Microsoft.SC-100.vSep-2024.by.Tany.102q

Number: SC-100
Passing Score: 800
Time Limit: 120
File Version: 42.0

Exam Code: SC-100
Exam Name: Microsoft Cybersecurity Architect

Case Study

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 D%) forest named Utvvare.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. 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. Business Requirements

Litware identifies the following business requirements:

- Minimize any additional on-premises infrastructure.
- Minimize the operational costs associated with administrative overhead.

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. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAK) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOQ by using Microsoft Sentinel.

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.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

- insure 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.

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.

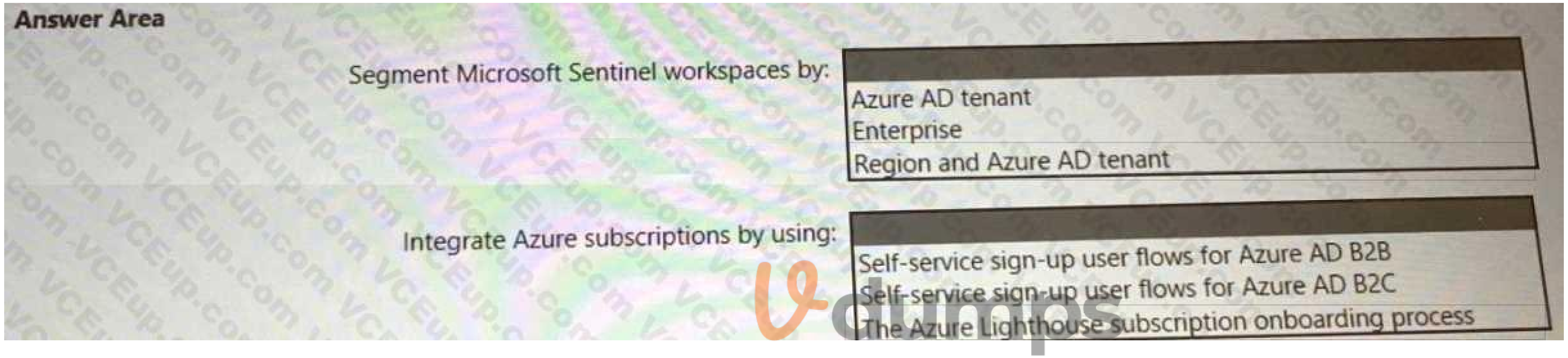
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

- Be created in a dedicated subscription.
- Use a DNS namespace of litware.com.

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 1
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:

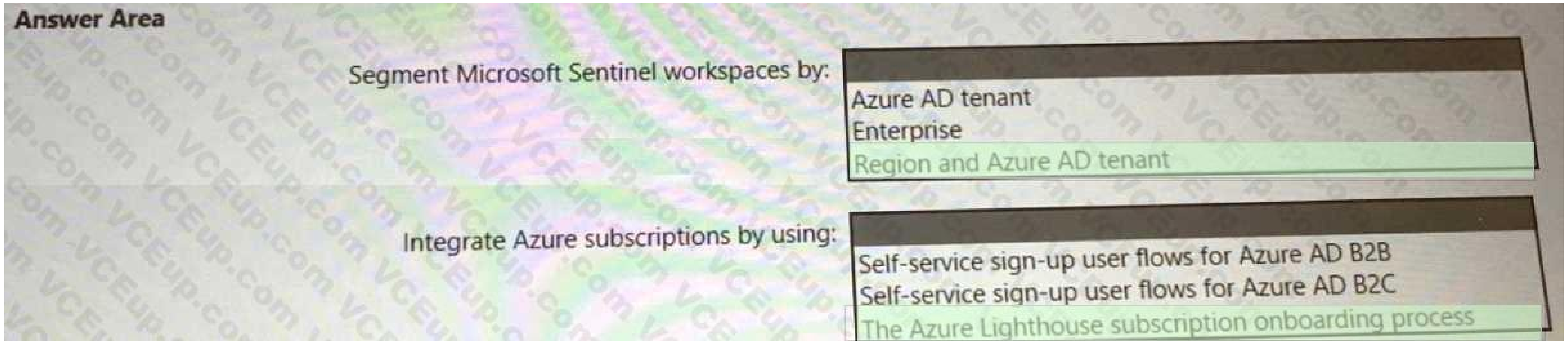


Answer Area

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

Answer Area:



Answer Area

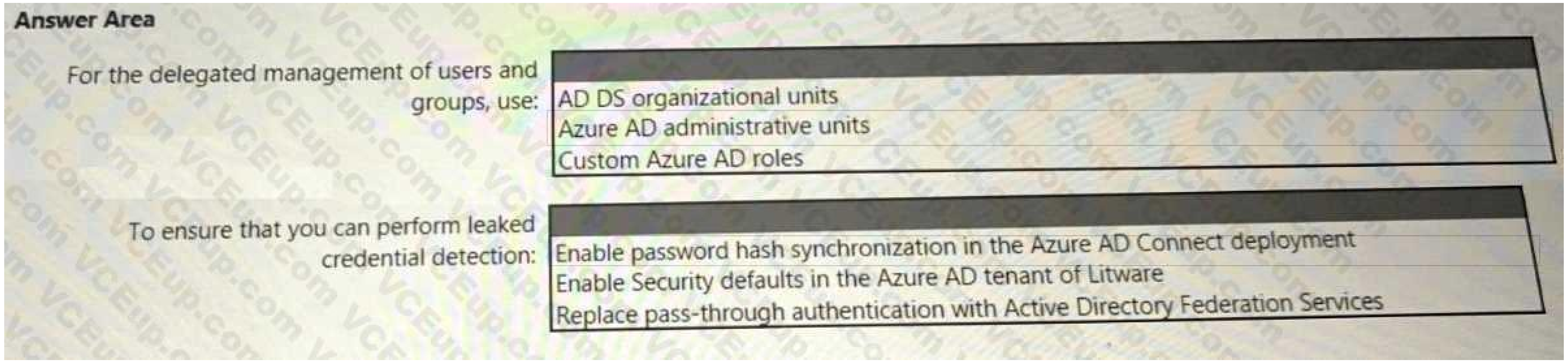
Segment Microsoft Sentinel workspaces by:
- Azure AD tenant
- Enterprise
- [✓ Region and Azure AD tenant]

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]

Section:
Explanation:

QUESTION 2
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

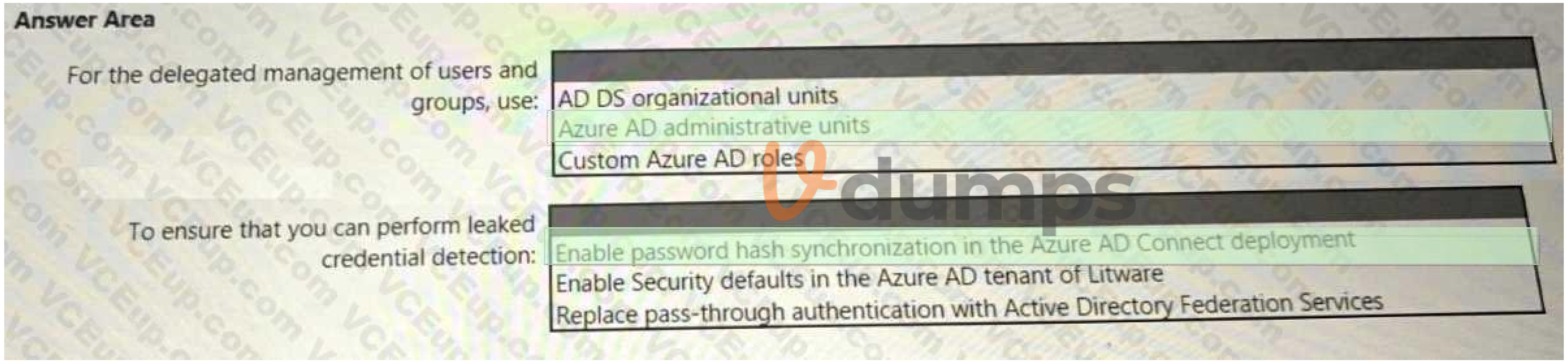
For the delegated management of users and groups, use:

- AD DS organizational units
- Azure AD administrative units
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

- Enable password hash 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

Answer Area:



Answer Area

For the delegated management of users and groups, use:

- AD DS organizational units
- [✓ Azure AD administrative units]
- Custom Azure AD roles

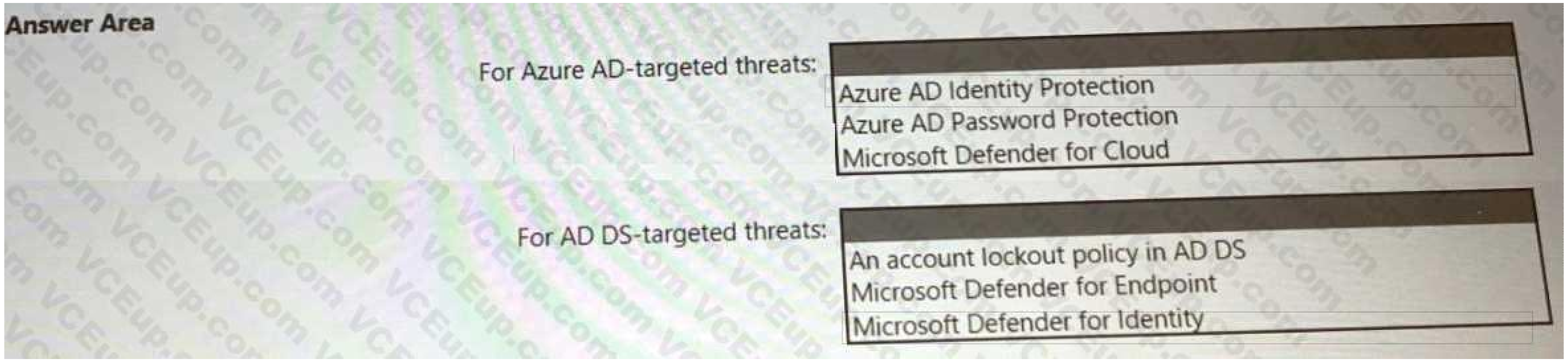
To ensure that you can perform leaked credential detection:

- [✓ Enable password hash 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

Section:
Explanation:

QUESTION 3
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 are a. NOTE; Each correct selection is worth one point.

Hot Area:



Answer Area

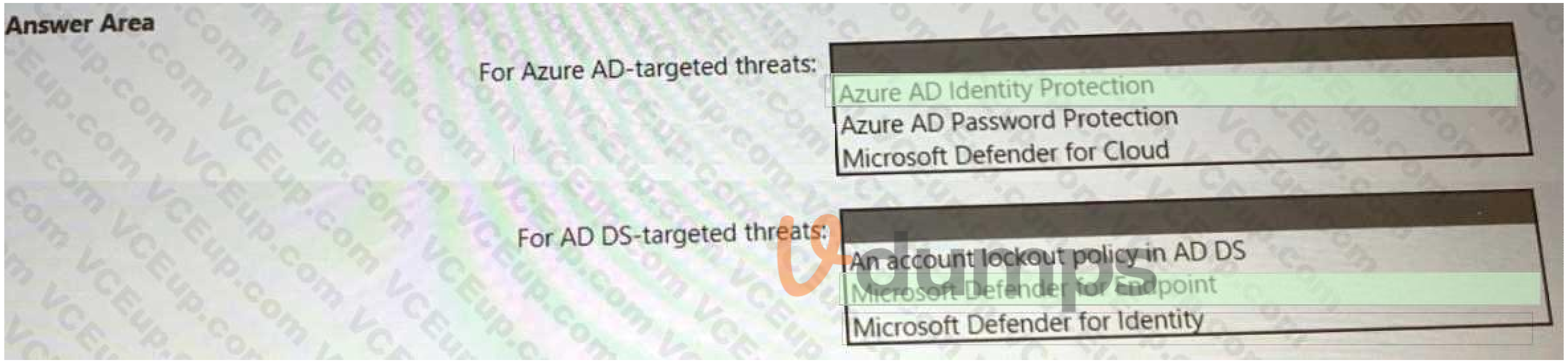
For Azure AD-targeted threats:

- 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

Answer 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

Section:

Explanation:

1. Azure AD Identity Protection

Brute Force Detection: https://docs.microsoft.com/en-us/azure/active-directory/identity- protection/overview-identity-protection 2. Defender for Identity

MDI can detect brute force attacks: ref: https://docs.microsoft.com/en-us/defender-for- identity/compromised-credentials-alerts#suspected-brute-force-attack-ldap-external-id-2004

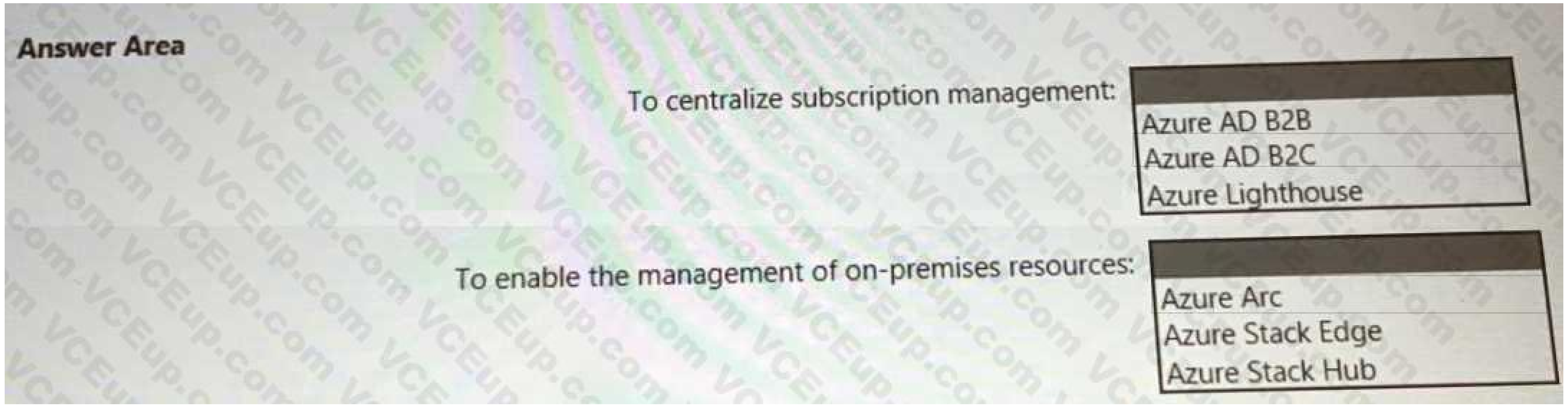
QUESTION 4

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:



Answer Area

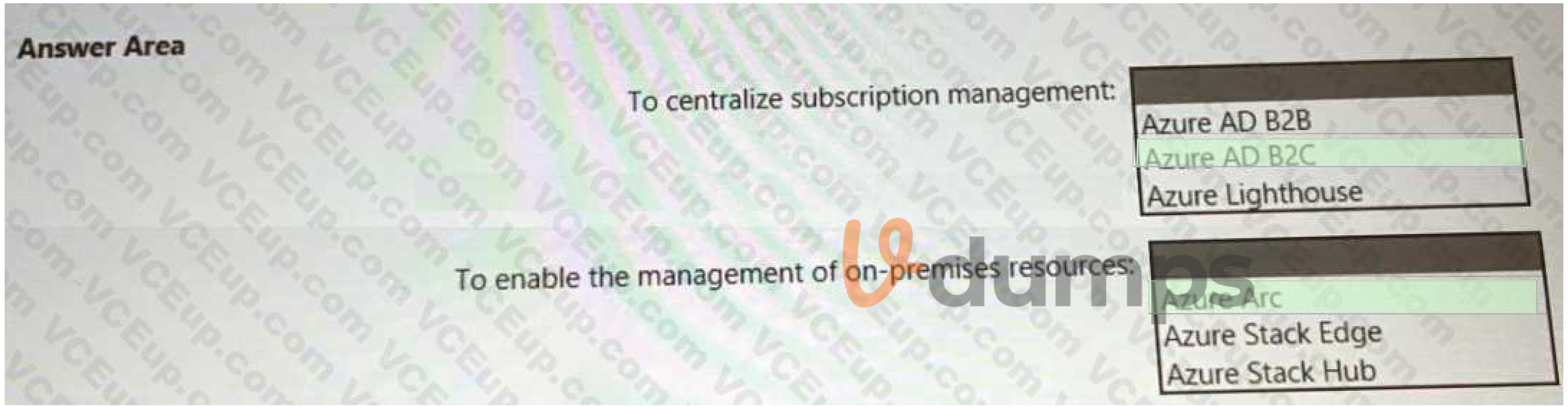
To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

Answer Area:



Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

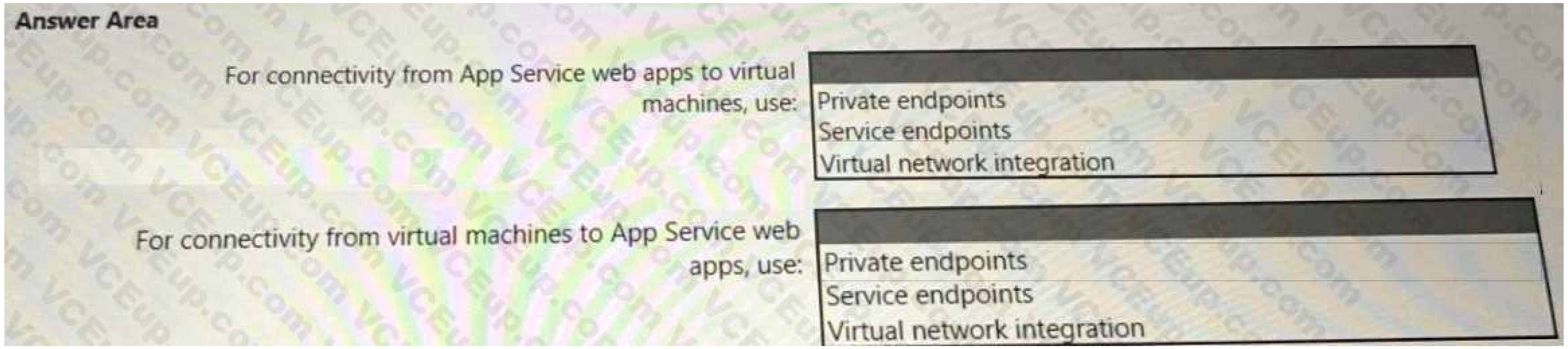
To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

Section:
Explanation:

QUESTION 5
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:



Answer Area

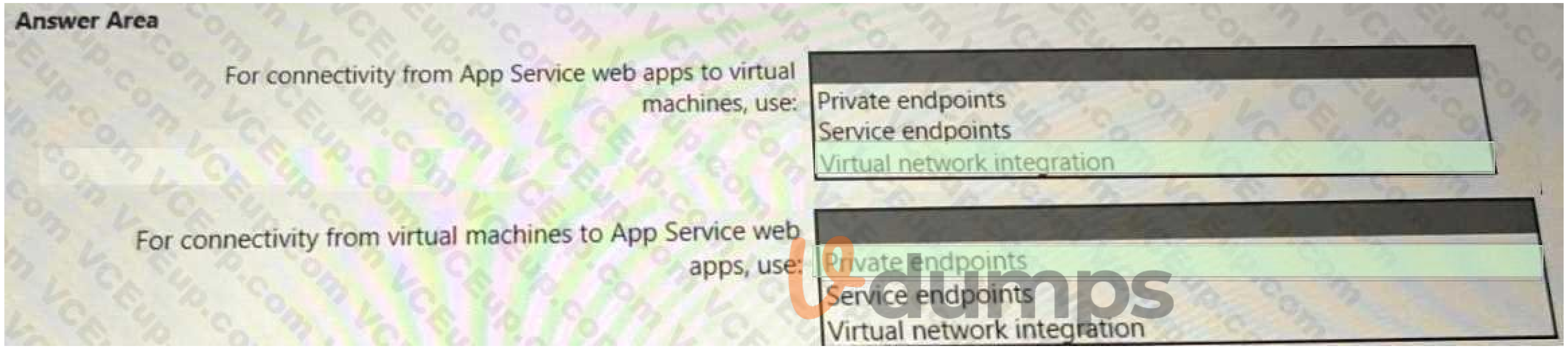
For connectivity from App Service web apps to virtual machines, use:

- Private endpoints
- Service endpoints
- Virtual network integration

For connectivity from virtual machines to App Service web apps, use:

- Private endpoints
- Service endpoints
- Virtual network integration

Answer Area:



Answer Area

For connectivity from App Service web apps to virtual machines, use:

- Private endpoints
- Service endpoints
- [✓ Virtual network integration]

For connectivity from virtual machines to App Service web apps, use:

- [✓ Private endpoints]
- Service endpoints
- Virtual network integration

Section:

Explanation:

Box 1: Virtual Network Integration - correct 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. Box 2: Private Endpoints. - correct You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.

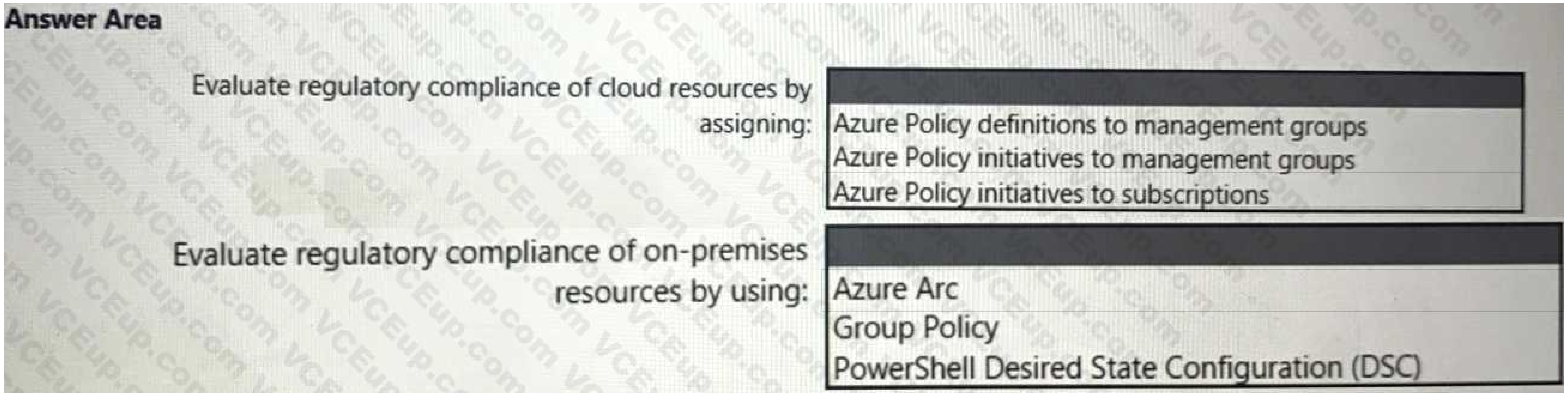
QUESTION 6

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

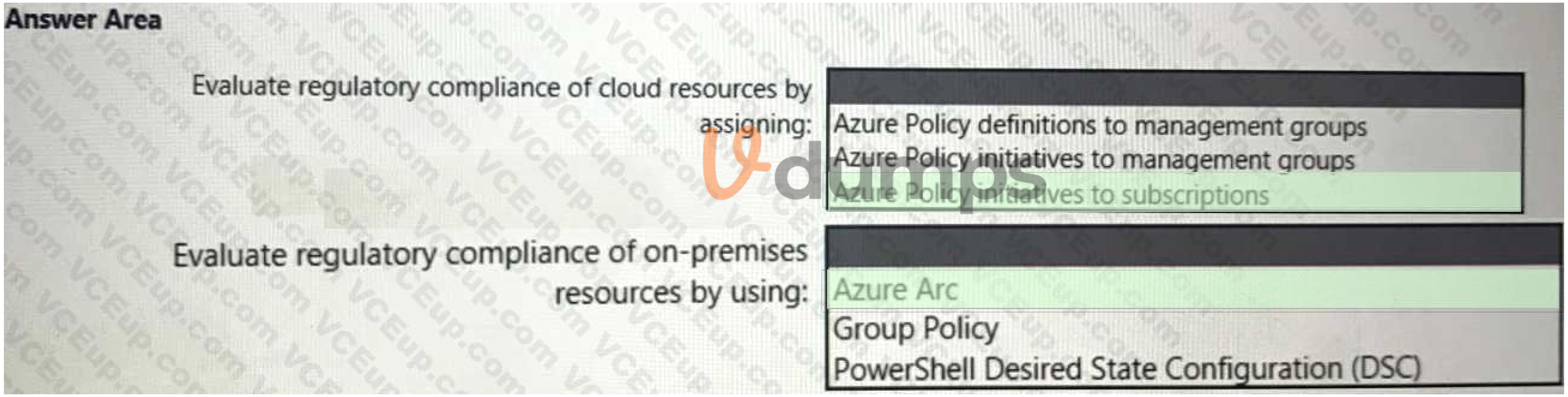
Evaluate regulatory compliance of cloud resources by assigning:

- 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)

Answer 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)

Section:
Explanation:

QUESTION 7

You need to design a strategy for securing the SharePoint Online and Exchange Online dat a. 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. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. Microsoft Defender for Endpoint
E. access reviews in Azure AD

Correct Answer: A, B

Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional- access-session#conditional-access-application-control
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate- with-microsoft-cloud-application-security

QUESTION 8
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: A, D
Section:

QUESTION 9
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?

