

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

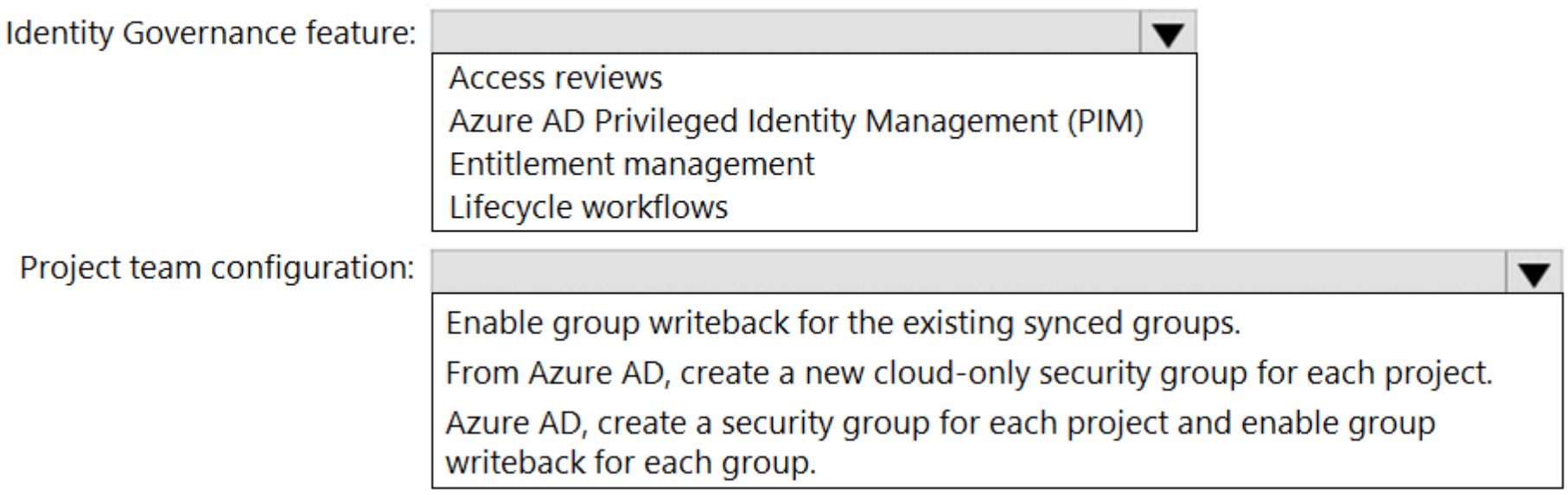
You need to recommend an Azure AD Identity Governance solution that meets the following requirements:

• Project managers must verify that their project group contains only the current members of their project team.
• The members of each project team must only have access to the resources of the project to which they are assigned.
• Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days.
• Administrative effort must be minimized.

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

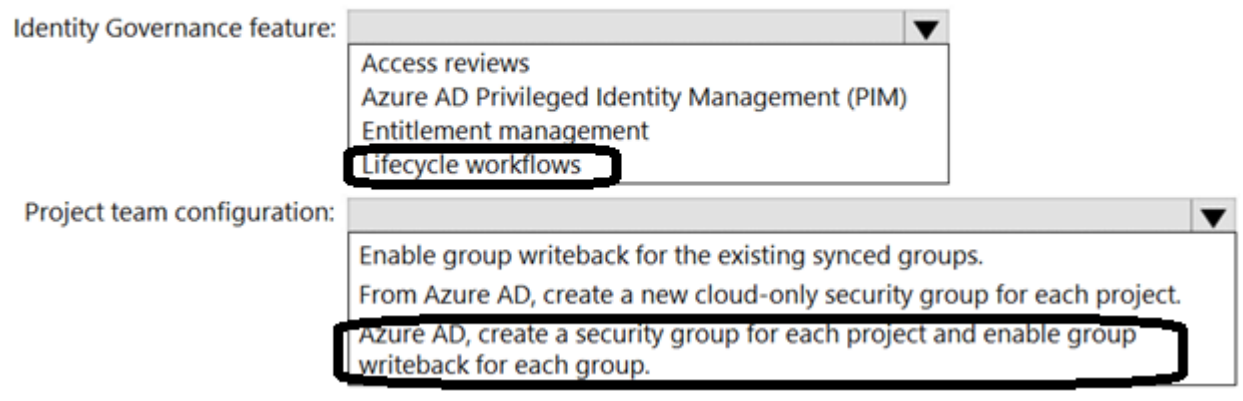
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Question #43 *Topic 2*

HOTSPOT
-

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

You need to provide the Fabrikam users with access to the Contoso resources by using access packages. The solution must meet the following requirements:

• Ensure that the Fabrikam users can use the Contoso access packages without explicitly creating guest accounts in contoso.com.
• Allow non-administrative users in contoso.com to create the access packages.

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

NOTE: Each correct selection is worth one point.

Answer Area

Ensure that the Fabrikam users can use the access packages without explicitly creating guest accounts in contoso.com:
- A connected organization
- An external organization
- An identity provider

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

Correct Answer:

Answer Area

Ensure that the Fabrikam users can use the access packages without explicitly creating guest accounts in contoso.com: **A connected organization**
- An external organization
- An identity provider

Allow non-administrative users in contoso.com to create the access packages by creating: **Catalogs**
- Administrative units
- Programs

Question #44 *Topic 2*

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

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

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

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app registrations in Azure AD

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: *D*

Question #45 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, add a regulatory compliance standard.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #46 *Topic 2*

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

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app registrations in Azure AD

B. Azure AD Conditional Access App Control policies

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

D. adaptive application controls in Defender for Cloud

Correct Answer: *D*

Community vote distribution

D (100%)

Question #47 *Topic 2*

You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.

You need to design a security solution to assess whether all the devices meet the customer's compliance rules.

What should you include in the solution?

A. Microsoft Sentinel

B. Microsoft Purview Information Protection

C. Microsoft Intune

D. Microsoft Defender for Endpoint

Correct Answer: *D*

Community vote distribution

C (96%) 4%

Topic 3 - Question Set 3

Question #1 *Topic 3*

You have Microsoft Defender for Cloud assigned to Azure management groups.
You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation.
Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel threat intelligence workbooks

B. Microsoft Sentinel notebooks

C. threat intelligence reports in Defender for Cloud

D. workload protections in Defender for Cloud

Correct Answer: *AC*
A: Workbooks provide insights about your threat intelligence
Workbooks provide powerful interactive dashboards that give you insights into all aspects of Microsoft Sentinel, and threat intelligence is no exception. You can use the built-in Threat Intelligence workbook to visualize key information about your threat intelligence, and you can easily customize the workbook according to your business needs. You can even create new dashboards combining many different data sources so you can visualize your data in unique ways. Since
Microsoft Sentinel workbooks are based on Azure Monitor workbooks, there is already extensive documentation available, and many more templates.
C: What is a threat intelligence report?
Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.
Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:
Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
Campaign Report: focuses on details of specific attack campaigns.
Threat Summary Report: covers all of the items in the previous two reports.
This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future.
Incorrect:
Not B: When to use Jupyter notebooks
While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data.
For example, use notebooks to:
Perform analytics that aren't provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features
Create data visualizations that aren't provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees
Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.
Not D: Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. For example, you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Community vote distribution

AC (100%)

Question #2 *Topic 3*

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions.
You are evaluating the security posture of the customer.
You discover that the AKS resources are excluded from the secure score recommendations.
You need to produce accurate recommendations and update the secure score.
Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Defender plans.

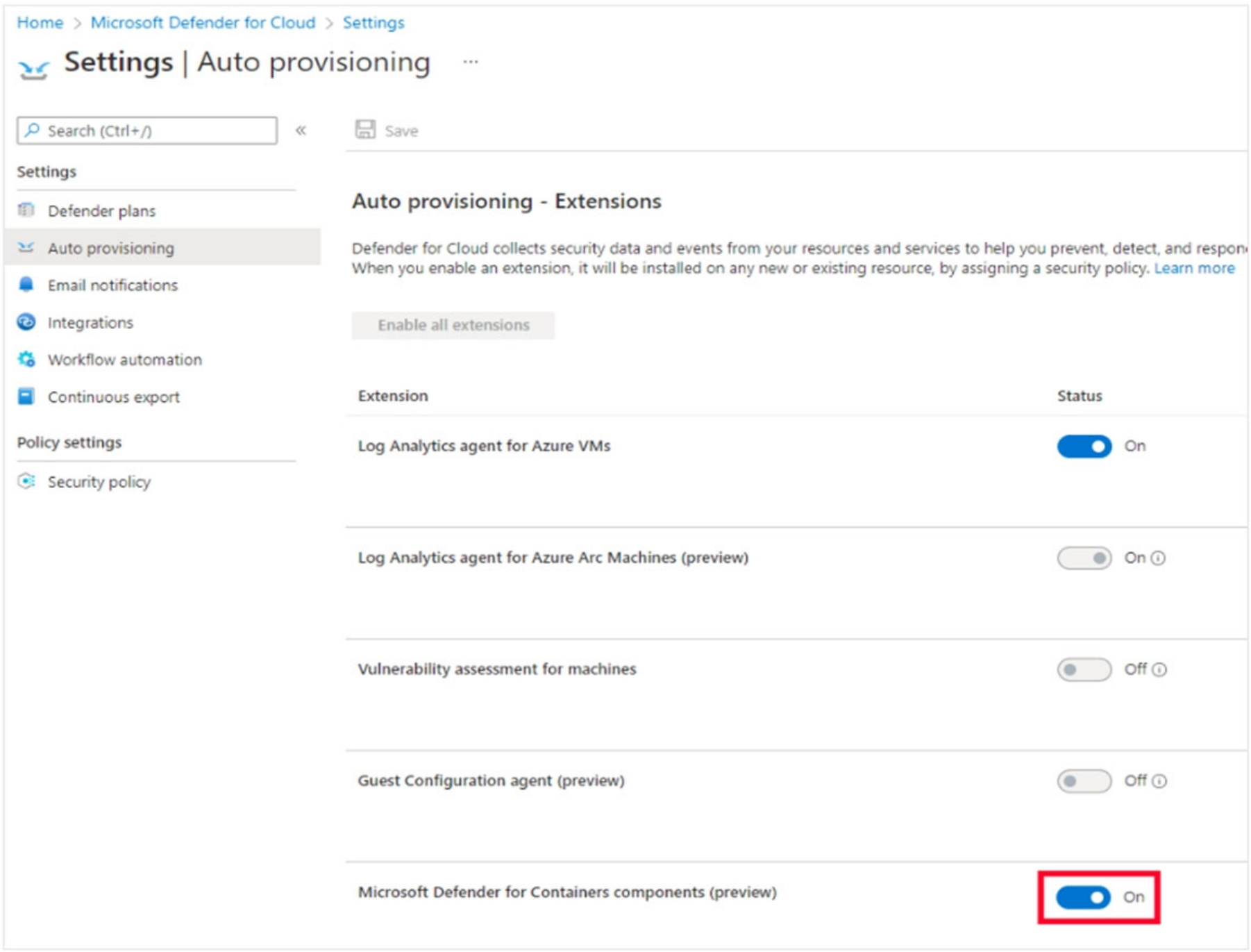
B. Configure auto provisioning.

C. Add a workflow automation.

D. Assign regulatory compliance policies.

E. Review the inventory.

Correct Answer: *BD*
D: How are regulatory compliance standards represented in Defender for Cloud?
Industry standards, regulatory standards, and benchmarks are represented in Defender for Cloud's regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.
To see compliance data mapped as assessments in your dashboard, add a compliance standard to your management group or subscription from within the
Security policy page.
When you've assigned a standard or benchmark to your selected scope, the standard appears in your regulatory compliance dashboard with all associated compliance data mapped as assessments.
B: Configure Defender for Containers components
If you disabled any of the default protections when you enabled Microsoft Defender for Containers, you can change the configurations and reenable them via auto provisioning.
1. To configure the Defender for Containers components:
2. Sign in to the Azure portal.
3. Navigate to Microsoft Defender for Cloud > Environment settings.
4. Select the relevant subscription.
5. From the left side tool bar, select Auto provisioning.
6. Ensure that Microsoft Defenders for Containers components (preview) is toggled to On.



Incorrect:

Not A: When you enable Microsoft Defender for Containers, Azure Kubernetes Service clusters, and Azure Arc enabled Kubernetes clusters (Preview) protection are both enabled by default.

To upgrade to Microsoft Defender for Containers, open the Defender plans page in the portal and enable the new plan:

Not C: No need for automation.

Note: Automate responses to Microsoft Defender for Cloud triggers.

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can.

Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Community vote distribution

AB (75%) 14% 11%

Question #3 *Topic 3*

Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks.
The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:
- Prevent exposing the public IP addresses of the virtual machines.
- Provide the ability to connect without using a VPN.
- Minimize costs.

Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a hub and spoke network by using virtual network peering.

B. Deploy Azure Bastion to each virtual network.

C. Deploy Azure Bastion to one virtual network.

D. Create NAT rules and network rules in Azure Firewall.

E. Enable just-in-time VM access on the virtual machines.

Correct Answer: *AC*
Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
Incorrect:
Not B: Two Azure Bastions would increase the cost.
Reference:
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

Community vote distribution
AC (97%)

Question #4 *Topic 3*

HOTSPOT -

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

You need to recommend a solution to secure the components of the copy process.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Data security:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Network access control:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Correct Answer:

Answer Area

Data security:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Network access control:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Box 1: Azure Web Application Firewall with network service tags

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to define network access controls on network security groups, Azure Firewall, and user-defined routes.

Incorrect:

* Not Azure private link with network service tags

Network service tags are not used with Private links.

Box 2: Automation Contributor built-in role
The Automation Contributor role allows you to manage all resources in the Automation account, except modifying other user's access permissions to an
Automation account.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control

Question #5 *Topic 3*

You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.
What should you include in the recommendation?

A. Compliance Manager

B. Microsoft Defender for Cloud Apps

C. Microsoft Endpoint Manager

D. Microsoft Defender for Endpoint

Correct Answer: *D*
Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.
Note: Turn on web content filtering
From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering. Switch the toggle to On and Save preferences.
Configure web content filtering policies
Web content filtering policies specify which site categories are blocked on which device groups. To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering

Community vote distribution
D (92%) 8%

Question #6 *Topic 3*

Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10.
You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
☞ Ensure that only authorized applications can run on the kiosks.
☞ Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

B. Onboard the kiosks to Microsoft intune and Microsoft Defender for Endpoint.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

D. Onboard the kiosks to Azure Monitor.

E. Implement Privileged Access Workstation (PAW) for the kiosks.

Correct Answer: *BE*
Onboard devices and configure Microsoft Defender for Endpoint capabilities.
Deploying Microsoft Defender for Endpoint is a two-step process.
* Onboard devices to the service
* Configure capabilities of the service
B: Depending on the device, follow the configuration steps provided in the onboarding section of the Defender for Endpoint portal.
E: A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses credential guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and web traffic is restricted to a limit set of permitted destinations (Deny all).
Note: Privileged Access Workstation (PAW) ג€" This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised. The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive job tasks. This makes the
PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing. To provide productivity to these users, separate accounts and workstations must be provided for productivity applications and web browsing.
While inconvenient, this is a necessary control to protect users whose account could inflict damage to most or all resources in the organization.
Incorrect:
Not A: What is automated investigation and remediation?
Automated investigation and response capabilities help your security operations team by: Determining whether a threat requires action. Taking (or recommending) any necessary remediation actions. Determining whether and what other investigations should occur. Repeating the process as necessary for other alerts.
Not C: Threat & Vulnerability Management is a component of Microsoft Defender for Endpoint, and provides both security administrators and security operations teams with unique value, including:
- Real-time endpoint detection and response (EDR) insights correlated with endpoint vulnerabilities.
- Invaluable device vulnerability context during incident investigations.
- Built-in remediation processes through Microsoft Intune and Microsoft System Center Configuration Manager.
Note: Microsoft's threat and vulnerability management is a built-in module in Microsoft Defender for Endpoint that can:
Discover vulnerabilities and misconfigurations in near real time.
Prioritize vulnerabilities based on the threat landscape and detections in your organization.
If you've enabled the integration with Microsoft Defender for Endpoint, you'll automatically get the threat and vulnerability management findings without the need for additional agents.
As it's a built-in module for Microsoft Defender for Endpoint, threat and vulnerability management doesn't require periodic scans.
Not D: You do not use Azure Monitor for onboarding.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure https://docs.microsoft.com/en-us/security/compass/privileged-access-devices https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-tvm

Community vote distribution

BC (79%) BE (21%)

Question #7 *Topic 3*

You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data.
What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps

B. Microsoft Information Protection

C. insider risk management

D. Azure Purview

Correct Answer: *A*
Microsoft Defender for Cloud Apps File policies.
File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases. Defender for Cloud Apps can monitor any file type based on more than 20 metadata filters (for example, access level, file type).
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

Community vote distribution

B (90%) 8%

Question #8 *Topic 3*

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.
You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface.
What should you include in the recommendation?

A. Azure Firewall Premium

B. Azure Traffic Manager and application security groups

C. Azure Application Gateway Web Application Firewall (WAF)

D. network security groups (NSGs)

Correct Answer: *B*
* Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.
* Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.
Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint.
Incorrect:
Not C: Azure Application Gateway Web Application Firewall is too small a scale solution in this scenario.
Note: Attacks against a web application can be monitored by using a real-time Application Gateway that has Web Application Firewall, enabled with integrated logging from Azure Monitor to track Web Application Firewall alerts and easily monitor trends.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

Community vote distribution

C (100%)

Question #9 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Need to use customer-managed keys instead.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution

B (83%) A (17%)

Question #10 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses Microsoft-managed keys.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Need to use customer-managed keys instead.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution

B (88%) 13%

Question #11 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
We need to use customer-managed keys.
Azure Storage encryption for data at rest.
Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments.
Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.
Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to manage encryption with your own keys, you have two options. You can use either type of key management, or both:
* You can specify a customer-managed key to use for encrypting and decrypting data in Blob Storage and in Azure Files.
* You can specify a customer-provided key on Blob Storage operations. A client making a read or write request against Blob Storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution

A (100%)

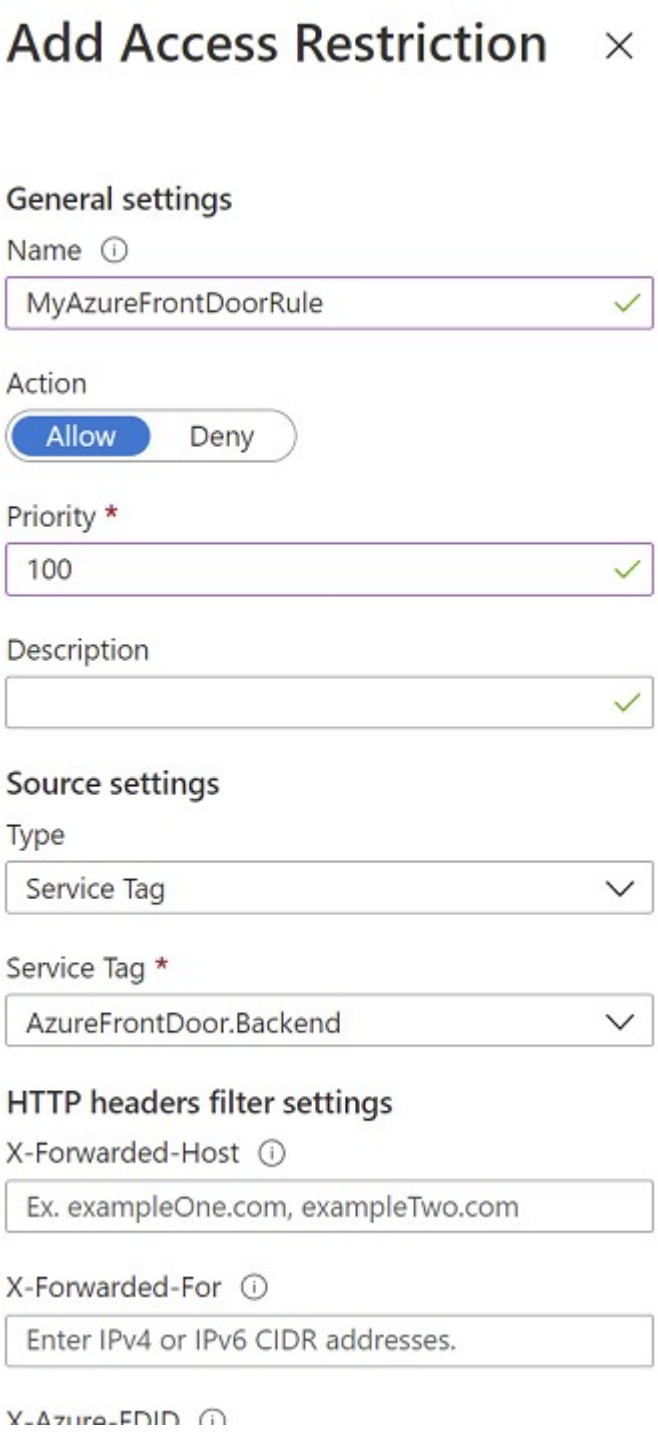
Question #12 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.



Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

Community vote distribution
B (71%) A (29%)

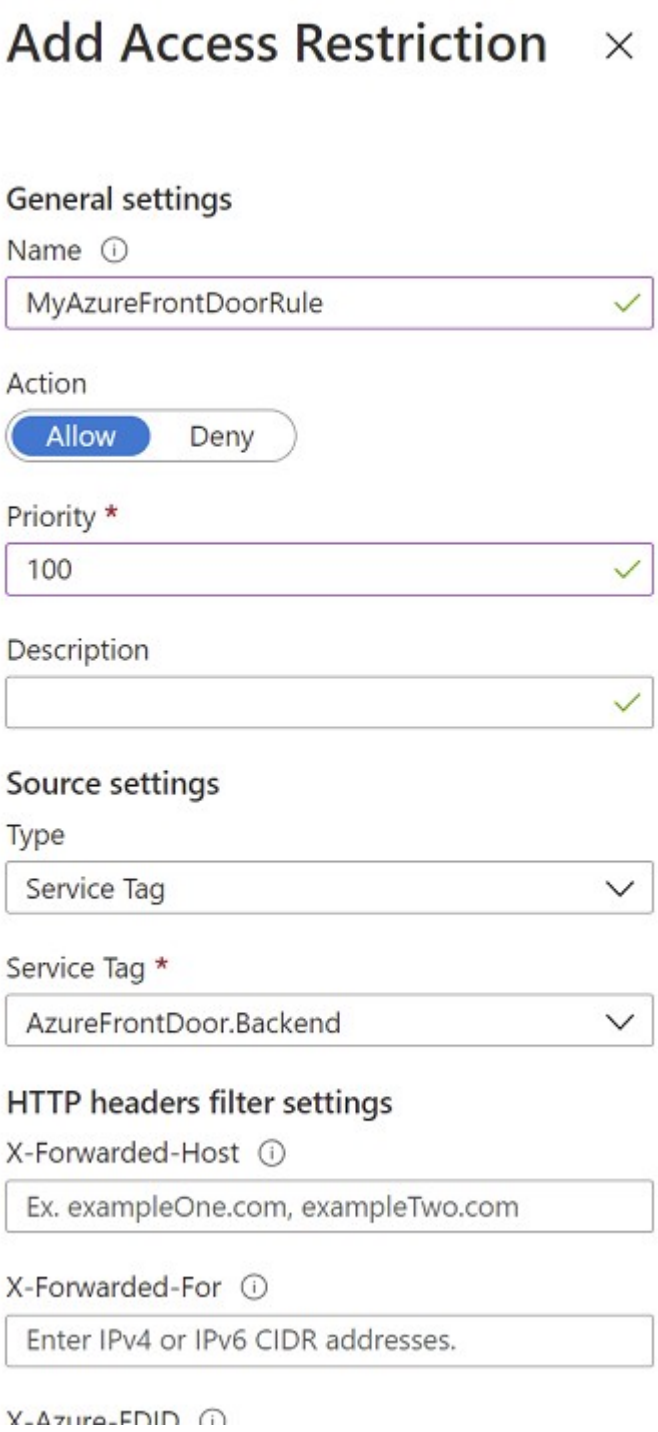
Question #13 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions that allow traffic from the Front Door service tags.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.



Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

Community vote distribution
B (53%) A (47%)

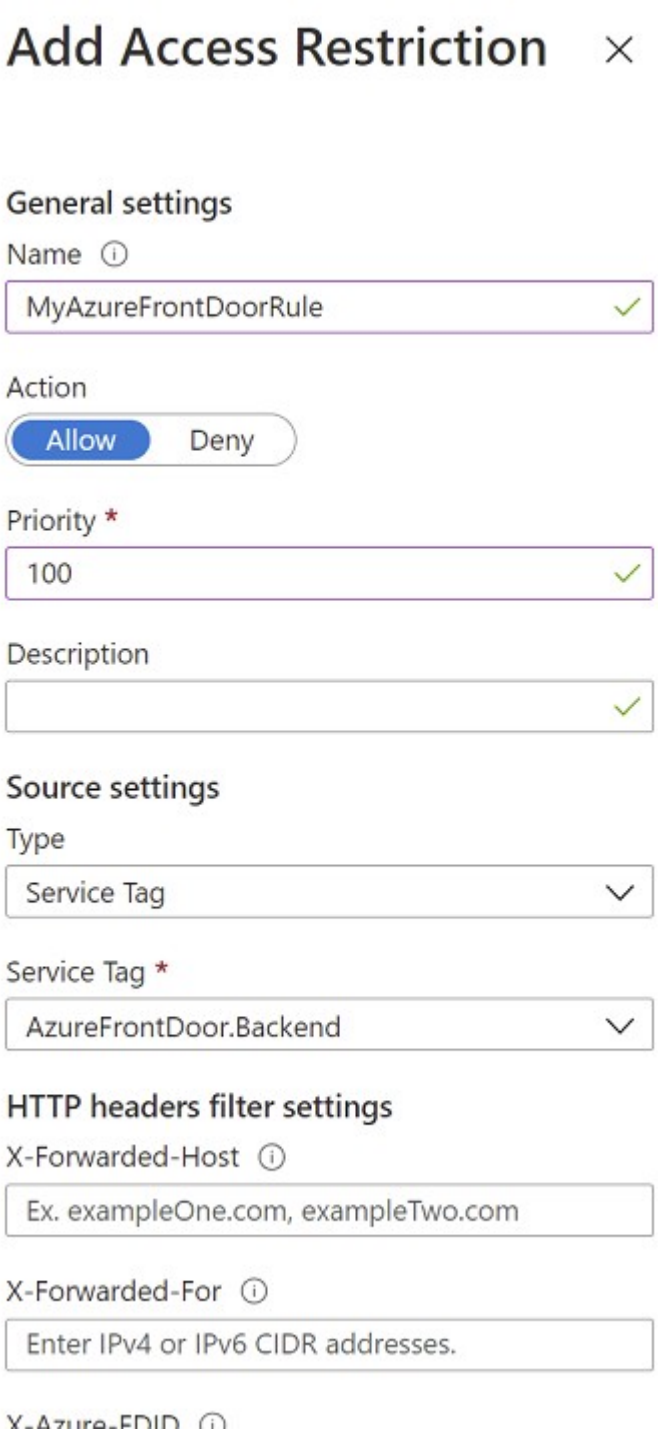
Question #14 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

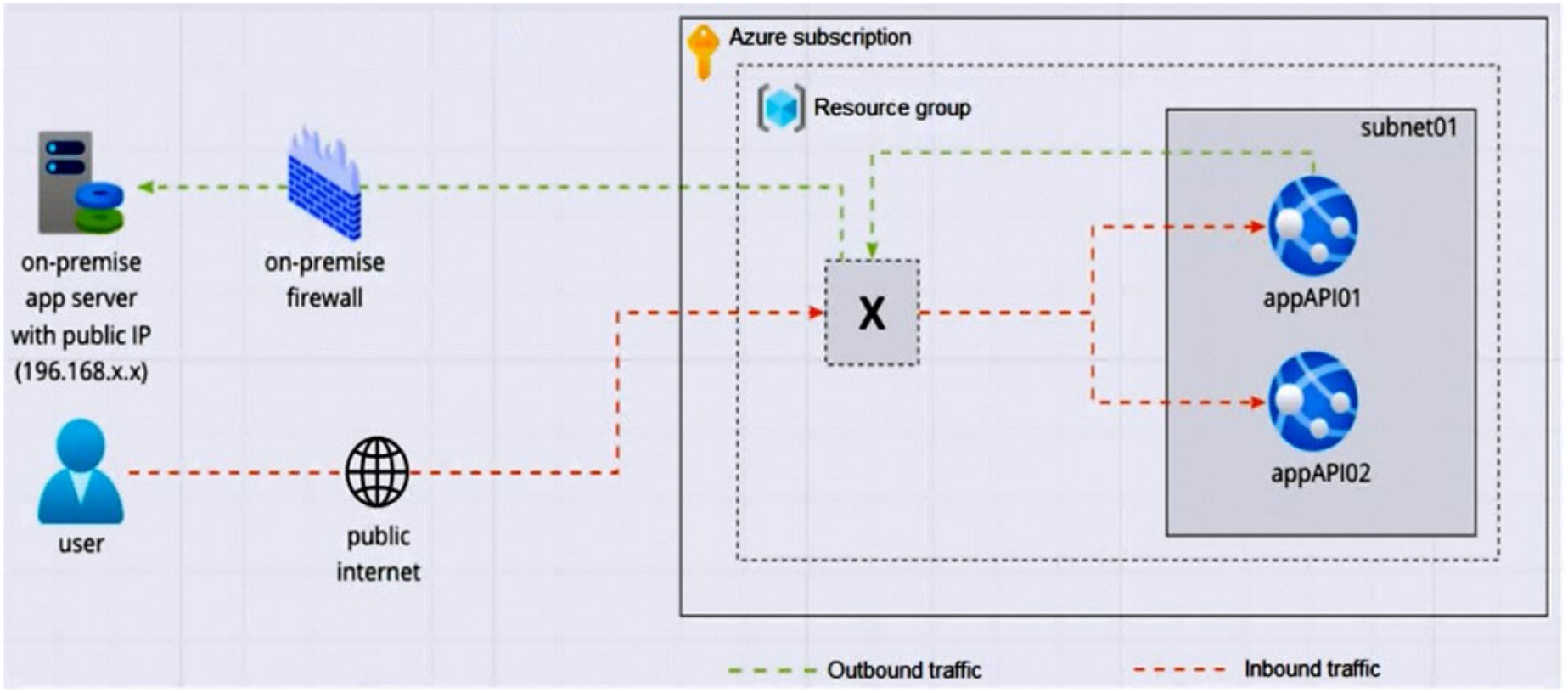


Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

Community vote distribution
A (70%) B (30%)

Question #15 *Topic 3*

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)

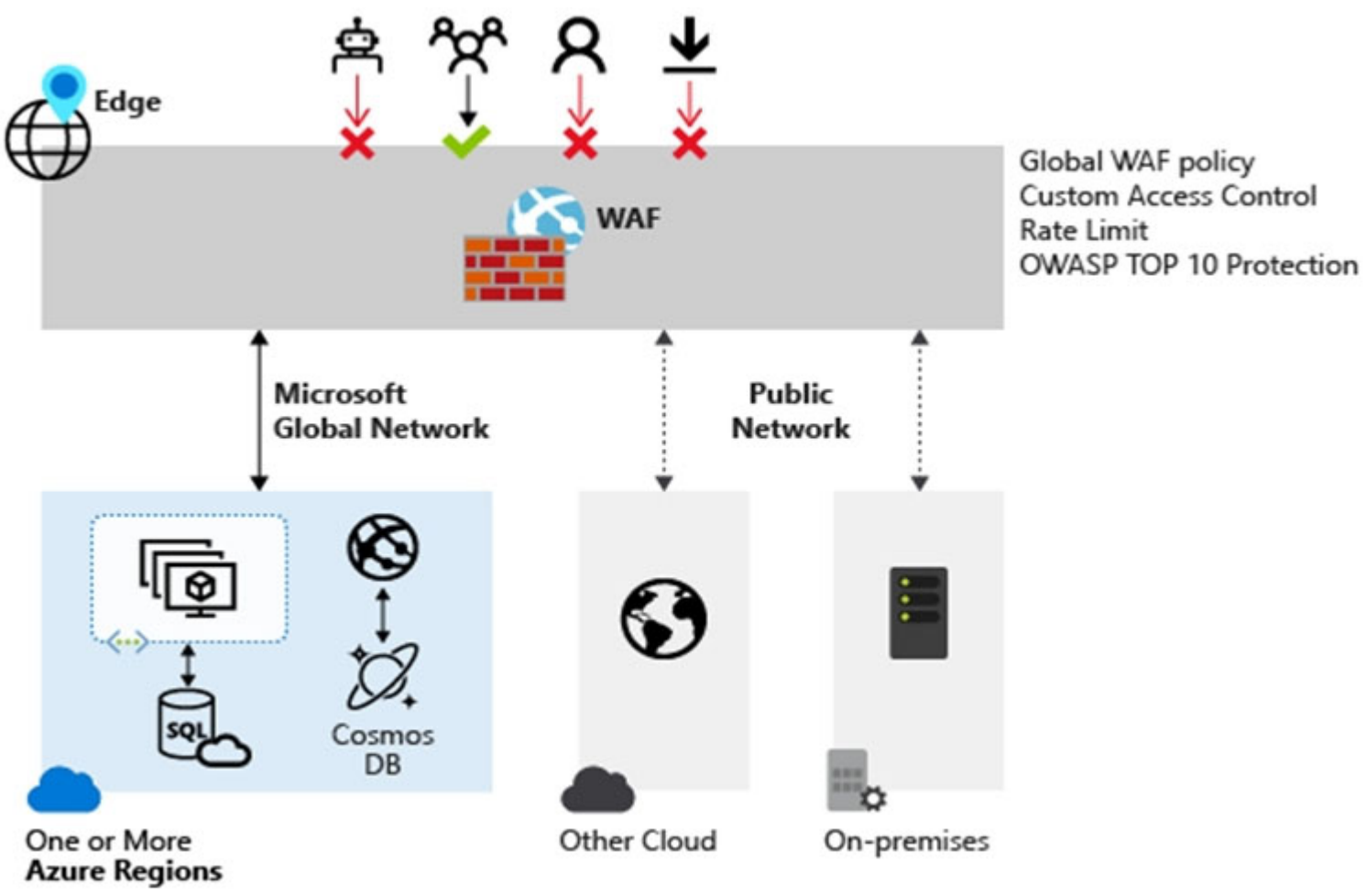
D. Azure Application Gateway v2 with user-defined routes (UDRs)

Correct Answer: *C*

Azure Web Application Firewall (WAF) on Azure Front Door provides centralized protection for your web applications. WAF defends your web services against common exploits and vulnerabilities. It keeps your service highly available for your users and helps you meet compliance requirements.

WAF on Front Door is a global and centralized solution. It's deployed on Azure network edge locations around the globe. WAF enabled web applications inspect every incoming request delivered by Front Door at the network edge.

WAF prevents malicious attacks close to the attack sources, before they enter your virtual network.



Incorrect:

Not D: Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.
You could use Azure Application Gateway with the Azure Web Application Firewall (WAF).
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

Community vote distribution

B (84%) Other

Question #16 *Topic 3*

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.

Correct Answer: *AD*
A: LT-2: Enable threat detection for Azure identity and access management
Guidance: Azure Active Directory (Azure AD) provides the following user logs, which can be viewed in Azure AD reporting or integrated with Azure Monitor,
Microsoft Sentinel, or other SIEM/monitoring tools for more sophisticated monitoring and analytics use cases:
Sign-ins - The sign-ins report provides information about the usage of managed applications and user sign-in activities.
Audit logs - Provides traceability through logs for all changes done by various features within Azure AD. Examples of audit logs include changes made to any resources within Azure AD, like adding or removing users, apps, groups, roles, and policies.
D: Disable local authentication methods so that your Cosmos DB database accounts exclusively require Azure Active Directory identities for authentication.
Enforcing RBAC as the only authentication method
In situations where you want to force clients to connect to Azure Cosmos DB through RBAC exclusively, you have the option to disable the account's primary/ secondary keys. When doing so, any incoming request using either a primary/secondary key or a resource token will be actively rejected.
Incorrect:
Not C: We use the Azure Active Directory (Azure AD) sign-in logs, not the Azure Cosmos db logs.
Not E: Microsoft Defender for Cosmos DB, though useful from a security perspective, does not help with auditing the users.
Note: Logging and Threat Detection, LT-1: Enable threat detection for Azure resources
Guidance: Use the Microsoft Defender for Cloud built-in threat detection capability and enable Microsoft Defender for your Cosmos DB resources. Microsoft
Defender for Cosmos DB provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your
Cosmos DB resources.
Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline https://docs.microsoft.com/en-us/azure/cosmos-db/policy-reference https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac#disable-local-auth

Community vote distribution

AD (47%) AC (43%) 8%

Question #17 *Topic 3*

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.

Correct Answer: *B*
A read-only lock on a storage account prevents users from listing the account keys. A POST request handles the Azure Storage List Keys operation to protect access to the account keys. The account keys provide complete access to data in the storage account.
Incorrect:
Not A:
If any clients are currently accessing data in your storage account with Shared Key, then Microsoft recommends that you migrate those clients to Azure AD before disallowing Shared Key access to the storage account.
However, in this scenario we cannot migrate to Azure AD due to the legacy applications.

Note: Shared Key -
A shared key is a very long string. You can simply access Azure storage by using this long string. It's almost like a password. Actually, it's worse: this is a master password. It gives you all sorts of rights on the Azure storage account. You can imagine why this isn't my favorite mechanism of accessing Azure storage. What happens when this key is compromised? You don't get an alert. Perhaps you can set up monitoring to see misuse of your Azure storage account. But it's still less than an ideal situation. Alerts will tell you of damage after it has already occurred.
Not C: Data breaches caused by cloud misconfiguration have been seen for the past few years. One of the most common misconfigurations is granting public access to cloud storage service. Such a data is often unprotected, making them to be accessed without any authentication method. Microsoft recently introduced a new protection feature to help avoid public access on storage account. The feature introduces a new property named allowBlobPublicAccess.
Not D: Key rotation would improve security.
Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources https://docs.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution
B (77%) A (19%) 4%

Question #18 *Topic 3*

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)

Correct Answer: *CD*
The new plan merges the capabilities of the two existing Microsoft Defender for Cloud plans, Microsoft Defender for Kubernetes and Microsoft Defender for container registries.
Azure container registries can include both Windows and Linux images.
You can use Defender for Containers to scan the container images stored in your Azure Resource Manager-based Azure Container Registry, as part of the protections provided within Microsoft Defender for Cloud.
To enable scanning of vulnerabilities in containers, you have to enable Defender for Containers. When the scanner, powered by Qualys, reports vulnerabilities,
Defender for Cloud presents the findings and related information as recommendations. In addition, the findings include related information such as remediation steps, relevant CVEs, CVSS scores, and more. You can view the identified vulnerabilities for one or more subscriptions, or for a specific registry.
Note: Defender for Containers includes an integrated vulnerability scanner for scanning images in Azure Container Registry registries. The vulnerability scanner runs on an image:
When you push the image to your registry
Weekly on any image that was pulled within the last 30
When you import the image to your Azure Container Registry
Continuously in specific situations
View vulnerabilities for running images
The recommendation Running container images should have vulnerability findings resolved shows vulnerabilities for running images by using the scan results from ACR registries and information on running images from the Defender security profile/extension.
Incorrect:
Not A: The new plan merges the capabilities of the two existing Microsoft Defender for Cloud plans, Microsoft Defender for Kubernetes and Microsoft Defender for container registries
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-usage
https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/introducing-microsoft-defender-for-containers/ba-p/2952317
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction

Community vote distribution
DE (73%) 13% 10%

Question #19 *Topic 3*

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

Correct Answer: *A*
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal.
Azure AD Application Proxy is:
Secure. On-premises applications can use Azure's authorization controls and security analytics. For example, on-premises applications can use Conditional
Access and two-step verification. Application Proxy doesn't require you to open inbound connections through your firewall.
Simple to use. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don't need to change or update your applications to work with Application Proxy.
Incorrect:

Not D: Azure Virtual WAN -
Azure Virtual WAN is for end users, not for applications.
Note: Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:
Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).
Site-to-site VPN connectivity.
Remote user VPN connectivity (point-to-site).
Private connectivity (ExpressRoute).
Intra-cloud connectivity (transitive connectivity for virtual networks).
VPN ExpressRoute inter-connectivity.
Routing, Azure Firewall, and encryption for private connectivity.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

Community vote distribution

A (100%)

Question #20 *Topic 3*

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?

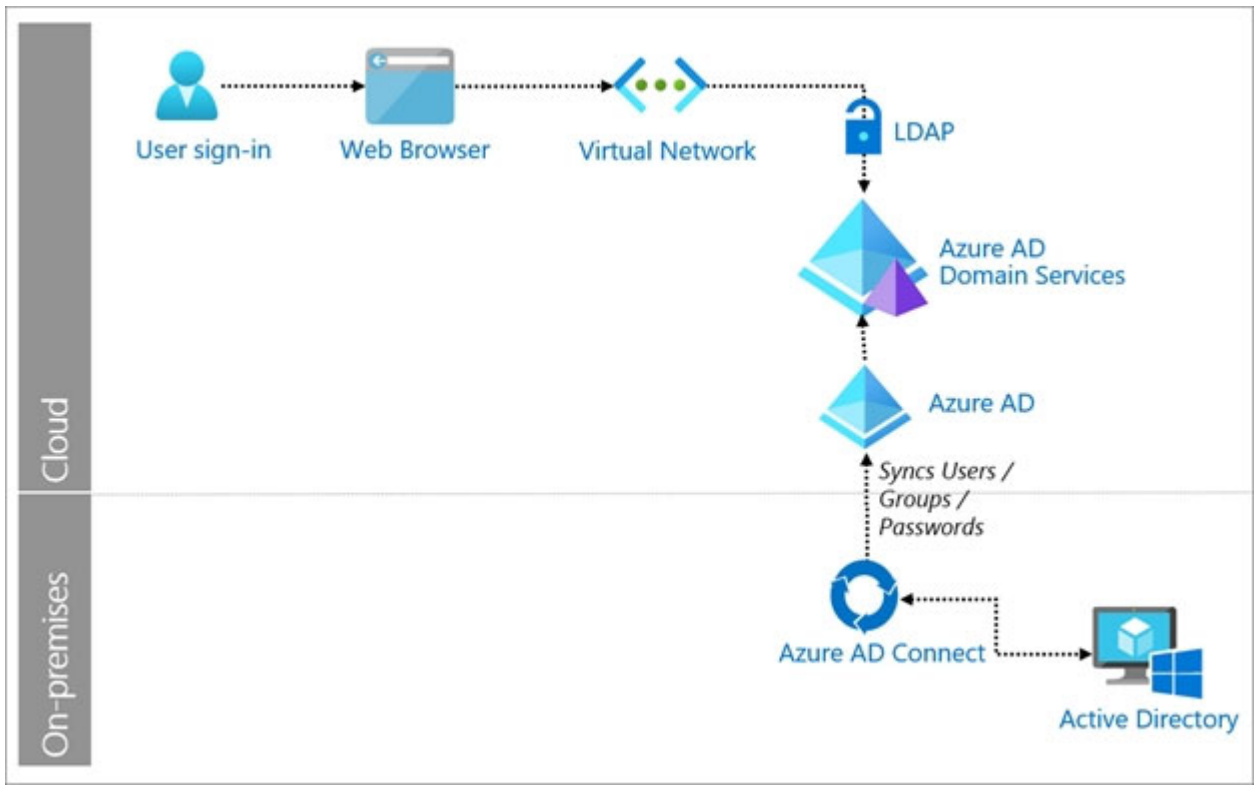
A. Azure Active Directory (Azure AD) B2C

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

C. Azure Active Directory (Azure AD)

D. Active Directory Domain Services (AD DS)

Correct Answer: *B*
Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services. Directory services, such as Active Directory, store user and account information, and security information like passwords. The service then allows the information to be shared with other devices on the network. Enterprise applications such as email, customer relationship managers (CRMs), and Human Resources (HR) software can use LDAP to authenticate, access, and find information.
Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud-first strategy to modernize their environment by moving off their on-premises LDAP resources to the cloud. The immediate benefits will be:
Integrated with Azure AD. Additions of users and groups, or attribute changes to their objects are automatically synchronized from your Azure AD tenant to AD
DS. Changes to objects in on-premises Active Directory are synchronized to Azure AD, and then to AD DS.
Simplify operations. Reduces the need to manually keep and patch on-premises infrastructures.
Reliable. You get managed, highly available services



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-ldap

Community vote distribution

B (100%)

Question #21 *Topic 3*

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

Correct Answer:

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

Box 1: Azure AD B2C authentication

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

You can set up sign-up and sign-in with a Facebook account using Azure Active Directory B2C.

Box 2: Azure AD B2B authentication with access package assignments

Govern access for external users in Azure AD entitlement management

Azure AD entitlement management uses Azure AD business-to-business (B2B) to share access so you can collaborate with people outside your organization.

With Azure AD B2B, external users authenticate to their home directory, but have a representation in your directory. The representation in your directory enables the user to be assigned access to your resources.

Incorrect:

Not: Password hash synchronization in Azure AD connect

The partners are not integrated with AD DS.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration

Question #22 *Topic 3*

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.

