Microsoft Cybersecurity Architect
SC-100: V32.01 - Demo

Question #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 Privacy

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

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/wor flow-automation

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 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

HOTSPOT -

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

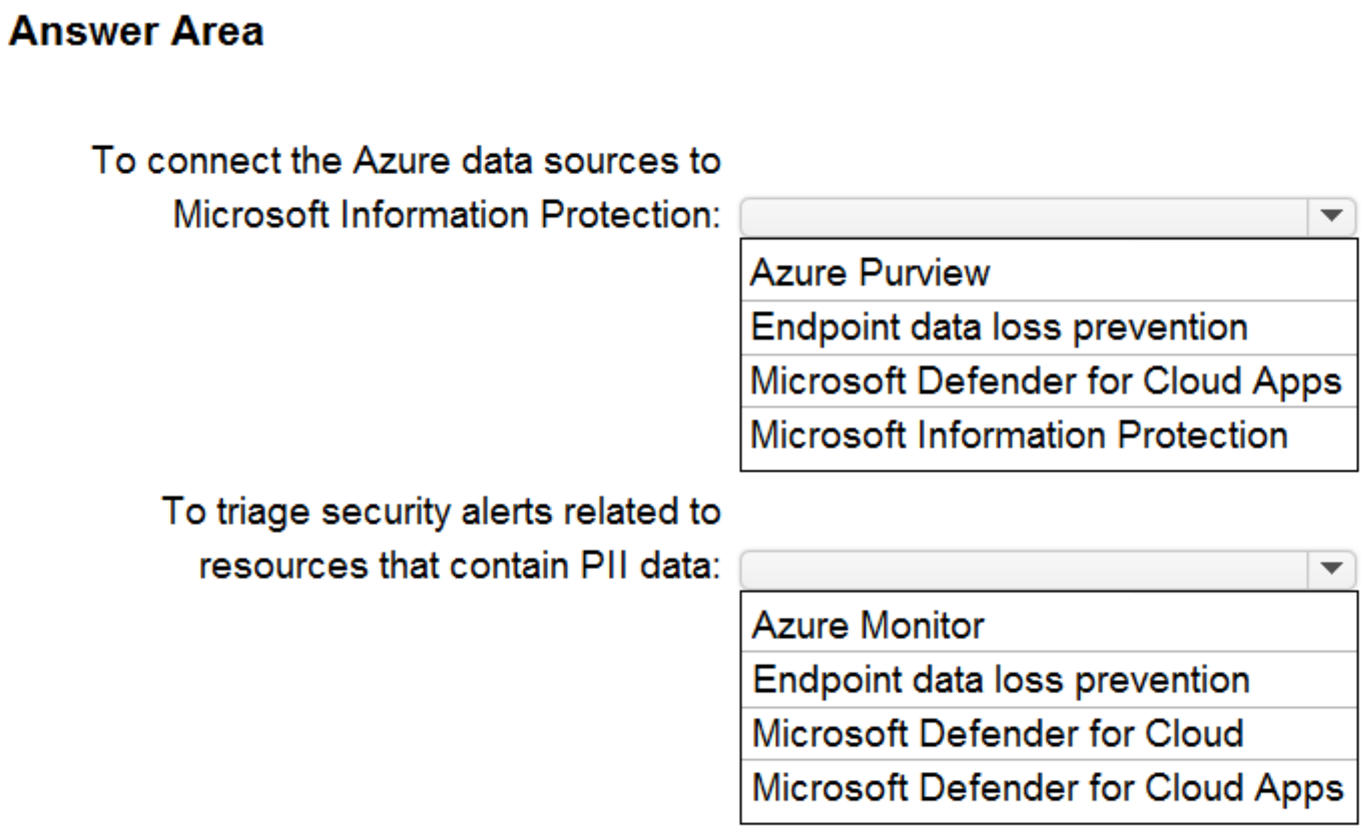
The company plans to use Microsoft Information Protection for the PII data store in Azure.