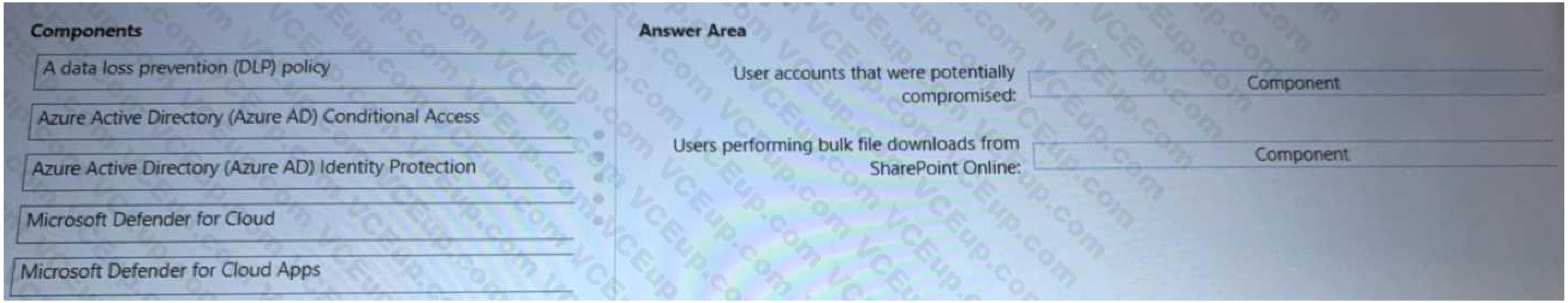
A. Azure DDoS Protection Standard
B. an Azure Private DNS zone
C. Microsoft Defender for Cloud
D. an ExpressRoute gateway

Correct Answer: D
Section:
Explanation:
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

Exam A

QUESTION 1
DRAG DROP
You have a Microsoft 365 subscription
You need to recommend a security solution to monitor the following activities:
• User accounts that were potentially compromised
• Users performing bulk file downloads from Microsoft SharePoint Online What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each Correct selection is worth one Point.

Select and Place:



Components

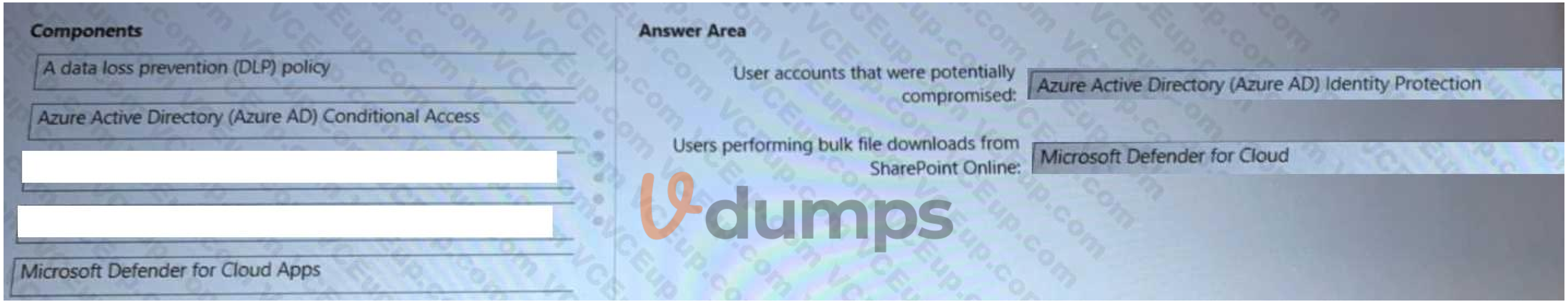
- A data loss prevention (DLP) policy
- Azure Active Directory (Azure AD) Conditional Access
- Azure Active Directory (Azure AD) Identity Protection
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer Area

User accounts that were potentially compromised: Component

Users performing bulk file downloads from SharePoint Online: Component

Correct Answer:



Components

- A data loss prevention (DLP) policy
- Azure Active Directory (Azure AD) Conditional Access
- Microsoft Defender for Cloud Apps

Answer Area

User accounts that were potentially compromised: Azure Active Directory (Azure AD) Identity Protection

Users performing bulk file downloads from SharePoint Online: Microsoft Defender for Cloud

Section:

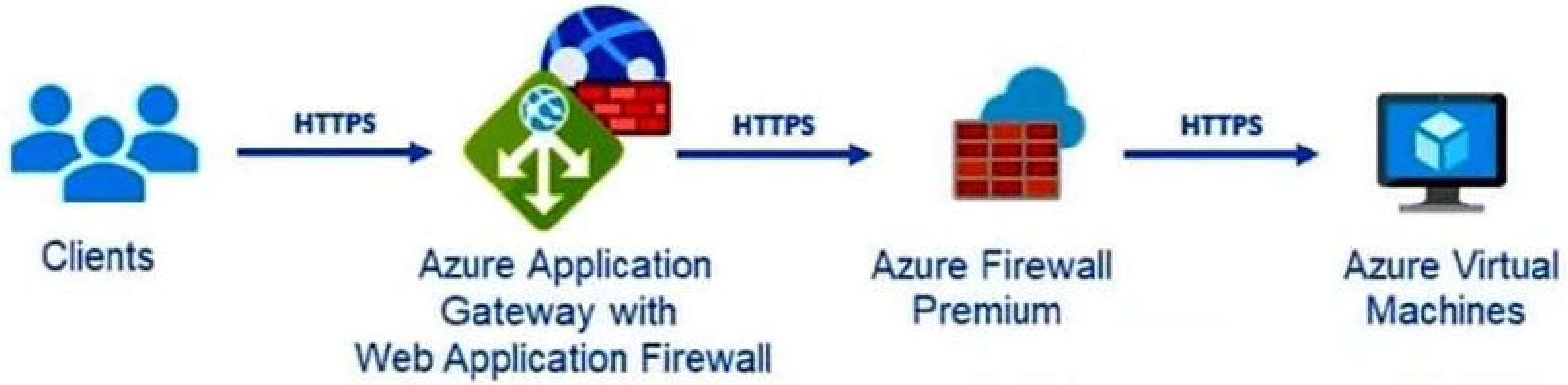
Explanation:

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 2

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.

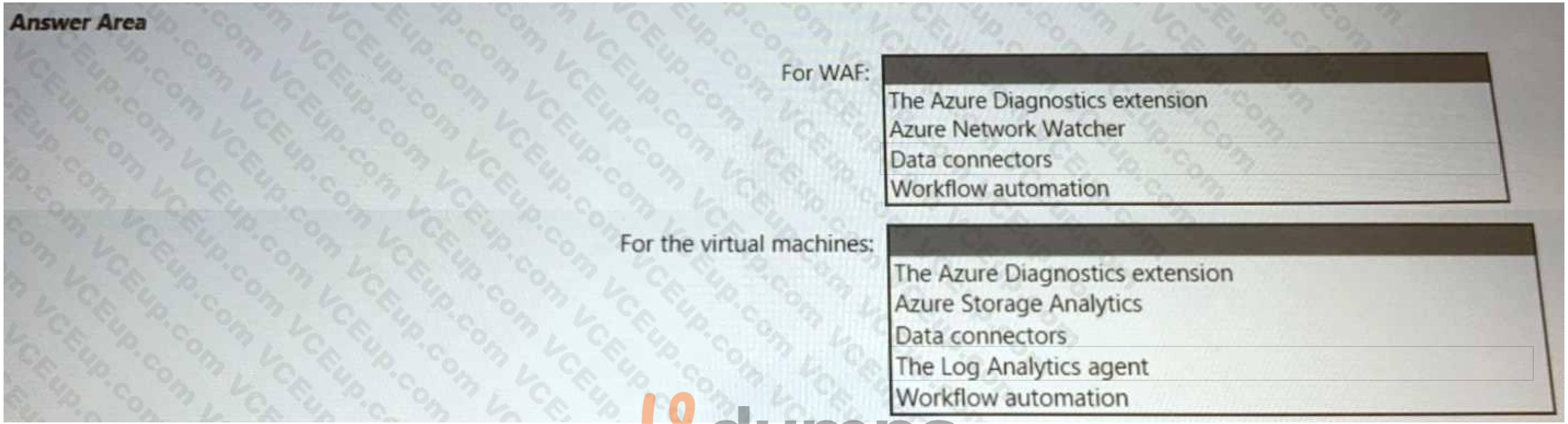


You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

- 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 are a. NOTE: Each correct selection is worth one point.

Hot Area:

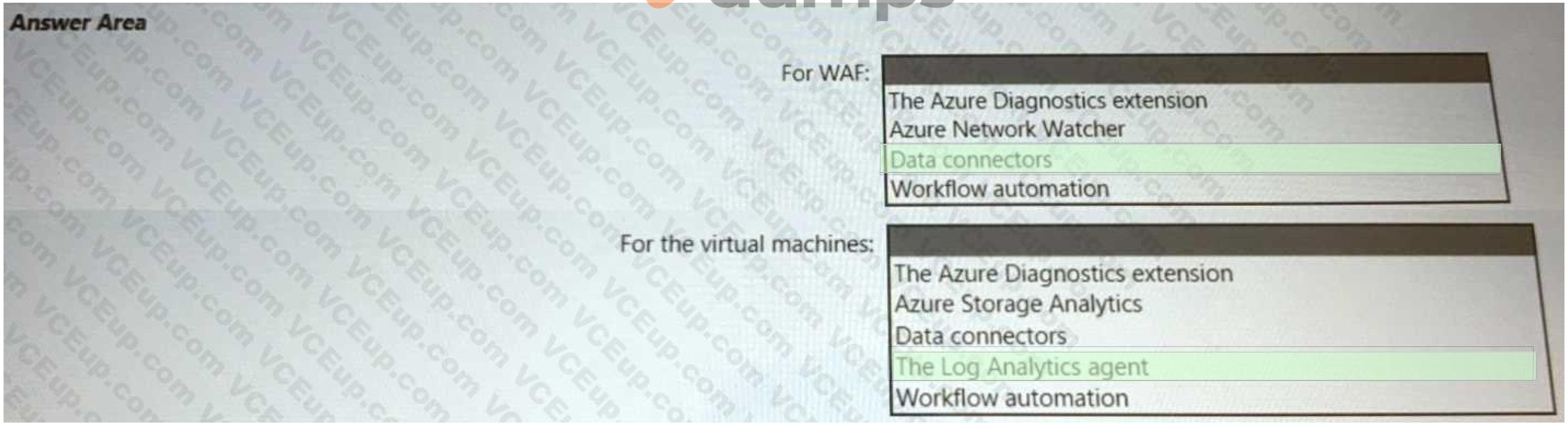


Answer Area

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

Answer 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

Section:

Explanation:

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.

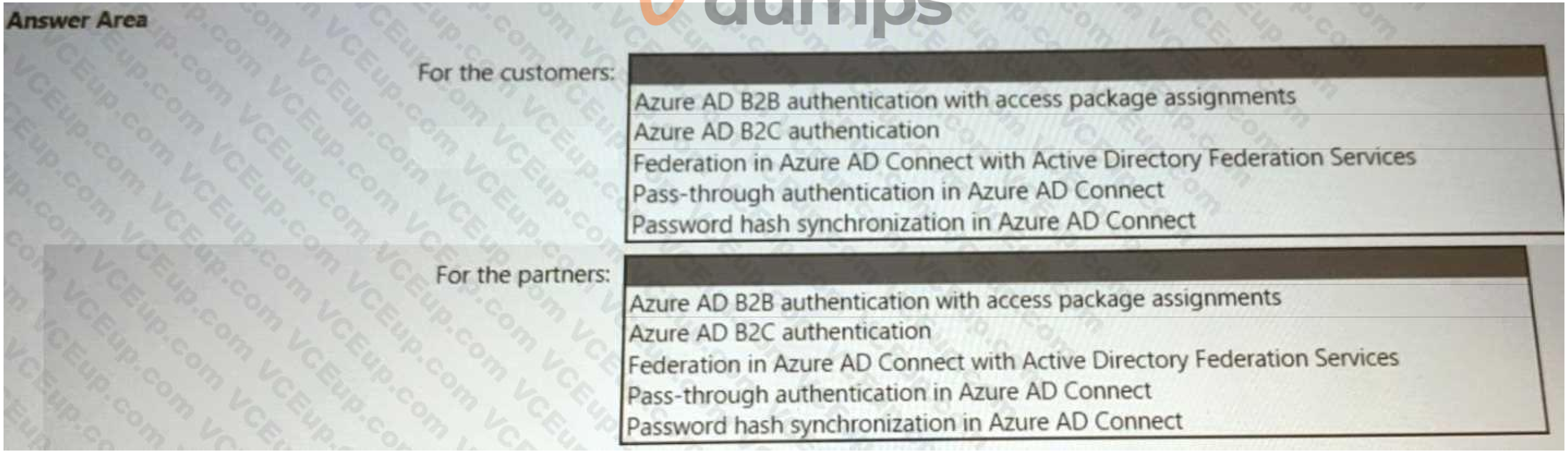
Box 2: The Log Analytics agent -
Use the Log Analytics agent to integrate with Microsoft Defender for cloud.

QUESTION 3
HOTSPOT
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DSV 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:

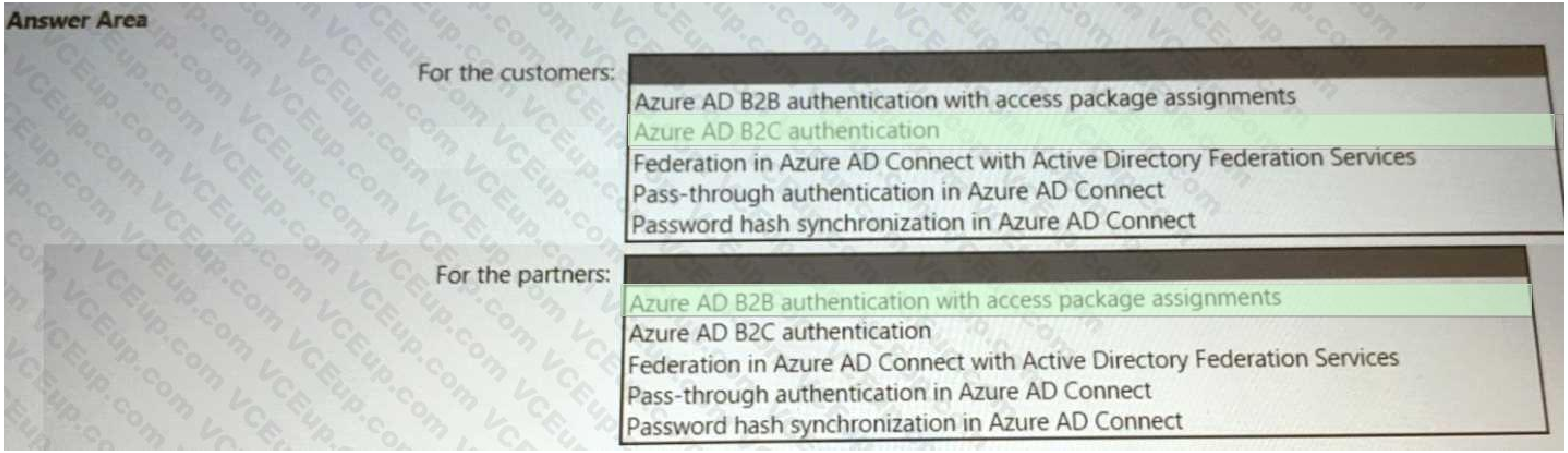


Answer Area

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

Answer 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

Section:

Explanation:

Box 1 --> https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview

Box 2 -- > https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity- providers

QUESTION 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:

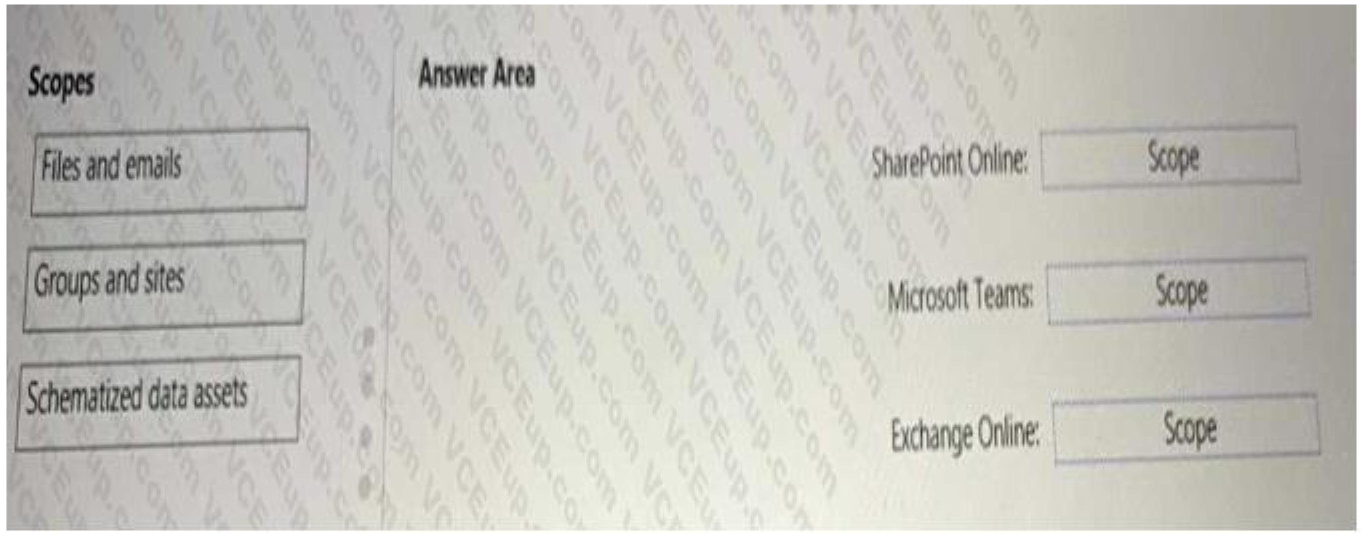
- Microsoft SharePoint Online
- Microsoft Exchange Online
- Microsoft Teams

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 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:



Scopes

Files and emails

Groups and sites

Schematized data assets

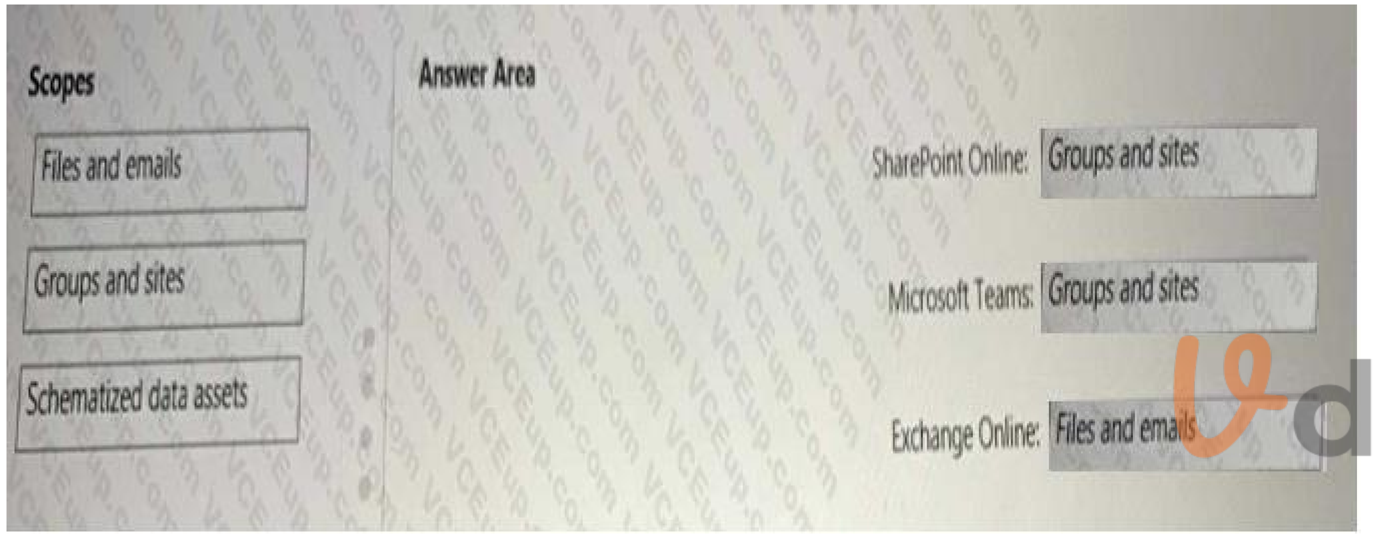
Answer Area

SharePoint Online: Scope

Microsoft Teams: Scope

Exchange Online: Scope

Correct Answer:



Scopes

Files and emails

Groups and sites

Schematized data assets

Answer Area

SharePoint Online: Groups and sites

Microsoft Teams: Groups and sites

Exchange Online: Files and emails

Section:

Explanation:

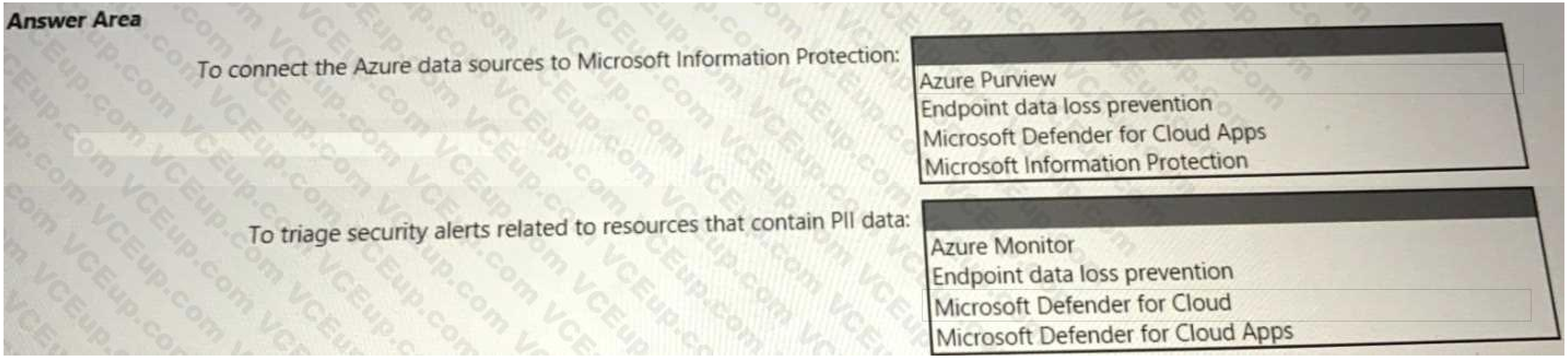
Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails – https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide Go to label scopes

QUESTION 5

HOTSPOT

Your company is migrating data to Azure. The data contains Personally Identifiable Information (Pll). The company plans to use Microsoft Information Protection for the Pll data store in Azure. You need to recommend a solution to discover Pll 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