Correct Answer: *CD*
C: Bastion provides secure remote access.
It uses RDP/SSH session is over TLS on port 443.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
D: Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.
Meets the requirement: Only provide permission to connect the virtual machines when required
Incorrect:
Not B: Does not address: Only provide permission to connect the virtual machines when required
Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. With JEA, you can:
Reduce the number of administrators on your machines using virtual accounts or group-managed service accounts to perform privileged actions on behalf of regular users.
Limit what users can do by specifying which cmdlets, functions, and external commands they can run.
Better understand what your users are doing with transcripts and logs that show you exactly which commands a user executed during their session.
Not E: Does not help with the remote access.
Note: Classic Virtual Machine Contributor: Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
Reference:
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Community vote distribution
CD (81%) CE (19%)

Question #23 *Topic 3*

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

Correct Answer: *A*
Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise
Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.
Note: Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking. Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.
Incorrect:
Not D: SQL Server does not support dynamic data masking.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql
https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

Community vote distribution
A (51%) C (49%)

Question #24 *Topic 3*

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

Correct Answer: *C*

The peering network Hub VNet, VNet1 and VNet2 requires one Bastion.

VNet3 also requires one Bastion.

Finally, VNet3 also requires one Bastion.

Note:

VNet peering -

Can I still deploy multiple Bastion hosts across peered virtual networks?

Yes. By default, a user sees the Bastion host that is deployed in the same virtual network in which VM resides. However, in the Connect menu, a user can see multiple Bastion hosts detected across peered networks. They can select the Bastion host that they prefer to use to connect to the VM deployed in the virtual network.

Make sure that you have set up an Azure Bastion host for the virtual network in which the virtual machine scale set resides.

Azure Bastion requires a dedicated subnet: AzureBastionSubnet. You must create this subnet in the same virtual network that you want to deploy Azure Bastion to.

Can I deploy multiple Azure resources in my Azure Bastion subnet?

No. The Azure Bastion subnet (AzureBastionSubnet) is reserved only for the deployment of your Azure Bastion resource.

Reference:

https://docs.microsoft.com/en-us/azure/bastion/configuration-settings#subnet https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-scale-set https://docs.microsoft.com/en-us/azure/bastion/bastion-faq

Community vote distribution

B (89%) 11%

Question #25 *Topic 3*

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

Correct Answer:

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

Box 1: GitHub Enterprise -

A GitHub Advanced Security license provides the following additional features:

Code scanning - Search for potential security vulnerabilities and coding errors in your code.

Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also detects secrets when they are pushed to your repository.

Etc.

Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub Enterprise Cloud.

Box 2: Azure Pipelines -

Building Containers with Azure DevOps using DevTest Pattern with Azure Pipelines

The pattern enabled as to build container for development, testing and releasing the container for further reuse (production ready).

Azure Pipelines integrates metadata tracing into your container images, including commit hashes and issue numbers from Azure Boards, so

that you can inspect your applications with confidence.
Incorrect:
* Not Azure Boards: Azure Boards provides software development teams with the interactive and customizable tools they need to manage their software projects.
It provides a rich set of capabilities including native support for Agile, Scrum, and Kanban processes, calendar views, configurable dashboards, and integrated reporting.
* Not Microsoft Defender for Cloud
Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.
You cannot use Microsoft Defender for Cloud to scan code, it scans images.
Reference:
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-security
https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-container-dev-test-release/

Question #26 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes

B. No

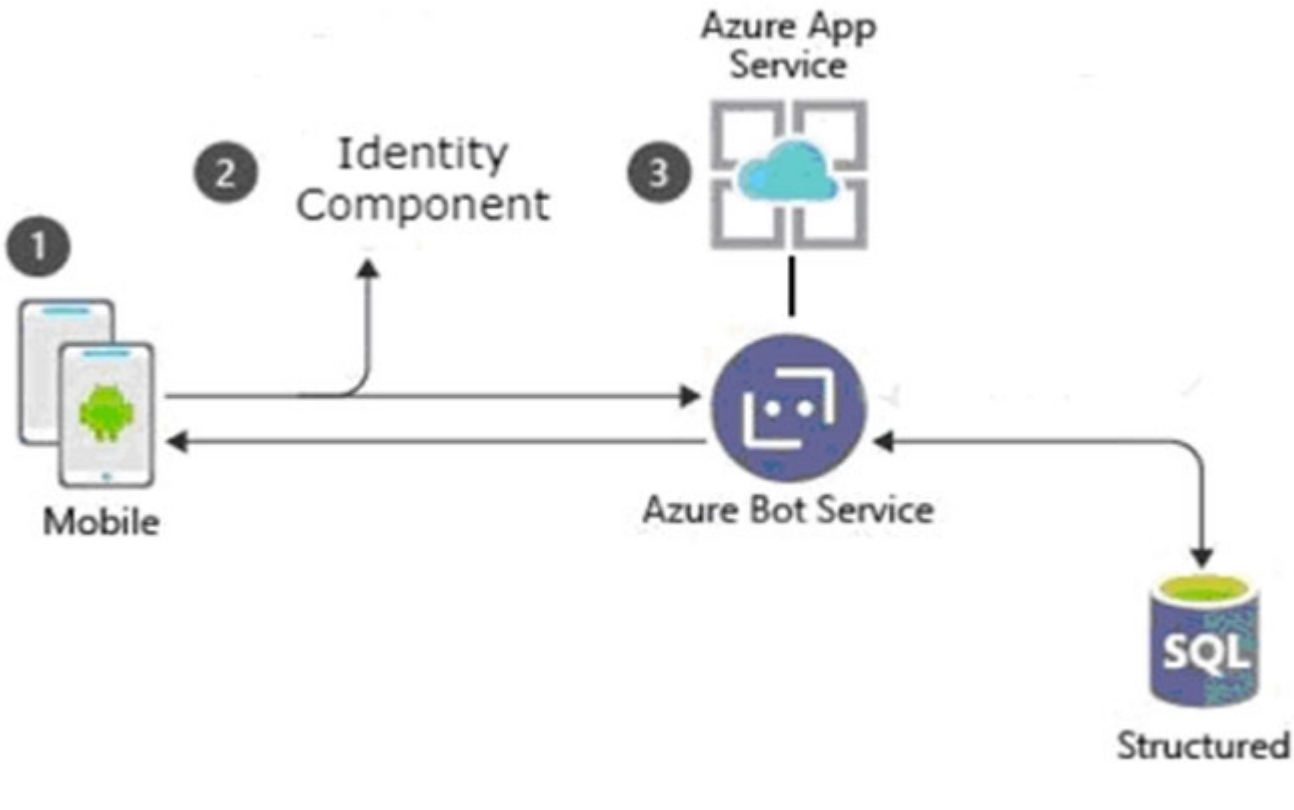
Correct Answer: *A*
We need to use customer-managed keys.
Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.
In Azure, the default setting for TDE is that the Database Encryption Key (DEK) is protected by a built-in server certificate. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256.
TDE protector is either a service-managed certificate (service-managed transparent data encryption) or an asymmetric key stored in Azure Key Vault (customer- managed transparent data encryption).
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Community vote distribution

A (100%)

Question #27 *Topic 3*

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

Correct Answer: *C*

Azure Active Directory B2C (Azure AD B2C), an identity store, is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page (SPA), and other applications.
You can set up sign-up and sign-in with a Facebook/Google account using Azure Active Directory B2C.

Branding -
Branding and customizing the user interface that Azure Active Directory B2C (Azure AD B2C) displays to your customers helps provide a seamless user experience in your application. These experiences include signing up, signing in, profile editing, and password resetting. This article introduces the methods of user interface (UI) customization.
Incorrect:
Not D: Azure AD Connect is a tool for connecting on-premises identity infrastructure to Microsoft Azure AD.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/
https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

Community vote distribution

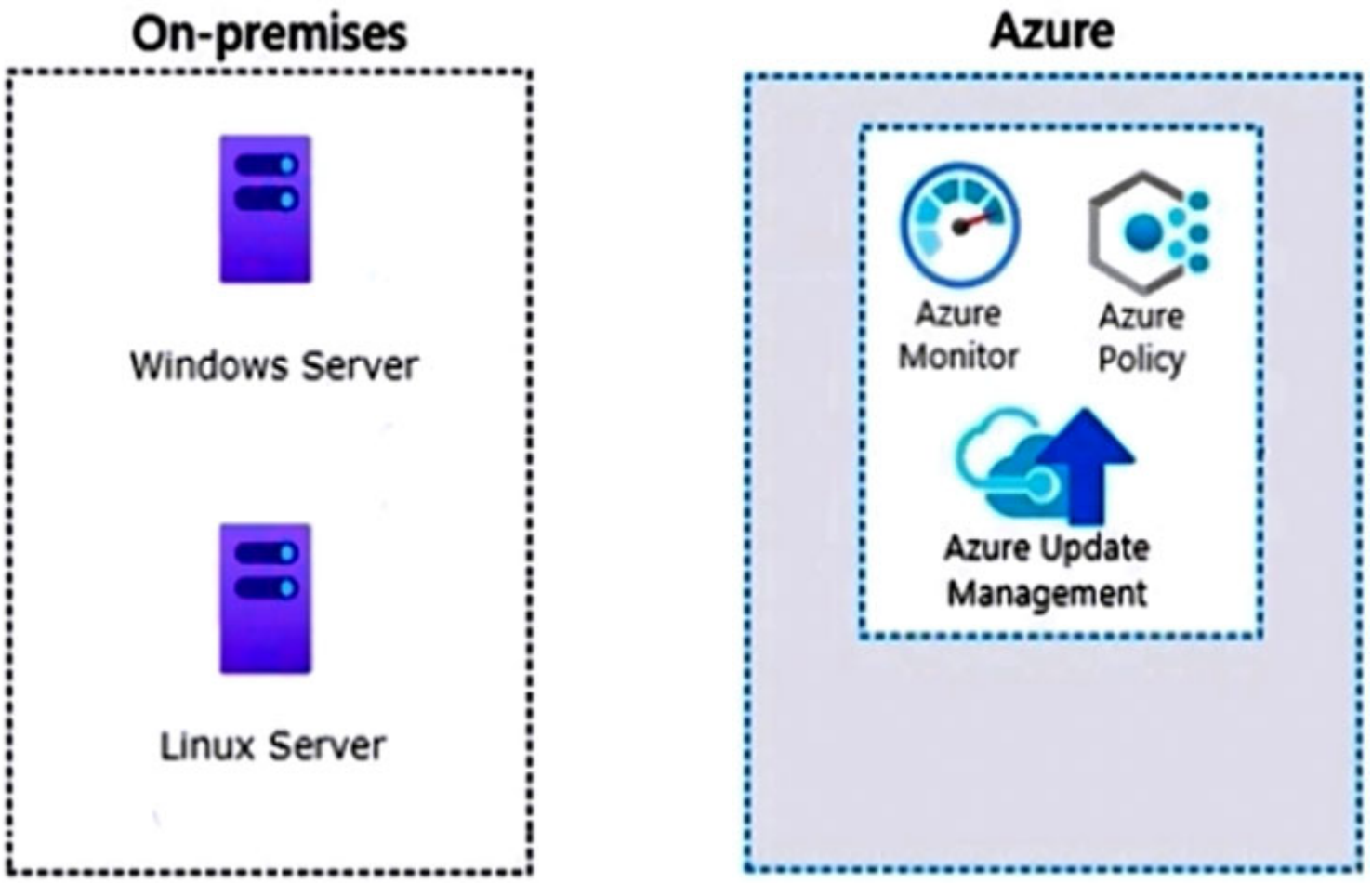
C (100%)

Question #28 *Topic 3*

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

Correct Answer: *CD*

C: Azure Policy's guest configuration feature provides native capability to audit or configure operating system settings as code, both for machines running in Azure and hybrid Arc-enabled machines. The feature can be used directly per-machine, or at-scale orchestrated by Azure Policy.

Configuration resources in Azure are designed as an extension resource. You can imagine each configuration as an additional set of properties for the machine.

Configurations can include settings such as:

Operating system settings -

Application configuration or presence

Environment settings -

Configurations are distinct from policy definitions. Guest configuration utilizes Azure Policy to dynamically assign configurations to machines.

D: Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.

Microsoft recently [2019/2020] released Azure Arc, which unlocks new hybrid scenarios for organizations by bringing new Azure services and management features to any infrastructure.

By the time of writing this post, the public preview supports the following operating systems:

Windows Server 2012 R2 and newer

Ubuntu 16.04 and 18.04 -

Register the required Resource Providers in Azure

First, we need to register the required resource providers in Azure. Therefore, take the following steps:

Open a browser and navigate to the Azure portal at: https://portal.azure.com/

Login with your administrator credentials.

Open Cloud Shell in the top right menu, and add the following lines of code to register the Microsoft.HybridCompute and the Microsoft.GuestConfiguration resource providers:

Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute

Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration

This will result in the following output:

```
Azure:/
PS Azure:\> Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute

ProviderNamespace : Microsoft.HybridCompute
RegistrationState : Registering
ResourceTypes     : {machines, operations}
Locations         : {West US 2, West Europe, Southeast Asia}


Azure:/
PS Azure:\> Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration

ProviderNamespace : Microsoft.GuestConfiguration
RegistrationState : Registering
ResourceTypes     : {guestConfigurationAssignments, software, softwareUpdates, softwareUpdateProfile…}
Locations         : {East US 2, South Central US}
```

Note that the resource providers are only registered in specific locations.

(Networking

During installation and runtime, the agent requires connectivity to Azure Arc service endpoints. If outbound connectivity is blocked by the firewall, make sure that the following URLs are not blocked:

Required Azure service endpoints include:

Guest Configuration)

Incorrect:

Not A, Not B: Connect the on-premises machine to Azure Arc

To connect the on-premises machine to Azure Arc, we first need install the agent on the on-premises machine (not any Gateways).

Not E: Azure Bastion now supports connectivity to Azure virtual machines or on-premises resources via specified IP address.

Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.

Reference:

https://techcommunity.microsoft.com/t5/azure-developer-community-blog/azure-arc-for-servers-getting-started/ba-p/1262062

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/guest-configuration

Community vote distribution

CD (100%)

Question #29 *Topic 3*

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

Correct Answer: *D*
Microsoft Sentinel is a scalable, cloud-native solution that provides:
Security information and event management (SIEM)
Security orchestration, automation, and response (SOAR)
Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.
Microsoft Sentinel is your bird's-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.
Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
Respond to incidents rapidly with built-in orchestration and automation of common tasks.
Microsoft Sentinel natively incorporates proven Azure services, like Log Analytics and Logic Apps. Microsoft Sentinel enriches your investigation and detection with AI. It provides Microsoft's threat intelligence stream and enables you to bring your own threat intelligence.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/overview

Community vote distribution

D (100%)

Question #30 *Topic 3*

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

Correct Answer:

Answer Area

Infrastructure scanning [▼] Build and test

Static application security testing [▼] Commit the code

Question #31 *Topic 3*

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.

Correct Answer: *ACE*

Community vote distribution

ACE (70%) ABE (30%)

Question #32 *Topic 3*

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

Correct Answer: *A*

Community vote distribution

A (56%) C (44%)

Question #33 *Topic 3*

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

Correct Answer: *C*

Community vote distribution

C (88%) 12%

Question #34 *Topic 3*

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

Correct Answer: *A*

Community vote distribution

A (92%) 8%

Question #35 *Topic 3*

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

Correct Answer: *B*

Community vote distribution

B (100%)

Question #36 *Topic 3*

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

Correct Answer: *B*

Community vote distribution

B (100%)

Question #37 *Topic 3*

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

Correct Answer: *D*

Community vote distribution

D (100%)

Question #38 *Topic 3*

HOTSPOT
-

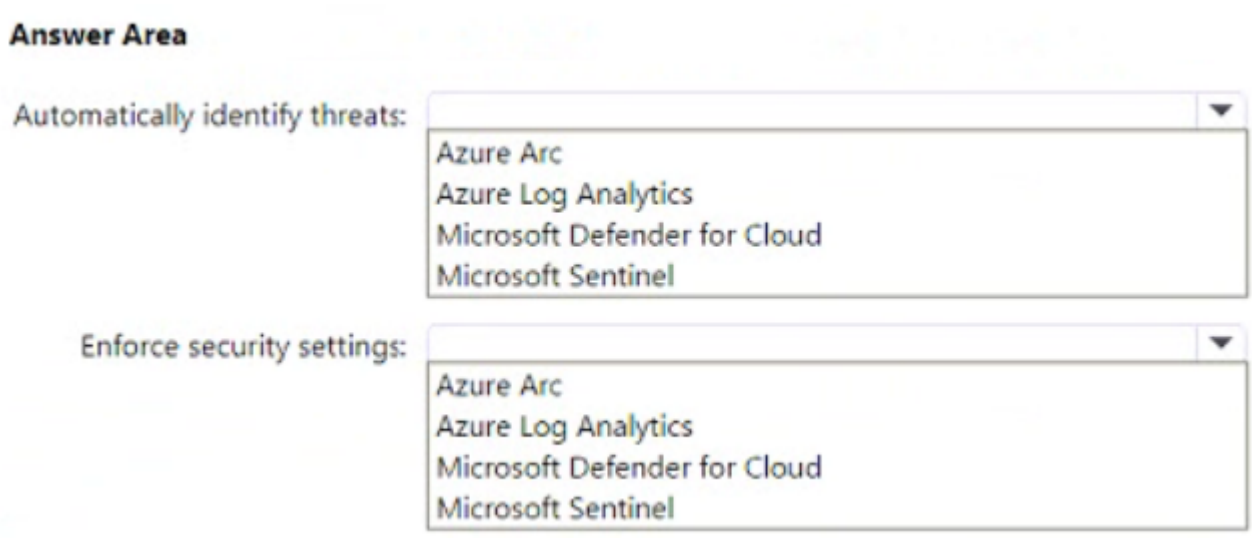
You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.

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

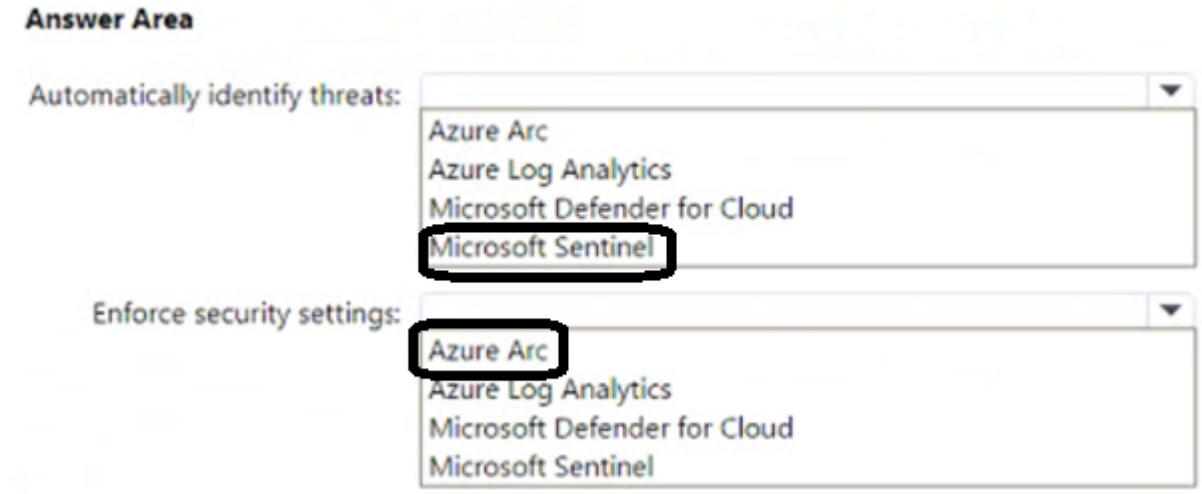
• Automatically identify threats found in AWS CloudTrail events.
• Enforce security settings on AWS virtual machines by using Azure policies.

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.



Correct Answer:



Question #39 *Topic 3*

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)

Correct Answer: *A*

Community vote distribution

A (100%)

Topic 4 - Question Set 4

Question #1 *Topic 4*

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

Correct Answer: *B*
Microsoft Defender for Cloud Apps OAuth app policies.
OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and
Salesforce. You're also able to mark these permissions as approved or banned. Marking them as banned will revoke permissions for each app for each user who authorized it.
Incorrect:
Not D: Windows Defender Application cannot be used for virtual machines.
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

Community vote distribution

D (92%) 8%

Question #2 *Topic 4*

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)

Correct Answer: *C*
Configure Azure Storage firewalls and virtual networks.
To secure your storage account, you should first configure a rule to deny access to traffic from all networks (including internet traffic) on the public endpoint, by default. Then, you should configure rules that grant access to traffic from specific VNets. You can also configure rules to grant access to traffic from selected public internet IP address ranges, enabling connections from specific internet or on-premises clients. This configuration enables you to build a secure network boundary for your applications.
Storage firewall rules apply to the public endpoint of a storage account. You don't need any firewall access rules to allow traffic for private endpoints of a storage account. The process of approving the creation of a private endpoint grants implicit access to traffic from the subnet that hosts the private endpoint.
Incorrect:
Not B: You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.
Not E: A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

Community vote distribution

C (100%)

Question #3 *Topic 4*

Your company is developing a modern application that will un as an Azure App Service web app.
You plan to perform threat modeling to identity potential security issues by using the Microsoft Threat Modeling Tool.
Which type of diagram should you create?

A. system flow

B. data flow

C. process flow

D. network flow

Correct Answer: *C*
Process flow diagrams are the result of a maturing threat modeling discipline. They genuinely allow incorporation of developers in the threat modeling process during the application design phase. This helps developers working within an Agile development methodology initially write secure code.
Application threat models use process-flow diagrams, representing the architectural point of view. Operational threat models are created from an attacker point of view based on DFDs. This approach allows for the integration of VAST into the organization's development and DevOps lifecycles.
Incorrect:
Not B: Data-flow diagrams are graphical representations of your system and should specify each element, their interactions and helpful context. Data-flow diagrams are made up of shapes that create graphical representations of your system. Each shape represents a unique function. Each interaction is analyzed to help you identify potential threats and ways to reduce risk.
Using shapes correctly allows you to receive better input from colleagues and security teams. Everyone will then understand how the system works. It can also help them avoid going through countless design documents and development plans to get them up and running.
Reference:
https://threatmodeler.com/data-flow-diagrams-process-flow-diagrams/ https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/1b-elements

Community vote distribution

B (93%) 7%

Question #4 *Topic 4*

Your company has an on-premises network and an Azure subscription.
The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.
You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.
You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet- accessible endpoints to the on-premises network.
What should you include in the recommendation?