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

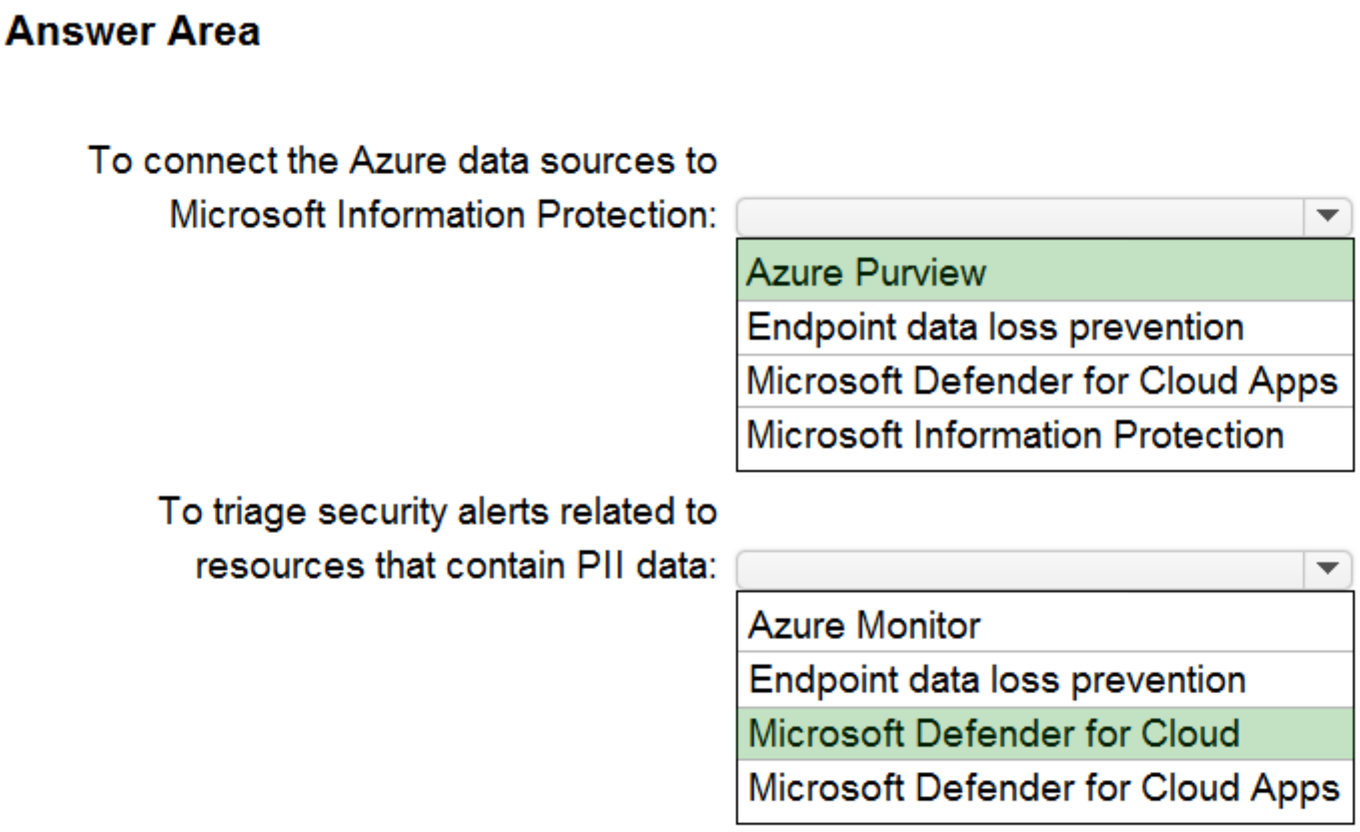
To connect the Azure data sources to Microsoft Information Protection:

- 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

Correct Answer:



Answer Area

To connect the Azure data sources to Microsoft Information Protection:

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

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

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

Box 1: Azure Purview -

Microsoft Purview is a united 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

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

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.

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 delete backup data, 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

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.