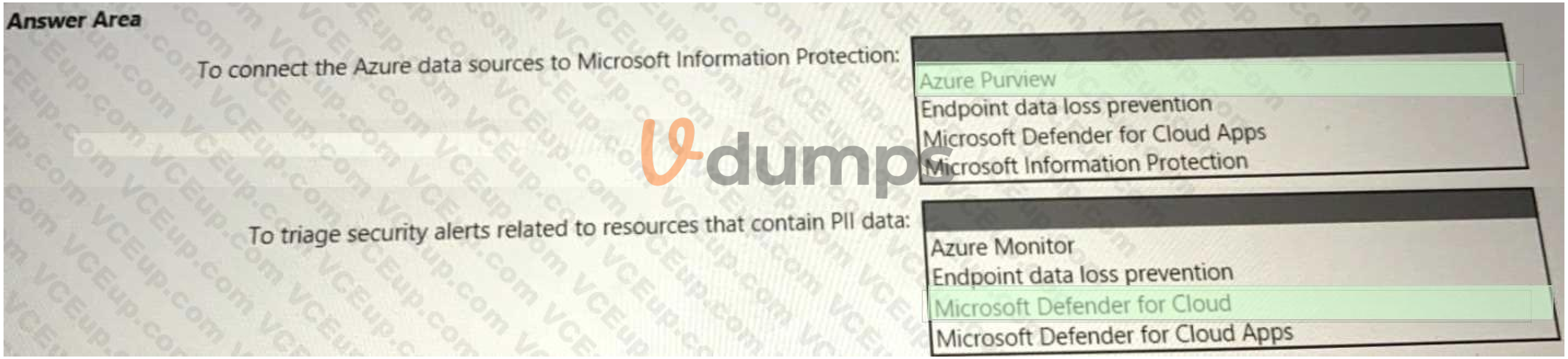
To connect the Azure data sources to Microsoft Information Protection:

- 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:



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

Section:

Explanation:

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 6

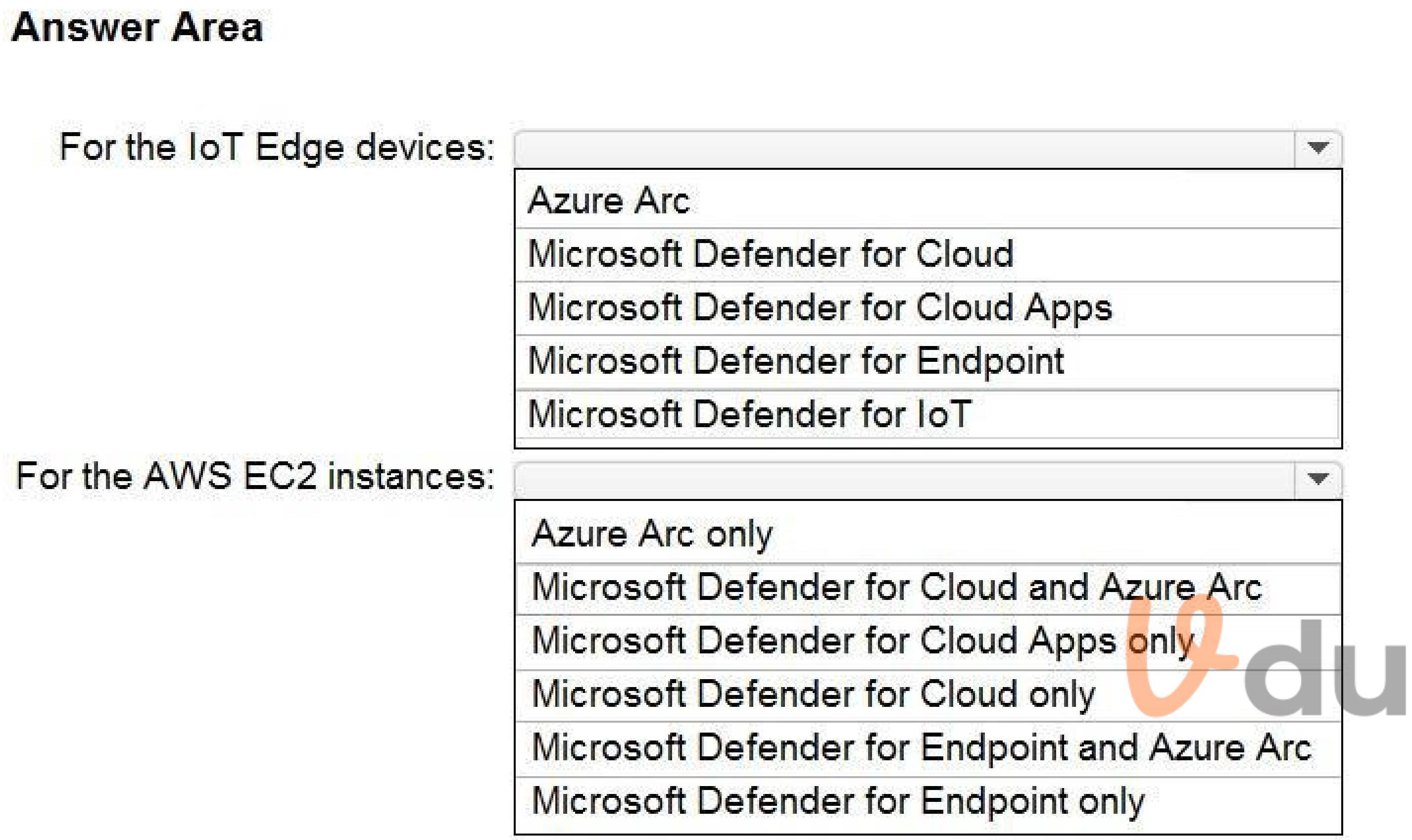
HOTSPOT

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

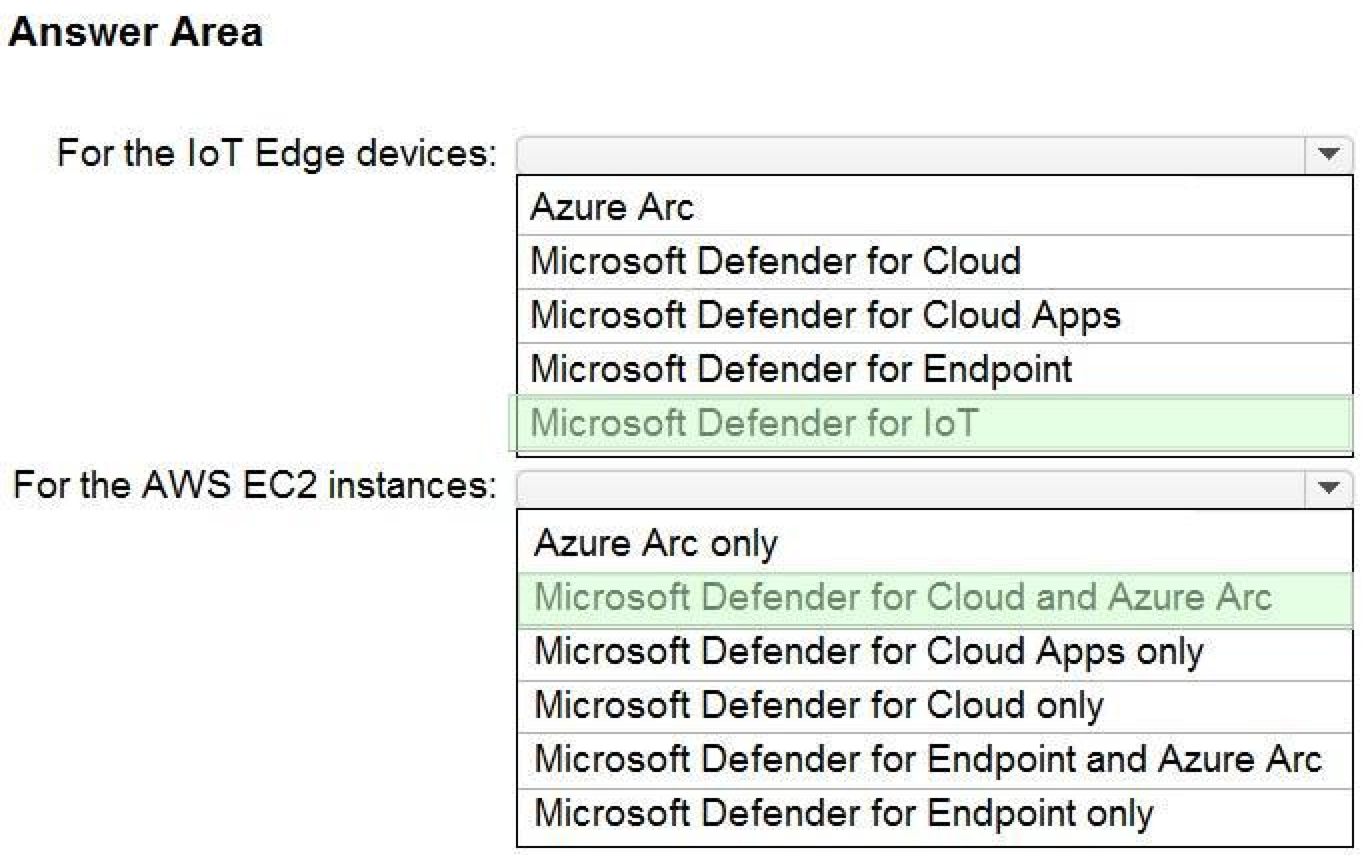
For the IoT Edge devices: ▼

- 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:



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

Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env- settings https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations

QUESTION 7

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.

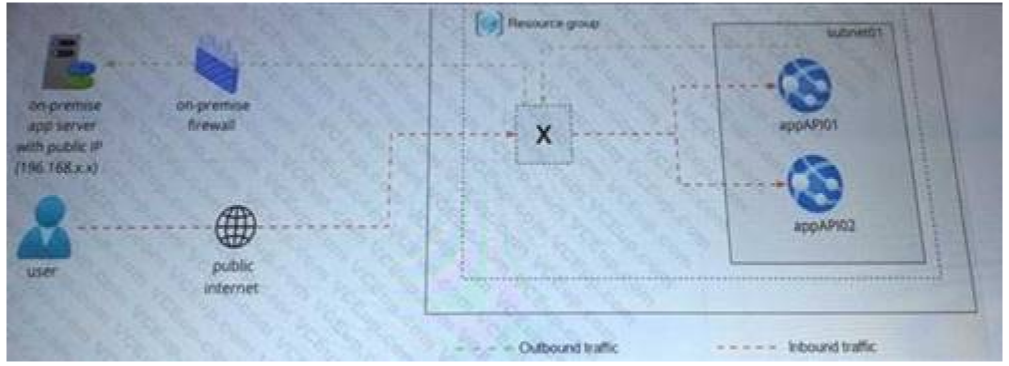
Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
B. Configure Azure VPN Gateway.
C. Enable Just Enough Administration (JEA).
D. Enable just-in-time (JIT) VM access.
E. Configure Azure Bastion.

Correct Answer: D, E
Section:
Explanation:
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

QUESTION 8

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 onpremises 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 Application Gateway v2 with user-defined routes (UDRs).
C. Azure Front Door with Azure Web Application Firewall (WAF)
D. Azure Firewall with policy rule sets

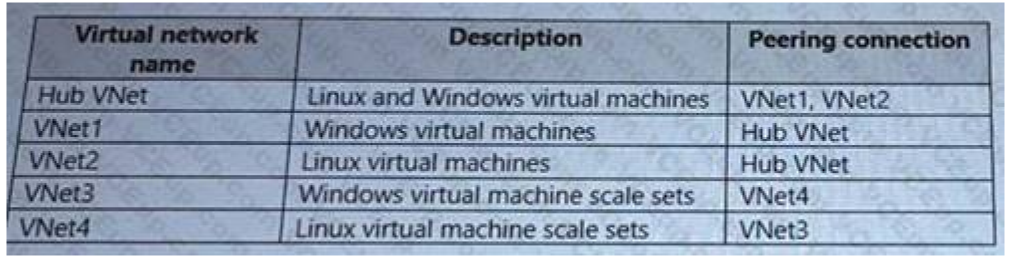
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

QUESTION 9
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. Microsoft Endpoint Manager
B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Correct Answer: D
Section:
Explanation:
ttps://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content- filtering?view=o365-worldwide#configure-web-content-filtering-policies

QUESTION 10
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

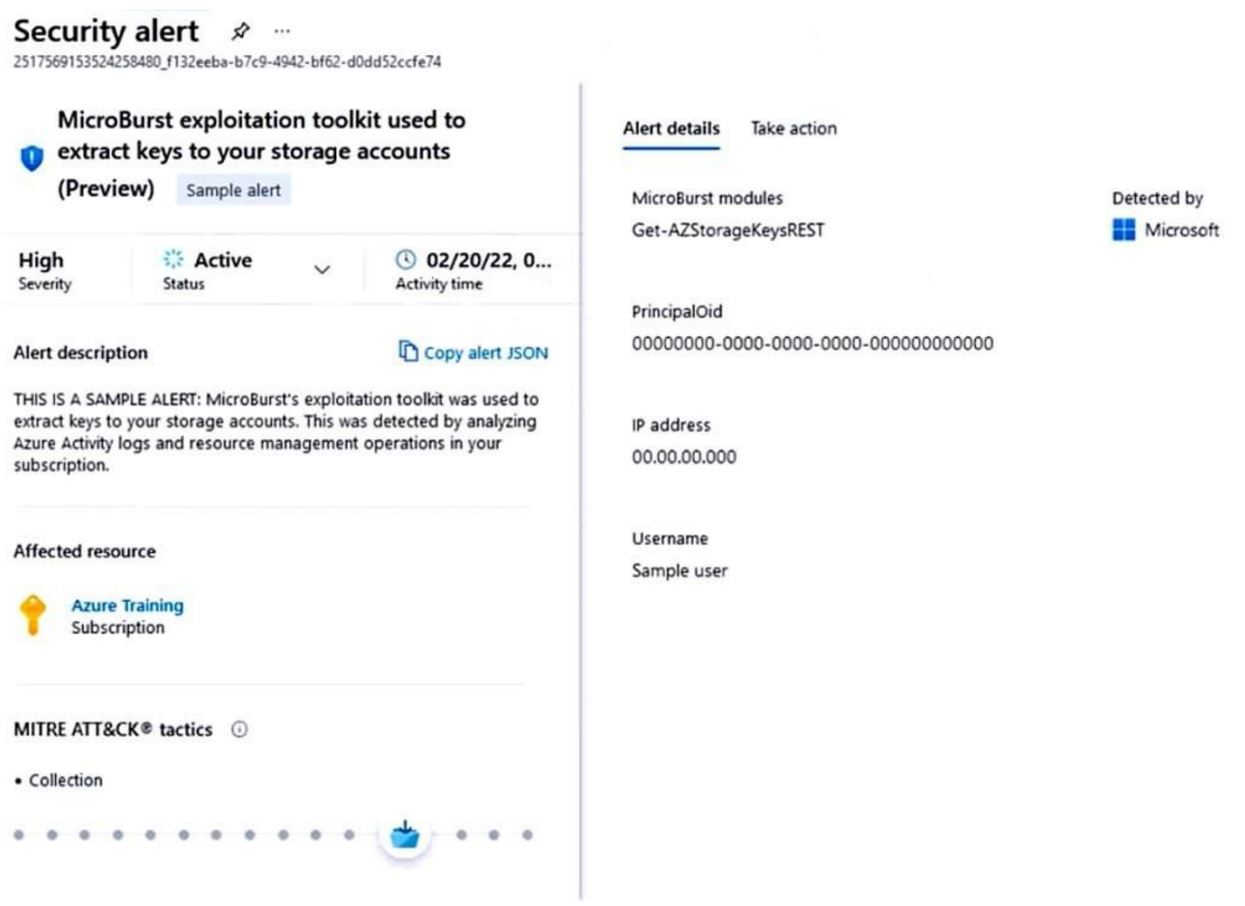
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure- bastion

QUESTION 11
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically. What should you use?

A. the regulatory compliance dashboard in Defender for Cloud
B. Azure Policy
C. Azure Blueprints
D. Azure role-based access control (Azure RBAC)

Correct Answer: B
Section:
Explanation:
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

QUESTION 12
You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



Security alert

2517569153524258480_f132eeba-b7c9-4942-bf62-d0dd52ccfe74

MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview) Sample alert

High
Severity

Active
Status

02/20/22, 0...
Activity time

Alert description

Copy alert JSON

THIS IS A SAMPLE ALERT: MicroBurst's exploitation toolkit was used to extract keys to your storage accounts. This was detected by analyzing Azure Activity logs and resource management operations in your subscription.

Affected resource

Azure Training
Subscription

MITRE ATT&CK® tactics

- Collection

Alert details | Take action

MicroBurst modules
Get-AZStorageKeysREST

Detected by
Microsoft

PrincipalOid
00000000-0000-0000-0000-000000000000

IP address
00.00.00.000

Username
Sample user

After remediating the threat which policy definition should you assign to prevent the threat from reoccurring?

A. Storage account public access should be disallowed

B. Azure Key Vault Managed HSM should have purge protection enabled

C. Storage accounts should prevent shared key access

D. Storage account keys should not be expired

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent

QUESTION 13

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 NOTE: Each correct selection is worth one point.

A. Azure Firewall

B. Azure Web Application Firewall (WAF)

C. Microsoft Defender for Cloud alerts

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

E. Microsoft Sentinel

Correct Answer: A, B
Section:
Explanation:

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

QUESTION 14
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 insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

Correct Answer: A, C
Section:
Explanation:
https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service- encryption/

QUESTION 15
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 Storage Analytics
B. Azure Network Watcher
C. Microsoft Sentinel
D. Azure Policy

Correct Answer: D
Section:
Explanation:
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

QUESTION 16
You have 50 Azure subscriptions.
You need to monitor 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.
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: A, F
Section:
Explanation:
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

QUESTION 17
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
Section:

QUESTION 18
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 Conditional Access integration with user flows and custom policies
B. Azure AD workbooks to monitor risk detections
C. custom resource owner password credentials (ROPC) flows in Azure AD B2C
D. access packages in Identity Governance
E. smart account lockout in Azure AD B2C

Correct Answer: A, C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user- flow?pivots=b2c-user-flow

QUESTION 19
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. insider risk management policies
B. data loss prevention (DLP) policies
C. sensitivity label policies
D. retention policies

Correct Answer: C
Section:

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp- policy?view=o365-worldwide

QUESTION 20
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 Registry
B. Linux containers deployed to Azure Kubernetes Service (AKS)
C. Windows containers deployed to Azure Container Registry
D. Windows containers deployed to Azure Kubernetes Service (AKS)
E. Linux containers deployed to Azure Container Instances

Correct Answer: A, C
Section:
Explanation:
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas- services/9-specify-security-requirements-for-containers https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabilities-for-running-images

QUESTION 21
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. a private endpoint
B. hybrid connections
C. virtual network NAT gateway integration
D. virtual network integration

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

QUESTION 22
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 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. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

QUESTION 23
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. Azure Event Hubs
B. Azure Data Factor
C. a Microsoft Sentinel workbook
D. a Microsoft Sentinel data connector

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

QUESTION 24
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. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) Conditional Access
C. Microsoft Defender for servers
D. Azure Policy
E. Microsoft Defender for Containers

Correct Answer: B, D, E
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint- solutions-clouds-containers?tabs=aws-eks

QUESTION 25
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 Domain Services (Azure AD DS)
B. Azure Active Directory (Azure AD) B2C
C. Azure Active Directory (Azure AD)
D. Active Directory Domain Services (AD DS)

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

QUESTION 26
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
Section:
Explanation:

QUESTION 27
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
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 28
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
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a- specific-azure-front-door-instance

QUESTION 29
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
Section:

QUESTION 30
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. service chaining
B. local network gateways
C. forced tunneling
D. a VNet-to-VNet connection

Correct Answer: A
Section:

QUESTION 31
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. Policy Analyzer
C. Local Group Policy Object (LGPO)
D. Windows Autopilot

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security- configuration-framework/security-compliance-toolkit-10

QUESTION 32
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 end point.
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. Microsoft Defender for Endpoint reports the endpoints as compliant.
B. Microsoft Intune reports the endpoints as compliant.
C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
D. The client access tokens are refreshed.

Correct Answer: B, D
Section:

QUESTION 33

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription. All the 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 configurations to meet the following requirements:

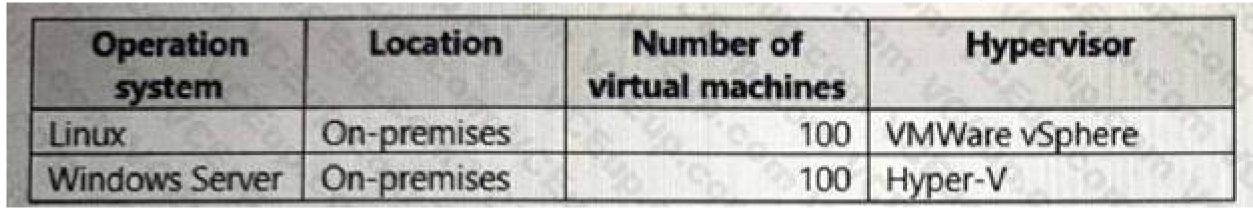
- Ensure that the security operations team can access the security logs and the operation logs.

• 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 configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Create a custom collector that uses the Log Analytics agent.

Correct Answer: B, C
Section:

QUESTION 34
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. Use customer-managed keys (CMKs) for encryption.
C. Require PINs to disable backups.
D. Implement Azure Site Recovery replication.

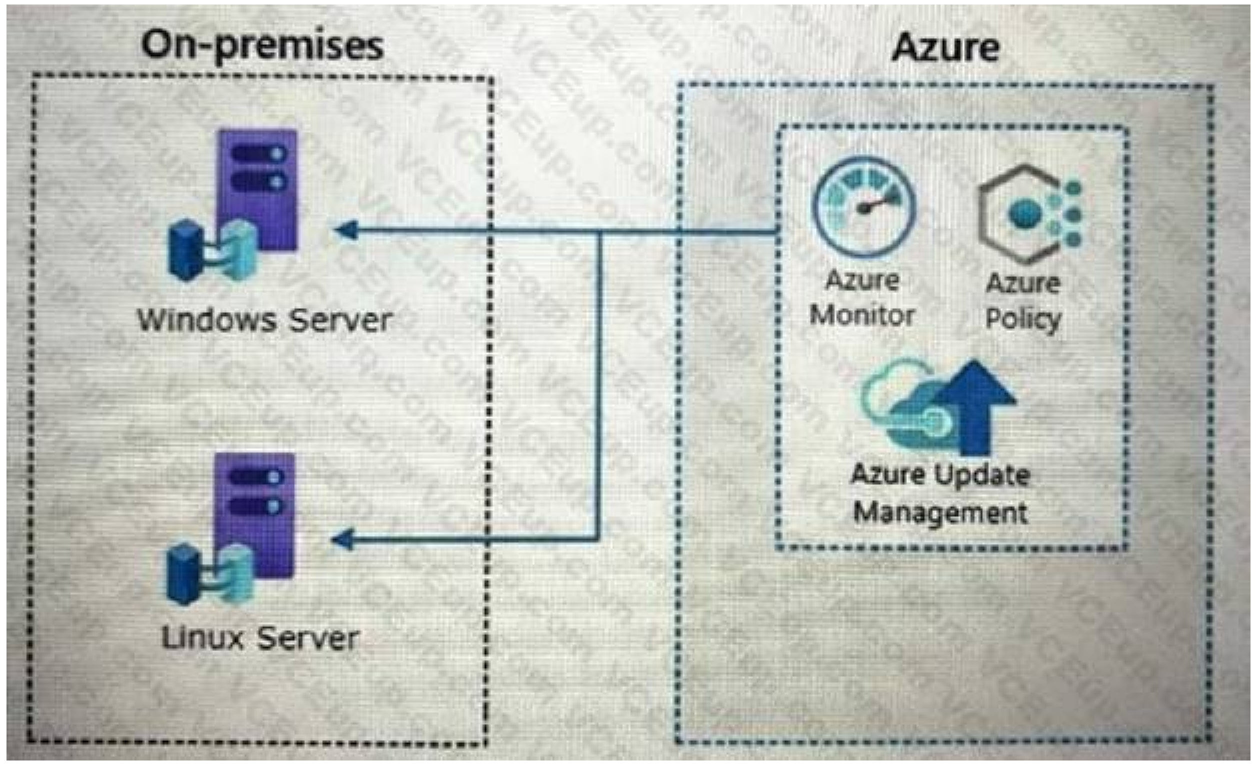
Correct Answer: C
Section:

QUESTION 35
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 Information Protection
B. Microsoft Defender for Endpoint
C. Microsoft Sentinel
D. Microsoft Endpoint Manager

Correct Answer: D
Section:

QUESTION 36
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 environment across the Azure policy.Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

A. Azure VPN Gateway
B. guest configuration in Azure Policy
C. on-premises data gateway
D. Azure Bastion
E. Azure Arc

Correct Answer: B, E
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

QUESTION 37
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. Enhanced Security Admin Environment (ESAE)
B. Microsoft Security Development Lifecycle (SDL)
C. Rapid Modernization Plan (RaMP)
D. Microsoft Operational Security Assurance (OSA)

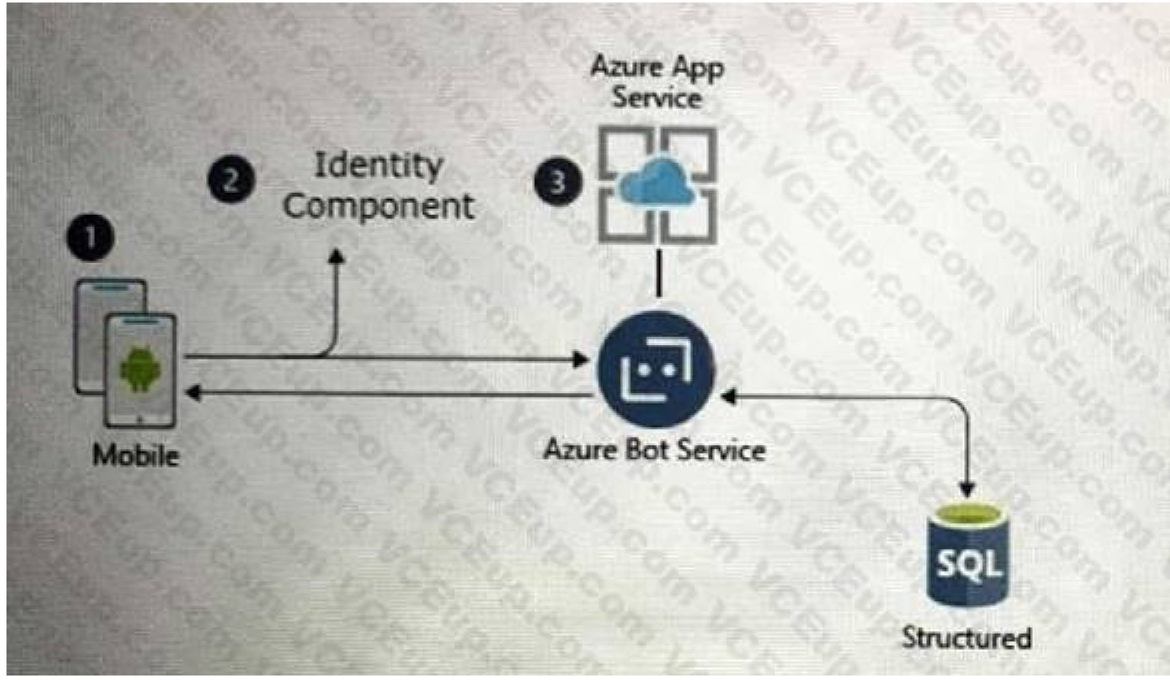
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

QUESTION 38
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. role-based authorization
B. Azure AD Privileged Identity Management (PIM)
C. resource-based authorization
D. Azure AD Multi-Factor Authentication

Correct Answer: D
Section:
Explanation:
(https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure) https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory- pricing?rtc=1

QUESTION 39
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.
• Be managed separately from the identity store of the customer.
• Support fully customizable branding for each app.
Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2C
B. Azure Active Directory (Azure AD) B2B
C. Azure AD Connect
D. Azure Active Directory Domain Services (Azure AD DS)

Correct Answer: A
Section:
Explanation:
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

QUESTION 40
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services. You need to recommend a solution for the customer. The solution must minimize costs.
What should you include in the recommendation?