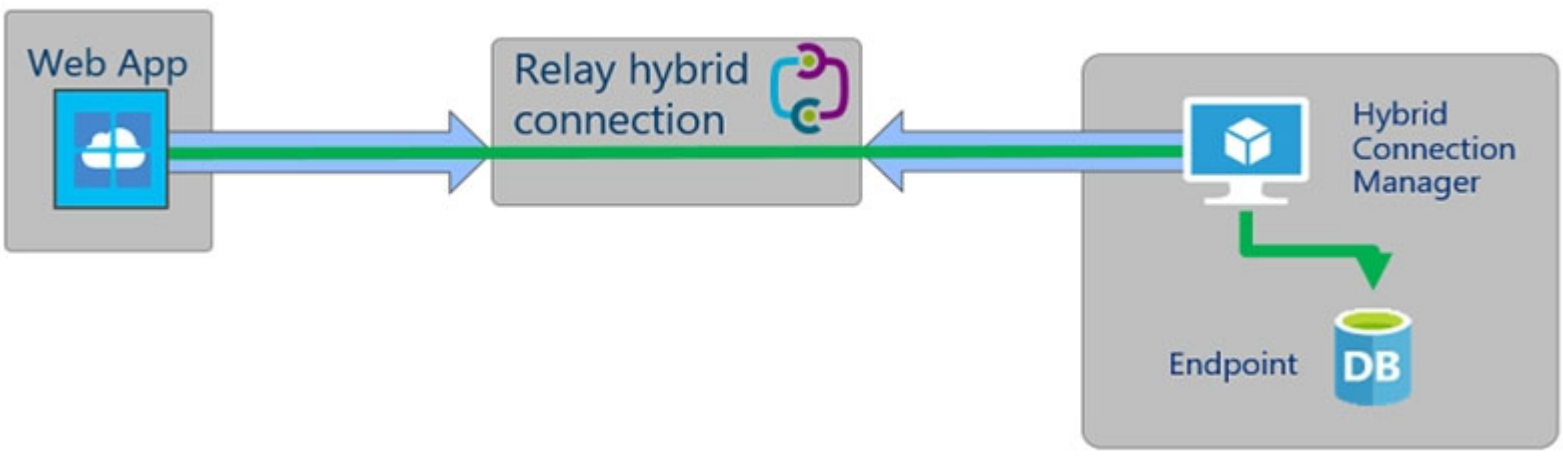
A. virtual network NAT gateway integration

B. hybrid connections

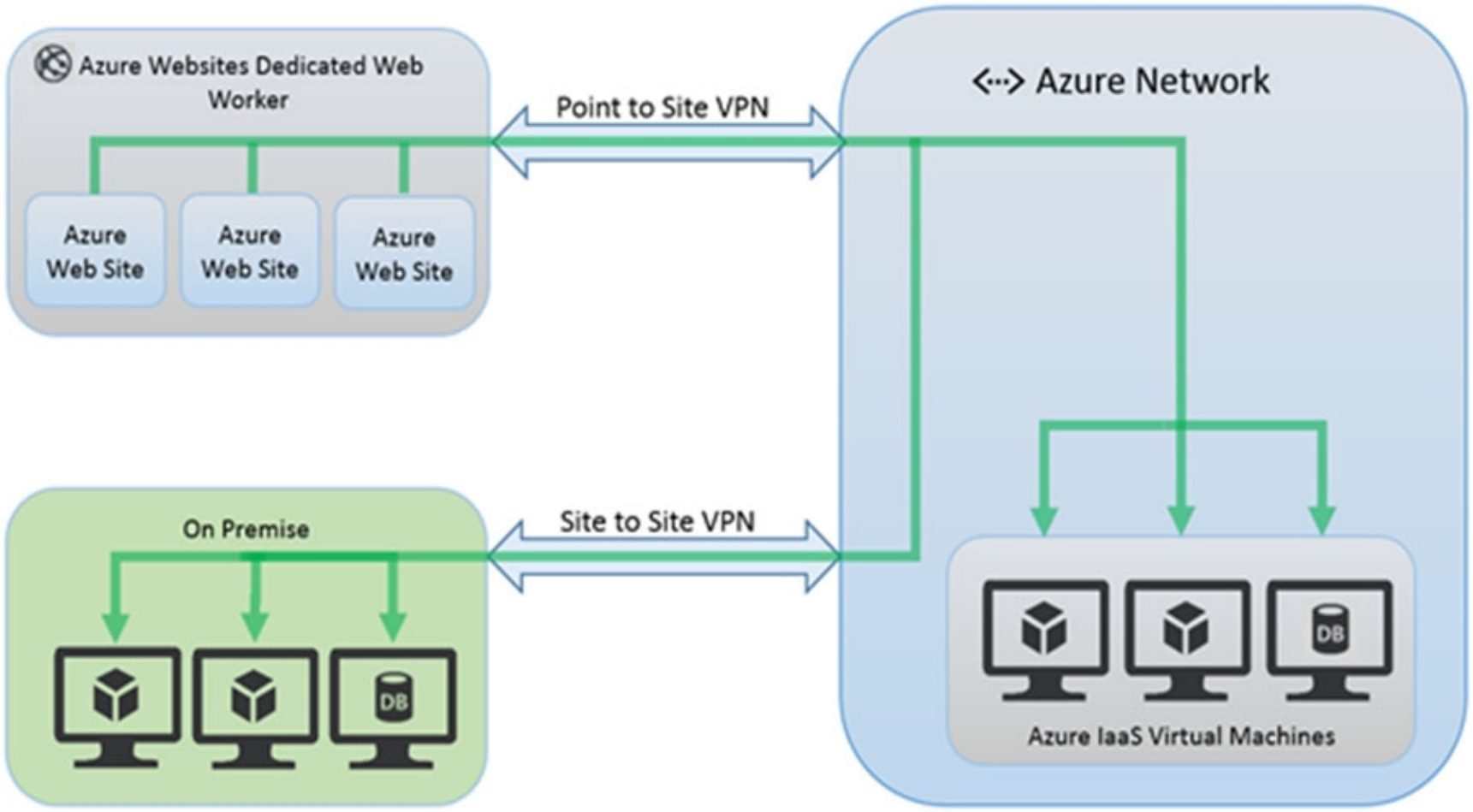
C. virtual network integration

D. a private endpoint

Correct Answer: *B*
Hybrid Connections can connect Azure App Service Web Apps to on-premises resources that use a static TCP port. Supported resources include Microsoft SQL
Server, MySQL, HTTP Web APIs, Mobile Services, and most custom Web Services.



Note: You can use an Azure App Service Hybrid Connections. To do this, you need to add and create Hybrid Connections in your app. You will download and install an agent (the Hybrid Connection Manager) in the database server or another server which is in the same network as the on-premise database.
You configure a logical connection on your app service or web app.
A small agent, the Hybrid Connection Manager, is downloaded and installed on a Windows Server (2012 or later) running in the remote network (on-premises or anywhere) that you need to communicate with.
You log into your Azure subscription in the Hybrid Connection manager and select the logical connection in your app service.
The Hybrid Connection Manager will initiate a secure tunnel out (TCP 80/443) to your app service in Azure.
Your app service can now communicate with TCP-based services, on Windows or Linux, in the remote network via the Hybrid Connection Manager.
You could get more details on how to Connect Azure Web Apps To On-Premises.
Incorrect:
Not A: NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway specifies which static IP addresses virtual machines use when creating outbound flows.
However, we need an inbound connection.
Not C: You can Azure web app service VNet integration with Azure VPN gateway to securely access the resource in an Azure VNet or on-premise network.
However, this would require a Site to Site VPN as in the picture below.



Note: Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network. The virtual network integration feature behaves differently when it's used with virtual networks in the same region and with virtual networks in other regions. The virtual network integration feature has two variations:

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

Reference:

https://github.com/uglide/azure-content/blob/master/articles/app-service-web/web-sites-hybrid-connection-connect-on-premises-sql-server.md https://docs.microsoft.com/en-us/answers/questions/701793/connecting-to-azure-app-to-onprem-datbase.html

Community vote distribution

B (88%) 13%

Question #5 *Topic 4*

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).
You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment.
What should you include during the application design phase?

A. software decomposition by using Microsoft Visual Studio Enterprise

B. dynamic application security testing (DAST) by using Veracode

C. threat modeling by using the Microsoft Threat Modeling Tool

D. static application security testing (SAST) by using SonarQube

Correct Answer: *C*
Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It's an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.
Incorrect:
Not B: Advantages of Veracode's DAST test solution
With a blackbox test tool from Veracode, you can:
Simulate the actions of an actual attacker to discover vulnerabilities not found by other testing techniques.
Run tests on applications developed in any language ג€" JAVA/JSP, PHP and other engine-driven web applications.
Provide development and QA teams with a report on critical vulnerabilities along with information that lets them recreate the flaws.
Fix issues more quickly with detailed remediation information.
Develop long-term strategies for improving application security across your software portfolio using guidance and proactive recommendations from Veracode's expert.
Not D: SonarQube is a leading automatic code review tool to detect bugs, vulnerabilities and code smells in your code. Using Static Application Security Testing
(SAST) you can do an analysis of vulnerabilities in your code, also known as white-box testing to find about 50% of likely issues.
Reference:
https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Community vote distribution

C (100%)

Question #6 *Topic 4*

DRAG DROP -

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

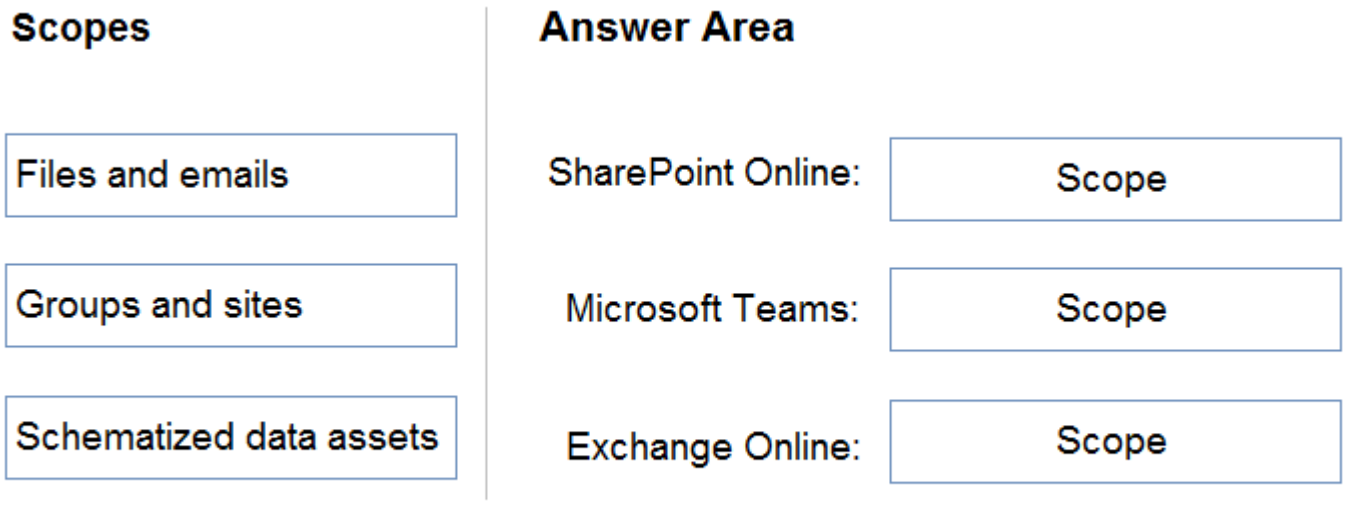
- Microsoft SharePoint Online
- Microsoft Exchange Online
- Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

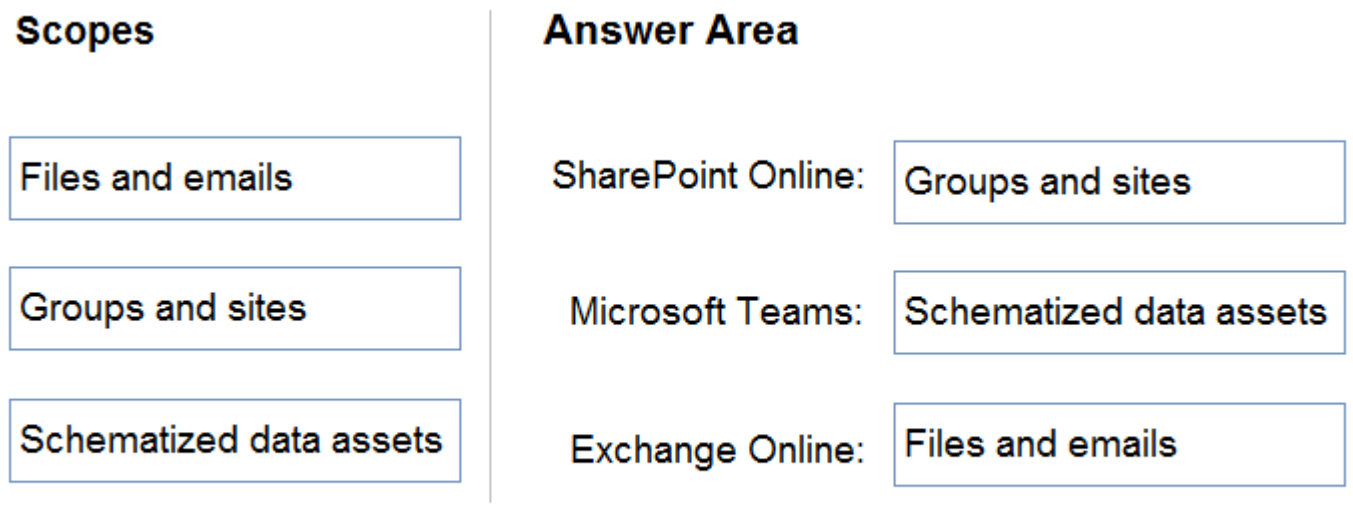
Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may only be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Groups and sites -

SharePoint online handles sites.

Azure Active Directory (Azure AD) supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups. Sensitivity labels apply to group across services like Outlook, Microsoft Teams, and SharePoint.

Box 2: Schematized data assets -

Label travels with the data: The sensitivity labels created in Microsoft Purview Information Protection can also be extended to the Microsoft Purview Data Map,

SharePoint, Teams, Power BI, and SQL. When you apply a label on an office document and then scan it into the Microsoft Purview Data Map, the label will be applied to the data asset.

After you enable and configure sensitivity labels for containers, users can additionally see and apply sensitivity labels to Microsoft team sites, Microsoft 365 groups, and SharePoint sites.

Box 3: Files and emails -

Exchange Online handles files and emails.

Reference:
https://docs.microsoft.com/en-us/azure/purview/create-sensitivity-label https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

Question #7 *Topic 4*

Your company is developing a new Azure App Service web app.
You are providing design assistance to verify the security of the web app.
You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection.
What should you include in the recommendation?

A. dynamic application security testing (DAST)

B. static application security testing (SAST)

C. interactive application security testing (IAST)

D. runtime application self-protection (RASP)

Correct Answer: *A*
Dynamic application security testing (DAST) is a process of testing an application in an operating state to find security vulnerabilities. DAST tools analyze programs while they are executing to find security vulnerabilities such as memory corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.
Incorrect:
Not B: SAST tools analyze source code or compiled versions of code when the code is not executing in order to find security flaws.
Not C: IAST (interactive application security testing) analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity ג€interactingג€ with the application functionality.
IAST works inside the application, which makes it different from both static analysis (SAST) and dynamic analysis (DAST). This type of testing also doesn't test the entire application or codebase, but only whatever is exercised by the functional test.
Not D: Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application's internal data and state to enable it to identify threats at runtime that may have otherwise been overlooked by other security solutions.
RASP's focused monitoring makes it capable of detecting a wide range of threats, including zero-day attacks. Since RASP has insight into the internals of an application, it can detect behavioral changes that may have been caused by a novel attack. This enables it to respond to even zero-day attacks based upon how they affect the target application.
Reference:
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

Community vote distribution

A (92%) 8%

Question #8 *Topic 4*

Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD).
You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications.
What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps

B. sign-in risk policies in Azure AD Identity Protection

C. Azure AD Conditional Access policies

D. device compliance policies in Microsoft Endpoint Manager

E. user risk poticies in Azure AD Identity Protection

Correct Answer: *A*
Microsoft Defender for Cloud Apps Activity policies.
Activity policies allow you to enforce a wide range of automated processes using the app provider's APIs. These policies enable you to monitor specific activities carried out by various users, or follow unexpectedly high rates of one certain type of activity.
After you set an activity detection policy, it starts to generate alerts - alerts are only generated on activities that occur after you create the policy.
Each policy is composed of the following parts:
Activity filters ג€" Enable you to create granular conditions based on metadata.
Activity match parameters ג€" Enable you to set a threshold for the number of times an activity repeats to be considered to match the policy.
Actions ג€" The policy provides a set of governance actions that can be automatically applied when violations are detected.
Incorrect:
Not C: Azure AD Conditional Access policies applies to users, not to applications.
Note: Blocking user logins by location can be an added layer of security to your environment. The following process will use Azure Active Directory conditional access to block access based on geographical location. For example, you are positive that nobody in your organization should be trying to login to select cloud applications from specific countries.
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/user-activity-policies https://cloudcompanyapps.com/2019/04/18/block-users-by-location-in-azure-o365/

Community vote distribution

C (94%) 6%

Question #9 *Topic 4*

Your company has an Azure subscription that uses Azure Storage.
The company plans to share specific blobs with vendors.
You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be time- limited.
What should you include in the recommendation?

A. Configure private link connections.

B. Configure encryption by using customer-managed keys (CMKs).

C. Share the connection string of the access key.

D. Create shared access signatures (SAS).

Correct Answer: *D*
A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:
What resources the client may access.
What permissions they have to those resources.
How long the SAS is valid.
Types of shared access signatures
Azure Storage supports three types of shared access signatures:

User delegation SAS -

Service SAS -

Account SAS -
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

Community vote distribution

D (94%) 6%

Question #10 *Topic 4*

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app.
You need to recommend a solution to the application development team to secure the application from identity-related attacks.
Which two configurations should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure AD workbooks to monitor risk detections

B. Azure AD Conditional Access integration with user flows and custom policies

C. smart account lockout in Azure AD B2C

D. access packages in Identity Governance

E. custom resource owner password credentials (ROPC) flows in Azure AD B2C

Correct Answer: *BD*
B: Add Conditional Access to user flows in Azure Active Directory B2C
Conditional Access can be added to your Azure Active Directory B2C (Azure AD B2C) user flows or custom policies to manage risky sign-ins to your applications.
Azure Active Directory (Azure AD) Conditional Access is the tool used by Azure AD B2C to bring signals together, make decisions, and enforce organizational policies.
Not C: Credential attacks lead to unauthorized access to resources. Passwords that are set by users are required to be reasonably complex. Azure AD B2C has mitigation techniques in place for credential attacks. Mitigation includes detection of brute-force credential attacks and dictionary credential attacks. By using various signals, Azure Active Directory B2C (Azure AD B2C) analyzes the integrity of requests. Azure AD B2C is designed to intelligently differentiate intended users from hackers and botnets.
Incorrect:
Not D: Identity Governance though useful, does not address this specific scenario: to secure the application from identity-related attack in an Azure AD B2C environment.
Note: Identity Governance gives organizations the ability to do the following tasks across employees, business partners and vendors, and across services and applications both on-premises and in clouds:

Govern the identity lifecycle -

Govern access lifecycle -
Secure privileged access for administration
Specifically, it is intended to help organizations address these four key questions:
Which users should have access to which resources?
What are those users doing with that access?
Are there effective organizational controls for managing access?
Can auditors verify that the controls are working?
Note: An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package.
Not E: In Azure Active Directory B2C (Azure AD B2C), the resource owner password credentials (ROPC) flow is an OAuth standard authentication flow. In this flow, an application, also known as the relying party, exchanges valid credentials for tokens. The credentials include a user ID and password.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

Community vote distribution

BC (100%)

Question #11 *Topic 4*

Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating.
The company identifies protected health information (PHI) within stored documents and communications.
What should you recommend using to prevent the PHI from being shared outside the company?

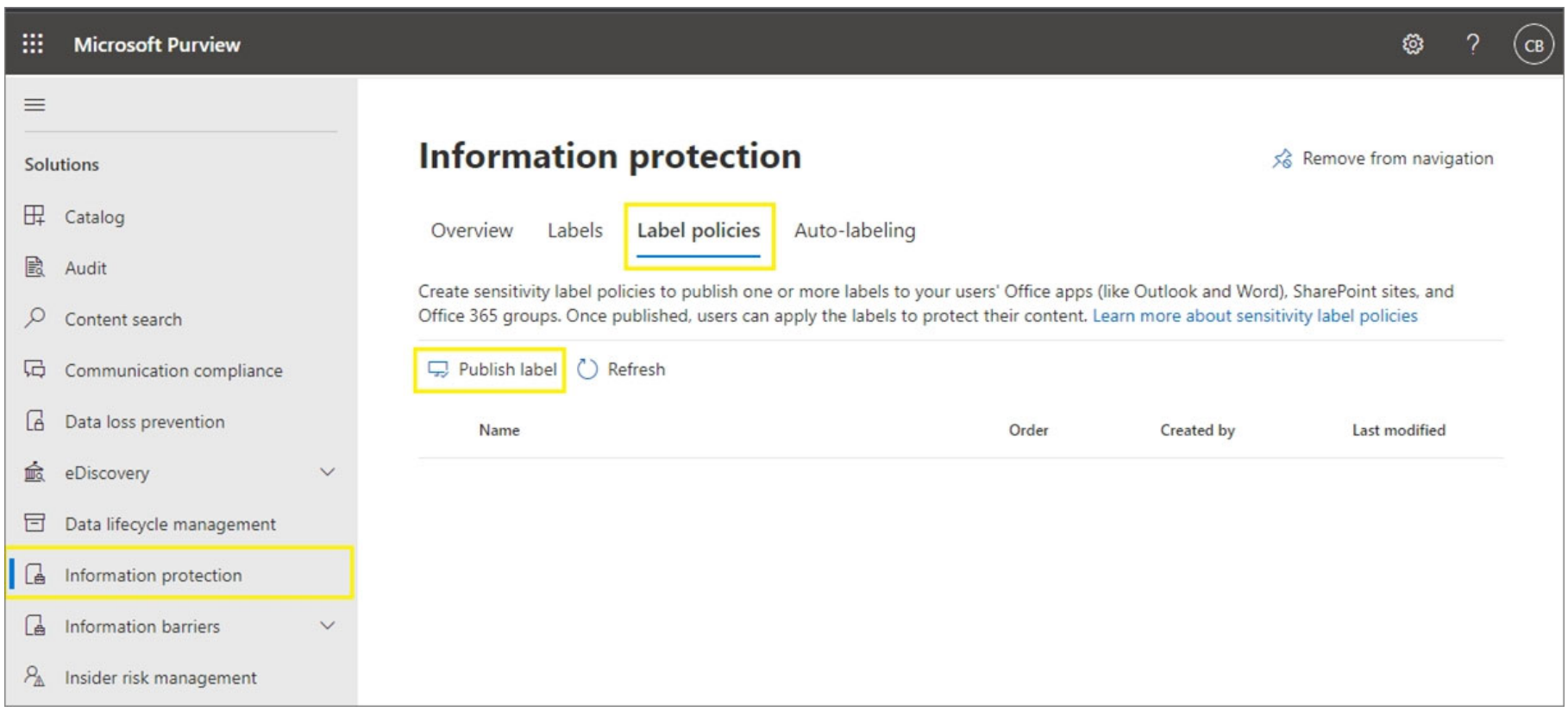
A. sensitivity label policies

B. data loss prevention (DLP) policies

C. insider risk management policies

D. retention policies

Correct Answer: *A*
What sensitivity labels can do -
After a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:
* Protect content in containers such as sites and groups when you enable the capability to use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and
SharePoint sites.
* Encrypt emails and documents to prevent unauthorized people from accessing this data. You can additionally choose which users or group have permissions to perform which actions and for how long. For example, you can choose to allow all users in your organization to modify a document while a specific group in another organization can only view it. Alternatively, instead of administrator-defined permissions, you can allow your users to assign permissions to the content when they apply the label.
* Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied. Watermarks can be applied to documents but not email.
* Etc.
Note: Publish sensitivity labels by creating a label policy
1. From the Microsoft Purview compliance portal, select Solutions > Information protection > Label policies
2. On the Label policies page, select Publish label to start the Create policy configuration:



3. On the Choose sensitivity labels to publish page, select the Choose sensitivity labels to publish link. Select the labels that you want to make available in apps and to services, and then select Add.
4. Etc.
Incorrect:
Not B: In this scenario the company itself has identified the sensitive information. This means that sensitive labels are enough, and there is no need for Data loss prevention (DLP) polices.
Note: With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.
Note: Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification with sensitivity and retention labels.
Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels https://docs.microsoft.com/en-us/security/compass/information-protection-and-storage-capabilities https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide#publish-sensitivity-labels-by-creating-a-label-policy

Community vote distribution

B (100%)

Question #12 *Topic 4*

Your company has a Microsoft 365 E5 subscription.
The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online.
You need to recommend a solution to identify documents that contain sensitive information.
What should you include in the recommendation?