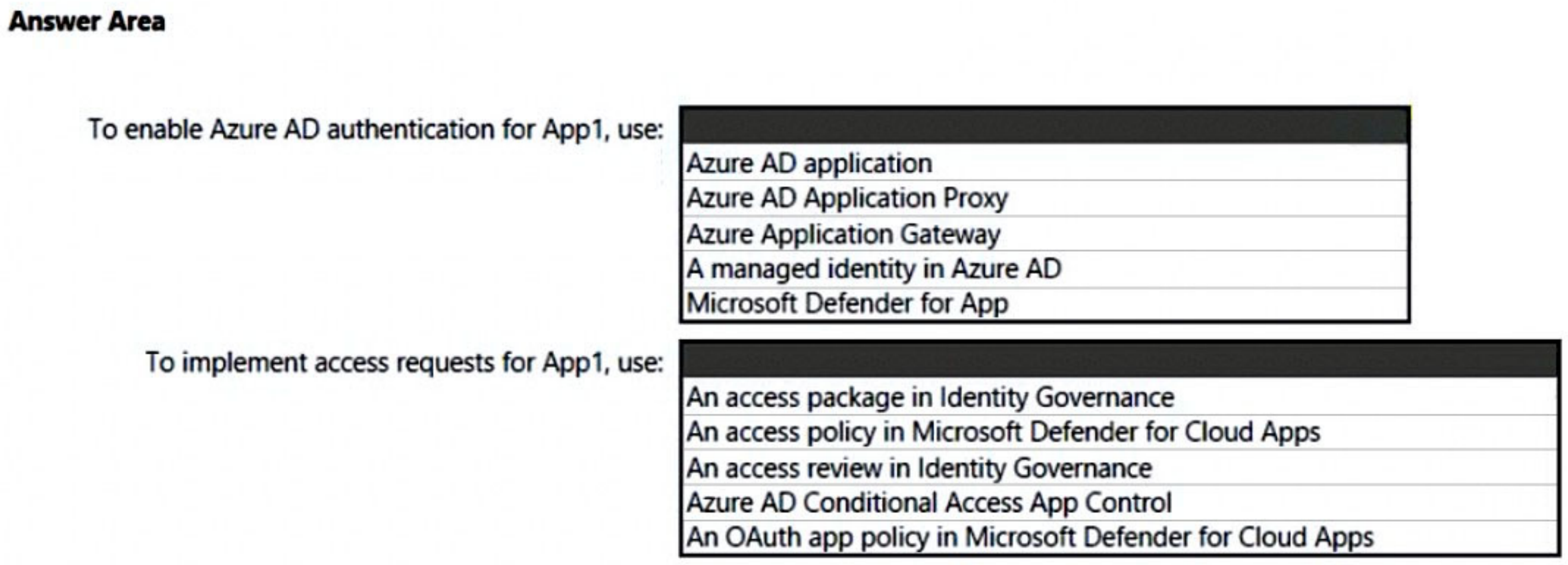
✑ Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

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

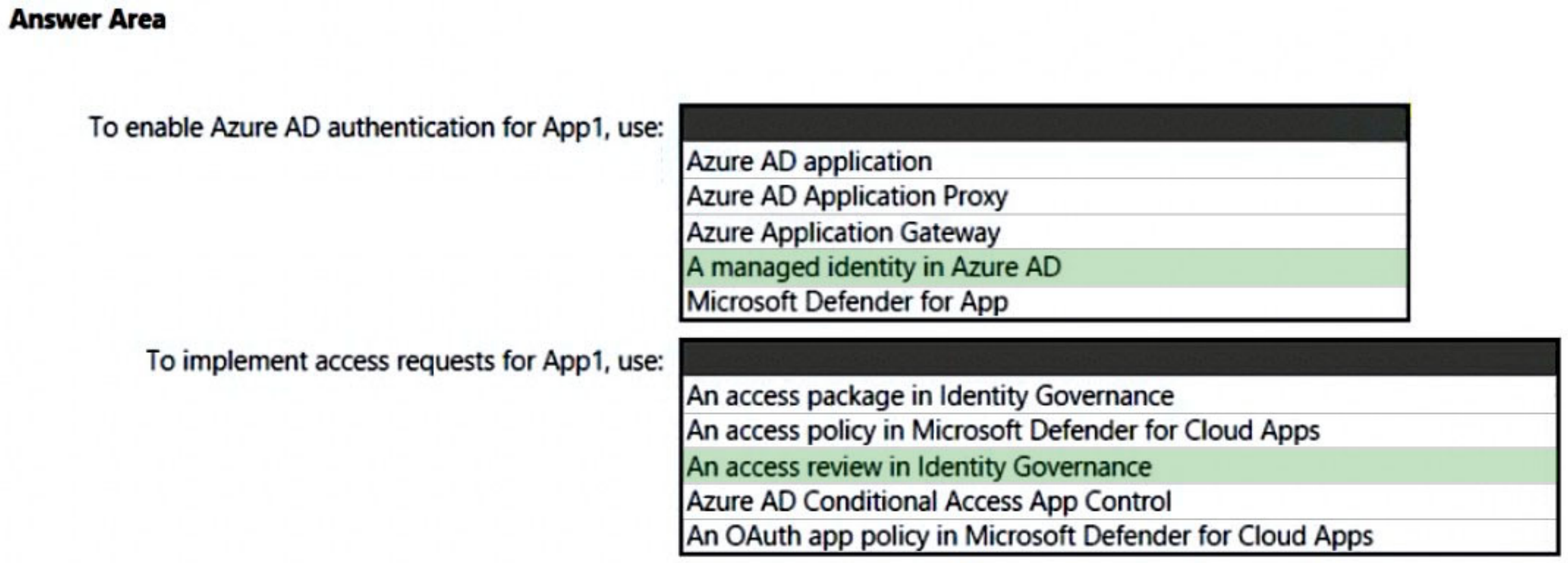
To enable Azure AD authentication for App1, use:

- 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

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 trace 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