A. Microsoft 365 Defender
B. Microsoft Defender for Cloud
C. Microsoft Defender for Cloud Apps
D. Microsoft Sentinel

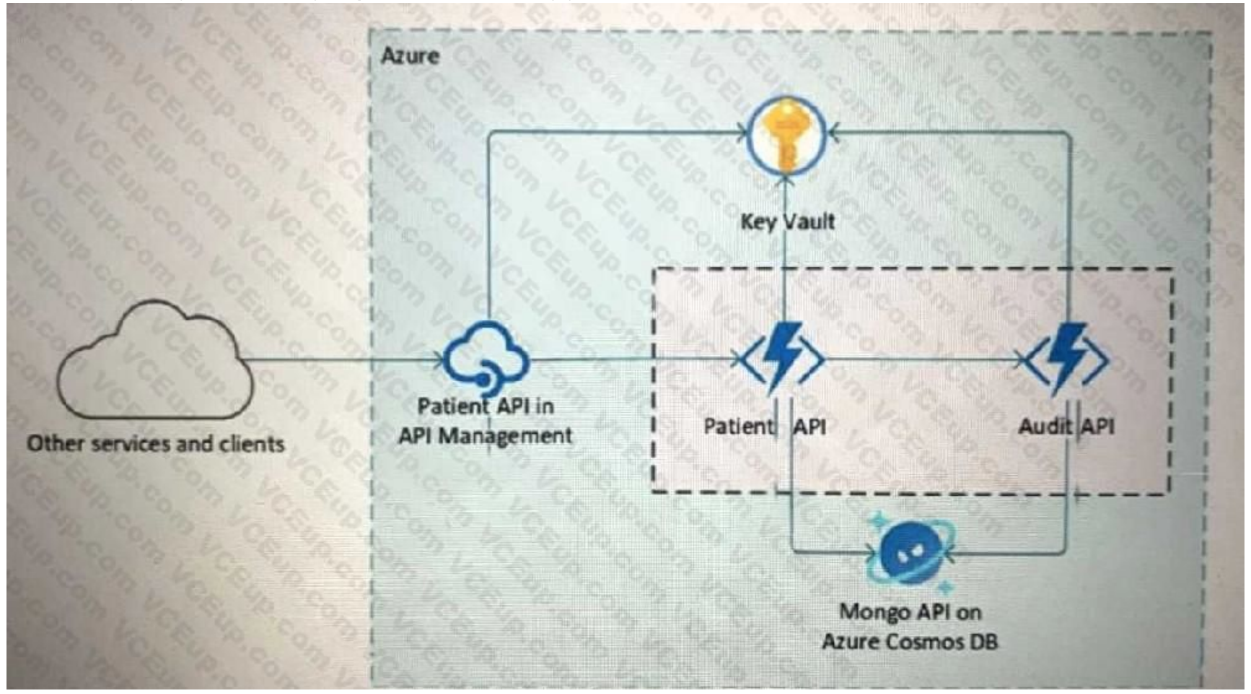
Correct Answer: D
Section:

QUESTION 41
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. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Correct Answer: A
Section:

QUESTION 42
Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.


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

You need to recommend a solution to isolate the compute components on an Azure virtual network.
What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications

B. an Azure App Service Environment (ASE)

C. Azure service endpoints

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

Correct Answer: B
Section:
Explanation:
App Service environments (ASEs) are appropriate for application workloads that require: Very high scale,Isolation and secure network access,High memory utilization.This capability can host your: Windows web apps,Linux web apps Docker containers,Mobile apps Functionshttps://docs.microsoft.com/en-us/azure/app-service/environment/overview

QUESTION 43
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 (Pll) 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. sensitivity label policies

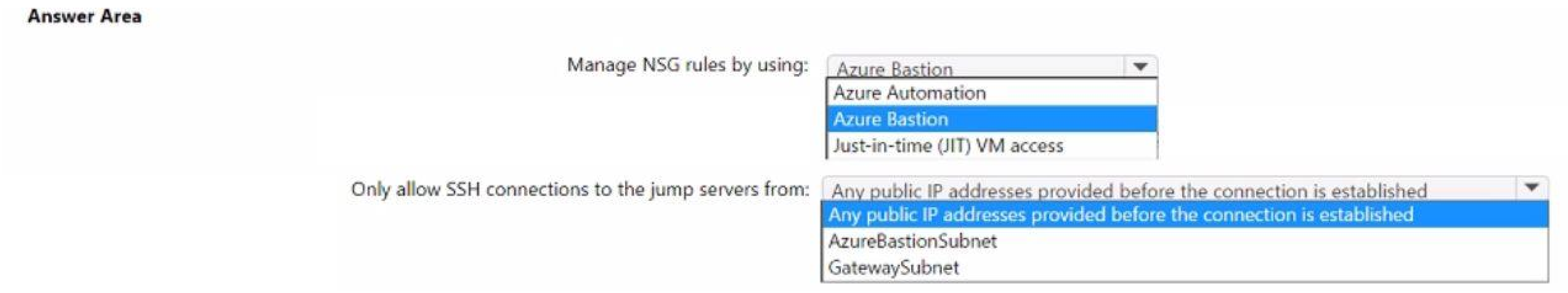
C. retention label policies

D. eDiscovery cases

Correct Answer: A, B
Section:
Explanation:
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.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.
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

QUESTION 44
HOTSPOT
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG).
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
* Ensure that each time the support staff connects to a jump server; they must request access to the server.
* Ensure that only authorized support staff can initiate SSH connections to the jump servers.
* Maximize protection against brute-force attacks from internal networks and the internet.
* Ensure that users can only connect to the jump servers from the internet.
* Minimize administrative effort.
What should you include in the solution? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

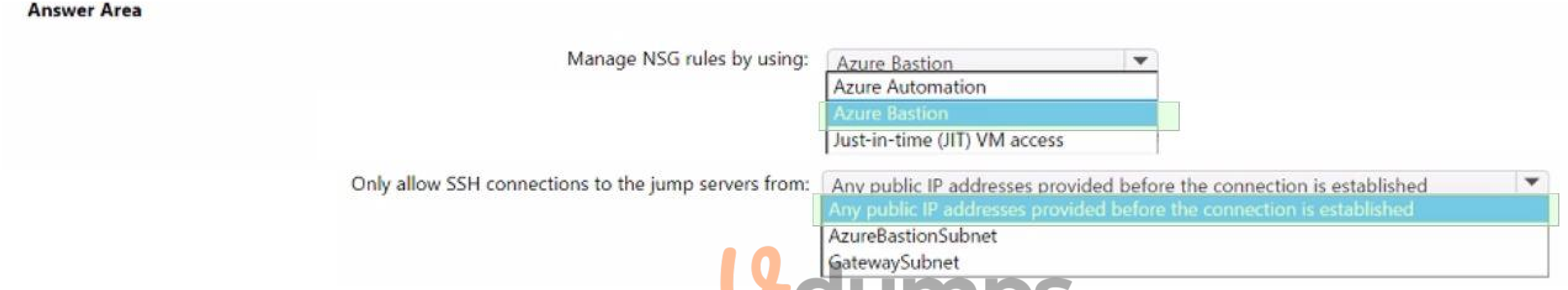
Manage NSG rules by using: Azure Bastion

- Azure Automation
- Azure Bastion
- Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established

- Any public IP addresses provided before the connection is established
- AzureBastionSubnet
- GatewaySubnet

Answer Area:



Answer Area

Manage NSG rules by using: Azure Bastion

- Azure Automation
- Azure Bastion
- Just-in-time (JIT) VM access

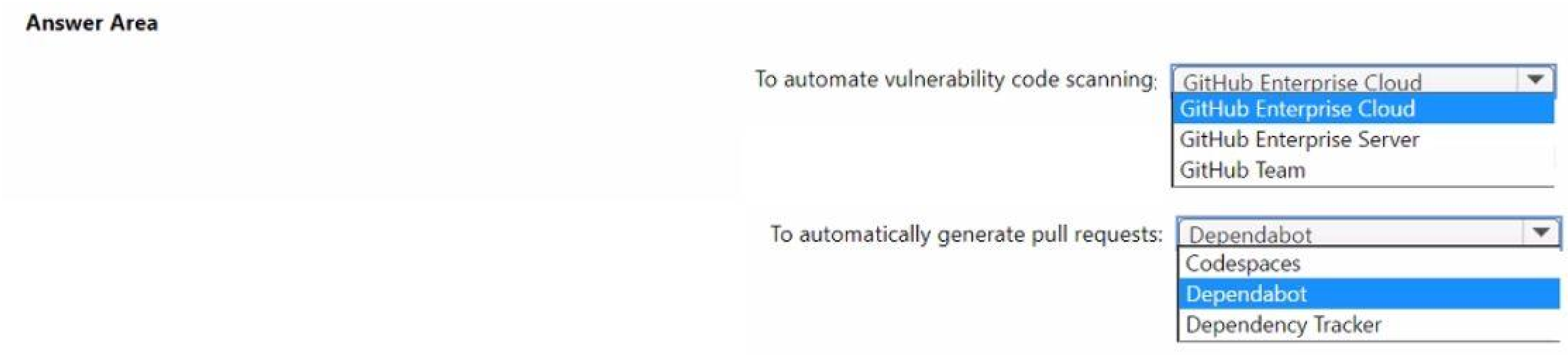
Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established

- Any public IP addresses provided before the connection is established
- AzureBastionSubnet
- GatewaySubnet

Section:
Explanation:

QUESTION 45
HOTSPOT
You plan to automate the development and deployment of a Nodejs-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.

Hot Area:

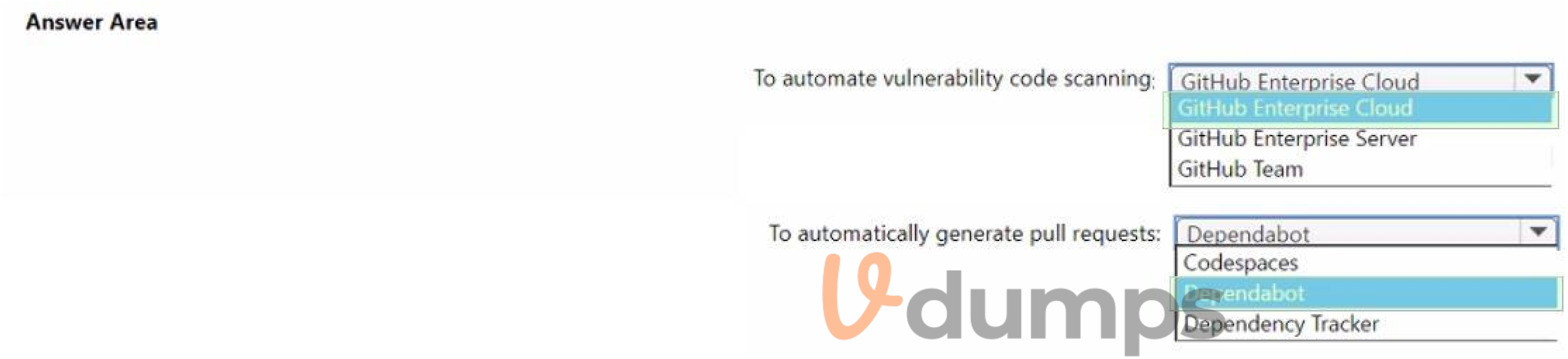


Answer Area

To automate vulnerability code scanning: GitHub Enterprise Cloud

To automatically generate pull requests: Dependabot

Answer Area:



Answer Area

To automate vulnerability code scanning: GitHub Enterprise Cloud

To automatically generate pull requests: Dependabot

Section:
Explanation:

QUESTION 46

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
Section:

QUESTION 47

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
Section:

QUESTION 48
You have an Azure AD tenant that contains 10 Windows 11 devices and two groups named Group1 and Group2. The Windows 11 devices are joined to the Azure AD tenant and are managed by using Microsoft Intune.
You are designing a privileged access strategy based on the rapid modernization plan (RaMP). The strategy will include the following configurations:
* Each user in Group1 will be assigned a Windows 11 device that will be configured as a privileged access device.
* The Security Administrator role will be mapped to the privileged access security level.
* The users in Group1 will be assigned the Security Administrator role.
* The users in Group2 will manage the privileged access devices.
You need to configure the local Administrators group for each privileged access device. The solution must follow the principle of least privilege.
What should you include in the solution?

A. Only add Group2 to the local Administrators group.
B. Configure Windows Local Administrator Password Solution (Windows LAPS) in legacy Microsoft LAPS emulation mode.
C. Add Group2 to the local Administrators group.
D. Add the user that is assigned the Security Administrator role to the local Administrators group of the user's assigned privileged access device.

Correct Answer: C
Section:

QUESTION 49
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. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

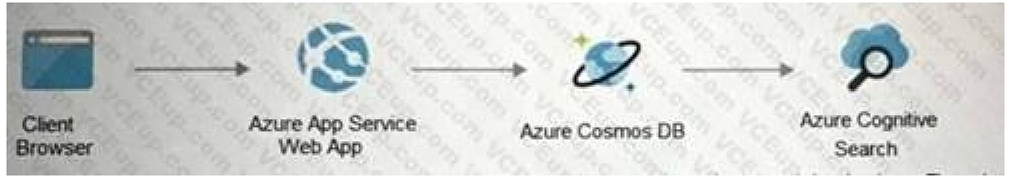
QUESTION 50

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
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access- to-my-backend-to-only-azure-front-door-

QUESTION 51
Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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

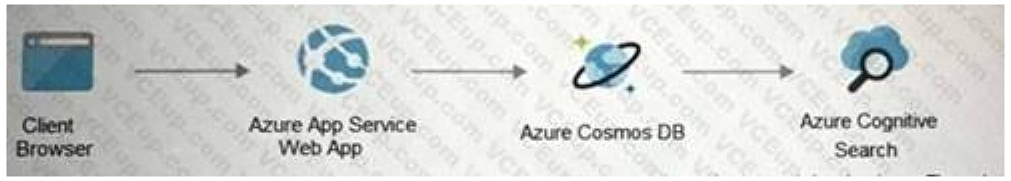
Correct Answer: A
Section:
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints

QUESTION 52
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
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 53
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
Section:
Explanation:
ttps://www.varonis.com/blog/securing-access-azure-webapps

QUESTION 54
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. adaptive application controls in Defender for Cloud
C. Azure Security Benchmark compliance controls m Defender for Cloud
D. app protection policies in Microsoft Endpoint Manager

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute- recommendations

QUESTION 55
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription. All the 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 configurations 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 configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

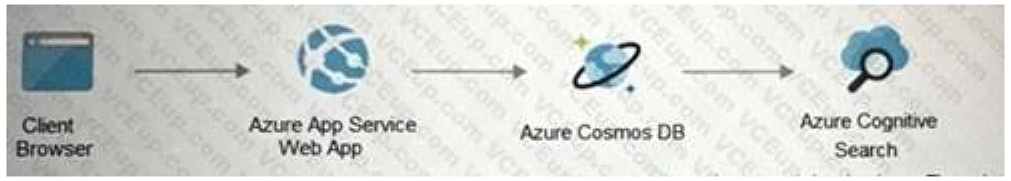
A. Azure Active Directory (Azure AD) Conditional Access policies
B. a custom collector that uses the Log Analytics agent
C. resource-based role-based access control (RBAC)
D. the Azure Monitor agent

Correct Answer: C, D
Section:
Explanation:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

QUESTION 56

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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.

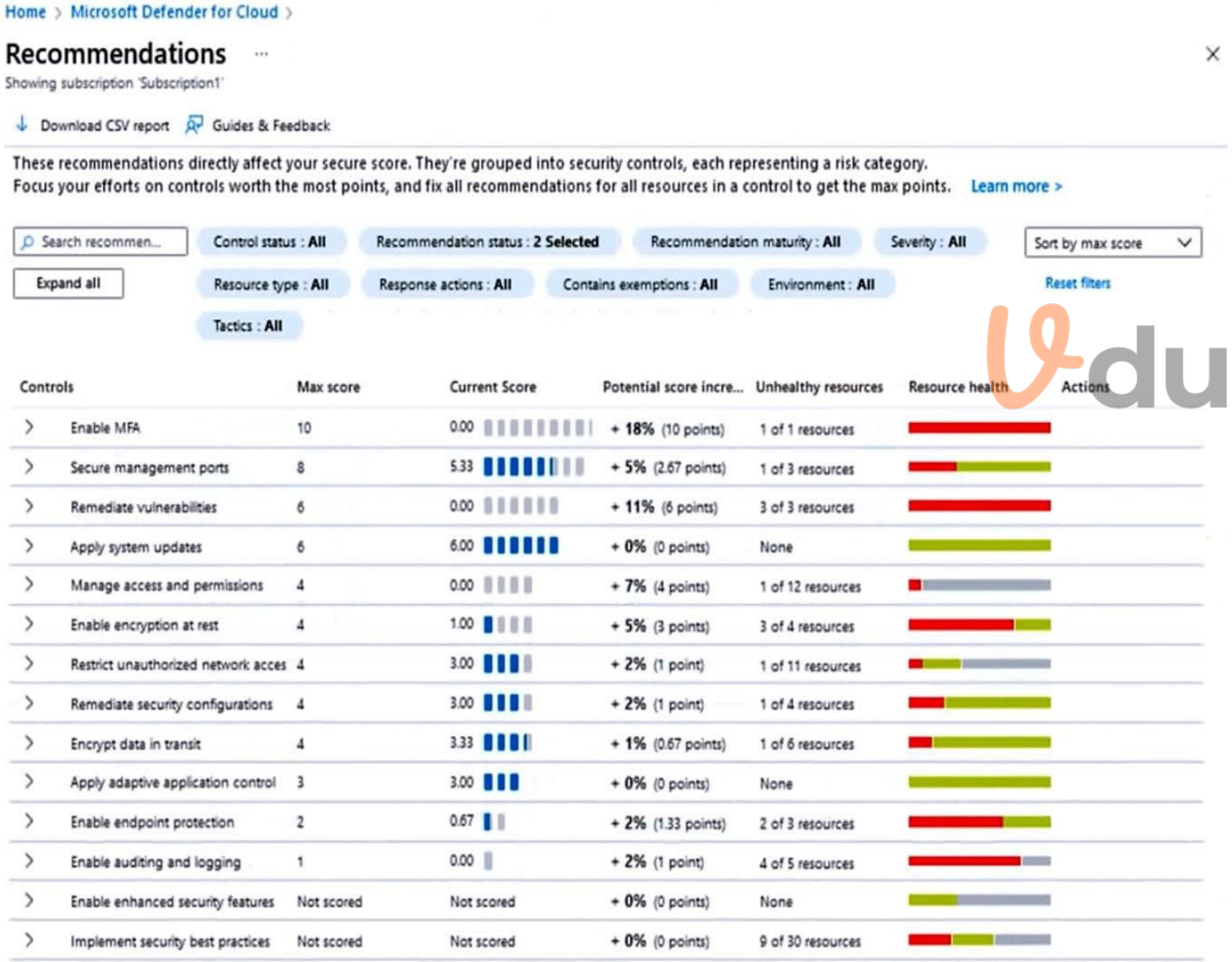

Client Browser
Azure App Service Web App
Azure Cosmos DB
Azure Cognitive Search

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.

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

QUESTION 57
HOTSPOT
You open Microsoft Defender for Cloud as shown in the following exhibit.



Recommendations ...