A. data classification content explorer

B. data loss prevention (DLP)

C. eDiscovery

D. Information Governance

Correct Answer: *B*
Data loss prevention (DLP)
With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.
Note: Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification with sensitivity and retention labels.
Incorrect:
Not A: Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.
Reference:
https://docs.microsoft.com/en-us/security/compass/information-protection-and-storage-capabilities https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer

Community vote distribution

A (74%) B (26%)

Question #13 *Topic 4*

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 configuring gateway-required virtual network integration.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.
Incorrect:
Virtual Network (VNet) integration for an Azure service enables you to lock down access to the service to only your virtual network infrastructure. The VNet infrastructure also includes peered virtual networks and on-premises networks.
VNet integration provides Azure services the benefits of network isolation and can be accomplished by one or more of the following methods:
Deploying dedicated instances of the service into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
Using Private Endpoint that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your
VNet, effectively bringing the service into your virtual network.
Accessing the service using public endpoints by extending a virtual network to the service, through service endpoints. Service endpoints allow service resources to be secured to the virtual network.
Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services

Community vote distribution

B (100%)

Question #14 *Topic 4*

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

Correct Answer: *B*
Instead: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services

Community vote distribution
B (61%) A (39%)

Question #15 *Topic 4*

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

Correct Answer: *A*
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions

Community vote distribution
A (73%) B (27%)

Question #16 *Topic 4*

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription.
The company uses the following devices:
- Computers that run either Windows 10 or Windows 11
- Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored.
What should you include in the recommendation?

A. eDiscovery

B. Microsoft Information Protection

C. Compliance Manager

D. retention policies

Correct Answer: *B*
Protect your sensitive data with Microsoft Purview.
Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.
Note: You can use Microsoft Information Protection: Microsoft Purview for Auditing and Analytics in Outlook for iOS, Android, and Mac (DoD).
Incorrect:
Not A: Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft Purview to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365
Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use Microsoft
Purview eDiscovery (Standard) cases to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365
E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the feature-rich Microsoft Purview eDiscovery (Premium) solution in Microsoft 365.
Not C: What does compliance Manager do?
Compliance managers ensure that a business, its employees and its projects comply with all relevant regulations and specifications. This could include health and safety, environmental, legal or quality standards, as well as any ethical policies the company may have.
Not D: A retention policy (also called a 'schedule') is a key part of the lifecycle of a record. It describes how long a business needs to keep a piece of information
(record), where it's stored and how to dispose of the record when its time.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

Community vote distribution

B (100%)

Question #17 *Topic 4*

You have a Microsoft 365 E5 subscription.
You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.
You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.
Which two components should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies

B. retention label policies

C. eDiscovery cases

D. sensitivity label policies

Correct Answer: *AD*
A: Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.

D: Sensitivity labels -
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate.
Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities like
Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.
Incorrect:
Not B: Retention labels help you retain what you need and delete what you don't at the item level (document or email). They are also used to declare an item as a record as part of a records management solution for your Microsoft 365 data.
Not C: eDiscovery cases in eDiscovery (Standard) and eDiscovery (Premium) let you associate specific searches and exports with a specific investigation. You can also assign members to a case to control who can access the case and view the contents of the case. Place content locations on legal hold.
Reference:
https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/ https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

Community vote distribution

AD (100%)

Question #18 *Topic 4*

Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.

You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.

What should you include in the recommendation?

A. Use geo-redundant storage (GRS).

B. Maintain multiple copies of the virtual machines.

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

D. Require PINs to disable backups.

Correct Answer: *D*

Azure Backup -

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.

Authentication to perform critical operations

As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN when you perform Stop Protection with Delete data and Change Passphrase operations.

Reference:

https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature#prevent-attacks

Community vote distribution

D (93%) 7%

Question #19 *Topic 4*

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. OAuth app policies in Microsoft Defender for Cloud Apps

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

Correct Answer: *A*

Community vote distribution

A (78%) C (22%)

Question #20 *Topic 4*

HOTSPOT

-

You have a hybrid cloud infrastructure.

You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

Answer Area

Correct Answer:

App1:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

Question #21 *Topic 4*

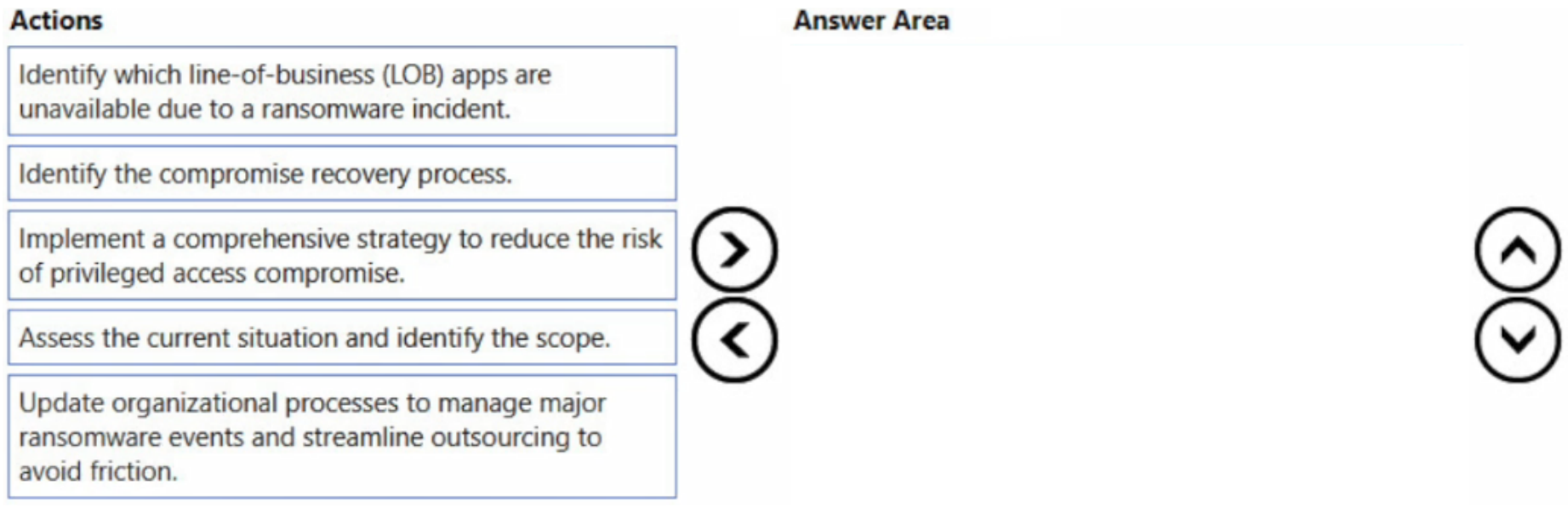
DRAG DROP

-

Your company wants to optimize ransomware incident investigations.

You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.

Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Correct Answer:

Answer Area

Assess the current situation and identify the scope.

Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.

Identify the compromise recovery process.

Question #22 *Topic 4*

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

A. From Microsoft Defender for Endpoint, perform a security scan.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. Disable Microsoft OneDrive sync and Exchange ActiveSync.

Correct Answer: *D*

Community vote distribution

D (92%) 8%

Question #23 *Topic 4*

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. OAuth app policies in Microsoft Defender for Cloud Apps

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. application control policies in Microsoft Defender for Endpoint

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

Correct Answer: *A*

Community vote distribution

C (92%) 8%

Question #24 *Topic 4*

Your company is developing an invoicing application that will use Azure AD B2C. The application will be deployed as an App Service web app.

You need to recommend a solution to the application development team to secure the application from identity-related attacks.

Which two configurations should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies

B. smart account lockout in Azure AD B2C

C. access packages in Identity Governance

D. custom resource owner password credentials (ROPC) flows in Azure AD B2C

Correct Answer: *AB*

Community vote distribution

AB (100%)

Question #25 *Topic 4*

Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

What should you recommend?

A. Compliance Manager in Microsoft Purview

B. Microsoft Defender for Cloud

C. Microsoft Sentinel

D. Microsoft Defender for Cloud Apps

Correct Answer: *D*

Community vote distribution

B (71%) A (18%) 12%

Question #26 *Topic 4*

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 AD Conditional Access App Control policies

C. adaptive application controls in Defender for Cloud

D. app protection policies in Microsoft Endpoint Manager

Correct Answer: *C*

Community vote distribution

C (100%)

Question #27 *Topic 4*

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. Azure AD Conditional Access App Control policies

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app protection policies in Microsoft Endpoint Manager

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: *D*

Community vote distribution

D (100%)

Question #28 *Topic 4*

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. application control policies in Microsoft Defender for Endpoint

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

D. Azure AD Conditional Access App Control policies

Correct Answer: *B*

Community vote distribution

B (100%)

Question #29 *Topic 4*

You have a Microsoft 365 subscription.

You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

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

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. Azure Data Catalog

C. Microsoft Purview Information Protection

D. Azure AD Application Proxy

E. Microsoft Defender for Cloud Apps

Correct Answer: *AE*

Community vote distribution

AE (82%) CE (18%)

Question #30 *Topic 4*

HOTSPOT
-

You have an Azure SQL database named DB1 that contains customer information.

A team of database administrators has full access to DB1.

To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information.

You need to design a security strategy for DB1. The solution must meet the following requirement:

• When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the CreditCard attribute of each customer record.
• When the operators view customer records in App1, they must view only the last four digits of the CreditCard attribute.

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

NOTE: Each correct selection is worth one point.

Answer Area

For the database administrators: ▼
- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators: ▼
- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

Answer Area

Correct Answer:

For the database administrators: ▼
- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators: ▼
- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

Question #31 *Topic 4*

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials.

You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. Azure AD B2C

C. an Azure AD enterprise application

D. a relying party trust in Active Directory Federation Services (AD FS)

Correct Answer: *A*

Community vote distribution

C (100%)

Question #32 *Topic 4*

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant.

You need to design a security strategy to meet the following requirements:

• Users must be able to request access to App1 by using a self-service request.
• When users request access to App1, they must be prompted to provide additional information about their request.
• Every three months, managers must verify that the users still require access to App1.

What should you include in the design?

A. Microsoft Entra Identity Governance

B. connected apps in Microsoft Defender for Cloud Apps

C. access policies in Microsoft Defender for Cloud Apps

D. Azure AD Application Proxy

Correct Answer: *A*

Community vote distribution

A (100%)

Question #33 *Topic 4*

You have an Azure subscription.

You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar.

Developers use Azure DevOps to deploy web apps to App Service Environments. When a new app is deployed, a CNAME record for the app is registered in contoso.com.

You need to recommend a solution to secure the DNS record for each web app. The solution must meet the following requirements:

• Ensure that when an app is deleted, the CNAME record for the app is removed also.
• Minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for DevOps

C. Microsoft Defender for App Service

D. Microsoft Defender for DNS

Correct Answer: *C*

Community vote distribution

C (100%)

Question #34 *Topic 4*

HOTSPOT
-

You have an on-premises datacenter named Site1.

You have an Azure subscription that contains a virtual network named VNet1 and multiple Azure App Service apps. Site1 is connected to VNet1 by using a Site-to-Site (P2S) VPN connection. The apps are accessed by using public internet connections.

You need to recommend a solution for providing secure access to the apps. The solution must meet the following requirements:

- Servers on Site1 must use a VPN connection to access the apps.
- Access to the apps must be restricted to specific servers on Site1.
- Security administrators for VNet1 must be able to control which servers can access the apps.
- Costs 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

Correct Answer:

Answer Area

Question #35 *Topic 4*

DRAG DROP
-

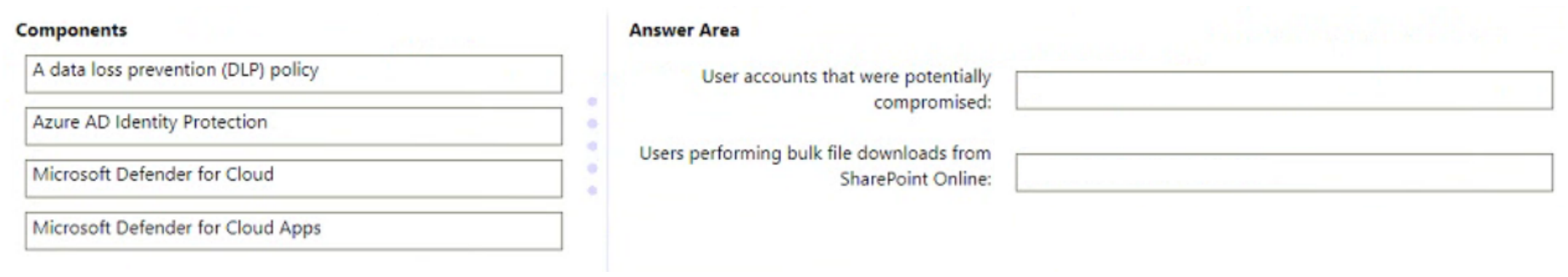
You have a Microsoft 365 subscription.

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.



Correct Answer:

Question #36 *Topic 4*

HOTSPOT
-

You plan to automate the development and deployment of a Node.js-based app by using GitHub.

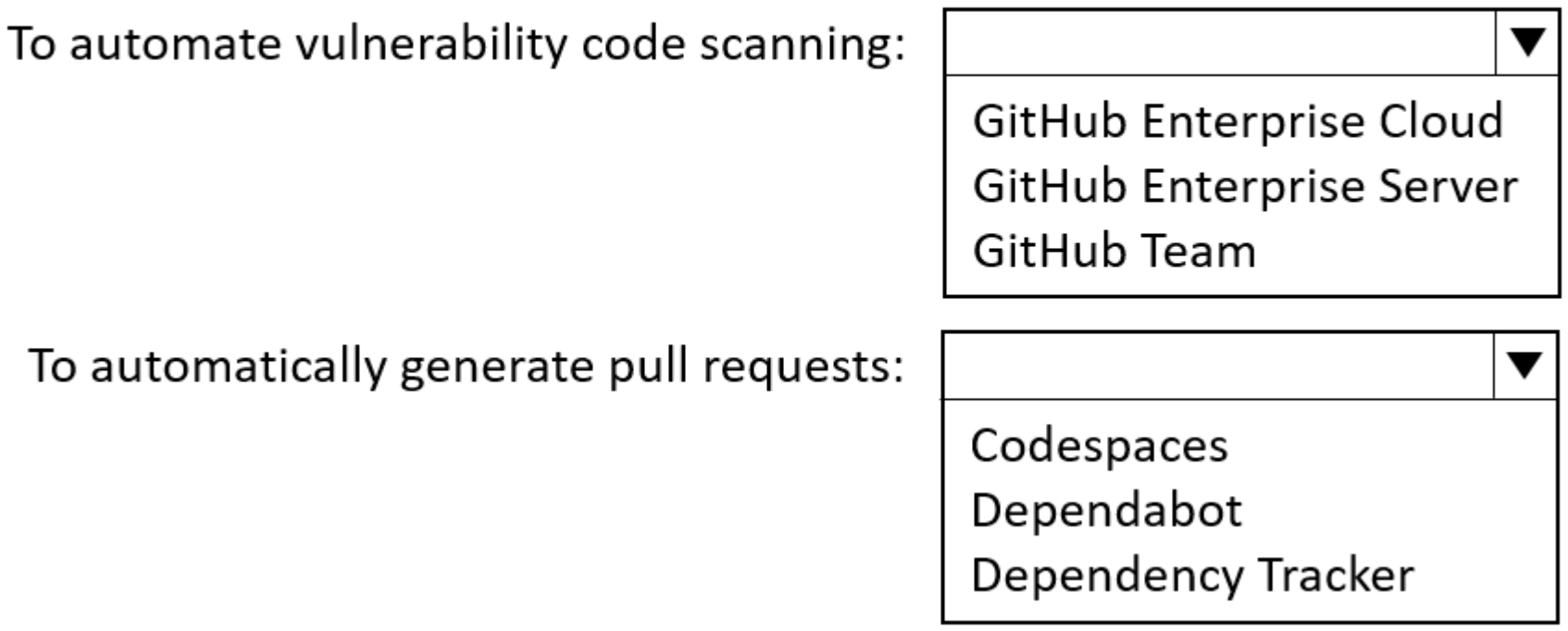
You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

- Automate the generation of pull requests that remediate identified vulnerabilities.
- Automate vulnerability code scanning for public and private repositories.
- Minimize administrative effort.
- Minimize costs.

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

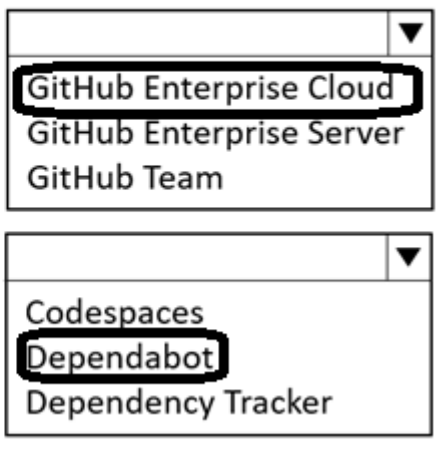
NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Correct Answer:



Topic 5 - Question Set 5

Question #1 *Topic 5*

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices.

You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

A. controlled folder access

B. application isolation

C. memory scanning

D. machine isolation

E. user isolation

Correct Answer: *D*

Community vote distribution

D (86%) 14%

Question #2 *Topic 5*

You have an operational model based on the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, databases, files, and storage accounts.

What should you include in the recommendation?

A. business resilience

B. modem access control

C. network isolation

D. security baselines in the Microsoft Cloud Security Benchmark

Correct Answer: *D*

Community vote distribution

D (100%)

Question #3 *Topic 5*

HOTSPOT
-

You use Azure Policy with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows.

You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.

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

NOTE: Each correct selection is worth one point.

Answer Area

Git workflow: [▼]
- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Secure deployment credentials: [▼]
- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Correct Answer:

Answer Area

Git workflow: [▼]
- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Secure deployment credentials: [▼]
- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Question #4 *Topic 5*

HOTSPOT
-

Your company wants to optimize using Azure to protect its resources from ransomware.

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure Backup:
- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Azure Storage:
- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Correct Answer:

Answer Area

Azure Backup:
- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Azure Storage:
- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Question #5 *Topic 5*

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

You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised administrator account cannot be used to delete the backups.

What should you do?

A. From Azure Backup, configure multi-user authorization by using Resource Guard.

B. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.

C. From a Recovery Services vault, generate a security PIN for critical operations.

D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

Correct Answer: *C*

Community vote distribution

A (51%) C (49%)

Question #6 *Topic 5*

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

You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out.

What should you include in the recommendation?

A. device compliance policies

B. Privileged Access Workstations (PAWs)

C. Customer Lockbox for Microsoft Azure

D. emergency access accounts

Correct Answer: *B*

Community vote distribution

B (100%)

Question #7 *Topic 5*

You design cloud-based software as a service (SaaS) solutions.

You need to recommend a recovery solution for ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend doing first?

A. Develop a privileged identity strategy.

B. Implement data protection.

C. Develop a privileged access strategy.

D. Prepare a recovery plan.

Correct Answer: *D*

Community vote distribution

D (79%) 14% 7%

Question #8 *Topic 5*

HOTSPOT
-

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.

During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Threat modeling: [Build and test / Commit the code / Go to production / Operate / Plan and develop]

Actionable intelligence: [Build and test / Commit the code / Go to production / Operate / Plan and develop]

Dynamic application security testing (DAST): [Build and test / Commit the code / Go to production / Operate / Plan and develop]

Answer Area

Correct Answer:

Threat modeling: Plan and develop

Actionable intelligence: Operate

Dynamic application security testing (DAST): Build and test

Question #9 *Topic 5*

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. unit testing

B. penetration testing

C. dependency checks

D. threat modeling

Correct Answer: *B*

Community vote distribution

B (100%)

Question #10 *Topic 5*

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online, SharePoint Online, and Teams in near-real-time (NRT) in response to the following Azure AD events:

• A user account is disabled or deleted.
• The password of a user is changed or reset.
• All the refresh tokens for a user are revoked.
• Multi-factor authentication (MFA) is enabled for a user.