Showing subscription 'Subscription1'

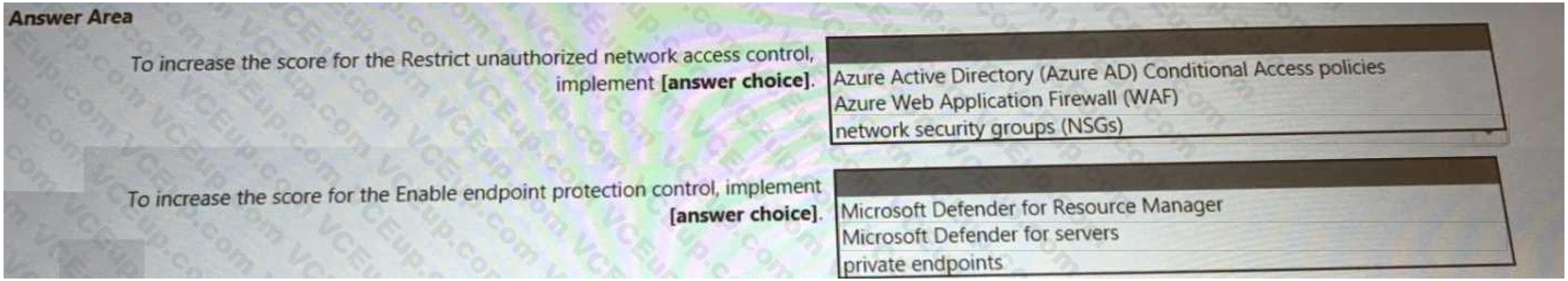
These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category.
Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points. Learn more >

Control status : All
Recommendation status : 2 Selected
Recommendation maturity : All
Severity : All
Resource type : All
Response actions : All
Contains exemptions : All
Environment : All
Tactics : All

Controls	Max score	Current Score	Potential score incre...	Unhealthy resources	Resource health	Actions
Enable MFA	10	0.00	+ 18% (10 points)	1 of 1 resources		
Secure management ports	8	5.33	+ 5% (2.67 points)	1 of 3 resources		
Remediate vulnerabilities	6	0.00	+ 11% (6 points)	3 of 3 resources		
Apply system updates	6	6.00	+ 0% (0 points)	None		
Manage access and permissions	4	0.00	+ 7% (4 points)	1 of 12 resources		
Enable encryption at rest	4	1.00	+ 5% (3 points)	3 of 4 resources		
Restrict unauthorized network acces	4	3.00	+ 2% (1 point)	1 of 11 resources		
Remediate security configurations	4	3.00	+ 2% (1 point)	1 of 4 resources		
Encrypt data in transit	4	3.33	+ 1% (0.67 points)	1 of 6 resources		
Apply adaptive application control	3	3.00	+ 0% (0 points)	None		
Enable endpoint protection	2	0.67	+ 2% (1.33 points)	2 of 3 resources		
Enable auditing and logging	1	0.00	+ 2% (1 point)	4 of 5 resources		
Enable enhanced security features	Not scored	Not scored	+ 0% (0 points)	None		
Implement security best practices	Not scored	Not scored	+ 0% (0 points)	9 of 30 resources		

Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

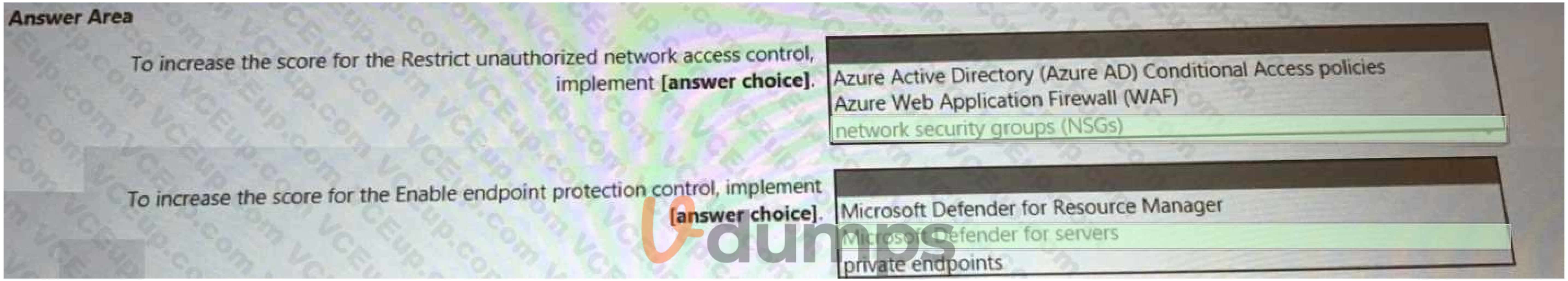
To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

- 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

Answer 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]**.

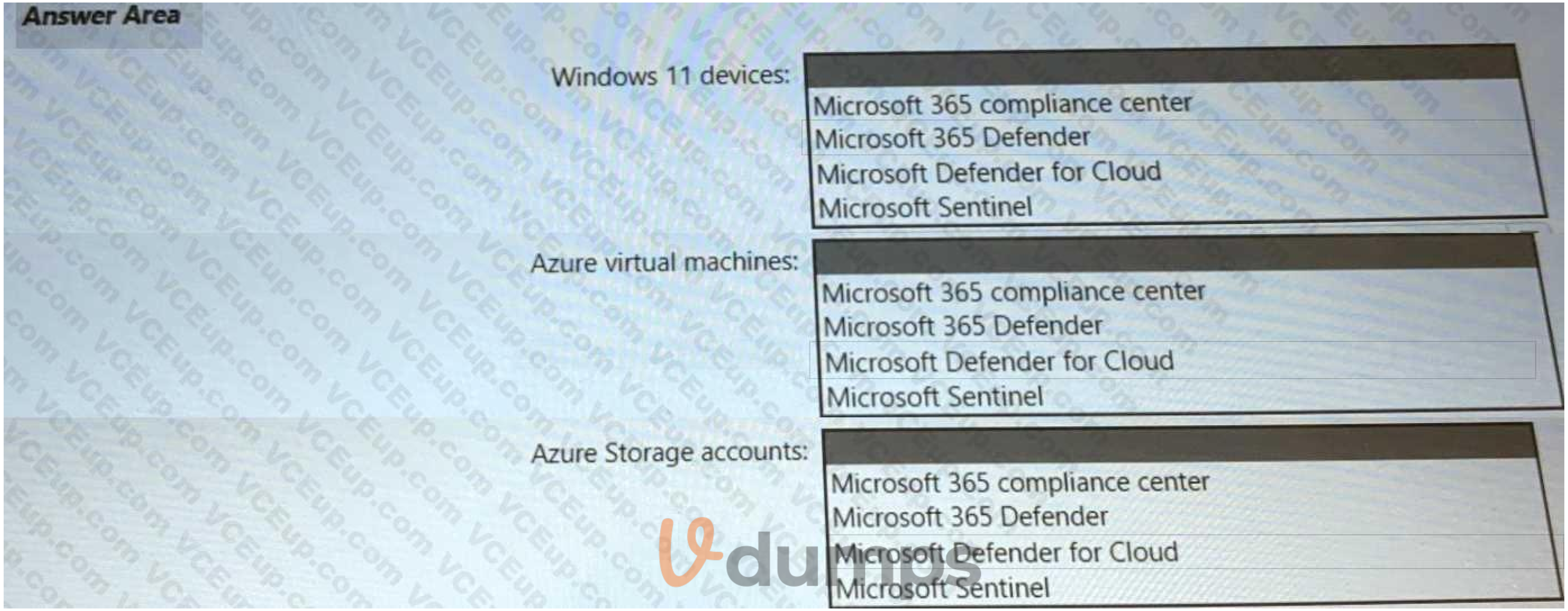
- Microsoft Defender for Resource Manager
- Microsoft Defender for servers
- private endpoints

Section:
Explanation:
Selection 1: NSG
https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833 Selection 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 58
HOTSPOT
You have a Microsoft 365 E5 subscription and an Azure subscripts 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.

Hot Area:



Answer Area

Windows 11 devices:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

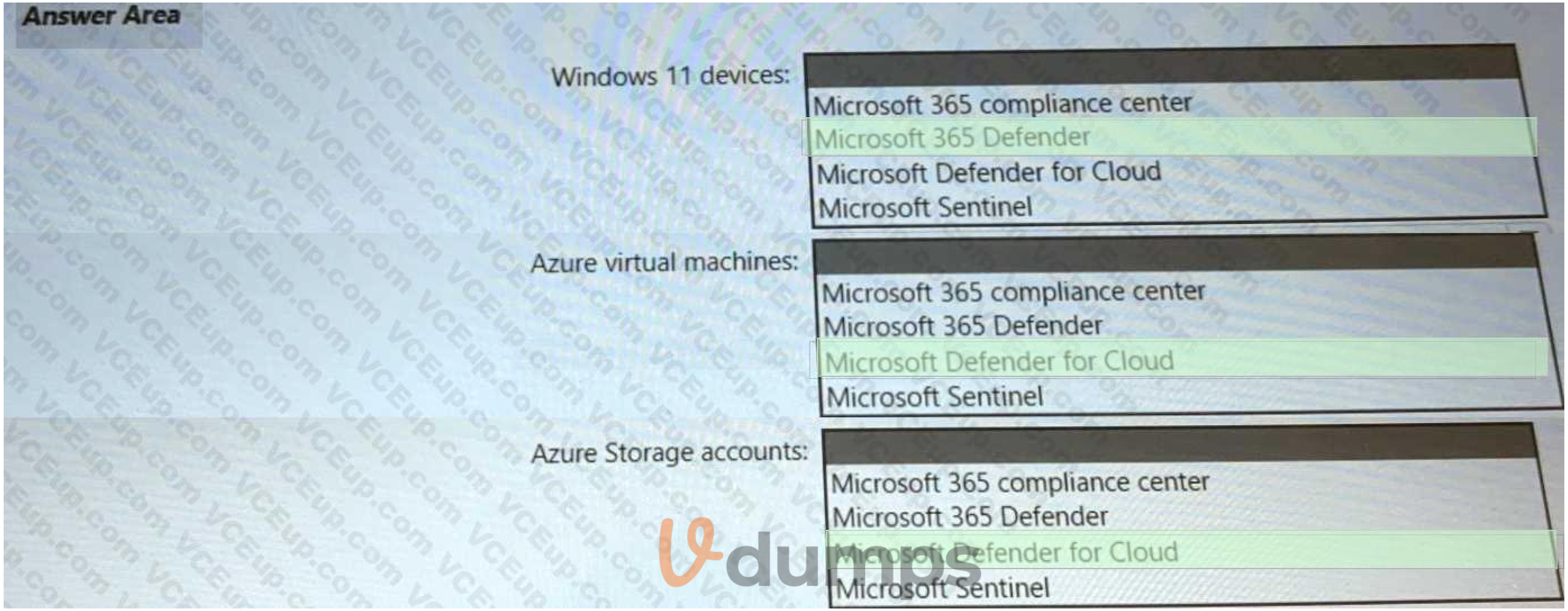
Azure virtual machines:

- 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:



Answer Area

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

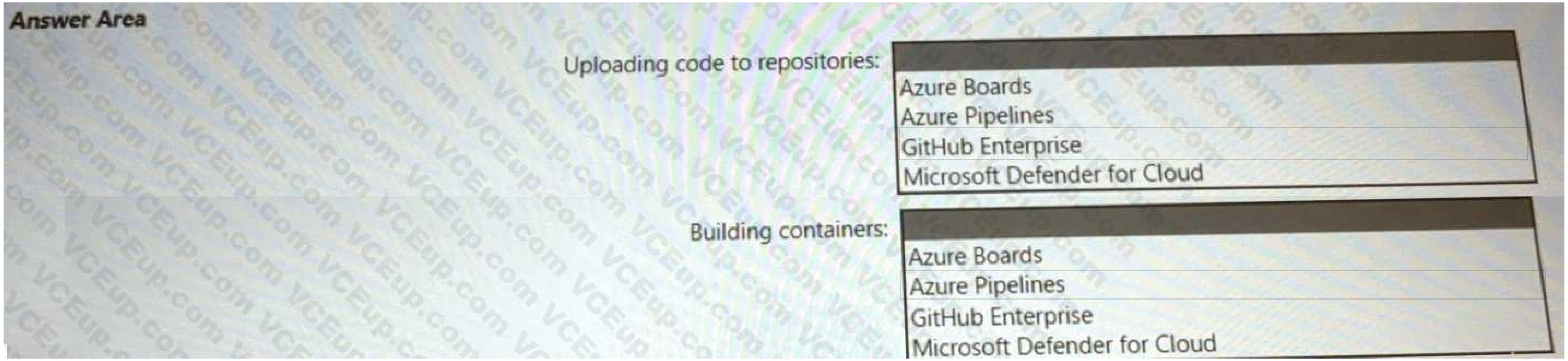
Azure virtual machines:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- [✓ Microsoft Defender for Cloud]
- Microsoft Sentinel

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

Section:
Explanation:
Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it).
Selection 2: Microsoft Defender for Cloud.
Selection 3: Microsoft Defender for Cloud.https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas- services/8-specify-security-requirements-for-storage-workloads

QUESTION 59
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.

Hot Area:



Answer Area

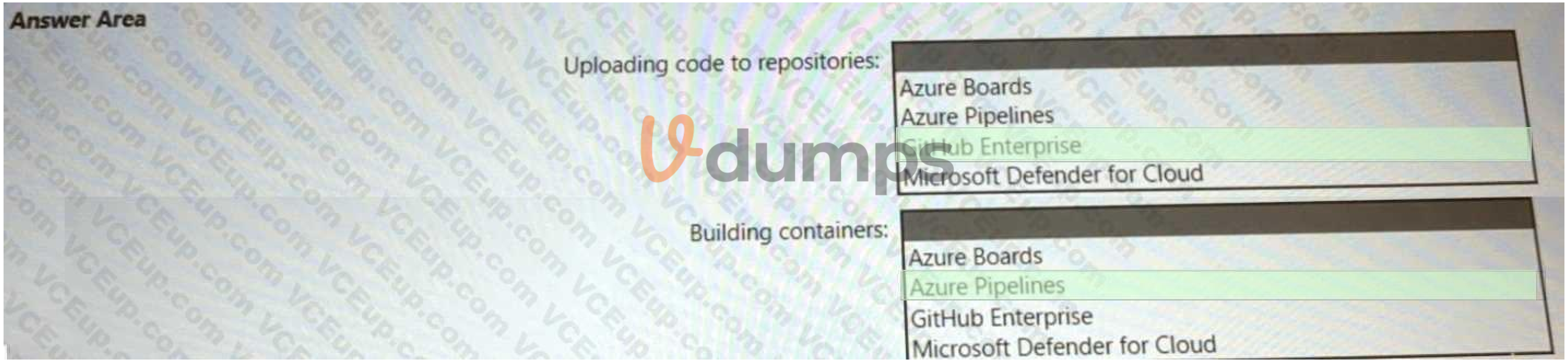
Uploading code to repositories:

- Azure Boards
- Azure Pipelines
- GitHub Enterprise
- Microsoft Defender for Cloud

Building containers:

- Azure Boards
- Azure Pipelines
- GitHub Enterprise
- Microsoft Defender for Cloud

Answer Area:



Answer Area

Uploading code to repositories:

- Azure Boards
- Azure Pipelines
- [✓ GitHub Enterprise]
- Microsoft Defender for Cloud

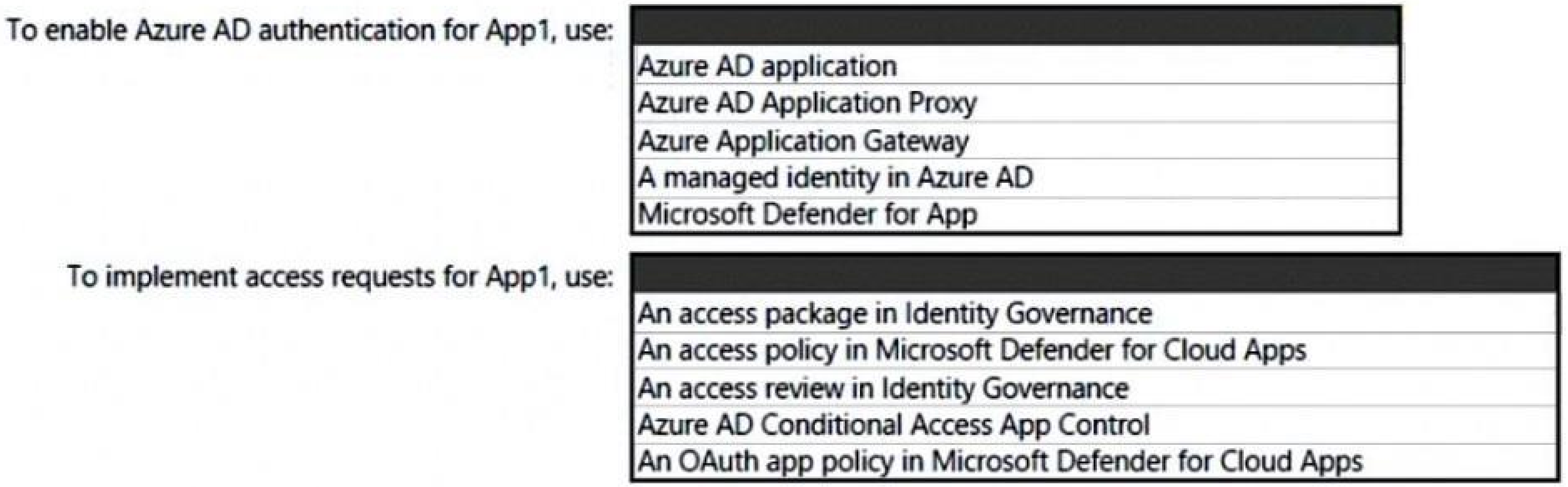
Building containers:

- Azure Boards
- [✓ Azure Pipelines]
- GitHub Enterprise
- Microsoft Defender for Cloud

Section:
Explanation:
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 60
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 are a. NOTE: Each correct selection is worth one point.

Hot Area:



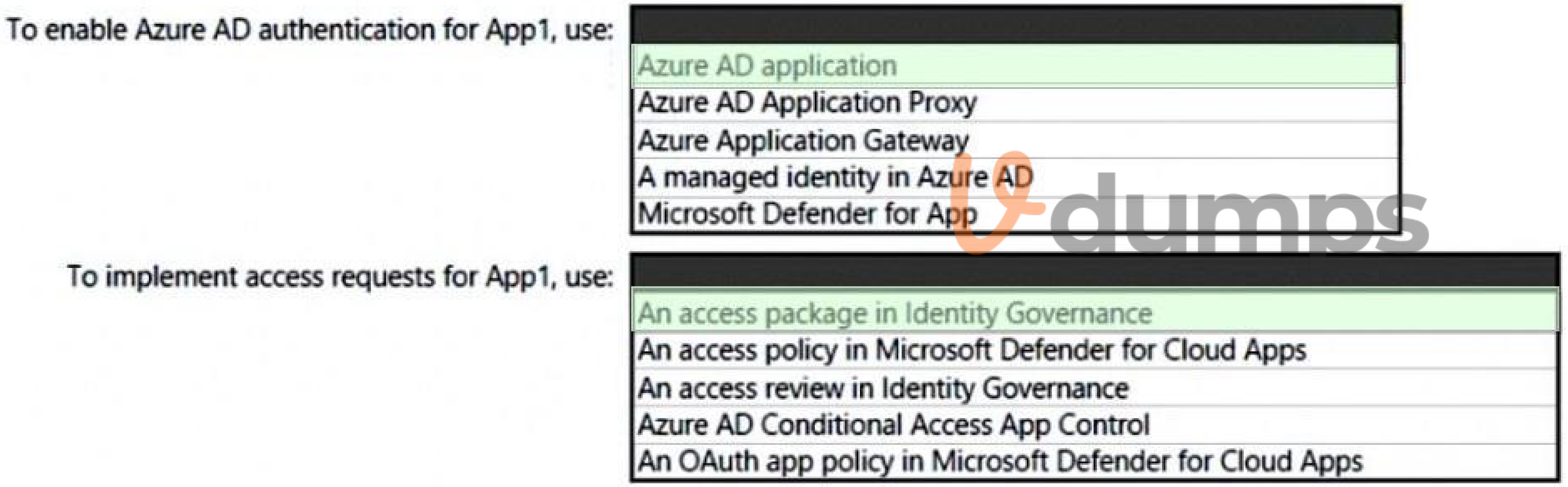
To enable Azure AD authentication for App1, use:

- 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

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

Section:
Explanation:
Azure AD application
(https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management) An access package in identity governance
(https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create)

QUESTION 61
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.

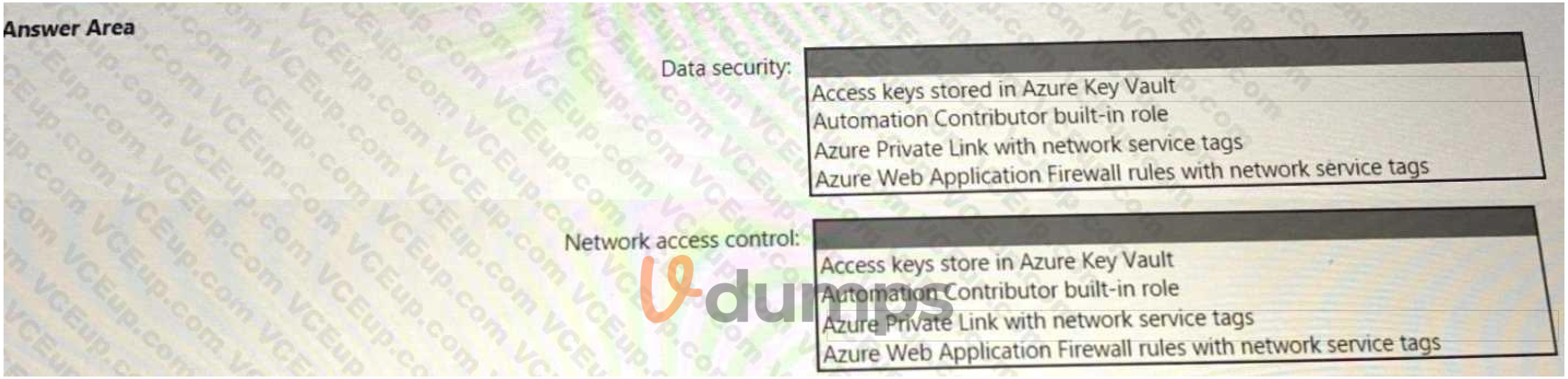
C. From Defender for Cloud, review the Azure security baseline for audit report.

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

Correct Answer: A
Section:

QUESTION 62
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:

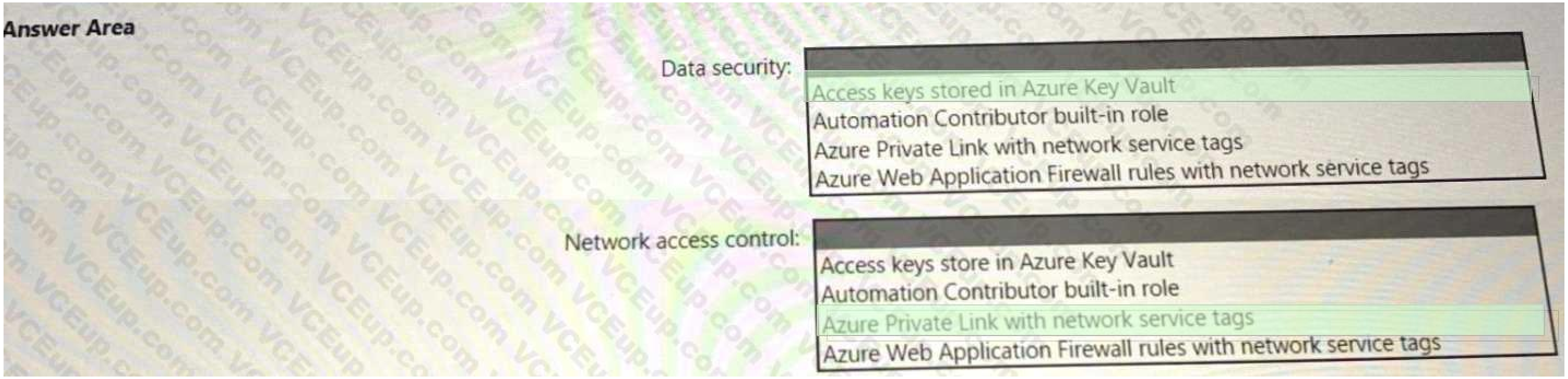


Answer Area

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 store 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

Answer 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 store 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

Section:
Explanation:

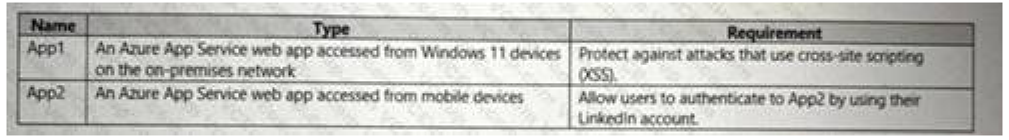
Data Security : Access Keys stored in Azure Key Vault
Network access control : Azure Private Link with network service tags

QUESTION 63

HOTSPOT

You have a hybrid cloud infrastructure.

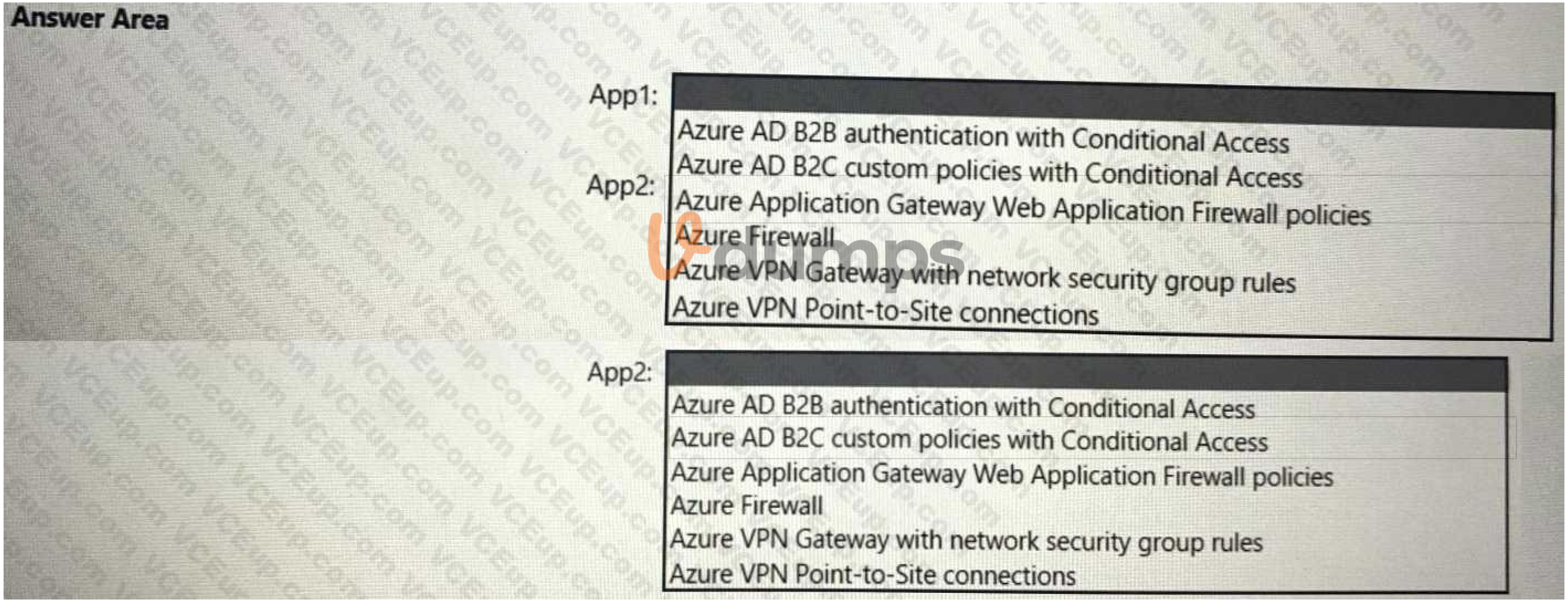
You plan to deploy the Azure applications shown in the following table.



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.

Hot Area:



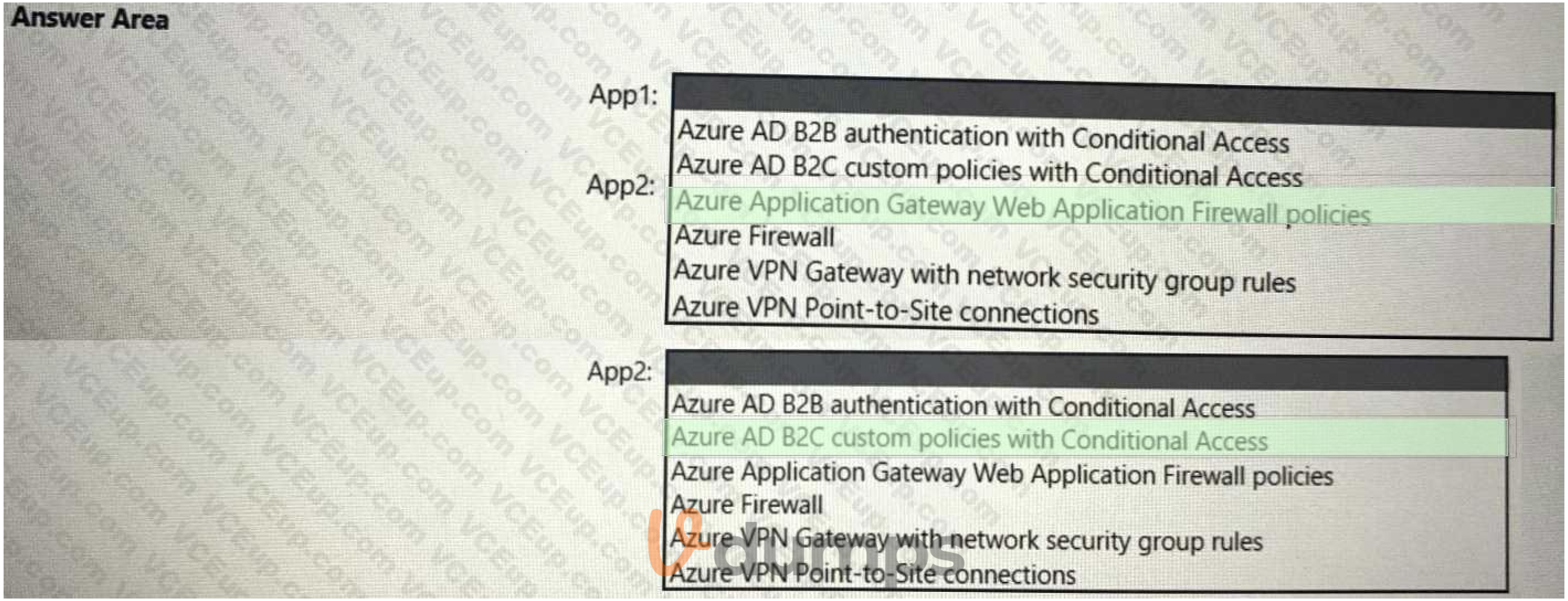
Answer Area

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:

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:



Answer Area

App1:

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

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

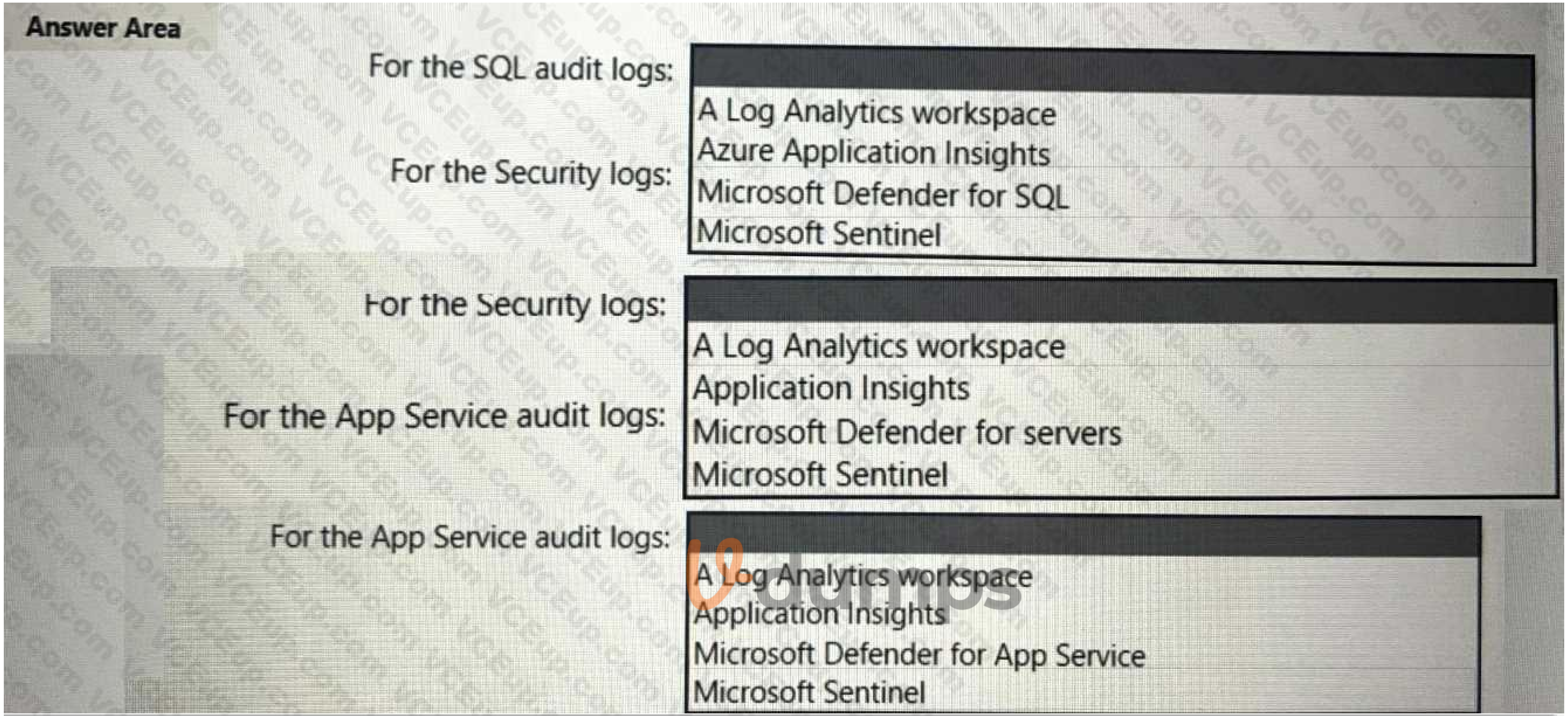
Section:
Explanation:

QUESTION 64
HOTSPOT
You are designing an auditing solution for Azure landing zones that will contain the following components:
- SQL audit logs for Azure SQL databases
- Windows Security logs from Azure virtual machines
- Azure App Service audit logs from App Service web apps

You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
- Log all privileged access.
- Retain logs for at least 365 days.
- Minimize costs.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

For the SQL audit logs:

For the Security logs:

- A Log Analytics workspace
- Azure Application Insights
- Microsoft Defender for SQL
- Microsoft Sentinel

For the Security logs:

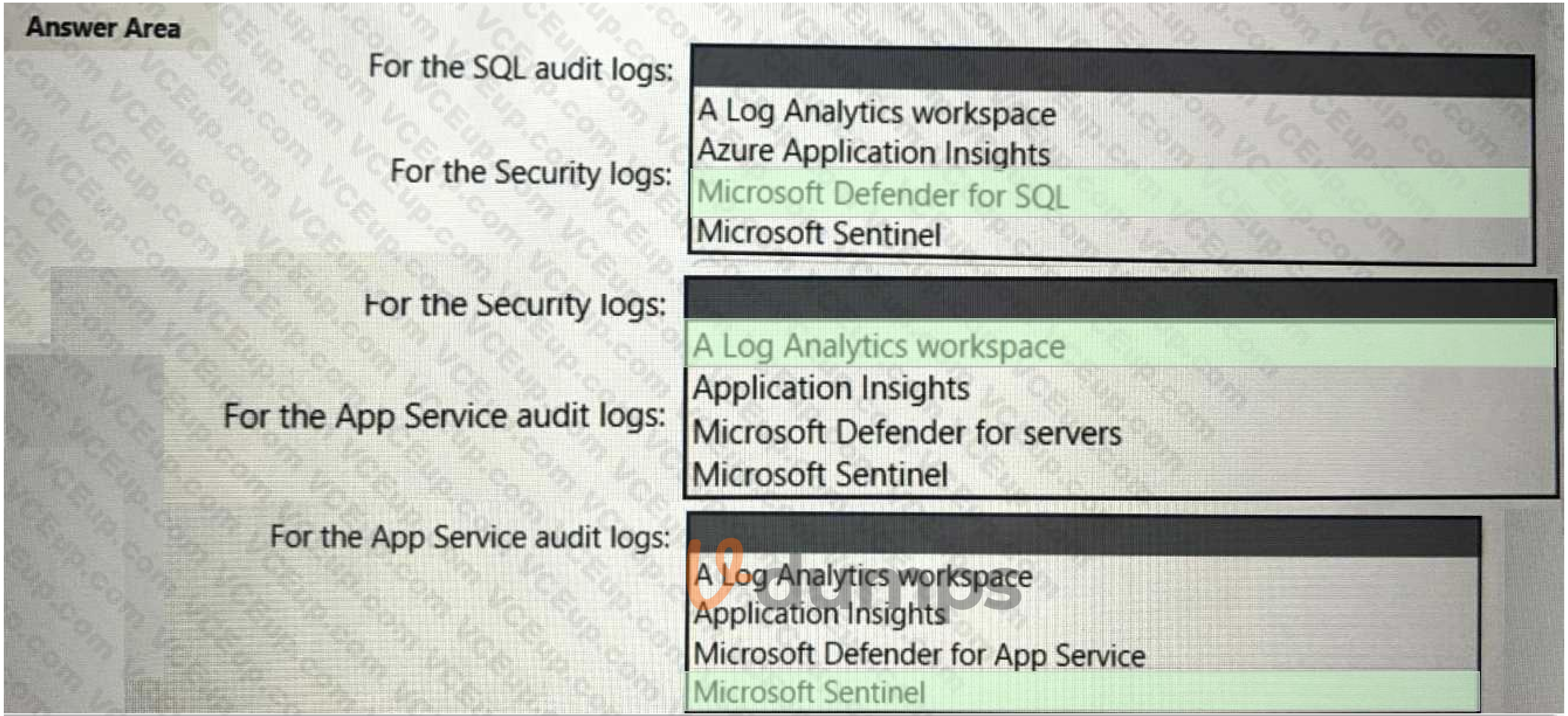
For the App Service audit logs:

- A Log Analytics workspace
- Application Insights
- Microsoft Defender for servers
- Microsoft Sentinel

For the App Service audit logs:

- A Log Analytics workspace
- Application Insights
- Microsoft Defender for App Service
- Microsoft Sentinel

Answer Area:



Answer Area

For the SQL audit logs:

For the Security logs:

- A Log Analytics workspace
- Azure Application Insights
- [✓ Microsoft Defender for SQL]
- Microsoft Sentinel

For the Security logs:

For the App Service audit logs:

- [✓ A Log Analytics workspace]
- Application Insights
- Microsoft Defender for servers
- Microsoft Sentinel

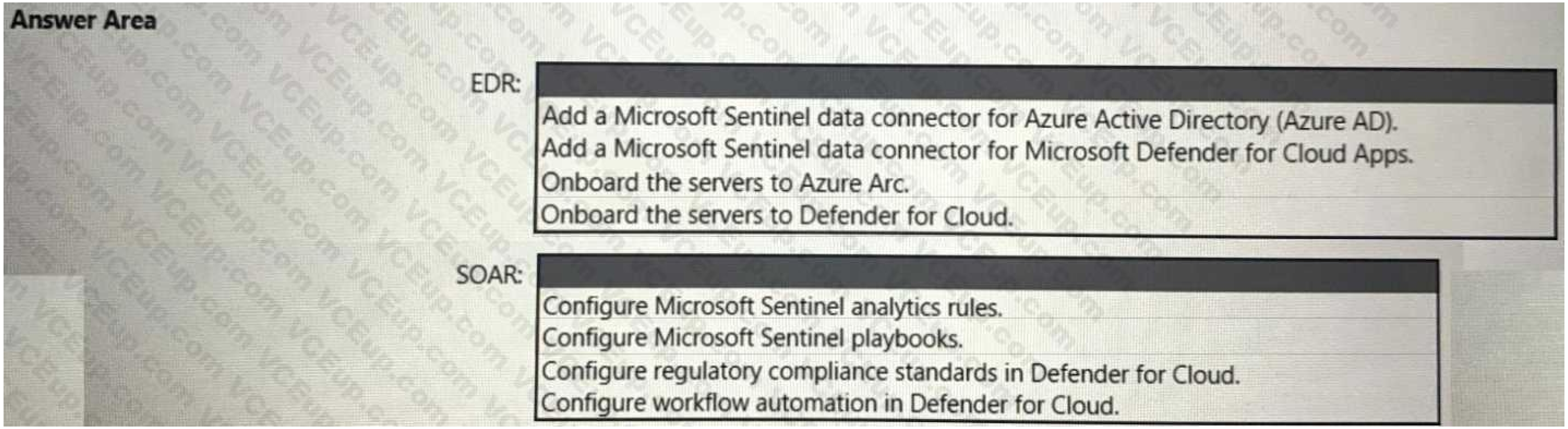
For the App Service audit logs:

- A Log Analytics workspace
- Application Insights
- Microsoft Defender for App Service
- [✓ Microsoft Sentinel]

Section:
Explanation:

QUESTION 65
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

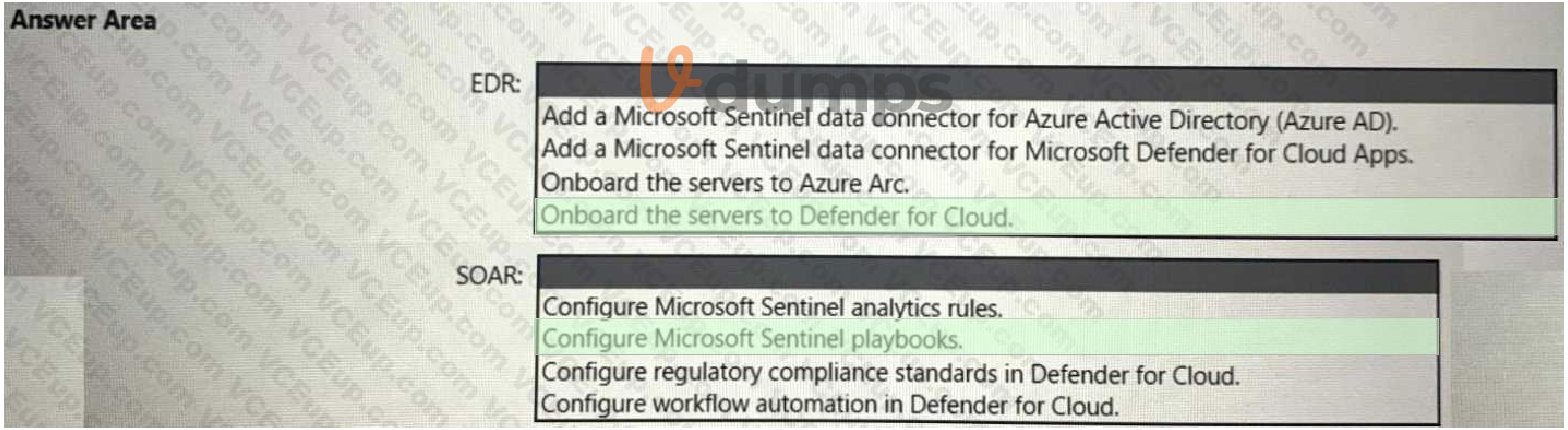
EDR:

- 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.

Answer 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.

Section:

Explanation:

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

QUESTION 66

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
Section:

QUESTION 67
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 customermanaged keys (CMKs). Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:

QUESTION 68
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 Microsoftmanaged keys within an encryption scope. Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

QUESTION 69
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
Section:
Explanation:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privilegedaccess#pa-2-avoid-standing-access-for-user-accounts-and-permissions Adaptive Network Hardening:
https://docs.microsoft.com/enus/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-securityconfiguration

QUESTION 70

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.

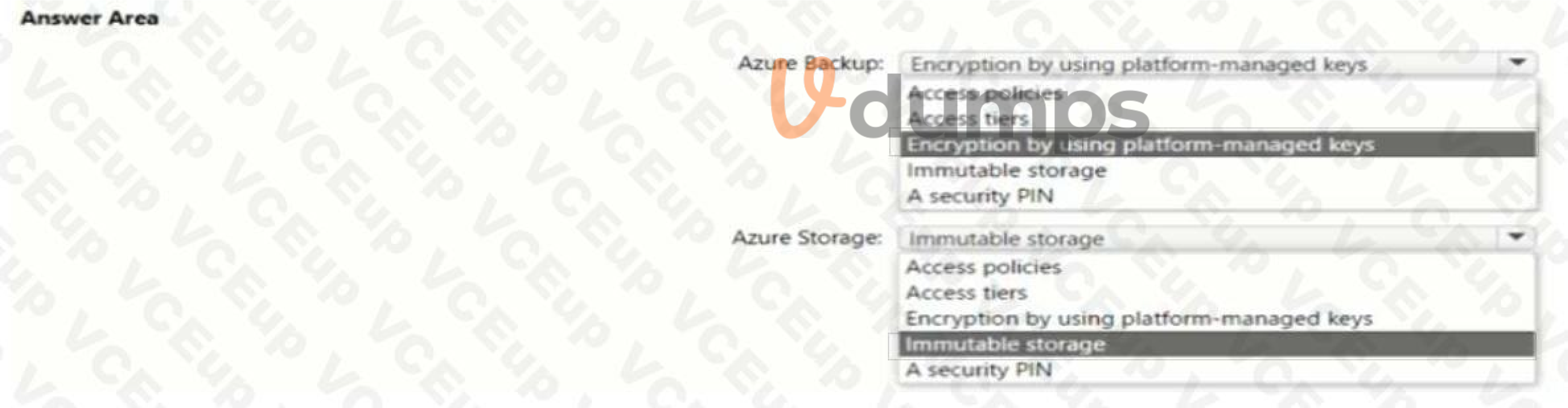
What should you do first?

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
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-are-available-in-defender-for-cloud

QUESTION 71
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.

Hot Area:

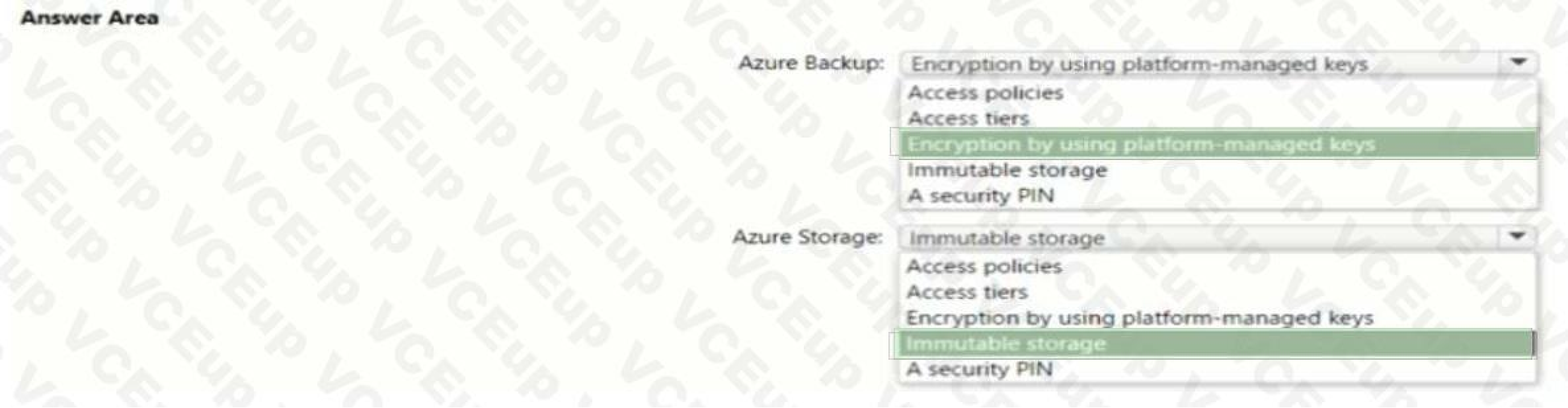


Answer Area

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

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

Answer Area:



Answer Area

Azure Backup: Encryption by using platform-managed keys

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

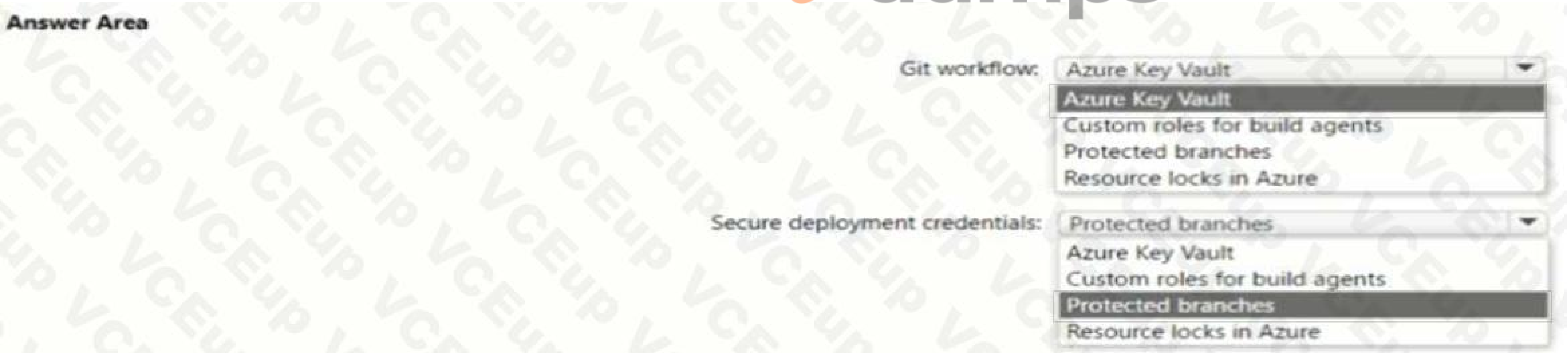
Azure Storage: Immutable storage

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

Section:
Explanation:

QUESTION 72
HOTSPOT
You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CO) 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.