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

NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. Azure AD Application Proxy

C. a sign-in risk policy

D. Azure AD Privileged Identity Management (PIM)

E. Conditional Access

Correct Answer: *AE*

Community vote distribution

AE (82%) AD (18%)

Question #11 *Topic 5*

HOTSPOT
-

You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

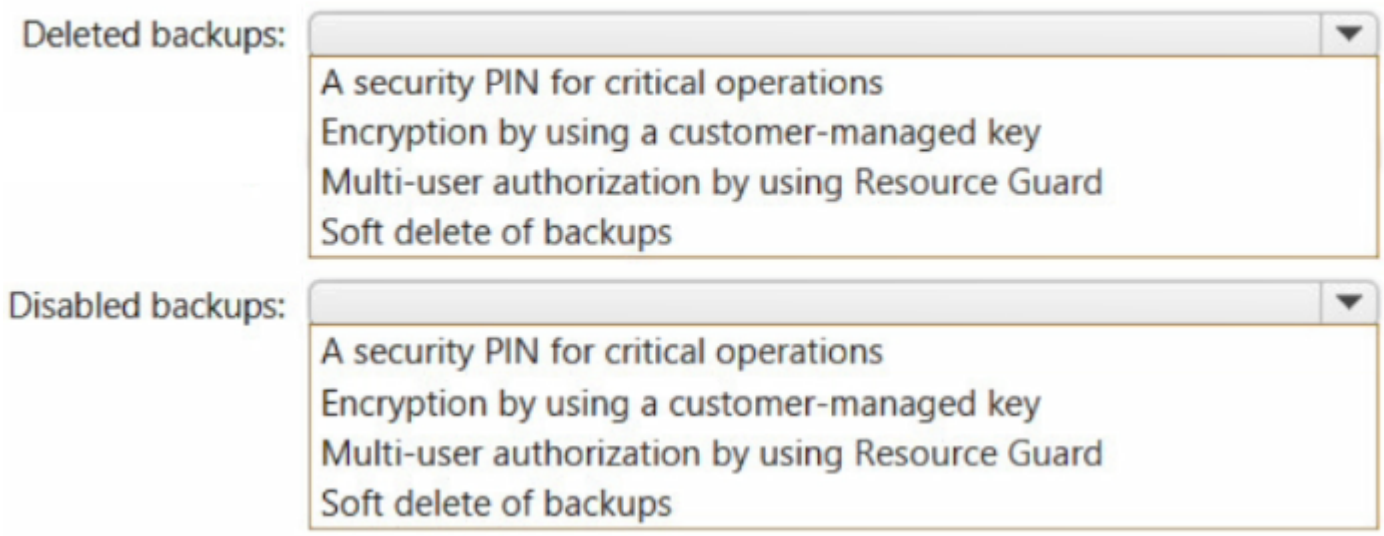
You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

• A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
• A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

What should you use for each risk? To answer, select the appropriate options in the answer area.

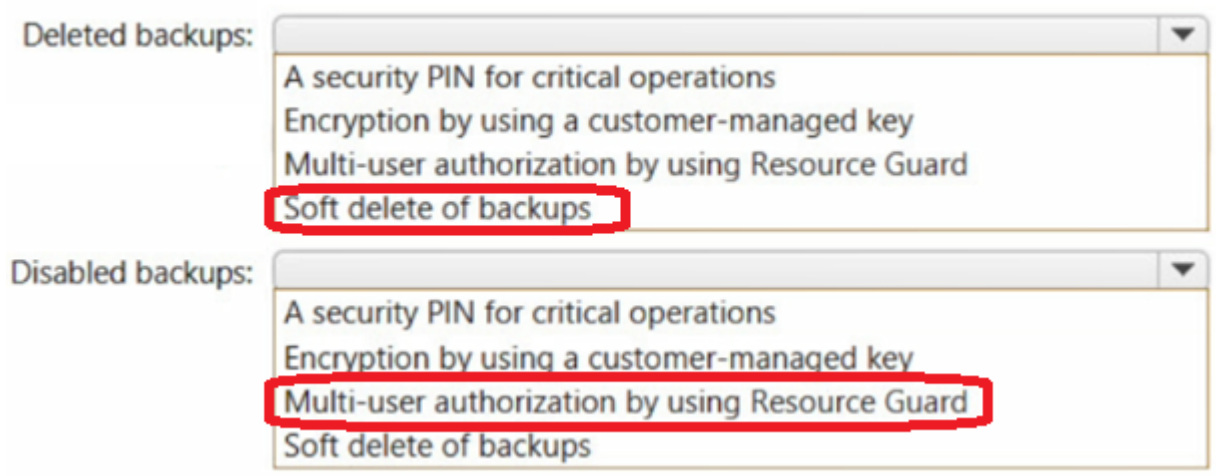
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Topic 6 - Testlet 1

Question #1 *Topic 6*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

Implement leaked credential detection in the Azure AD tenant of Litware.

Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:

- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units

Requirements. Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.

Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.

▪

Use the principle of least privilege.

Requirements. Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

Provide a secure score scoped to the landing zone.

Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

Minimize the possibility of data exfiltration.

Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

Be created in a dedicated subscription.

Use a DNS namespace of litware.com.

Requirements. Application Security Requirements

Litware identifies the following application security requirements:

Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question

HOTSPOT -

You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements.

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

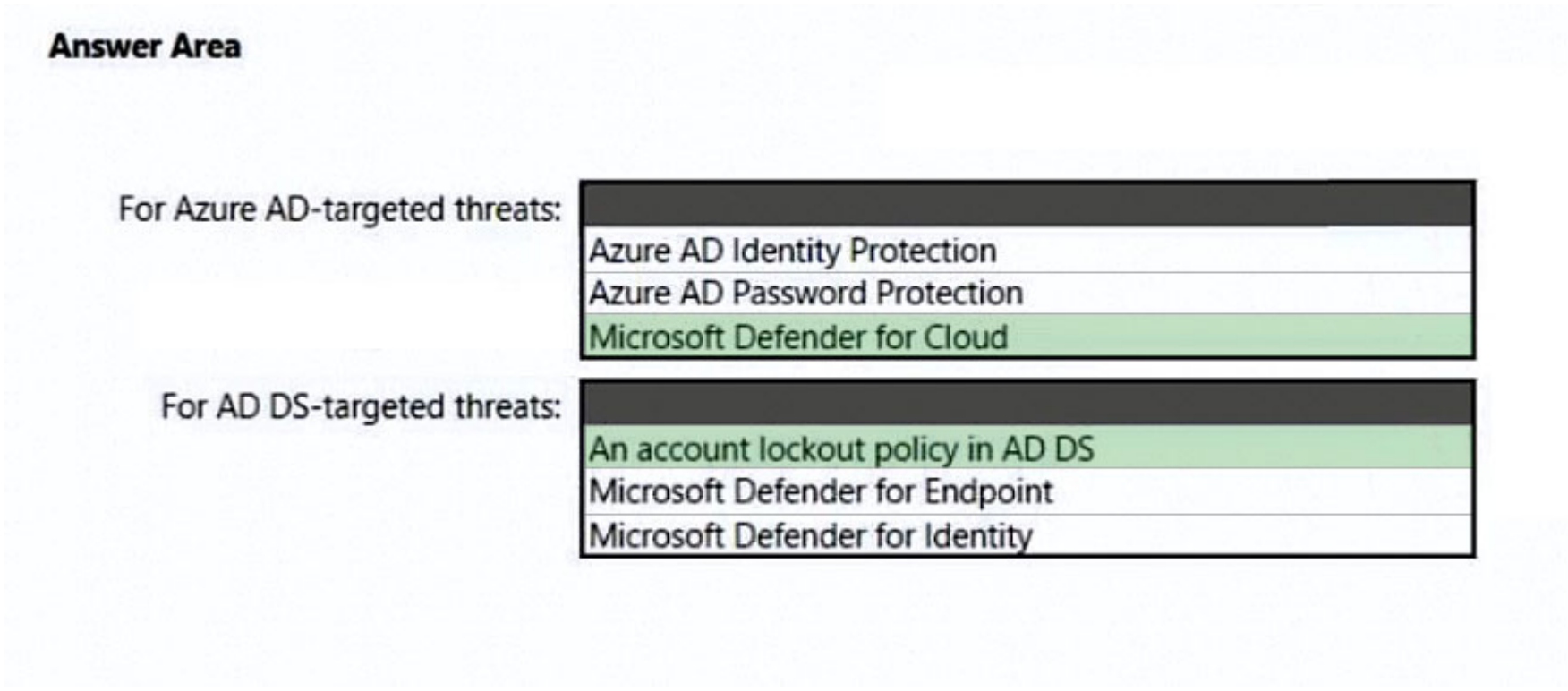
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

For Azure AD-targeted threats:	Azure AD Identity Protection Azure AD Password Protection Microsoft Defender for Cloud
For AD DS-targeted threats:	An account lockout policy in AD DS Microsoft Defender for Endpoint Microsoft Defender for Identity

Correct Answer:



Box 1: Microsoft defender for cloud

Scenario: Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

When Microsoft Defender for Cloud detects a Brute-force attack, it triggers an alert to bring you awareness that a brute force attack took place. The automation uses this alert as a trigger to block the traffic of the IP by creating a security rule in the NSG attached to the VM to deny inbound traffic from the IP addresses attached to the alert. In the alerts of this type, you can find the attacking IP address appearing in the 'entities' field of the alert.

Box 2: An account lockout policy in AD DS

Scenario:

Detect brute force attacks that directly target AD DS user accounts.

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

Verify on-premises account lockout policy

To verify your on-premises AD DS account lockout policy, complete the following steps from a domain-joined system with administrator privileges:

1. Open the Group Policy Management tool.
2. Edit the group policy that includes your organization's account lockout policy, such as, the Default Domain Policy.
3. Browse to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.
4. Verify your Account lockout threshold and Reset account lockout counter after values.

Reference:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/automation-to-block-brute-force-attacked-ip-detected-by/ba-p/1616825

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#verify-on-premises-account-lockout-policy

Question #2 *Topic 6*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question

HOTSPOT -
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Segment Microsoft Sentinel workspaces by:	Azure AD tenant Enterprise Region and Azure AD tenant
Integrate Azure subscriptions by using:	Self-service sign-up user flows for Azure AD B2B Self-service sign-up user flows for Azure AD B2C The Azure Lighthouse subscription onboarding process

Correct Answer:

Answer Area

Segment Microsoft Sentinel workspaces by:	Azure AD tenant Enterprise Region and Azure AD tenant
Integrate Azure subscriptions by using:	Self-service sign-up user flows for Azure AD B2B Self-service sign-up user flows for Azure AD B2C The Azure Lighthouse subscription onboarding process

Box 1: Azure tenant -

Microsoft Sentinel multiple workspace architecture

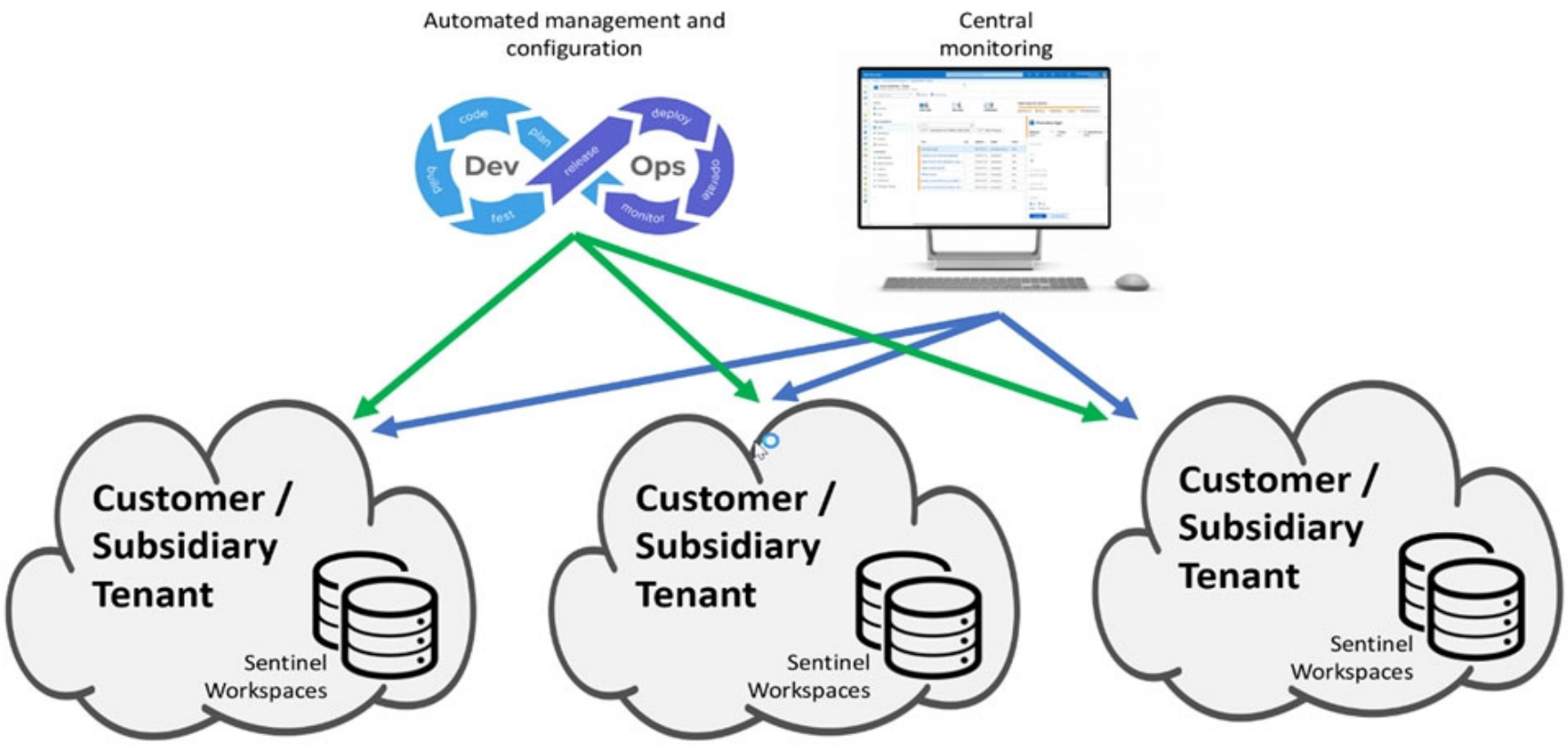
There are cases where a single SOC (Security Operations Center) needs to centrally manage and monitor multiple Microsoft Sentinel workspaces, potentially across Azure Active Directory (Azure AD) tenants.

An MSSP Microsoft Sentinel Service.

A global SOC serving multiple subsidiaries, each having its own local SOC.

A SOC monitoring multiple Azure AD tenants within an organization.

To address these cases, Microsoft Sentinel offers multiple-workspace capabilities that enable central monitoring, configuration, and management, providing a single pane of glass across everything covered by the SOC. This diagram shows an example architecture for such use cases.



This model offers significant advantages over a fully centralized model in which all data is copied to a single workspace.

Scenario:

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Hybrid Requirements -

Litware identifies the following hybrid cloud requirements:

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Box 2: Azure Lighthouse subscription onboarding process

You can use Azure Lighthouse to extend all cross-workspace activities across tenant boundaries, allowing users in your managing tenant to work on Microsoft

Sentinel workspaces across all tenants.

Azure Lighthouse enables you to see and manage Azure resources from different tenancies, in the one place, with the power of delegated administration. That tenancy may be a customer (for example, if you're a managed services provider with a support contract arrangement in place), or a separate Azure environment for legal or financial reasons (like franchisee groups or Enterprises with large brand groups).

Incorrect:

* not Azure AD B2B

Azure AD B2B uses guest account, which goes against the requirements in this scenario,

Note: Azure Active Directory (Azure AD) B2B collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants https://docs.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture https://techcommunity.microsoft.com/t5/itops-talk-blog/onboarding-to-azure-lighthouse-using-a-template/ba-p/1091786 https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

Question #3 *Topic 6*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

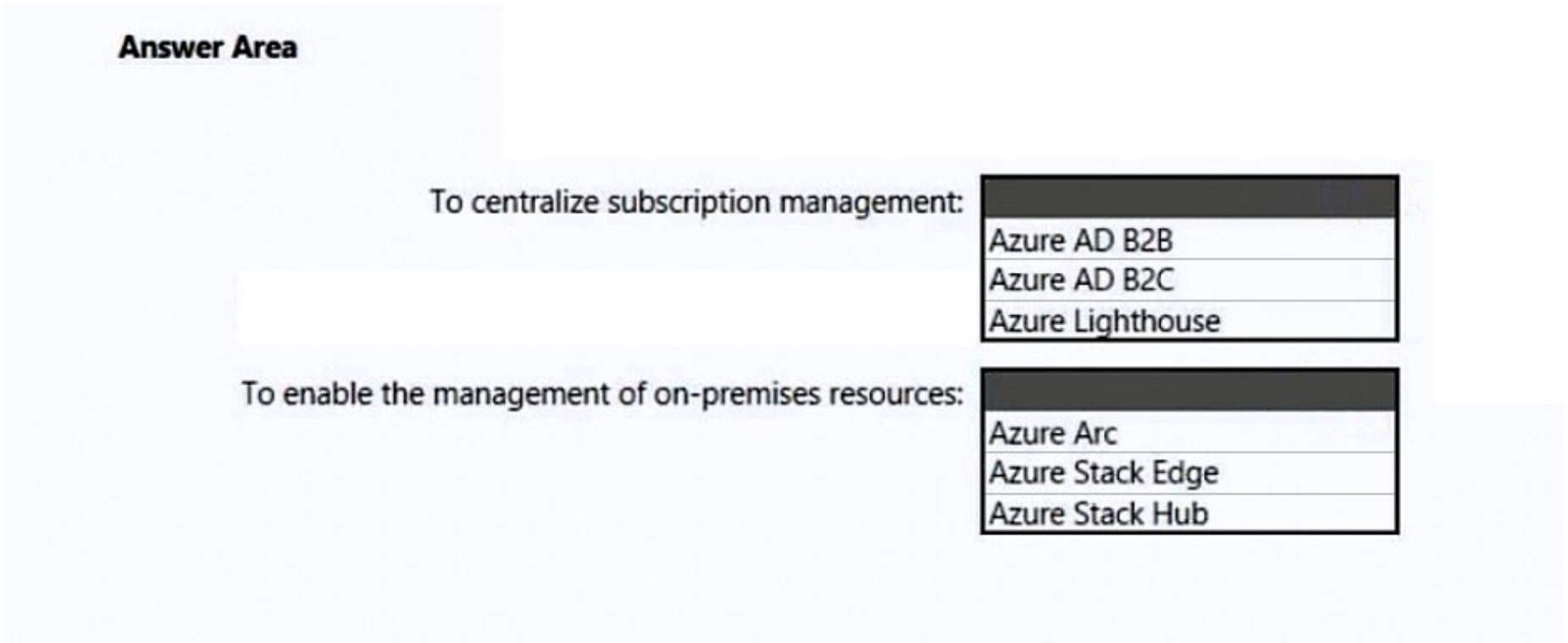
Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

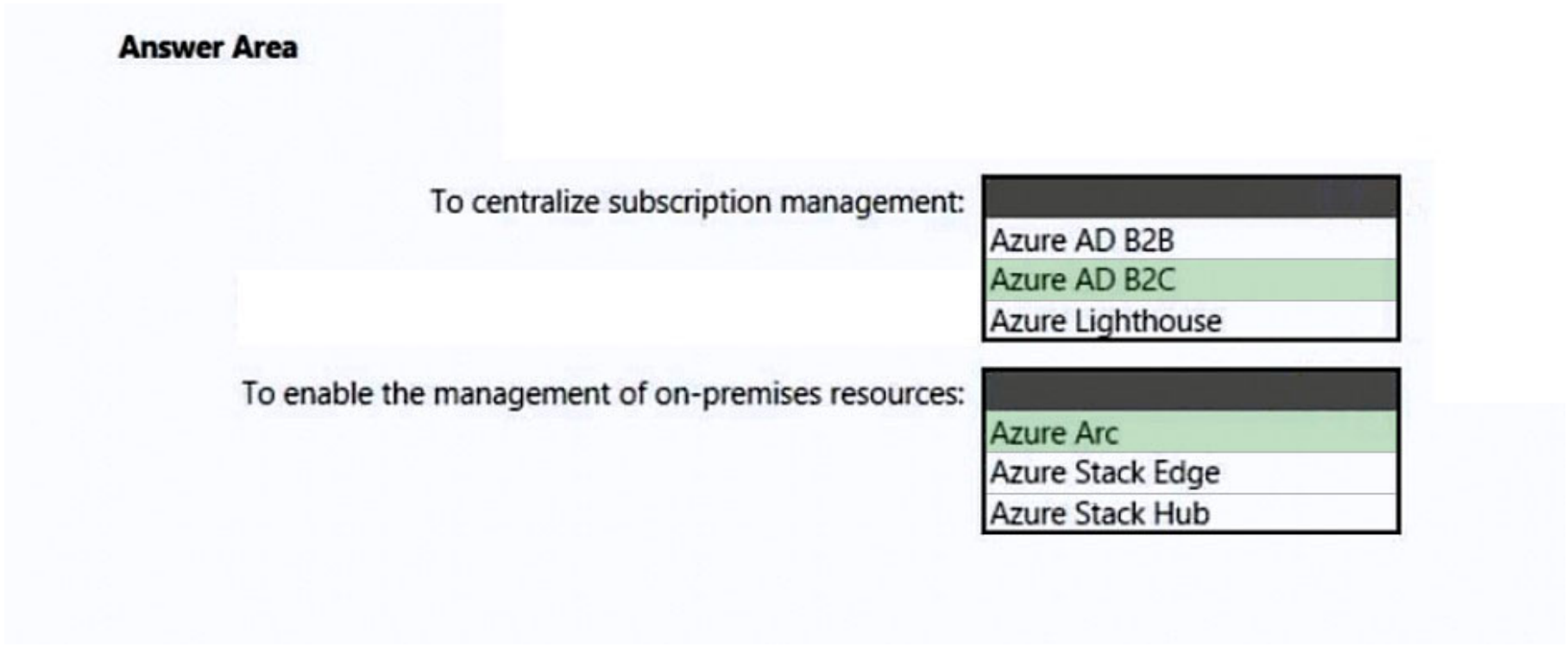
Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question

HOTSPOT -
You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Box 1: Azure AD B2C -

Scenario: Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Azure AD B2C -

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

By serving as the central authentication authority for your web applications, mobile apps, and APIs, Azure AD B2C enables you to build a single sign-on (SSO) solution for them all. Centralize the collection of user profile and preference information, and capture detailed analytics about sign-in behavior and sign-up conversion.

Note: Azure AD B2C is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

Incorrect:

Azure Lighthouse -

Cross-tenant management experiences

As a service provider, you can use Azure Lighthouse to manage resources for multiple customers from within your own Azure Active Directory (Azure AD) tenant.

With Azure Lighthouse, the onboarding process specifies users within the service provider's tenant who will be able to work on delegated subscriptions and resource groups in the customer's tenant. These users can then sign in to the Azure portal using their own credentials. Within the Azure portal, they can manage resources belonging to all customers to which they have access.

Box 2: Azure Arc -

Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Note:

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

*Enable the management of on-premises resources from Azure, including the following:

Use Azure Policy for enforcement and compliance evaluation.

Provide change tracking and asset inventory.

Implement patch management.

Incorrect:

* Azure Stack Edge acts as a cloud storage gateway and enables eyes-off data transfers to Azure, while retaining local access to files.

* Microsoft Azure Stack Hub is a hybrid cloud platform that lets you deliver services from your datacenter.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview https://docs.microsoft.com/en-us/azure/azure-arc/overview

https://docs.microsoft.com/en-us/azure/lighthouse/concepts/cross-tenant-management-experience

Question #4 *Topic 6*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question
You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.
What should you configure for each landing zone?

A. an ExpressRoute gateway
B. Microsoft Defender for Cloud
C. an Azure Private DNS zone
D. Azure DDoS Protection Standard

Correct Answer: *A*
ExpressRoute provides direct connectivity to Azure cloud services and connecting Microsoft's global network. All transferred data is not encrypted, and do not go over the public Internet. VPN Gateway provides secured connectivity to Azure cloud services over public Internet.
Note:
Litware identifies the following landing zone requirements:
ג€¢ Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
ג€¢ Provide a secure score scoped to the landing zone.
ג€¢ Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
ג€¢ Minimize the possibility of data exfiltration.
ג€¢ Maximize network bandwidth.
Litware identifies the following business requirements:
ג€¢ Minimize any additional on-premises infrastructure.
ג€¢ Minimize the operational costs associated with administrative overhead.
Reference:
https://medium.com/awesome-azure/azure-difference-between-azure-expressroute-and-azure-vpn-gateway-comparison-azure-hybrid-connectivity-
5f7ce02044f3

Community vote distribution

B (62%) C (37%)

Topic 7 - Testlet 2

Question #1 *Topic 7*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

HOTSPOT -

What should you create in Azure AD to meet the Contoso developer requirements?

Hot Area:

Answer Area

Account type for the developers:	A guest account in the contoso.onmicrosoft.com tenant A guest account in the fabrikam.onmicrosoft.com tenant A synced user account in the corp.fabrikam.com domain A user account in the fabrikam.onmicrosoft.com tenant
Component in Identity Governance:	A connected organization An access package An access review An Azure AD role An Azure resource role

Correct Answer:

Answer Area

Account type for the developers:	A guest account in the contoso.onmicrosoft.com tenant A guest account in the fabrikam.onmicrosoft.com tenant **A synced user account in the corp.fabrikam.com domain** A user account in the fabrikam.onmicrosoft.com tenant
Component in Identity Governance:	A connected organization An access package **An access review** An Azure AD role An Azure resource role

Box 1: A synced user account -

Need to use a synched user account.

Incorrect:

* Not A user account in the fabrikam.onmicrosoft.com tenant

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

* Guest accounts would not meet the requirements.

Note: Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Contoso Developers Requirements -

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Box 2: An access review -

Scenario: Every month, the membership of the ContosoDevelopers group must be verified.

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Access review is part of Azure AD Identity governance.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question #2 *Topic 7*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

You need to recommend a solution to meet the security requirements for the InfraSec group.

What should you use to delegate the access?

A. a subscription

B. a custom role-based access control (RBAC) role

C. a resource group

D. a management group

Correct Answer: *B*

Scenario: Requirements. Security Requirements include:

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in

Sub1.

If the Azure built-in roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group (in preview only), subscription, and resource group scopes.

Incorrect:

Not D: Management groups are useful when you have multiple subscriptions. This is not what is addressed in this question.

Scenario: Fabrikam has a single Azure subscription named Sub1.

Note: If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions.

Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.

Management groups give you enterprise-grade management at scale no matter what type of subscriptions you might have. However, all subscriptions within a single management group must trust the same Azure Active Directory (Azure AD) tenant.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

Community vote distribution

B (91%) 9%

Topic 8 - Testlet 3

Question #1 *Topic 8*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

HOTSPOT -

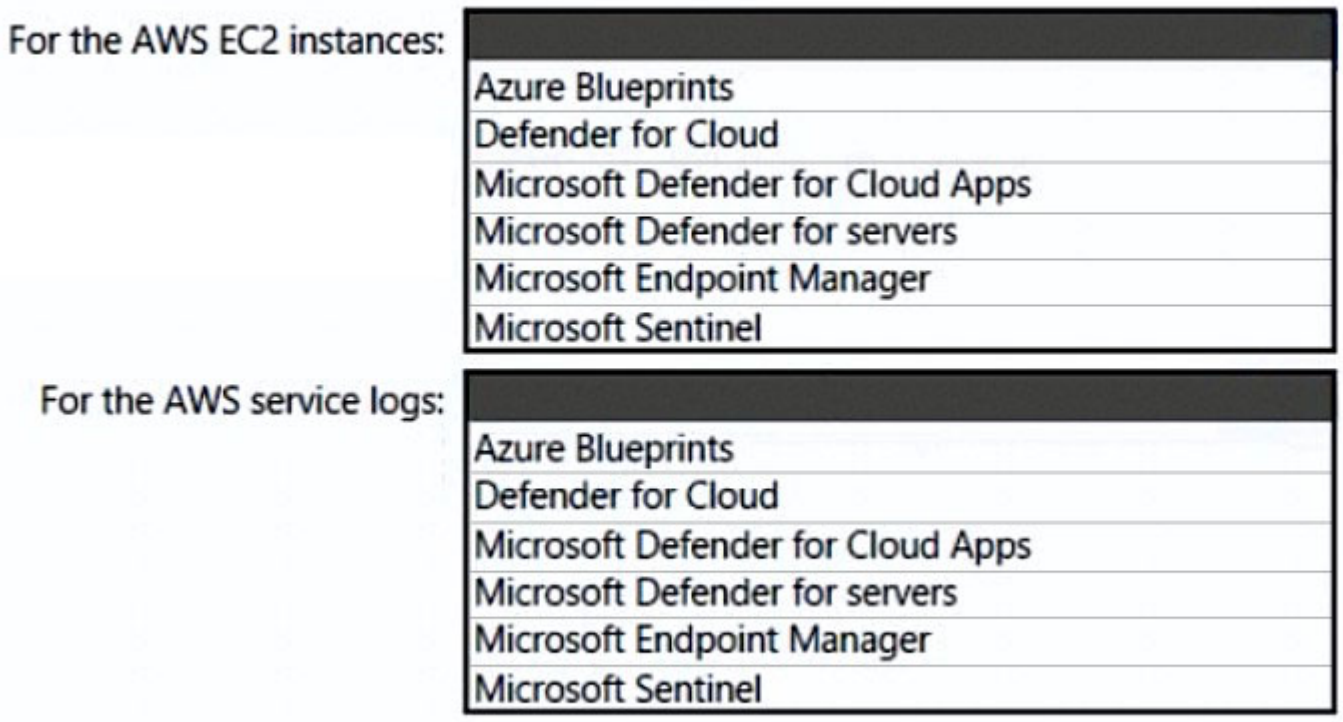
You need to recommend a solution to meet the AWS requirements.

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.

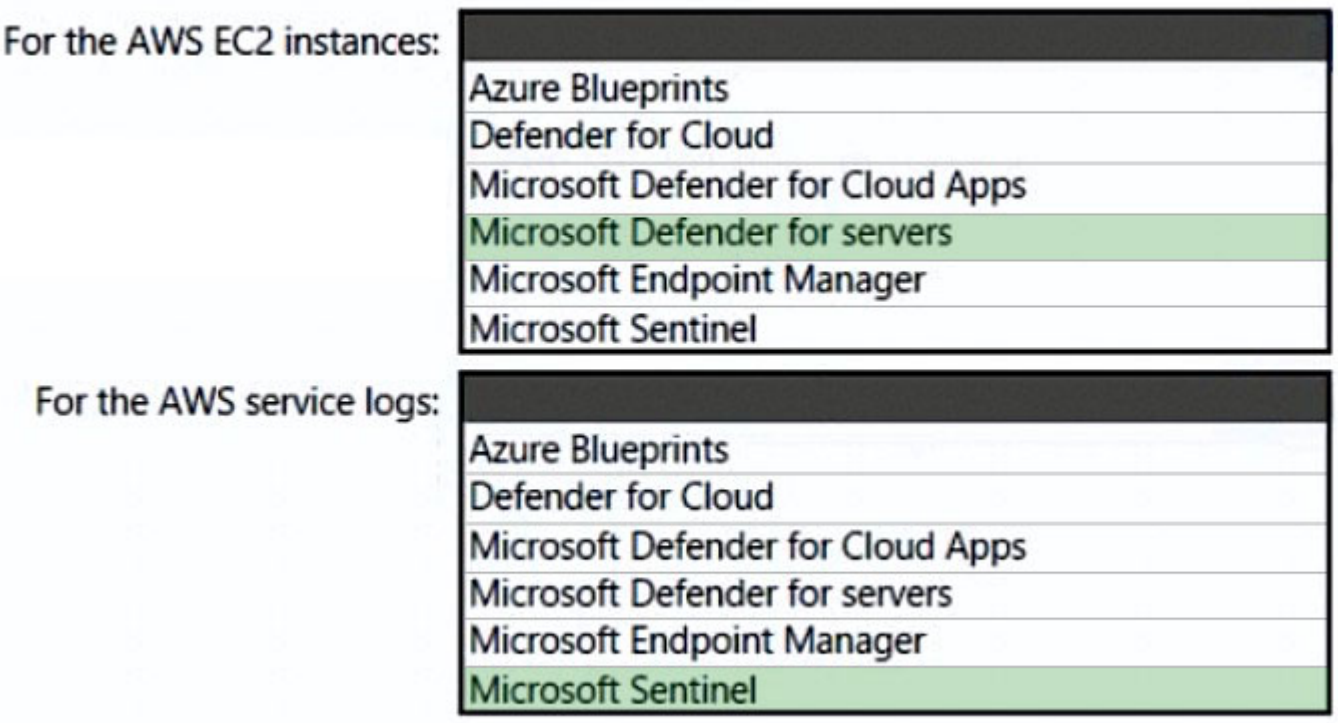
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Microsoft Defender for servers

Scenario: Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Defender for Servers is one of the enhanced security features available in Microsoft Defender for Cloud. You can use it to add threat detection and advanced defenses to your Windows and Linux machines that exist in hybrid and multicloud environments.

Available Defender for Server plans

Defender for Servers offers you a choice between two paid plans.

Both include automatic onboarding for resources in Azure, AWS, GCP.

Feature	Defender for Servers Plan 1	Defender for Servers Plan 2
Automatic onboarding for resources in Azure, AWS, GCP	✓	✓
Microsoft threat and vulnerability management	✓	✓
Flexibility to use Microsoft Defender for Cloud or Microsoft 365 Defender portal	✓	✓
Integration of Microsoft Defender for Cloud and Microsoft Defender for Endpoint (alerts, software inventory, Vulnerability Assessment)	✓	✓

Plan 1 includes the following benefits:
Automatic onboarding for resources in Azure, AWS, GCP
Microsoft threat and vulnerability management
Flexibility to use Microsoft Defender for Cloud or Microsoft 365 Defender portal
A Microsoft Defender for Endpoint subscription that includes access to alerts, software inventory, Vulnerability Assessment and an automatic integration with
Microsoft Defender for Cloud.
Plan 2 includes everything in Plan 1 plus some additional benefits.

Box 2: Microsoft Sentinel -

Scenario: AWS Requirements -
Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:
Ensure that the security administrators can query AWS service logs directly from the Azure environment.
Use the Amazon Web Services (AWS) connectors to pull AWS service logs into Microsoft Sentinel.
Note: These connectors work by granting Microsoft Sentinel access to your AWS resource logs. Setting up the connector establishes a trust relationship between
Amazon Web Services and Microsoft Sentinel. This is accomplished on AWS by creating a role that gives permission to Microsoft Sentinel to access your AWS logs.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws https://docs.microsoft.com/en-us/azure/sentinel/connect-aws

Question #2 *Topic 8*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

You need to recommend a solution to resolve the virtual machine issue.

What should you include in the recommendation?

A. Enable the Qualys scanner in Defender for Cloud.

B. Onboard the virtual machines to Microsoft Defender for Endpoint.

C. Create a device compliance policy in Microsoft Endpoint Manager.

D. Onboard the virtual machines to Azure Arc.

Correct Answer: *B*

Scenario: 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Note: Deploying Microsoft Defender for Endpoint is a two-step process.

Onboard devices to the service -

Configure capabilities of the service

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

Community vote distribution

A (78%) B (22%)

Question #3 *Topic 8*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

You need to recommend a solution to meet the security requirements for the virtual machines.

What should you include in the recommendation?

A. just-in-time (JIT) VM access

B. an Azure Bastion host

C. Azure Virtual Desktop

D. a network security group (NSG)

Correct Answer: *B*

Scenario: Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Reference:
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/hipaa-hitrust-9-2

Community vote distribution

C (93%) 7%

Question #4 *Topic 8*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

HOTSPOT -

You need to recommend a solution to meet the compliance requirements.

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 enforce compliance to the regulatory standard, create:

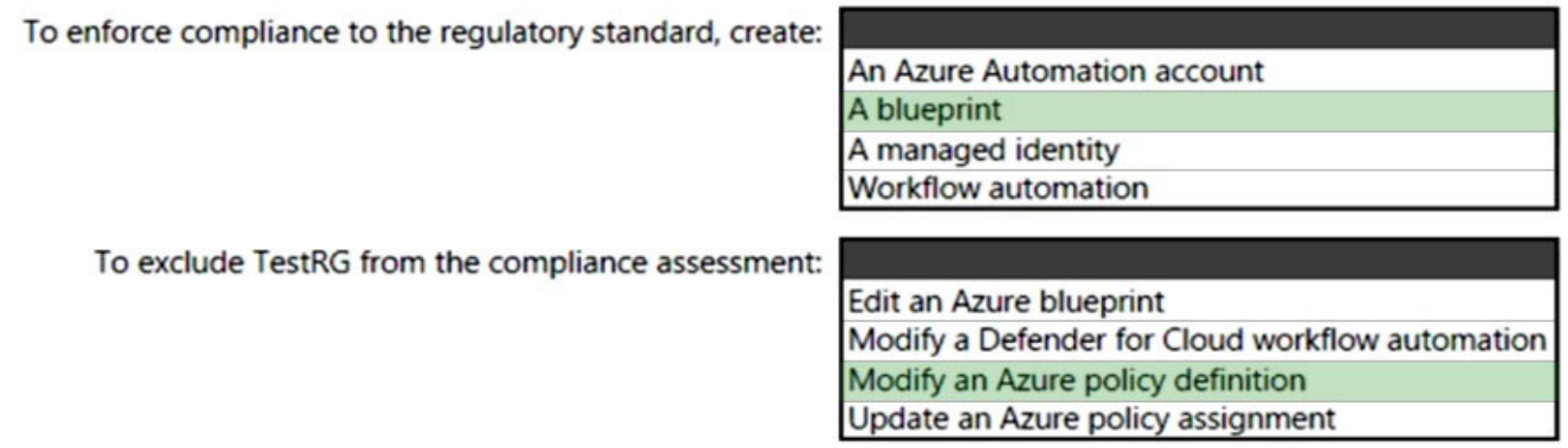
An Azure Automation account
A blueprint
A managed identity
Workflow automation

To exclude TestRG from the compliance assessment:

Edit an Azure blueprint
Modify a Defender for Cloud workflow automation
Modify an Azure policy definition
Update an Azure policy assignment

Correct Answer:

Answer Area



Box 1: A blueprint -

Scenario: Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard.

Microsoft releases automation for HIPAA/HITRUST compliance

I am excited to share our new Azure Security and Compliance Blueprint for HIPAA/HITRUST â€" Health Data & AI. Microsoft's Azure Blueprints are resources to help build and launch cloud-powered applications that comply with stringent regulations and standards. Included in the blueprints are reference architectures, compliance guidance and deployment scripts.

An Azure Blueprint is a package for creating specific sets of standards and requirements that govern the implementation of Azure services, security, and design.

Such packages are reusable so that consistency and compliance among resources can be maintained.

Incorrect:

* not Workflow automation

Workflow automation is an approach to making the flow of tasks, documents and information across work-related activities perform independently in accordance with defined business rules.

Box 2: Modify an Azure policy definition

Scenario: The virtual machines in TestRG must be excluded from the compliance assessment.

Use a Policy definition to include the TestRG virtual machines from the Blueprint.

Note: Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. A condition compares a resource property field or a value to a required value. Resource property fields are accessed by using aliases. When a resource property field is an array, a special array alias can be used to select values from all array members and apply a condition to each one.

By defining conventions, you can control costs and more easily manage your resources. For example, you can specify that only certain types of virtual machines are allowed. Or, you can require that resources have a particular tag. Policy assignments are inherited by child resources. If a policy assignment is applied to a resource group, it's applicable to all the resources in that resource group.

Incorrect:

* Not Update a policy assignment

A policy assignment assigns a Blueprint to a subscription. The scope is at the subscription level.

Note: Policy Assignments provide a means for applying policy to a subscription to which a blueprint is assigned. That said, the policy must be within the scope of the blueprint containing the policy. Parameters defined with a policy are assigned during blueprint creation or during blueprint assignment.

Reference:

https://azure.microsoft.com/en-us/blog/microsoft-releases-automation-for-hipaa-hitrust-compliance/ https://cloudacademy.com/blog/what-are-azure-blueprints/ https://k21academy.com/microsoft-azure/azure-rbac-vs-azure-policies-vs-azure-blueprints/

Topic 9 - Testlet 4

Question #1 *Topic 9*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

Implement leaked credential detection in the Azure AD tenant of Litware.

Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:

- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units

Requirements. Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.

Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.

▪

Use the principle of least privilege.

Requirements. Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

Provide a secure score scoped to the landing zone.

Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

Minimize the possibility of data exfiltration.

Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

Be created in a dedicated subscription.

Use a DNS namespace of litware.com.

Requirements. Application Security Requirements

Litware identifies the following application security requirements:

Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question

HOTSPOT -

You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Evaluate regulatory compliance of cloud resources by assigning:

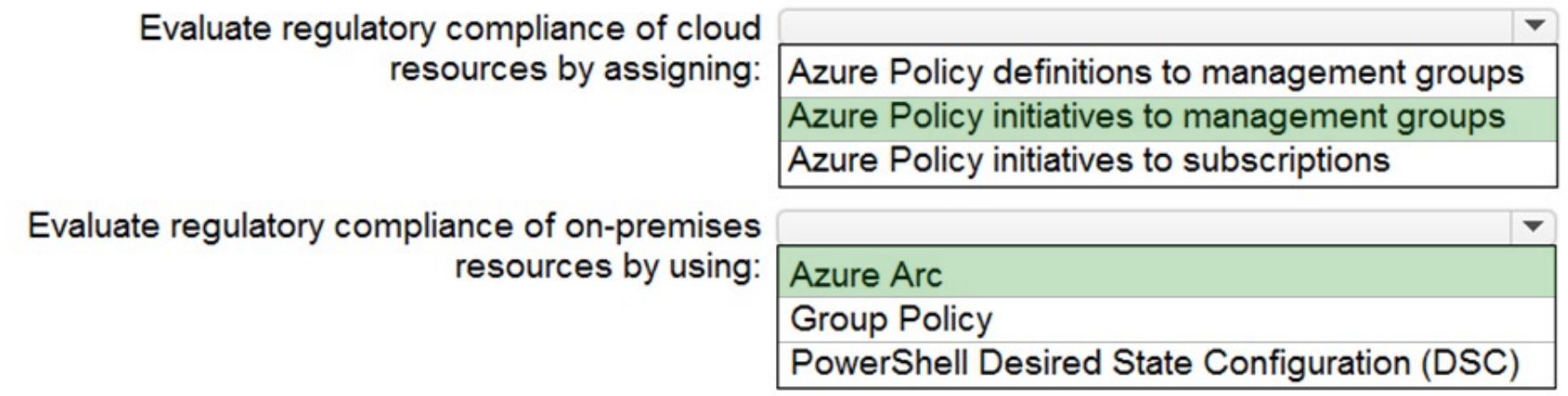
- Azure Policy definitions to management groups
- Azure Policy initiatives to management groups
- Azure Policy initiatives to subscriptions

Evaluate regulatory compliance of on-premises resources by using:

- Azure Arc
- Group Policy
- PowerShell Desired State Configuration (DSC)

Correct Answer:

Answer Area



Box 1: Azure Policy initiatives to management groups

If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions.

Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.

If you plan to apply a policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to.

The same is true for an initiative definition.

With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.

Incorrect:

Not: Azure Policy initiatives to subscriptions

Must use a management group as we have multiple subscriptions.

Scenario:

Requirements. Business Requirements

Litware identifies the following business requirements:

ג€¢ Minimize any additional on-premises infrastructure.

ג€¢ Minimize the operational costs associated with administrative overhead.

Box 2: Azure Arc -

With Azure Arc:

Meet governance and compliance standards for apps, infrastructure, and data with Azure Policy.

Take advantage of elastic scale, consistent on-premises and multicloud management, and cloud-style billing models.

Note: Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments. Develop cloud-native applications with a consistent development, operations, and security model. Azure Arc runs on both new and existing hardware, virtualization and Kubernetes platforms, IoT devices, and integrated systems.

Reference:

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://azure.microsoft.com/en-us/services/azure-arc/#product-overview

Topic 10 - Testlet 5

Question #1 *Topic 10*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements
Litware identifies the following identity requirements:
Detect brute force attacks that directly target AD DS user accounts.
Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question
You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements.
What should you recommend as part of the landing zone deployment?

A. local network gateways

B. forced tunneling

C. service chaining

Correct Answer: *C*
Service chaining.
Service chaining enables you to direct traffic from one virtual network to a virtual appliance or gateway in a peered network through user-defined routes.
You can deploy hub-and-spoke networks, where the hub virtual network hosts infrastructure components such as a network virtual appliance or VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic flows through network virtual appliances or VPN gateways in the hub virtual network.
Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway.
You can't route between virtual networks with a user-defined route that specifies an Azure ExpressRoute gateway as the next hop type.
Incorrect:
Not B: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. If you don't configure forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from the Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Unauthorized
Internet access can potentially lead to information disclosure or other types of security breaches.

ExpressRoute forced tunneling is not configured via this mechanism, but instead, is enabled by advertising a default route via the ExpressRoute BGP peering sessions.

Note:

Requirements. Planned Changes -

Litware plans to implement the following changes:

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

Requirements. Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

ג€¢ Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

ג€¢ Provide a secure score scoped to the landing zone.

ג€¢ Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

ג€¢ Minimize the possibility of data exfiltration.

ג€¢ Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

ג€¢ Be created in a dedicated subscription.

ג€¢ Use a DNS namespace of litware.com.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview#service-chaining https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

Community vote distribution

C (63%) B (37%)

Question #2 *Topic 10*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

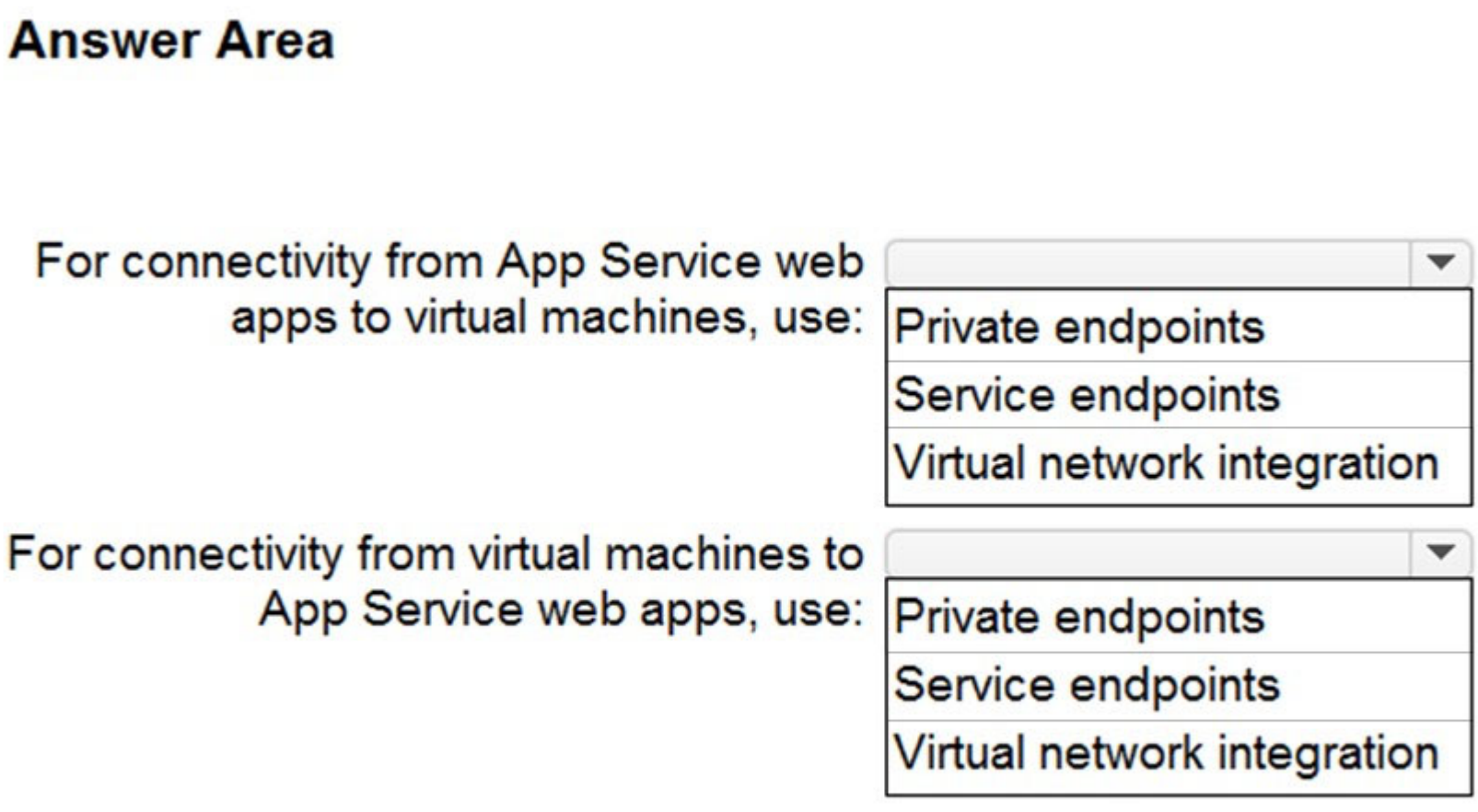
Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

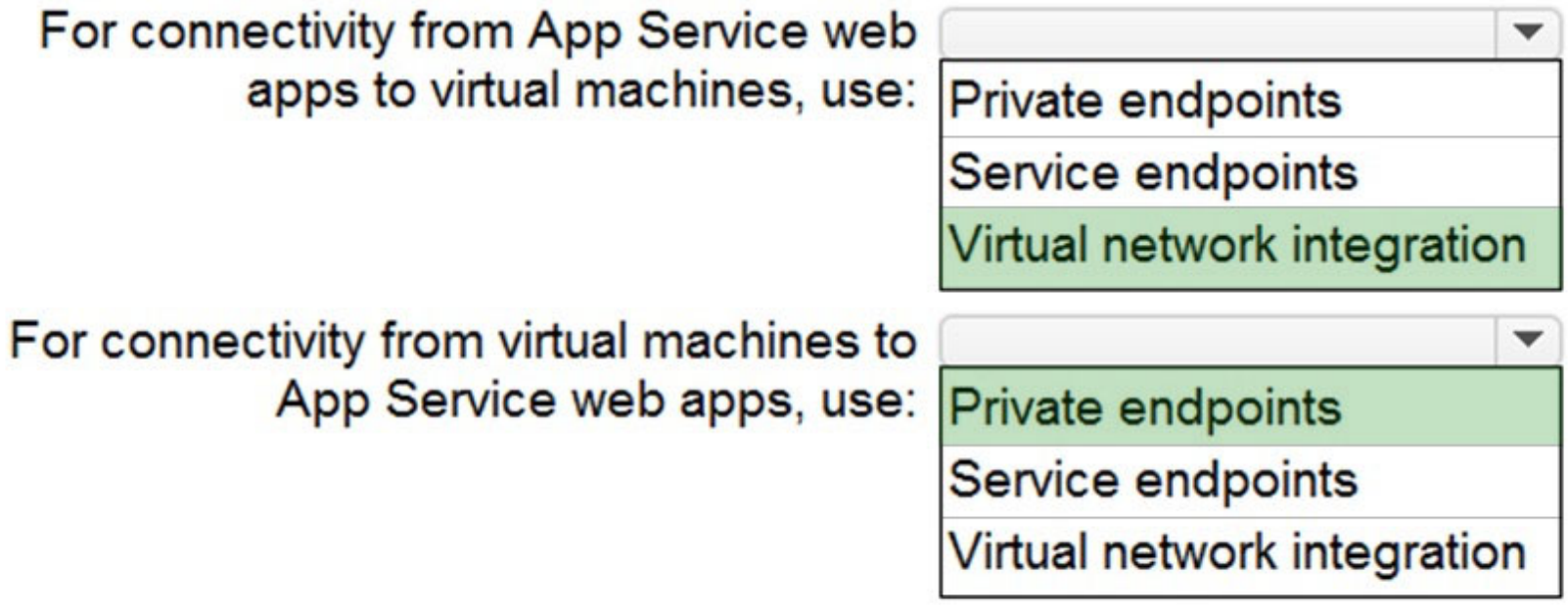
Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question
HOTSPOT -
You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:

Answer Area



Box 1: Virtual network integration
Integrate your app with an Azure virtual network.
With Azure virtual networks, you can place many of your Azure resources in a non-internet-routable network. The App Service virtual network integration feature enables your apps to access resources in or through a virtual network.

Box 2: Private endpoints -
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
A virtual machine can connect to the web app across the private endpoint.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-webapp-portal

Question #3 *Topic 10*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question
HOTSPOT -
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

For the delegated management of users and groups, use:

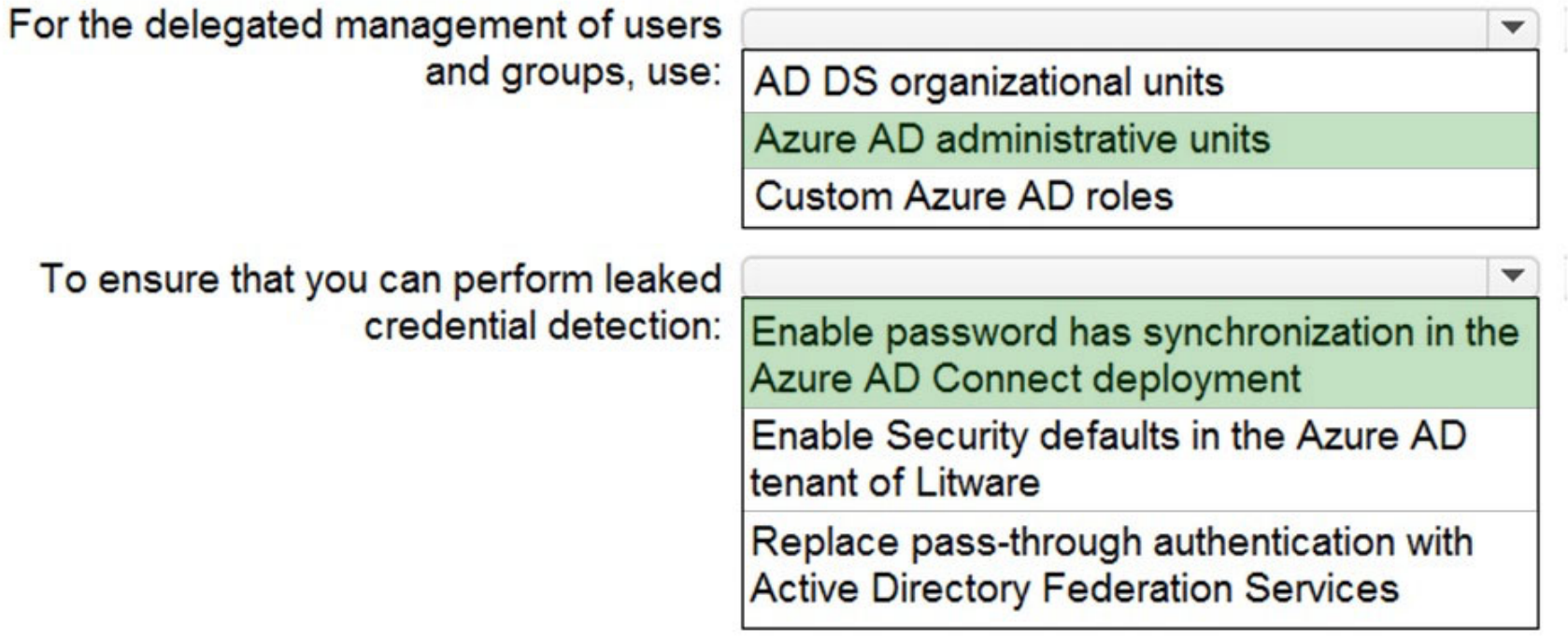
AD DS organizational units
Azure AD administrative units
Custom Azure AD roles

To ensure that you can perform leaked credential detection:

Enable password has synchronization in the Azure AD Connect deployment
Enable Security defaults in the Azure AD tenant of Litware
Replace pass-through authentication with Active Directory Federation Services

Correct Answer:

Answer Area



Box 1: Azure AD administrative units
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
* The delegation of user management based on business units
Without Azure AD administrative units, assigning a user to the User Administrator role in Azure AD gives them rights to manage all Azure AD users. With administrative units, the user is delegated the same role, User Administrator, but that role only applies to the specified administrative unit. The administrative unit contains the users and groups that are under the scope of management.
Box 2: Enable password hash synchronization in the Azure AD Connect deployment
Existing environment: Azure AD Connect is used to implement pass-through authentication.

Password hash synchronization -
Risk detections like leaked credentials require the presence of password hashes for detection to occur.
Reference:
https://4sysops.com/archives/an-introduction-to-azure-ad-administrative-units/ https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization

Topic 11 - Testlet 6

Question #1 *Topic 11*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

HOTSPOT -

You are evaluating the security of ClaimsApp.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	○
FD1 must be configured to have a certificate for claims.fabrikam.com.	○	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	●
FD1 must be configured to have a certificate for claims.fabrikam.com.	●	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	●	○

Box 1: No -

Box 2: Yes -
Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
Need certificate for HTTPS.

TLS/SSL certificates -
To enable the HTTPS protocol for securely delivering content on a Front Door custom domain, you must use a TLS/SSL certificate. You can choose to use a certificate that is managed by Azure Front Door or use your own certificate.

Box 3: Yes -
By default, Azure Front Door will respond to all user requests regardless of the location where the request is coming from. In some scenarios, you may want to restrict the access to your web application by countries/regions. The Web application firewall (WAF) service in Front Door enables you to define a policy using custom access rules for a specific path on your endpoint to either allow or block access from specified countries/regions.
Note: Requirements. Security Requirements
Fabrikam identifies the following security requirements:
ג€¢ Internet-accessible applications must prevent connections that originate in North Korea.
Reference:
https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/ba-p/2000173 https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#tlsssl-certificates

Question #2 *Topic 11*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

You need to recommend a solution to scan the application code. The solution must meet the application development requirements.

What should you include in the recommendation?

A. GitHub Advanced Security

B. Azure Key Vault

C. Azure DevTest Labs

D. Application Insights in Azure Monitor

Correct Answer: *A*

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

* All the application code must be stored in GitHub Enterprise.

* All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

A GitHub Advanced Security license provides the following additional features:

Code scanning - Search for potential security vulnerabilities and coding errors in your code.

Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also

detects secrets when they are pushed to your repository.
Dependency review - Show the full impact of changes to dependencies and see details of any vulnerable versions before you merge a pull request.
Security overview - Review the security configuration and alerts for an organization and identify the repositories at greatest risk.
Incorrect:
Not C:
Scenario: Azure DevTest labs will be used by developers for testing.
Azure DevTest Labs is a service for easily creating, using, and managing infrastructure-as-a-service (IaaS) virtual machines (VMs) and platform-as-a-service
(PaaS) environments in labs. Labs offer preconfigured bases and artifacts for creating VMs, and Azure Resource Manager (ARM) templates for creating environments like Azure Web Apps or SharePoint farms.
Lab owners can create preconfigured VMs that have tools and software lab users need. Lab users can claim preconfigured VMs, or create and configure their own
VMs and environments. Lab policies and other methods track and control lab usage and costs.
Reference:
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-security

Community vote distribution

A (100%)

Topic 12 - Testlet 7

Question #1 *Topic 12*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements
Litware identifies the following identity requirements:
Detect brute force attacks that directly target AD DS user accounts.
Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question
You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. access reviews in Azure AD

C. Microsoft Defender for Cloud

D. Microsoft Defender for Cloud Apps

E. Microsoft Defender for Endpoint

Correct Answer: *BD*
Scenario: Litware identifies the following application security requirements:
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.
B: Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.
D: The Defender for Cloud Apps framework
Discover and control the use of Shadow IT: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.
Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real time across all your cloud apps.

Etc.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Community vote distribution

AD (98%)

Question #2 *Topic 12*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:

Detect brute force attacks that directly target AD DS user accounts.

Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question
To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security Assertion Markup Language (SAML)

B. NTLMv2

C. certificate-based authentication

D. Kerberos

Correct Answer: *AD*
A: SAML -
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
You can provide single sign-on (SSO) to on-premises applications that are secured with SAML authentication and provide remote access to these applications through Application Proxy. With SAML single sign-on, Azure Active Directory (Azure AD) authenticates to the application by using the user's Azure AD account.
D: You can provide single sign-on for on-premises applications published through Application Proxy that are secured with integrated Windows authentication.
These applications require a Kerberos ticket for access. Application Proxy uses Kerberos Constrained Delegation (KCD) to support these applications.
Incorrect:
Not C: Certificate. This is not a custom domain scenario!
If you're using a custom domain, you also need to upload the TLS/SSL certificate for your application.
To configure an on-premises app to use a custom domain, you need a verified Azure Active Directory custom domain, a PFX certificate for the custom domain, and an on-premises app to configure.
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

Community vote distribution

AD (100%)

Topic 13 - Testlet 8

Question #1 *Topic 13*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

A. row-level security (RLS)

B. Transparent Data Encryption (TDE)

C. Always Encrypted

D. data classification

E. dynamic data masking

Correct Answer: *E*

Scenario: The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Dynamic data masking (DDM) limits sensitive data exposure by masking it to non-privileged users. It can be used to greatly simplify the design and coding of security in your application.

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to specify how much sensitive data to reveal with minimal impact on the application layer. DDM can be configured on designated database fields to hide sensitive data in the result sets of queries. With DDM, the data in the database isn't changed. DDM is easy to use with existing applications, since masking rules are applied in the query results.

Incorrect:

Not B: Transparent Data Encryption (TDE) encrypts the entire database, not specific columns.

Reference:

https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking

Community vote distribution

C (59%) E (40%)

Question #2 *Topic 13*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment. On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Existing Environment. Azure Environment

Fabrikam has the following Azure resources:

An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com

A single Azure subscription named Sub1

A virtual network named Vnet1 in the East US Azure region

A virtual network named Vnet2 in the West Europe Azure region

An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

A Microsoft Sentinel workspace

An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

A resource group named TestRG that is used for testing purposes only

▪

An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Existing Environment. Partners -

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

An Azure AD tenant named contoso.onmicrosoft.com

An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of

Fabrikam -

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named

ContosoDevelopers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db_owner role for the ClaimsDB database.

Existing Environment. Compliance Environment

Fabrikam deploys the following compliance environment:

Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

Qualys is used as the standard vulnerability assessment tool for servers.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Requirements. ClaimsApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

ClaimsApp will access data in ClaimsDB.

ClaimsDB must be accessible only from Azure virtual networks.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

▪

Requirements. Application Development Requirements

Fabrikam identifies the following requirements for application development:

Azure DevTest labs will be used by developers for testing.

All the application code must be stored in GitHub Enterprise.

Azure Pipelines will be used to manage application deployments.

All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text.

Scanning must be done at the time the code is pushed to a repository.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

Internet-accessible applications must prevent connections that originate in North Korea.

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

Requirements. AWS Requirements -

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Requirements. Contoso Developers Requirements

Fabrikam identifies the following requirements for the Contoso developers:

Every month, the membership of the ContosoDevelopers group must be verified.

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

The Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Requirements. Compliance Requirements

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question

HOTSPOT -

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ClaimsDB must be accessible only from Azure virtual networks:	A NAT gateway A network security group A private endpoint A service endpoint
The app services permission for ClaimsApp must be assigned to ClaimsDB:	A custom role-based access control (RBAC) role A managed identity An access package Azure AD Privileged Identity Management (PIM)

Correct Answer:

Answer Area

ClaimsDB must be accessible only from Azure virtual networks:	A NAT gateway A network security group **A private endpoint** A service endpoint
The app services permission for ClaimsApp must be assigned to ClaimsDB:	A custom role-based access control (RBAC) role **A managed identity** An access package Azure AD Privileged Identity Management (PIM)

Box 1: A private endpoint -

Scenario: An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

Requirements. ClaimsApp Deployment.

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

☞ ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

▪

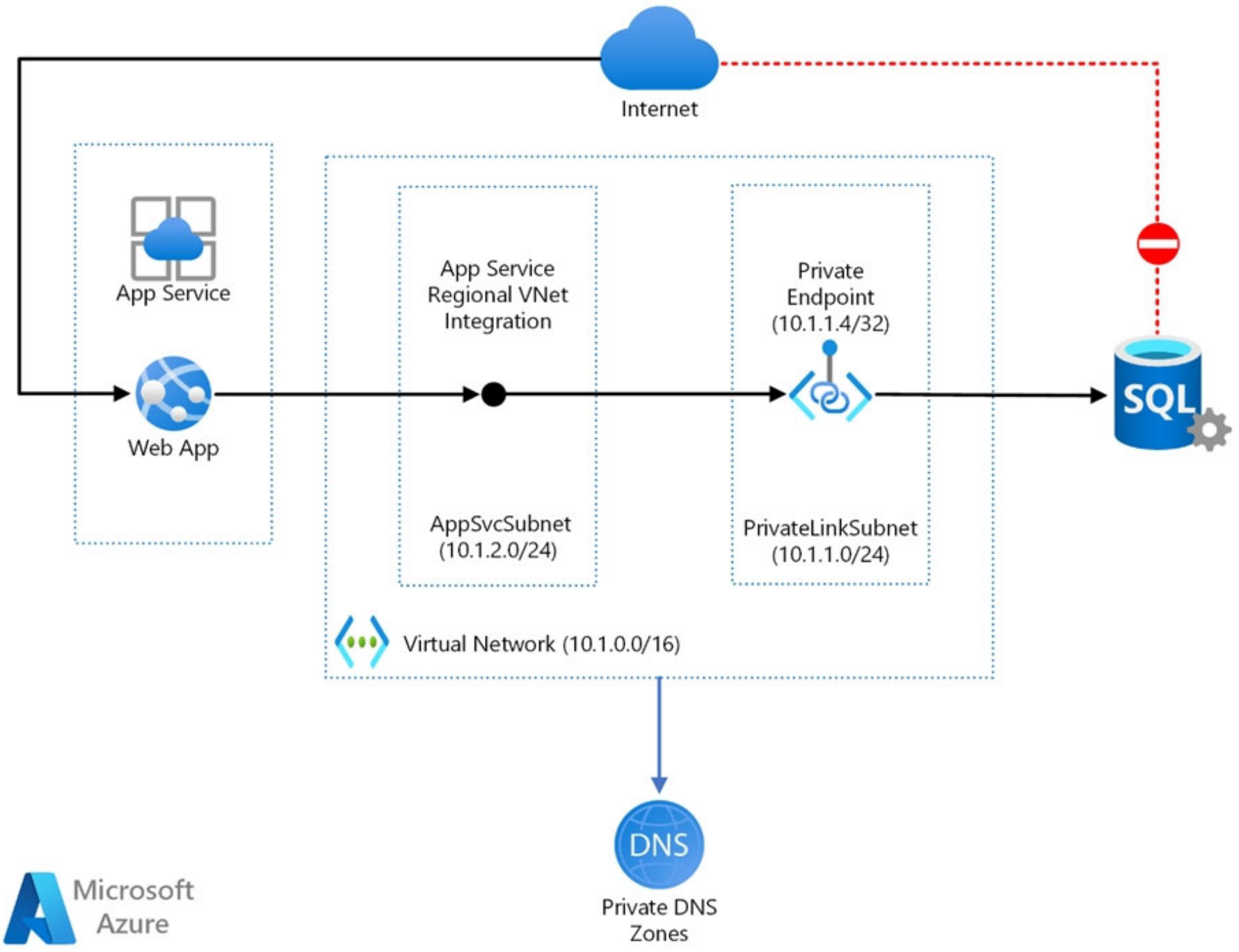
☞ ClaimsApp will access data in ClaimsDB.

☞ ClaimsDB must be accessible only from Azure virtual networks.

☞ The app services permission for ClaimsApp must be assigned to ClaimsDB.

Web app private connectivity to Azure SQL Database.

Architecture:



Workflow -

1. Using Azure App Service regional VNet Integration, the web app connects to Azure through an AppSvcSubnet delegated subnet in an Azure Virtual Network.
2. In this example, the Virtual Network only routes traffic and is otherwise empty, but other subnets and workloads could also run in the Virtual Network.
3. The App Service and Private Link subnets could be in separate peered Virtual Networks, for example as part of a hub-and-spoke network

configuration.
4. Azure Private Link sets up a private endpoint for the Azure SQL Database in the PrivateLinkSubnet of the Virtual Network.
5. The web app connects to the SQL Database private endpoint through the PrivateLinkSubnet of the Virtual Network.
The database firewall allows only traffic coming from the PrivateLinkSubnet to connect, making the database inaccessible from the public internet.

Box 2: A managed identity -
Managed identities for Azure resources provide Azure services with an automatically managed identity in Azure Active Directory. Using a managed identity, you can authenticate to any service that supports Azure AD authentication without managing credentials.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/private-web-app/private-web-app https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-status