Hot Area:



Answer Area

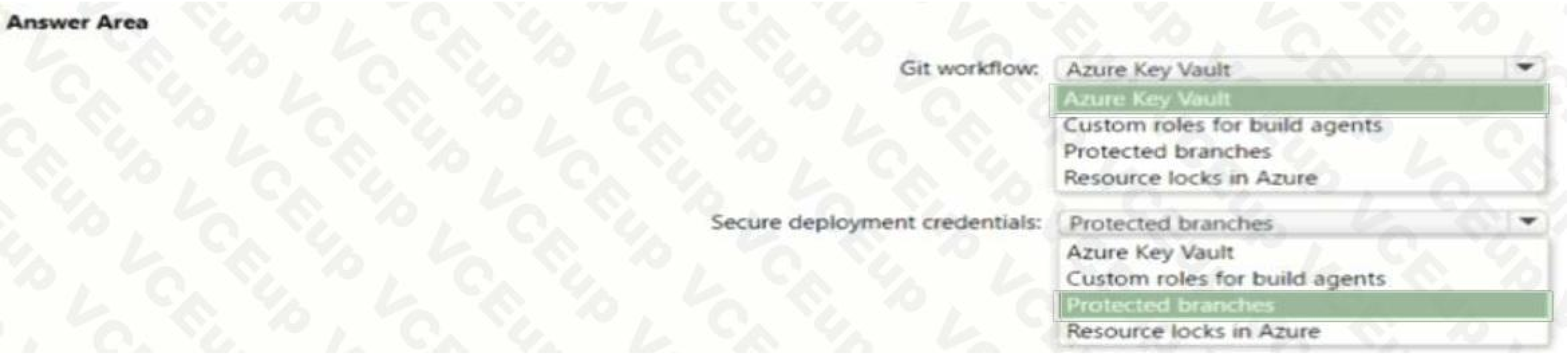
Git workflow: Azure Key Vault

- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Secure deployment credentials: Protected branches

- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Answer Area:



Answer Area

Git workflow: Azure Key Vault

- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Secure deployment credentials: Protected branches

- Azure Key Vault
- Custom roles for build agents
- Protected branches
- Resource locks in Azure

Section:
Explanation:

QUESTION 73
You are designing a ransomware response plan that follows Microsoft Security Best PracticesYou need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out. What should you include in the recommendations?

A. Privileged Access Workstations (PAWs)
B. emergency access accounts
C. device compliance policies
D. Customer Lockbox for Microsoft Azure

Correct Answer: B
Section:

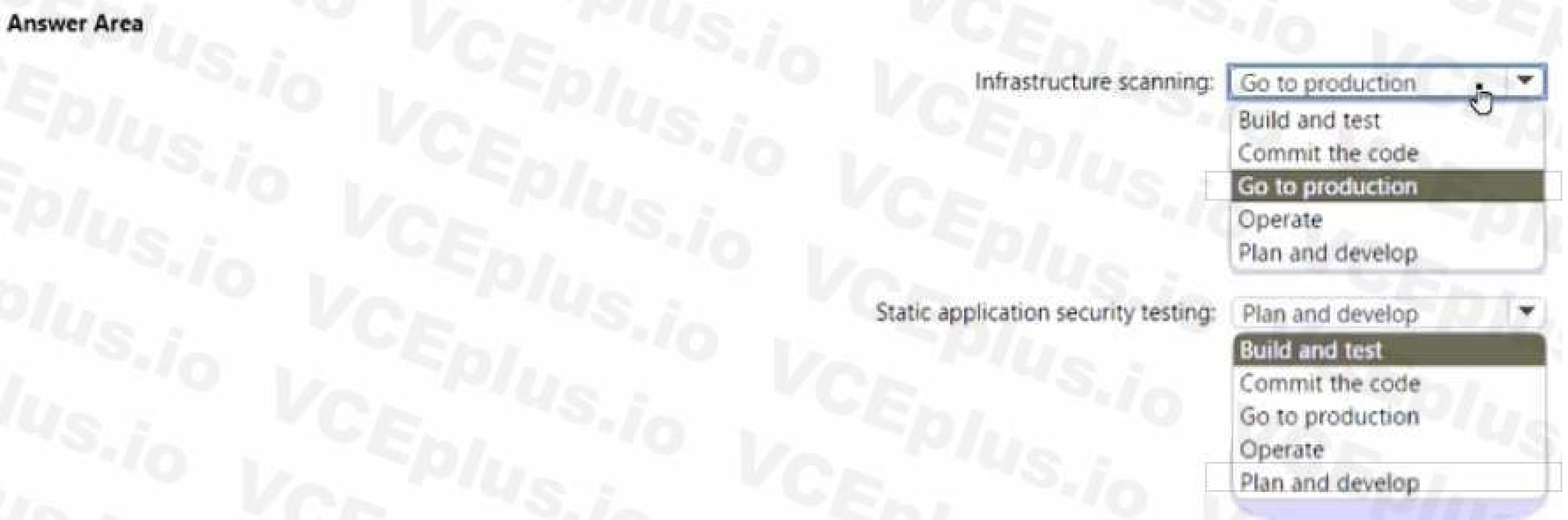
QUESTION 74
You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (O/CD) workflows for the deployment of applications to Azure. You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure. What should you recommend?

A. unit testing
B. penetration testing
C. dependency checks
D. threat modeling

Correct Answer: C
Section:

QUESTION 75
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 (Cl/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.

Hot Area:

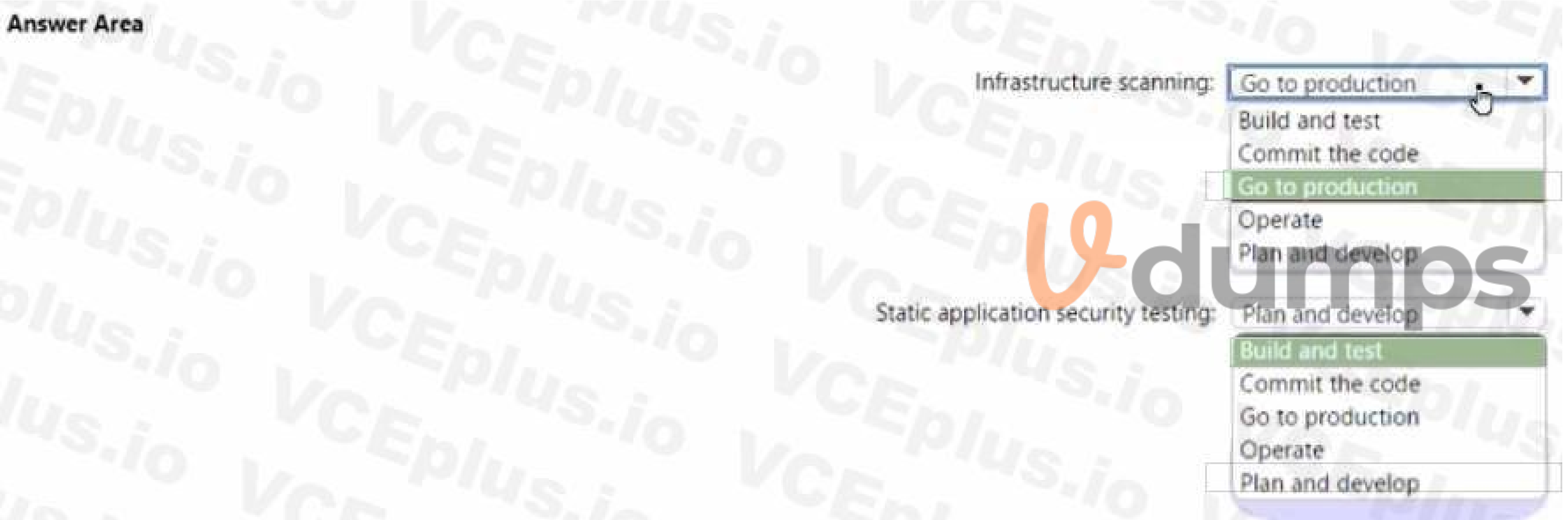


Answer Area

Infrastructure scanning: Go to production

Static application security testing: Plan and develop

Answer Area:



Answer Area

Infrastructure scanning: Go to production

Static application security testing: Build and test

Section:
Explanation:

QUESTION 76

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: A, C, E

Section:

QUESTION 77

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
D. Other options

Correct Answer: C
Section:

QUESTION 78

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 group 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. Privileged Access Workstations (PAWs)
C. Azure AD Privileged Identity Management (PIM)
D. Azure AD identity Protection

Correct Answer: A
Section:

QUESTION 79

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. Disable Microsoft OneDnve sync and Exchange ActiveSync.
B. Recover files to a cleaned computer or device.
C. Contact law enforcement.
D. From Microsoft Defender for Endpoint perform a security scan.

Correct Answer: A
Section:

QUESTION 80

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 a Recovery Services vault generate a security PIN for critical operations.
B. From Azure Backup, configure multi-user authorization by using Resource Guard.
C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault
D. From Azure AD Privileged identity Management (PIM), create a role assignment for the Backup Contributor role.

Correct Answer: A
Section:

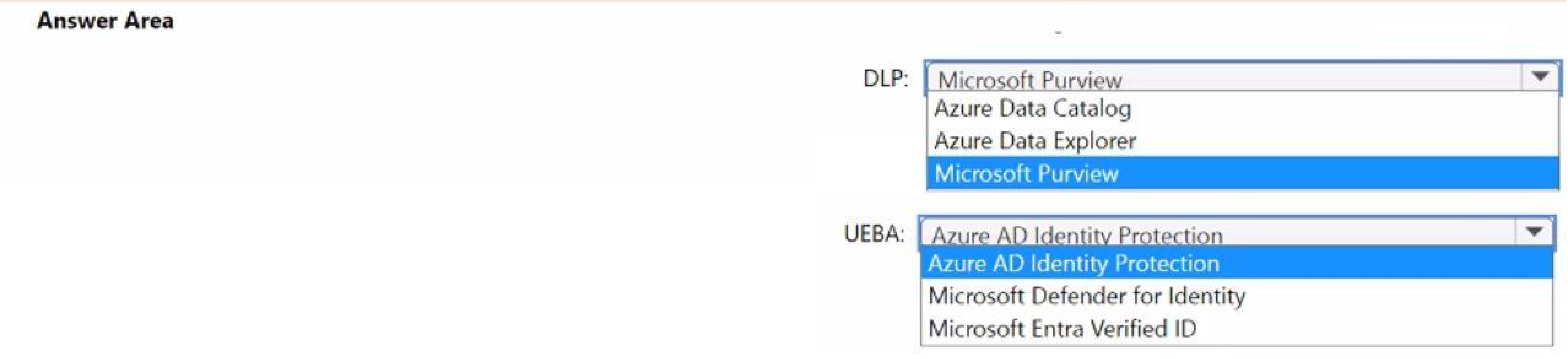
QUESTION 81
You have a Microsoft 365 subscription.
You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA). You need to recommend a solution that automatically restricts access to Microsoft Exchange Online.
SharePoint Online, and Teams m near-real-lime (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. a sign-in risk policy
C. Azure AD Privileged Identity Management (PIM)
D. Conditional Access
E. Azure AD Application Proxy

Correct Answer: B, D
Section:

QUESTION 82
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 are a. NOTE: Each correct selection is worth one point.

Hot Area:

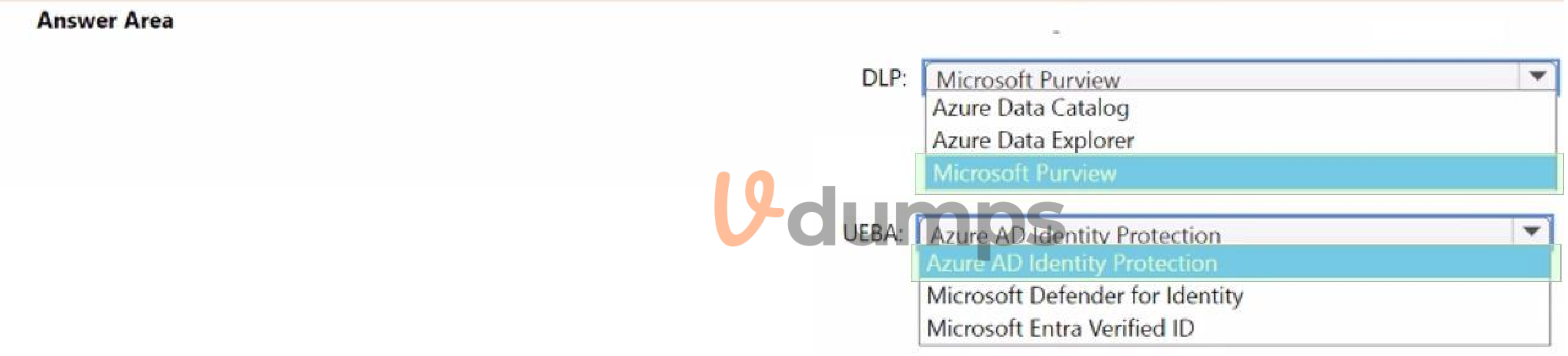


Answer Area

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

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

Answer Area:



Answer Area

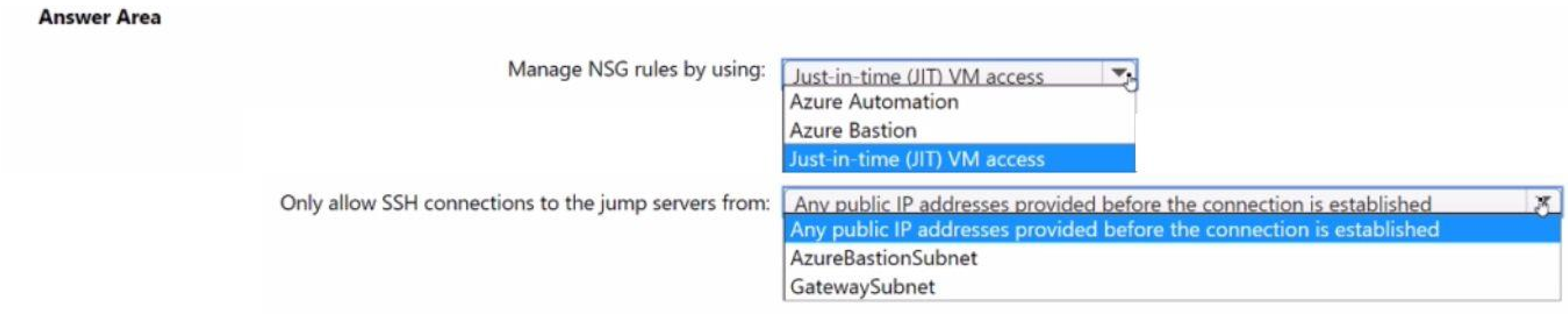
DLP: Microsoft Purview
- Azure Data Catalog
- Azure Data Explorer
- Microsoft Purview

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

Section:
Explanation:

QUESTION 83
HOTSPOT
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect f personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG)
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
* Ensure that each time the support staff connects to a jump server; they must request access to the server.
* Ensure that only authorized support staff can initiate SSH connections to the jump servers.
* Maximize protection against brute-force attacks from internal networks and the internet.
* Ensure that users can only connect to the jump servers from the internet.
* Minimize administrative effort
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

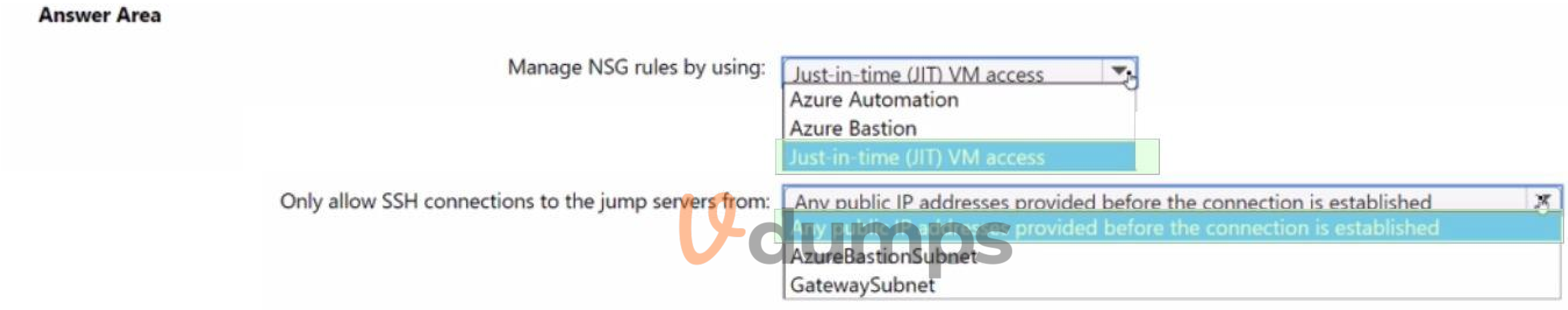
Manage NSG rules by using: Just-in-time (JIT) VM access

- Azure Automation
- Azure Bastion
- Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established

- Any public IP addresses provided before the connection is established
- AzureBastionSubnet
- GatewaySubnet

Answer Area:



Answer Area

Manage NSG rules by using: Just-in-time (JIT) VM access

- Azure Automation
- Azure Bastion
- Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established

- Any public IP addresses provided before the connection is established
- AzureBastionSubnet
- GatewaySubnet

Section:
Explanation:

QUESTION 84
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 Server3 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. Configure connectors and rules in Microsoft Defender for Cloud Apps.
B. Configure web protection in Microsoft Defender for Endpoint.
C. Publish the web apps by using Azure AD Application Proxy.
D. Configure the VPN to use Azure AD authentication.

Correct Answer: C
Section:

QUESTION 85

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

You need to recommend best practices for applying Zero Trust principles to the OT and loT 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. passive traffic monitoring

B. active scanning

C. threat monitoring

D. software patching

Correct Answer: C, D

Section:

QUESTION 86

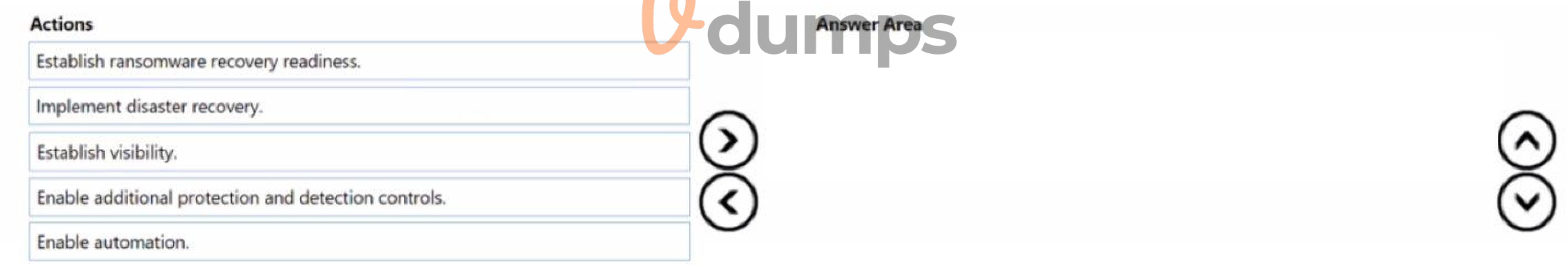
DRAG DROP

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.

Select and Place:

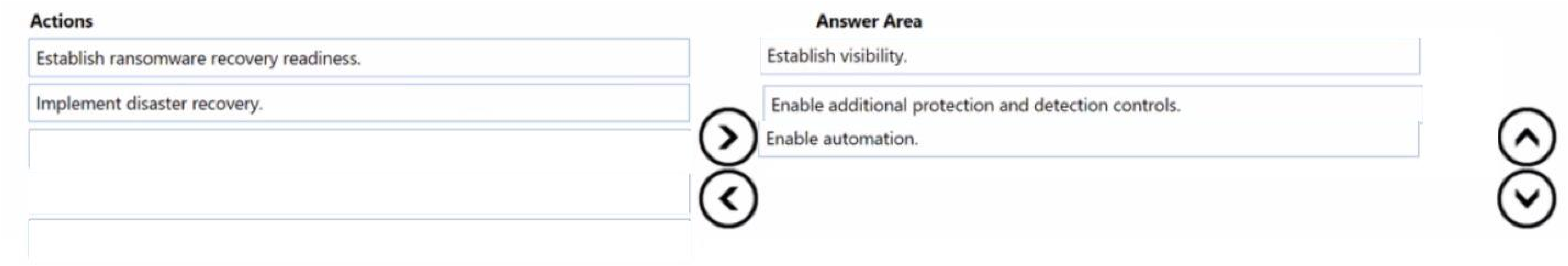


Actions

- Establish ransomware recovery readiness.
- Implement disaster recovery.
- Establish visibility.
- Enable additional protection and detection controls.
- Enable automation.

Answer Area

Correct Answer:



Actions

Establish ransomware recovery readiness.

Implement disaster recovery.

Answer Area

Establish visibility.

Enable additional protection and detection controls.

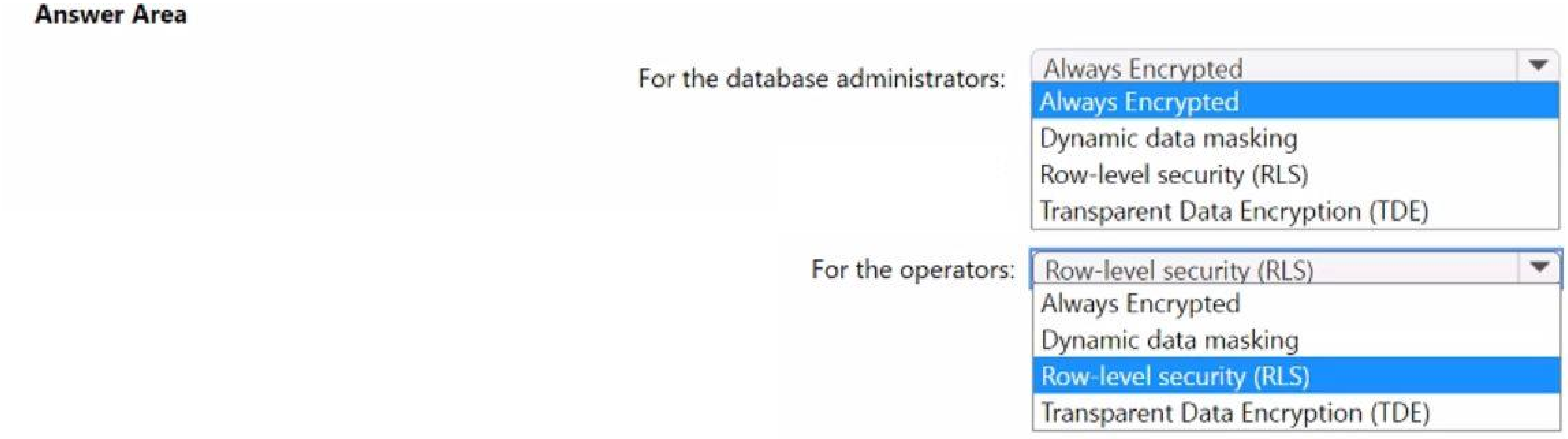
Enable automation.

Section:
Explanation:

Establish visibility.
Enable additional protection and detection control.
Enable automation.

QUESTION 87
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 D81. The solution must meet the following requirements:
* When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.
* When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.
What should you include in the design? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

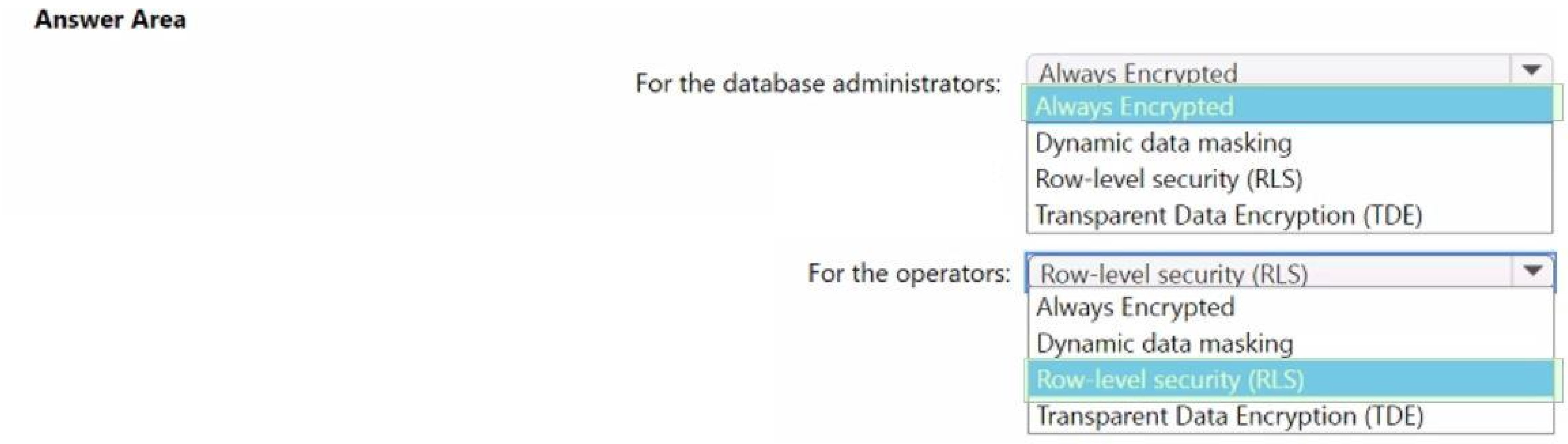
For the database administrators: Always Encrypted

- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators: Row-level security (RLS)

- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

Answer Area:



Answer Area

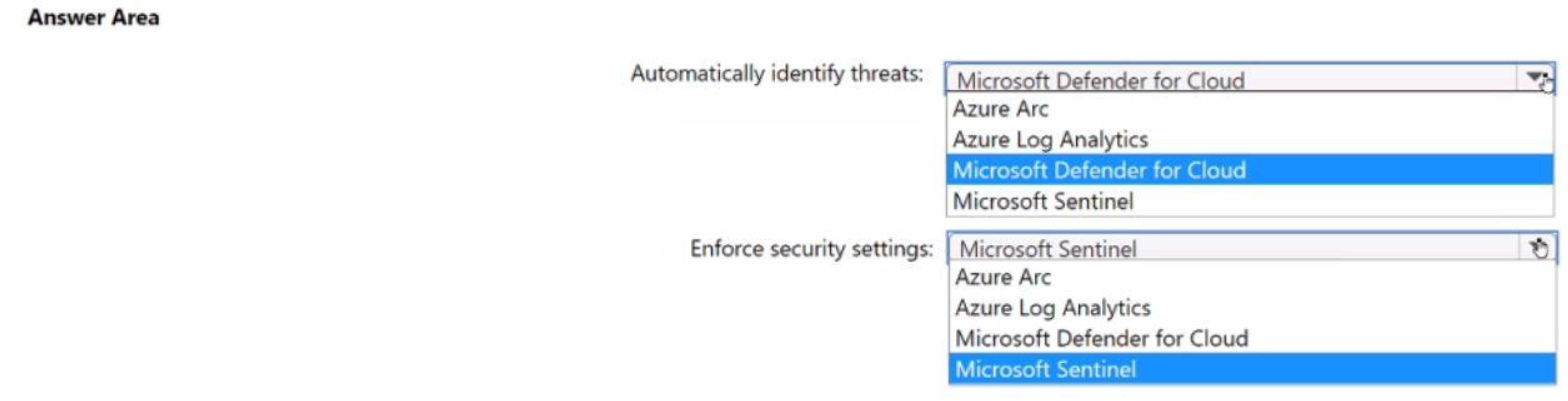
For the database administrators: Always Encrypted

For the operators: Row-level security (RLS)

Section:
Explanation:

QUESTION 88
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 are a. NOTE: Each correct selection is worth one point.

Hot Area:

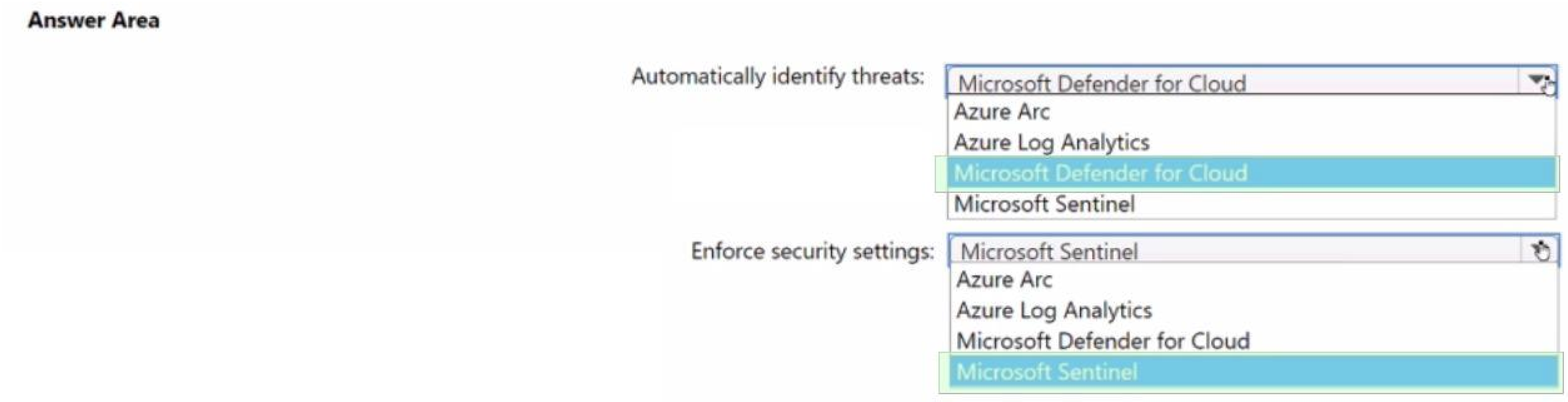


Answer Area

Automatically identify threats: Microsoft Defender for Cloud

Enforce security settings: Microsoft Sentinel

Answer Area:



Answer Area

Automatically identify threats: Microsoft Defender for Cloud

- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

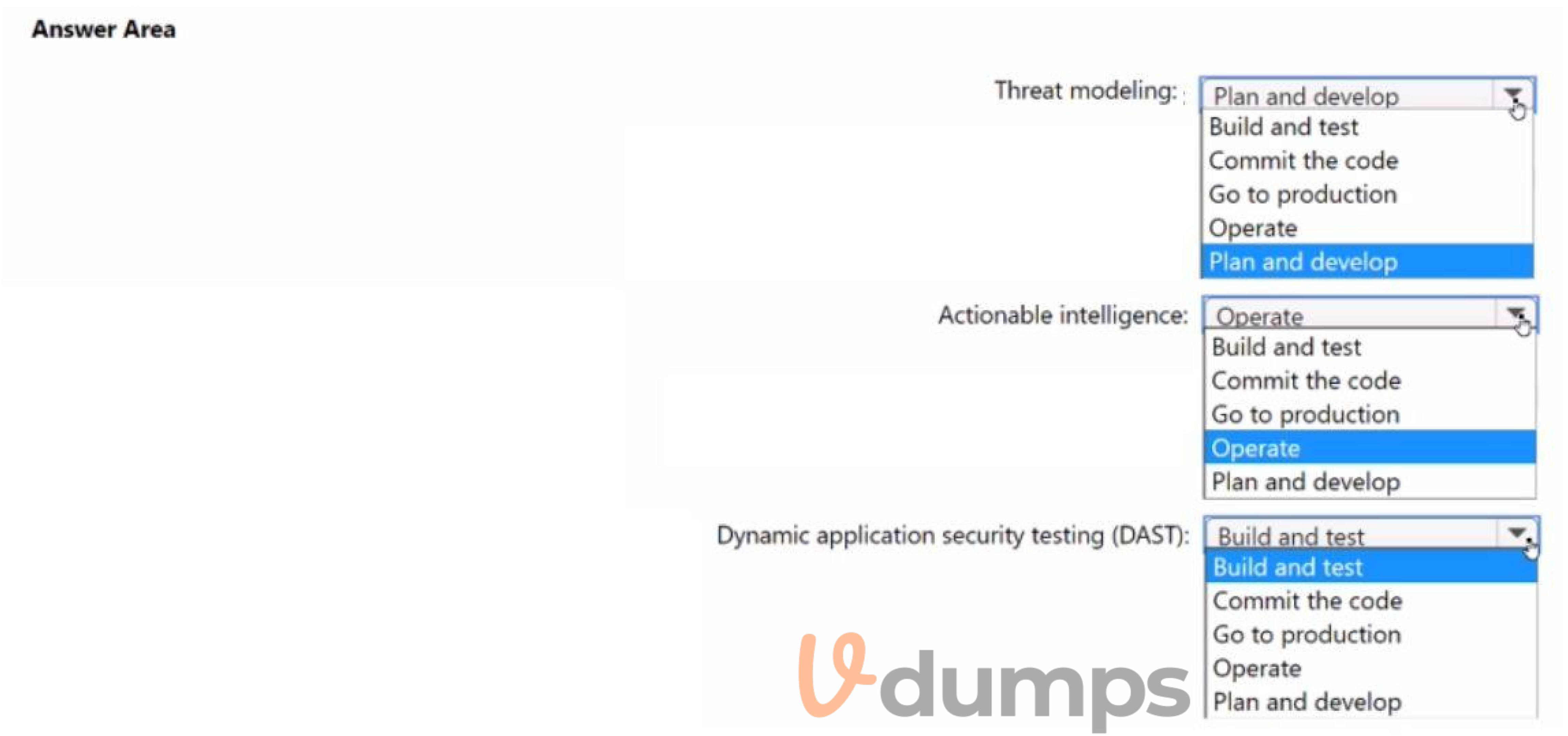
Enforce security settings: Microsoft Sentinel

- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Section:
Explanation:

QUESTION 89
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

Hot Area:



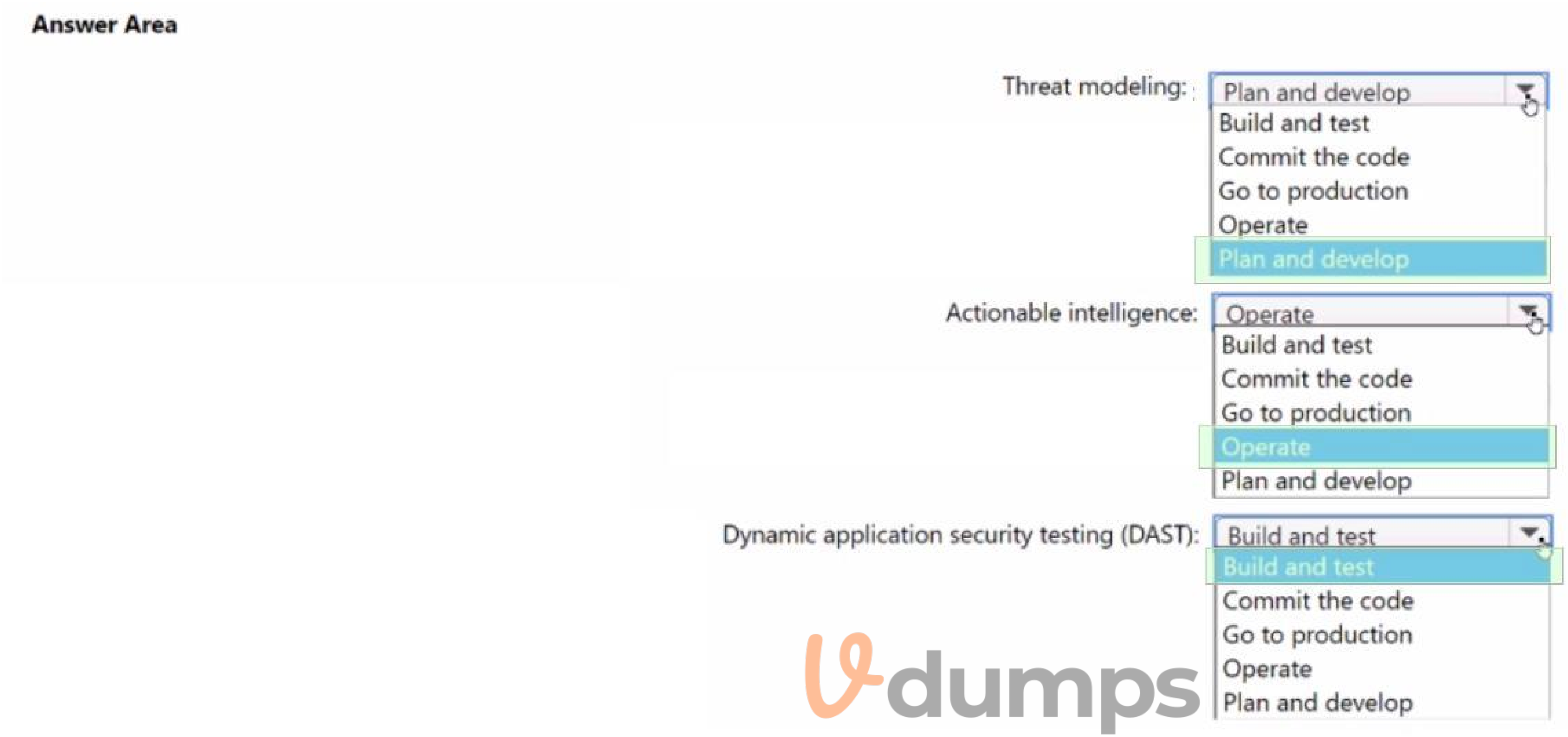
Answer Area

Threat modeling: Plan and develop

Actionable intelligence: Operate

Dynamic application security testing (DAST): Build and test

Answer Area:



Answer Area

Threat modeling: Plan and develop

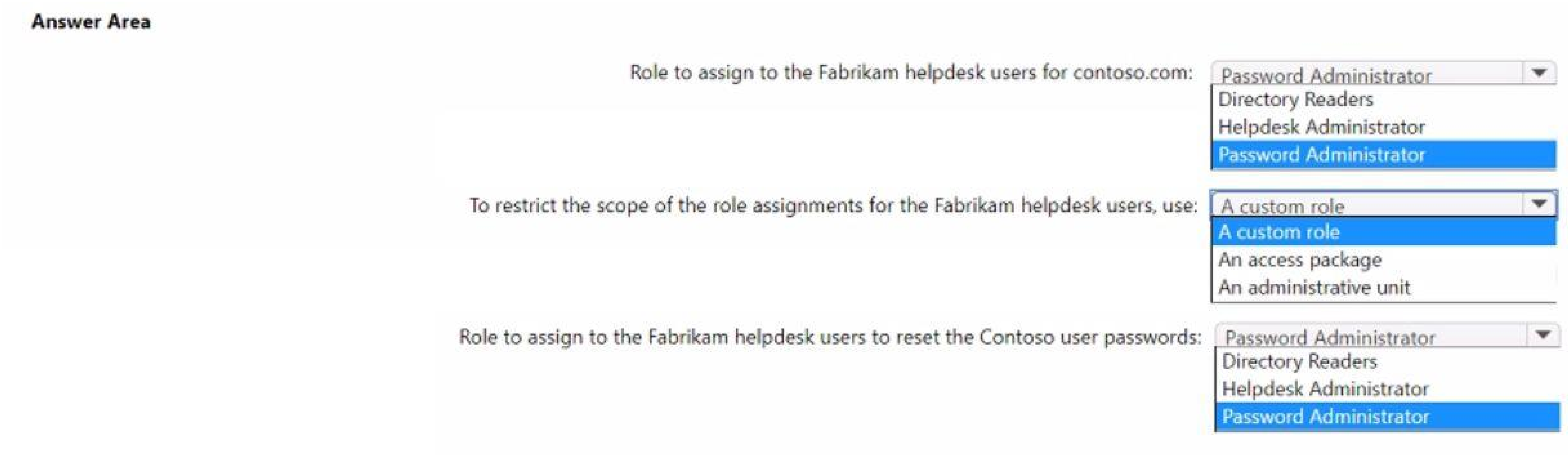
Actionable intelligence: Operate

Dynamic application security testing (DAST): Build and test

Section:
Explanation:

QUESTION 90
HOTSPOT
Your company, named Contoso. Ltd... has an Azure AD tenant namedcontoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:
* Follow the principle of least privilege.
* Minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



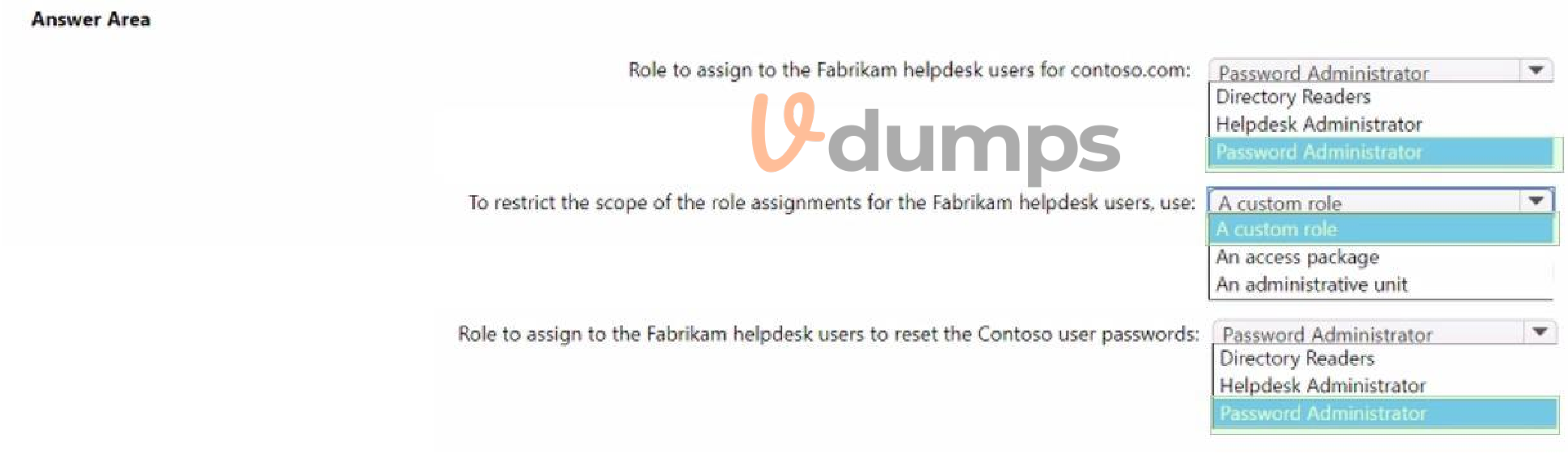
Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com: Password Administrator ▼
- Directory Readers
- Helpdesk Administrator
- Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use: A custom role ▼
- A custom role
- An access package
- An administrative unit

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords: Password Administrator ▼
- Directory Readers
- Helpdesk Administrator
- Password Administrator

Answer Area:



Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com: Password Administrator ▼
- Directory Readers
- Helpdesk Administrator
- Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use: A custom role ▼
- A custom role
- An access package
- An administrative unit

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords: Password Administrator ▼
- Directory Readers
- Helpdesk Administrator
- Password Administrator

Section:
Explanation:

QUESTION 91
You have a Microsoft 365 subscription. You have an Azure subscription.
You need to implement a Microsoft Purview communication compliance solution for Microsoft Teams and Yammer. The solution must meet the following requirements:
* Assign compliance policies to Microsoft 365 groups based on custom Microsoft Exchange Online attributes.
* Minimize the number of compliance policies
* Minimize administrative effort
What should you include in the solution?

A. Azure AD Information Protection labels

B. Microsoft 365 Defender user tags

C. adaptive scopes

D. administrative units

Correct Answer: C
Section:

QUESTION 92

HOTSPOT

You have an Azure subscription. The subscription contains an Azure application gateway that use Azure Web Application Firewall (WAF).

You deploy new Azure App Services web apps. Each app is registered automatically in the DNS domain of your company and accessible from the Internet.

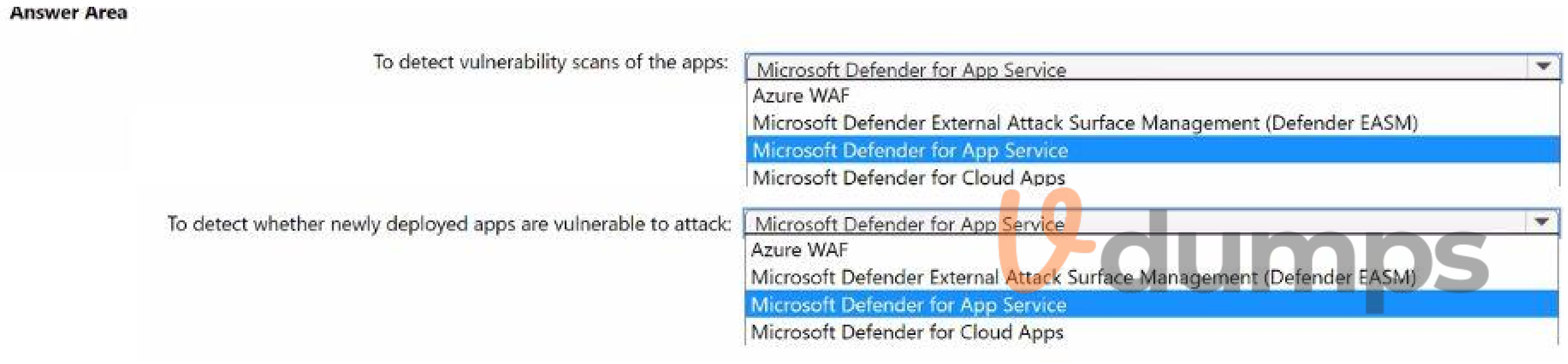
You need to recommend a security solution that meets the following requirements:

* Detects vulnerability scans of the apps

* Detects whether newly deployed apps are vulnerable to attack

What should you recommend using? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:

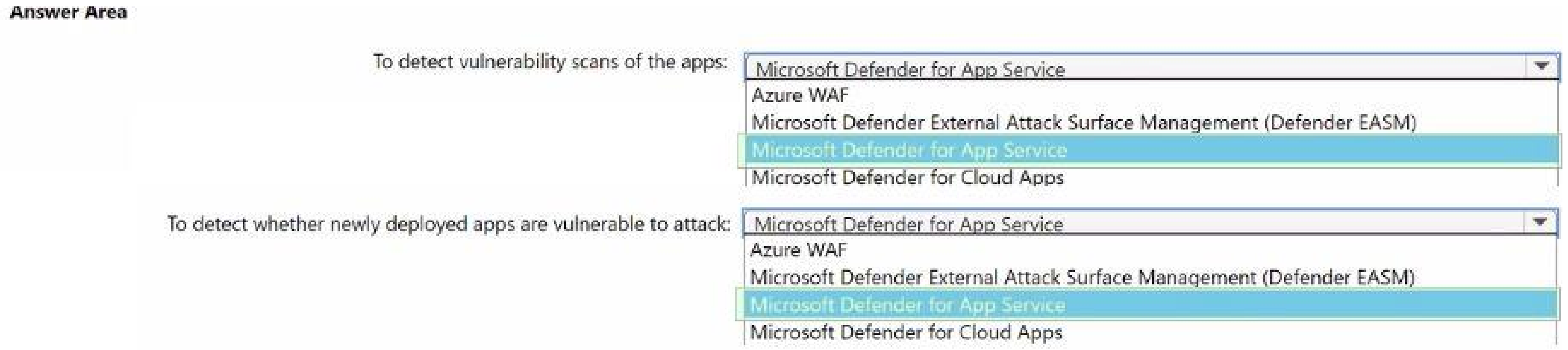


Answer Area

To detect vulnerability scans of the apps: Microsoft Defender for App Service
- Azure WAF
- Microsoft Defender External Attack Surface Management (Defender EASM)
- Microsoft Defender for App Service
- Microsoft Defender for Cloud Apps

To detect whether newly deployed apps are vulnerable to attack: Microsoft Defender for App Service
- Azure WAF
- Microsoft Defender External Attack Surface Management (Defender EASM)
- Microsoft Defender for App Service
- Microsoft Defender for Cloud Apps

Answer Area:



Answer Area

To detect vulnerability scans of the apps: Microsoft Defender for App Service
- Azure WAF
- Microsoft Defender External Attack Surface Management (Defender EASM)
- Microsoft Defender for App Service
- Microsoft Defender for Cloud Apps

To detect whether newly deployed apps are vulnerable to attack: Microsoft Defender for App Service
- Azure WAF
- Microsoft Defender External Attack Surface Management (Defender EASM)
- Microsoft Defender for App Service
- Microsoft Defender for Cloud Apps

Section:
Explanation:

QUESTION 93

You have an on-premises server that runs Windows Server and contains a Microsoft SQL Server database named DB1.

You plan to migrate DB1 to Azure.

You need to recommend an encrypted Azure database solution that meets the following requirements:

* Minimizes the risks of malware that uses elevated privileges to access sensitive data

* Prevents database administrators from accessing sensitive data

* Enables pattern matching for server-side database operations
* Supports Microsoft Azure Attestation
* Uses hardware-based encryption
What should you include in the recommendation?

A. SQL Server on Azure Virtual Machines with virtualization-based security (VBS) enclaves

B. Azure SQL Database with virtualization-based security (VBS) enclaves

C. Azure SQL Managed Instance that has Always Encrypted configured

D. Azure SQL Database with Intel Software Guard Extensions (Intel SGX) enclaves

Correct Answer: D
Section: