Number: SC-900
Passing Score: 800
Time Limit: 120
File Version: 12.0

Microsoft.SC-900.vJan-2024.by.Lan.87q

Exam Code: SC-900
Exam Name: Microsoft Security, Compliance, and Identity Fundamentals

Exam A

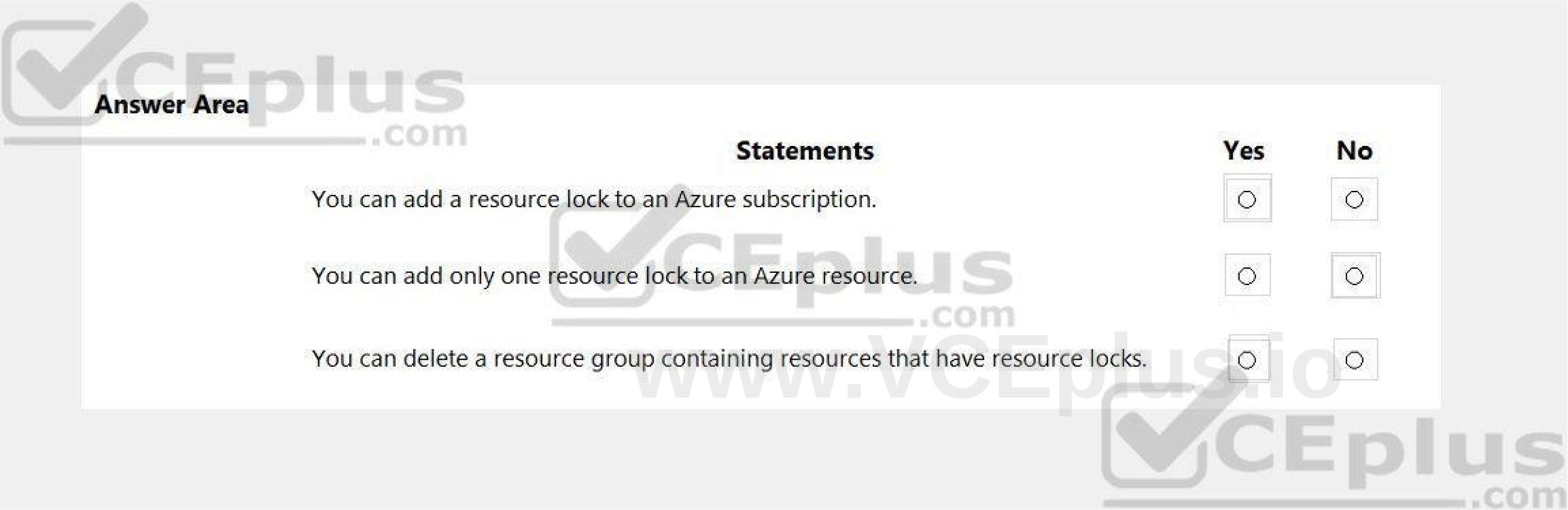
QUESTION 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

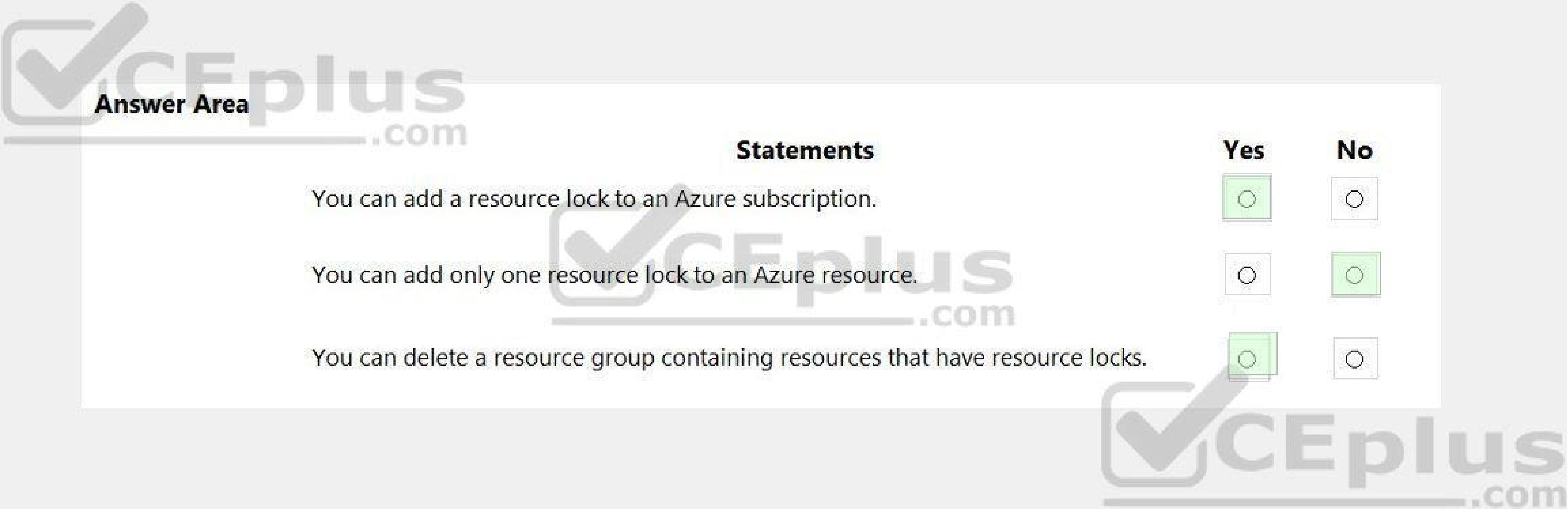
Hot Area:



Answer Area

Statements	Yes	No
You can add a resource lock to an Azure subscription.	○	○
You can add only one resource lock to an Azure resource.	○	○
You can delete a resource group containing resources that have resource locks.	○	○

Answer Area:



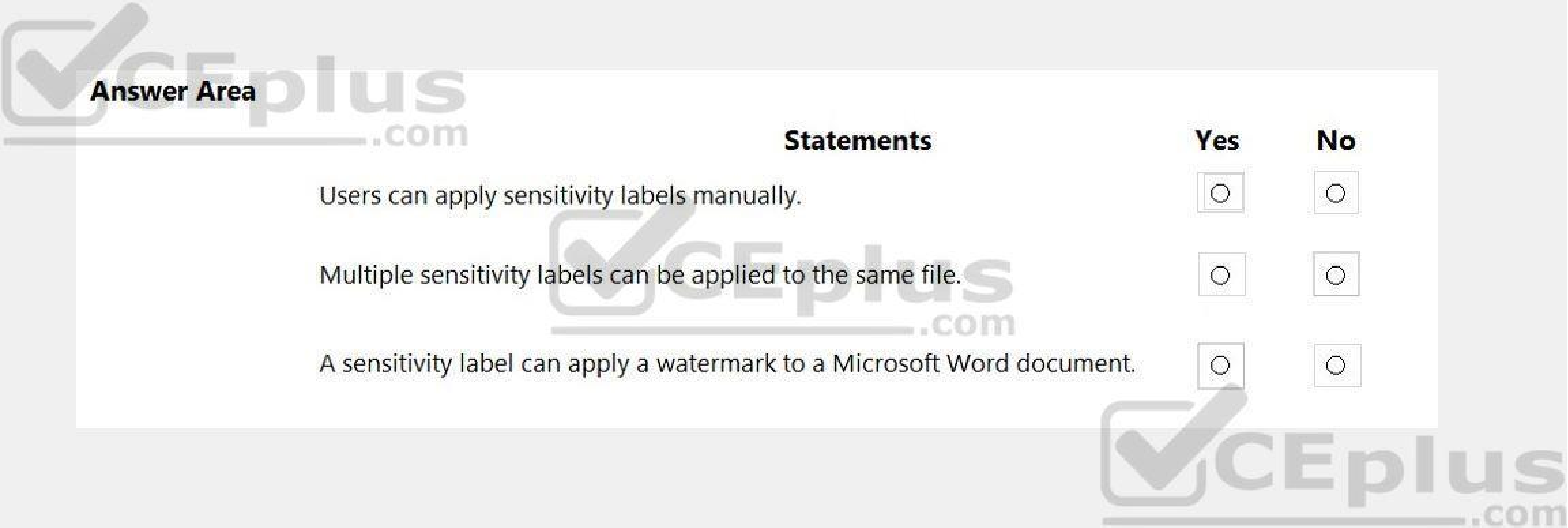
Answer Area

Statements	Yes	No
You can add a resource lock to an Azure subscription.	[✓ ○]	○
You can add only one resource lock to an Azure resource.	○	[✓ ○]
You can delete a resource group containing resources that have resource locks.	[✓ ○]	○

Section:
Explanation:

QUESTION 2
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

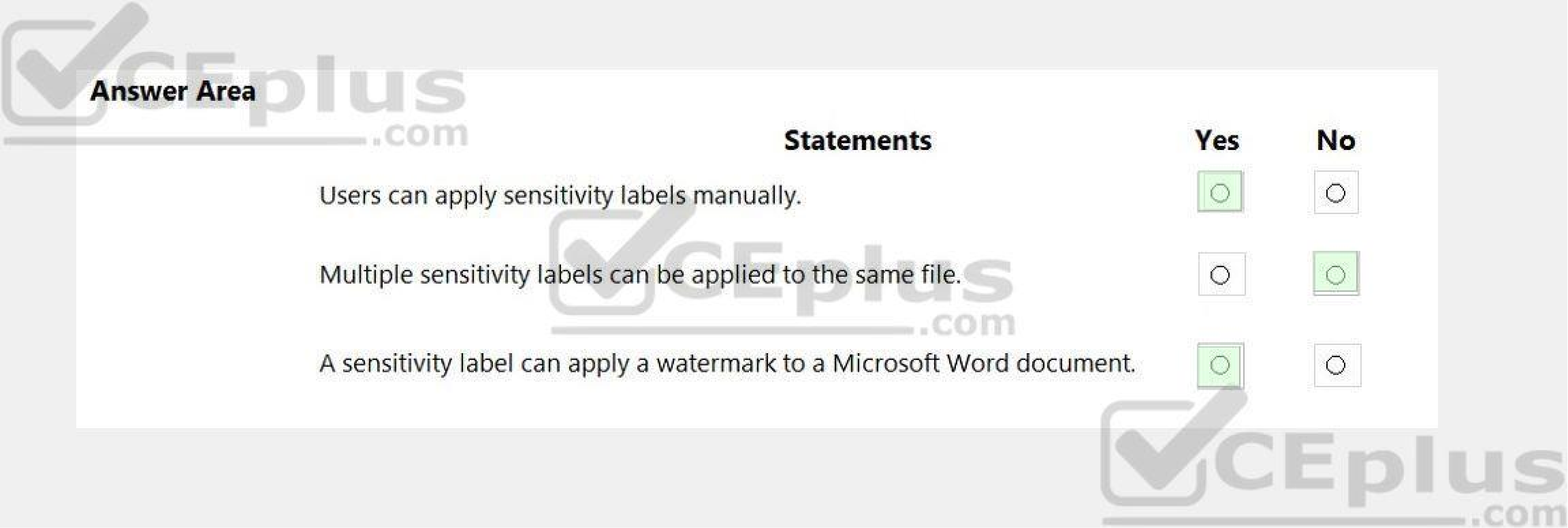
Hot Area:



Answer Area

Statements	Yes	No
Users can apply sensitivity labels manually.	○	○
Multiple sensitivity labels can be applied to the same file.	○	○
A sensitivity label can apply a watermark to a Microsoft Word document.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Users can apply sensitivity labels manually.	[✓ ○]	○
Multiple sensitivity labels can be applied to the same file.	○	[✓ ○]
A sensitivity label can apply a watermark to a Microsoft Word document.	[✓ ○]	○

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

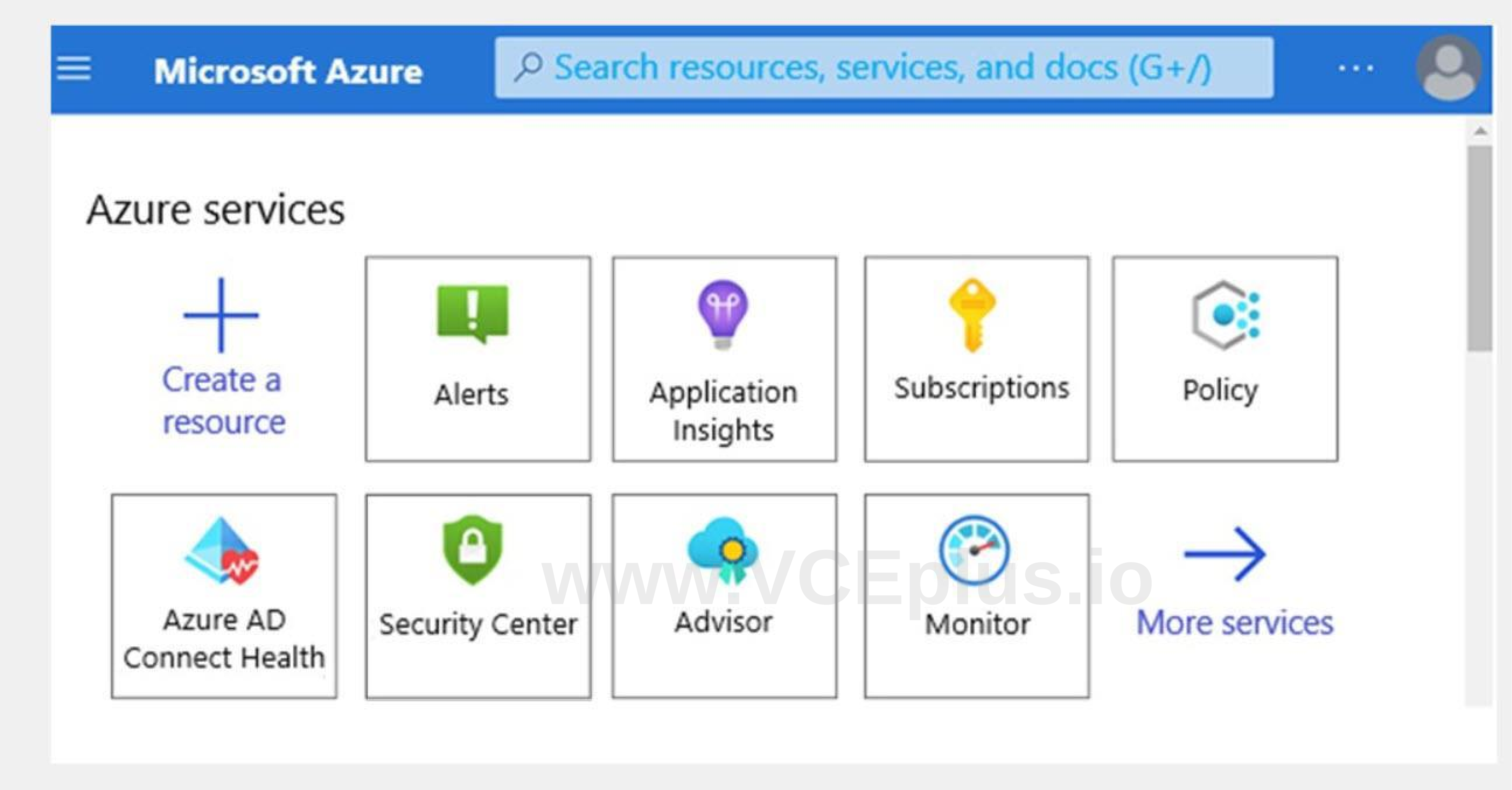
QUESTION 3
Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Define the perimeter by physical locations.
B. Use identity as the primary security boundary.
C. Always verify the permissions of a user explicitly.
D. Always assume that the user system can be breached.
E. Use the network as the primary security boundary.

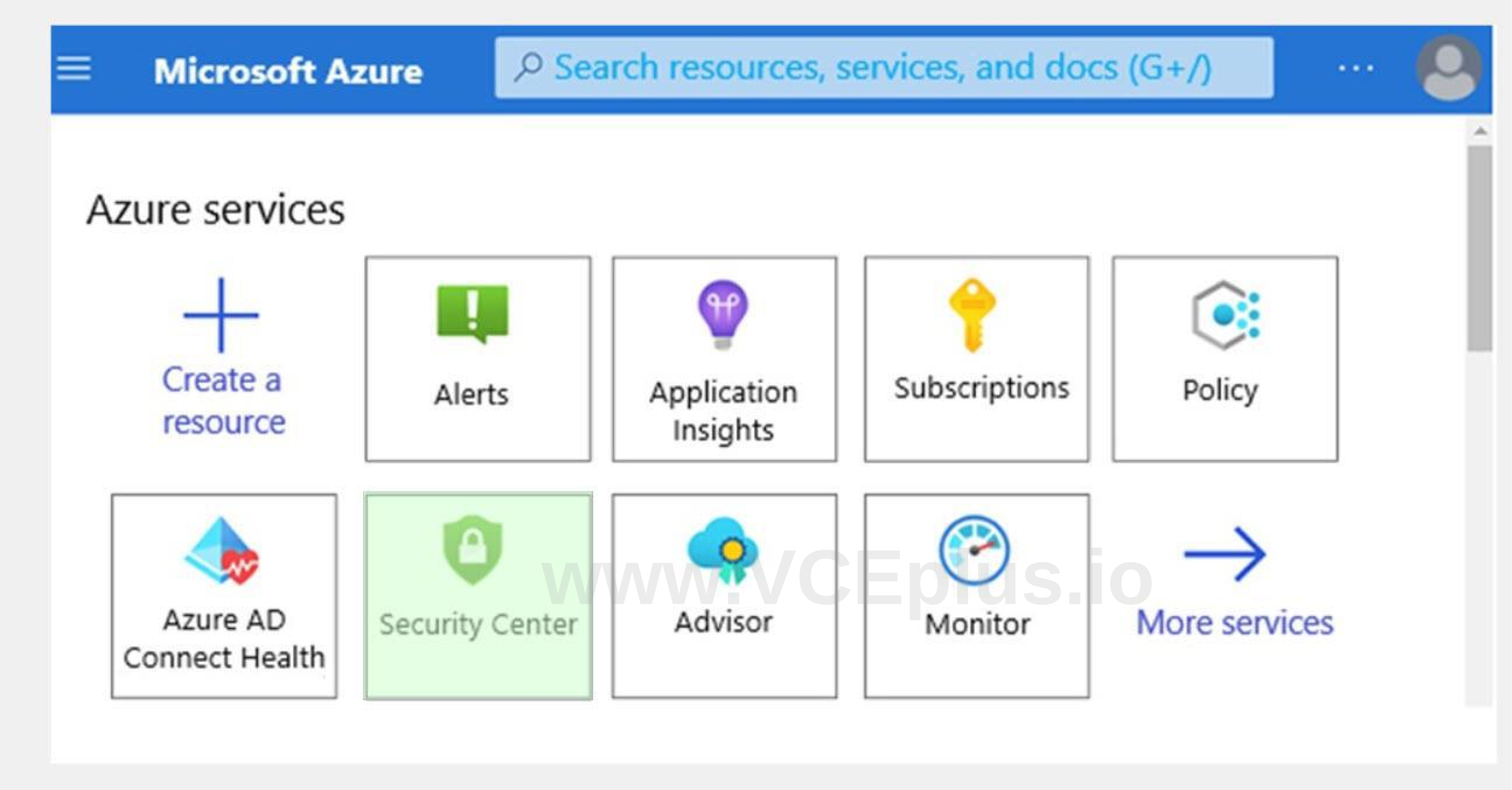
Correct Answer: B, C, D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/security/zero-trust/

QUESTION 4
HOTSPOT
Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.

Hot Area:


Microsoft Azure
Search resources, services, and docs (G+/)
Azure services
Create a resource
Alerts
Application Insights
Subscriptions
Policy
Azure AD Connect Health
Security Center
Advisor
Monitor
More services

Answer Area:



Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track

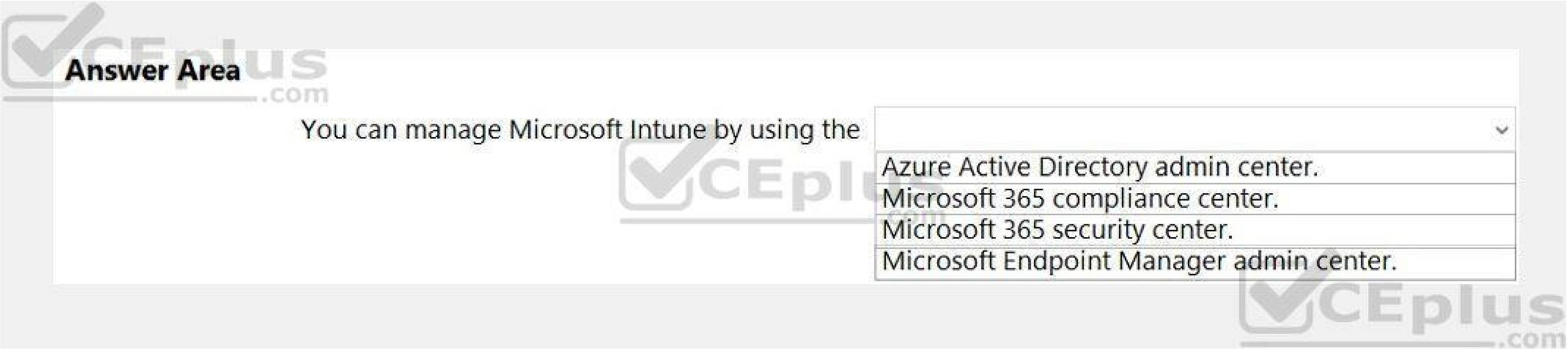
QUESTION 5
You have an Azure subscription.
You need to implement approval-based, time-bound role activation.
What should you use?

A. Windows Hello for Business
B. Azure Active Directory (Azure AD) Identity Protection
C. access reviews in Azure Active Directory (Azure AD)
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

QUESTION 6
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

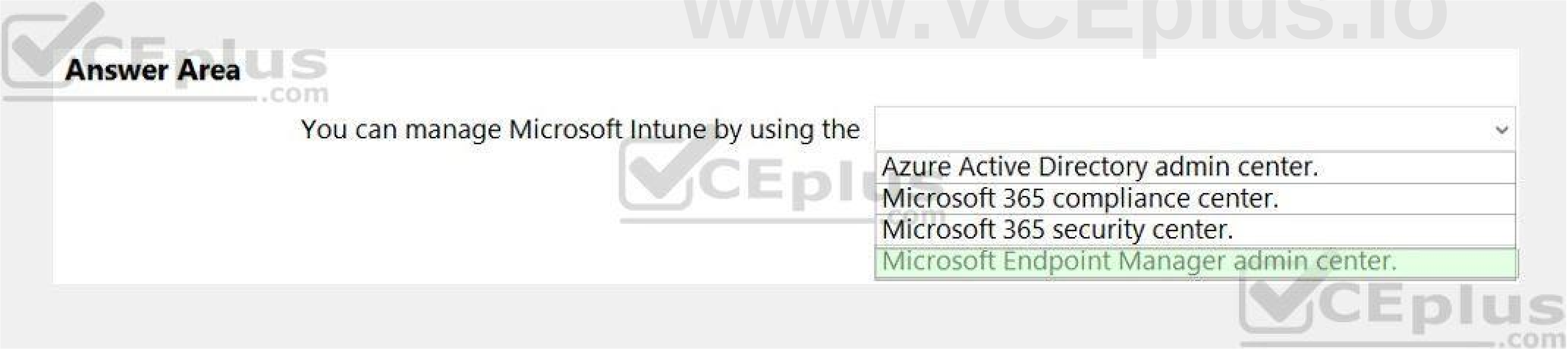


Answer Area

You can manage Microsoft Intune by using the

- Azure Active Directory admin center.
- Microsoft 365 compliance center.
- Microsoft 365 security center.
- Microsoft Endpoint Manager admin center.

Answer Area:



Answer Area

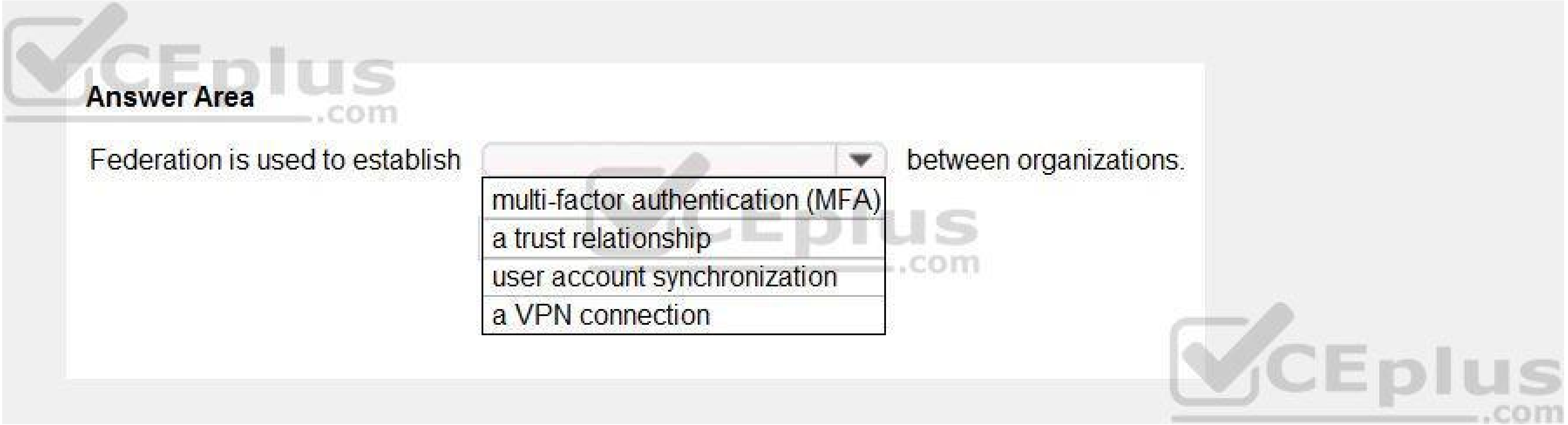
You can manage Microsoft Intune by using the

- Azure Active Directory admin center.
- Microsoft 365 compliance center.
- Microsoft 365 security center.
- Microsoft Endpoint Manager admin center.

Section:
Explanation:

QUESTION 7
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

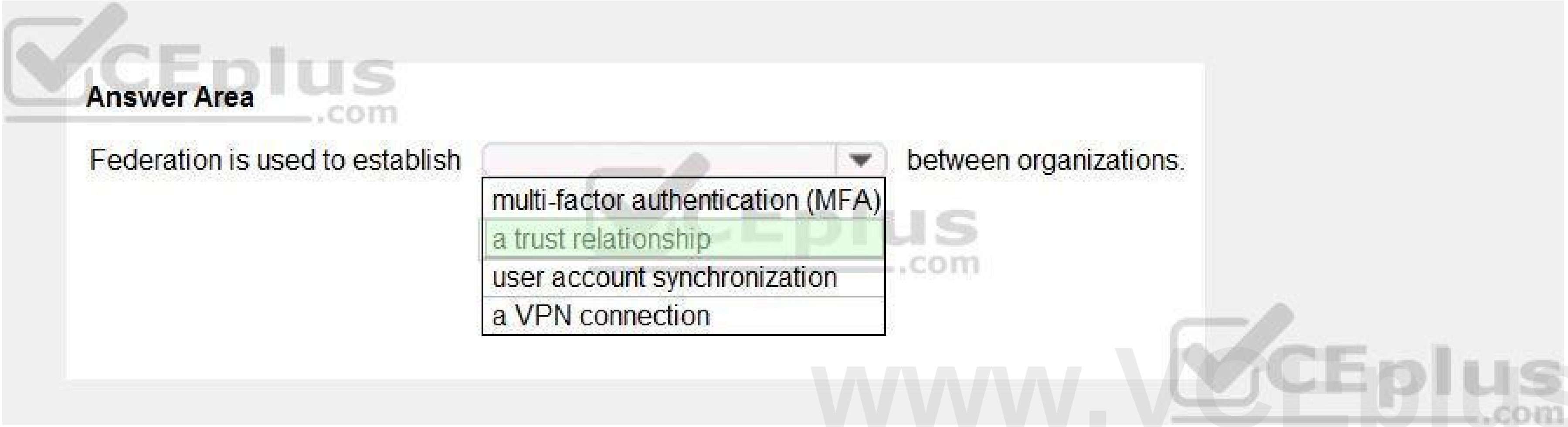


Answer Area

Federation is used to establish [▼] between organizations.

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Answer Area:



Answer Area

Federation is used to establish [▼] between organizations.

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Section:

Explanation:

Federation is a collection of domains that have established trust.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

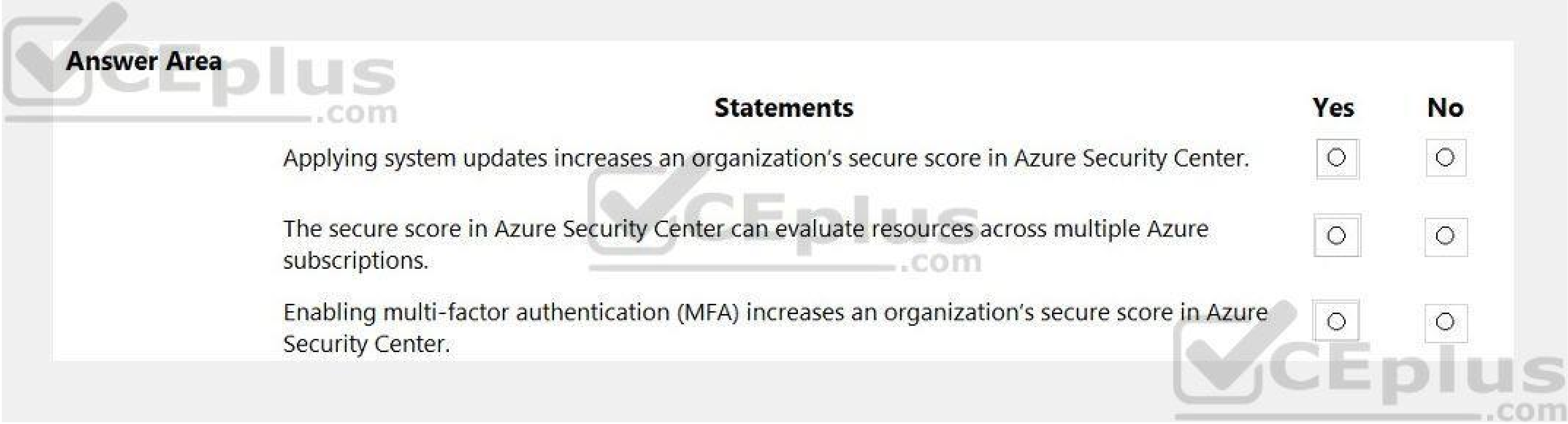
QUESTION 8

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

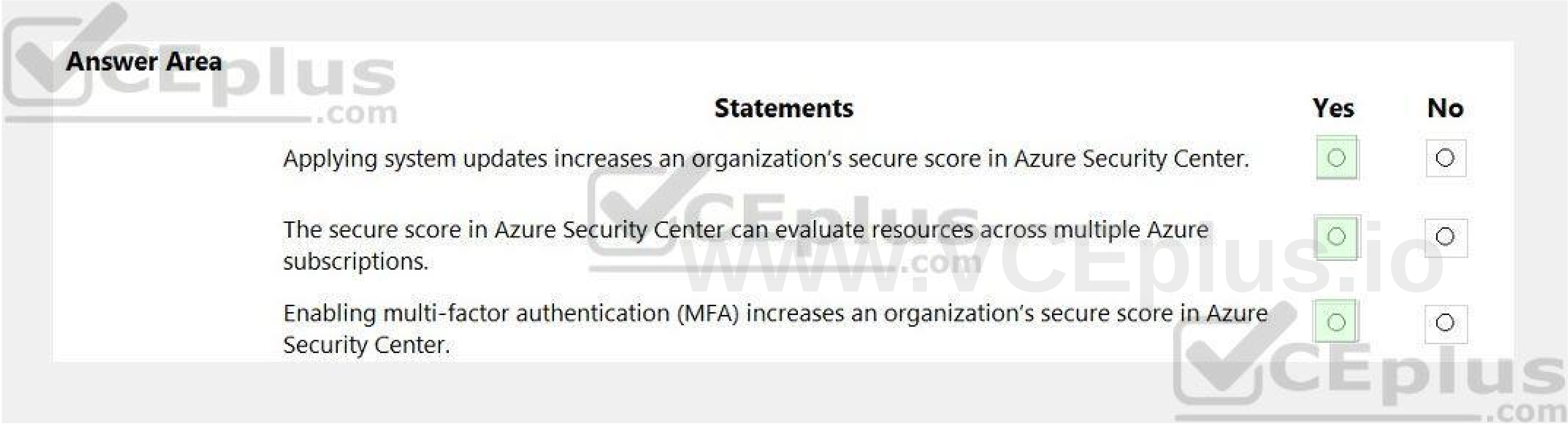
Hot Area:



Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	○	○
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	○	○
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	[✓ ○]	○
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	[✓ ○]	○
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	[✓ ○]	○

Section:

Explanation:

Box 1: Yes

System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes

Box 3: Yes

If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls

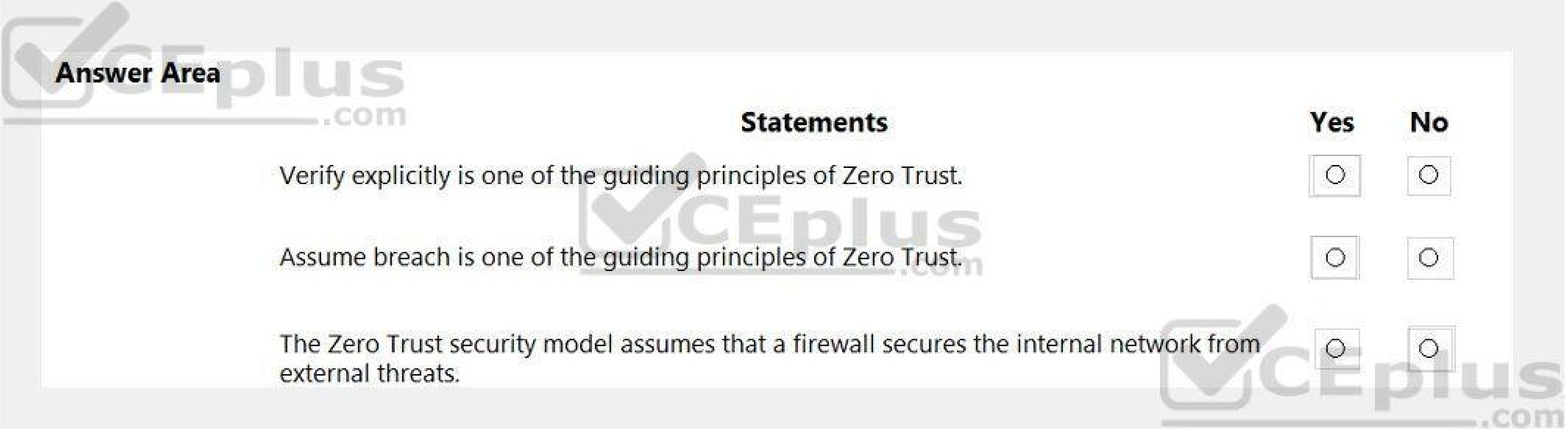
QUESTION 9

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

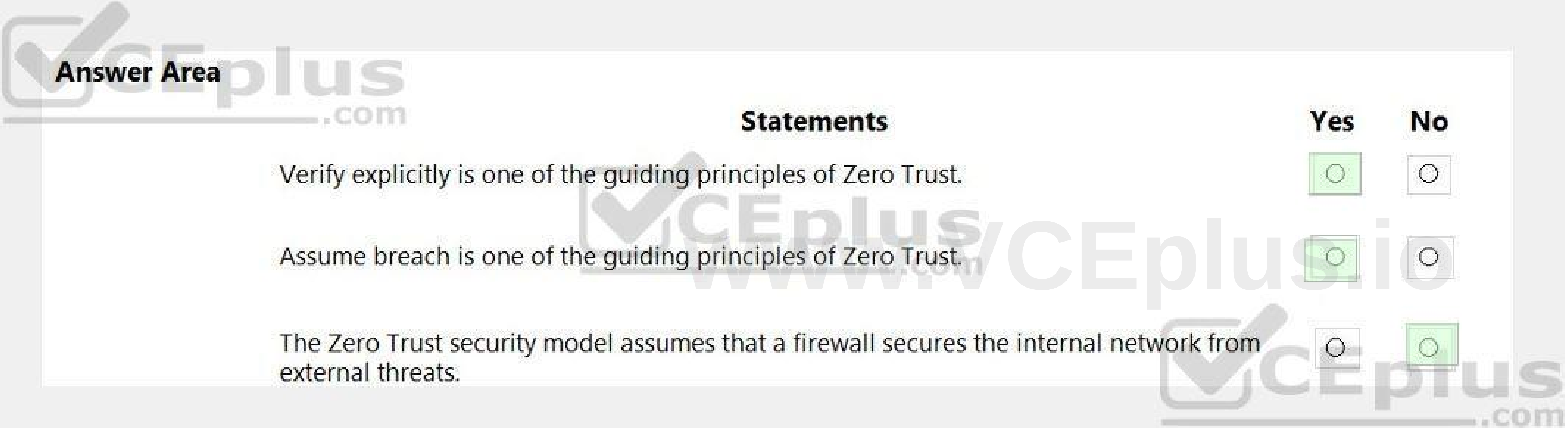
Hot Area:



Answer Area

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	○	○
Assume breach is one of the guiding principles of Zero Trust.	○	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	○

Answer Area:



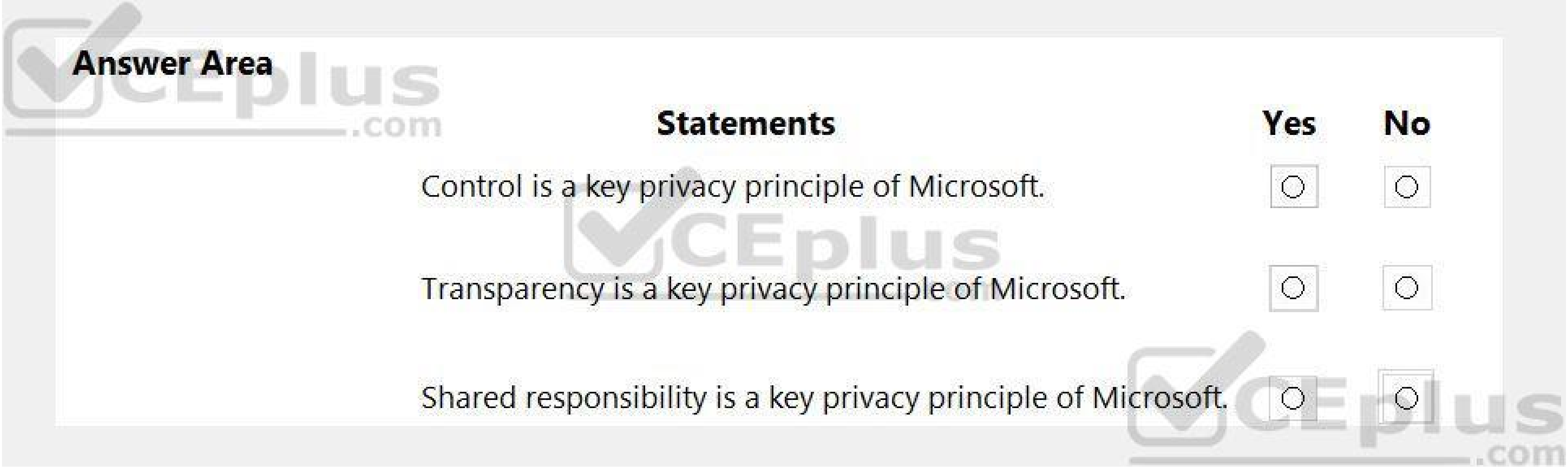
Answer Area

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	[✓ ○]	○
Assume breach is one of the guiding principles of Zero Trust.	[✓ ○]	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	[✓ ○]

Section:
Explanation:
Box 1: Yes
Box 2: Yes
Box 3: No
The Zero Trust model does not assume that everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.
Reference:
https://docs.microsoft.com/en-us/security/zero-trust/

QUESTION 10
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

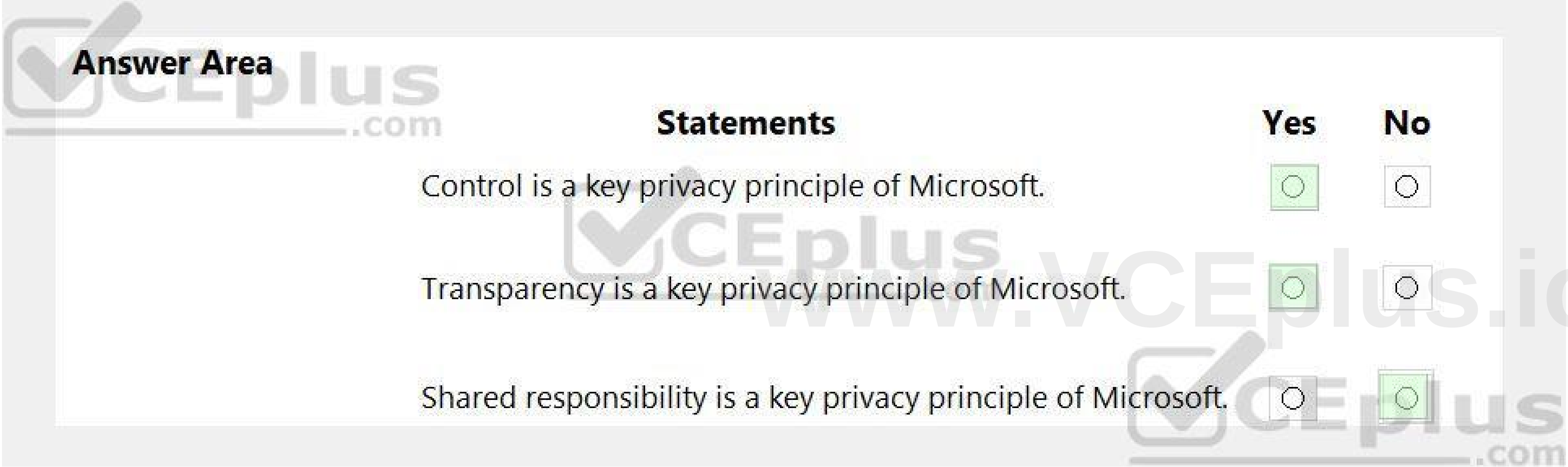
Hot Area:



Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	○	○
Transparency is a key privacy principle of Microsoft.	○	○
Shared responsibility is a key privacy principle of Microsoft.	○	○

Answer Area:



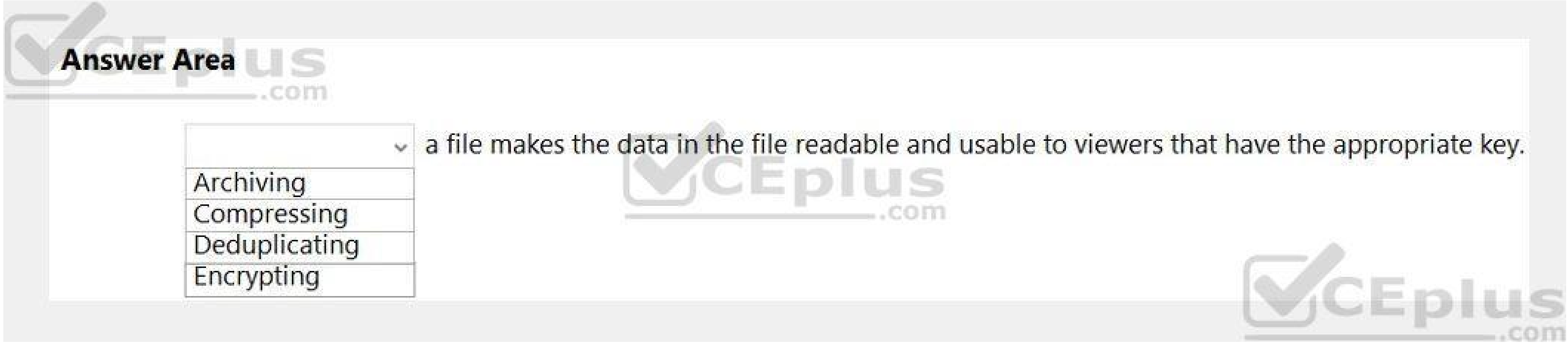
Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	[✓ ○]	○
Transparency is a key privacy principle of Microsoft.	[✓ ○]	○
Shared responsibility is a key privacy principle of Microsoft.	○	[✓ ○]

Section:
Explanation:
Reference:
https://privacy.microsoft.com/en-US/

QUESTION 11
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

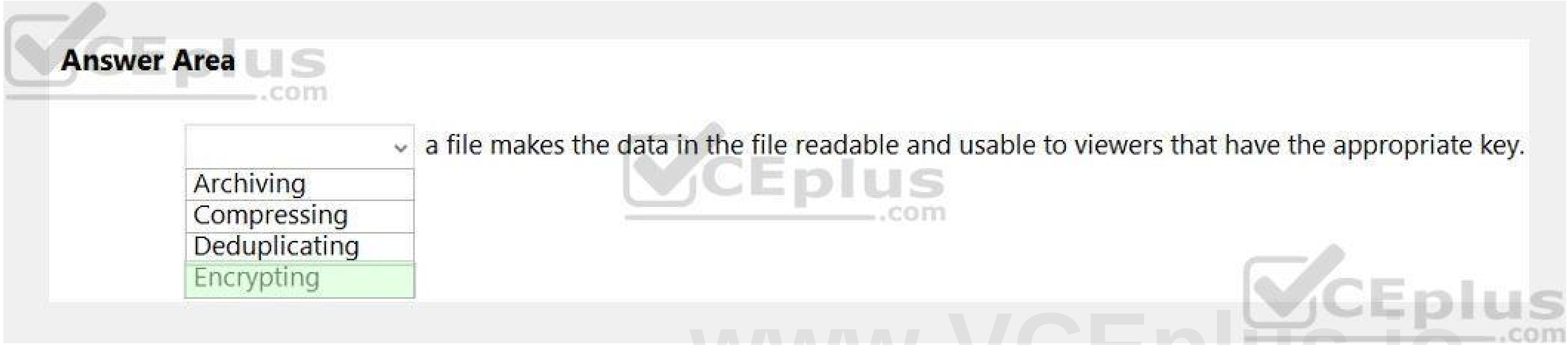


Answer Area

[⌄] a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- Encrypting

Answer Area:



Answer Area

[⌄] a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- [✓ Encrypting]

Section:
Explanation:

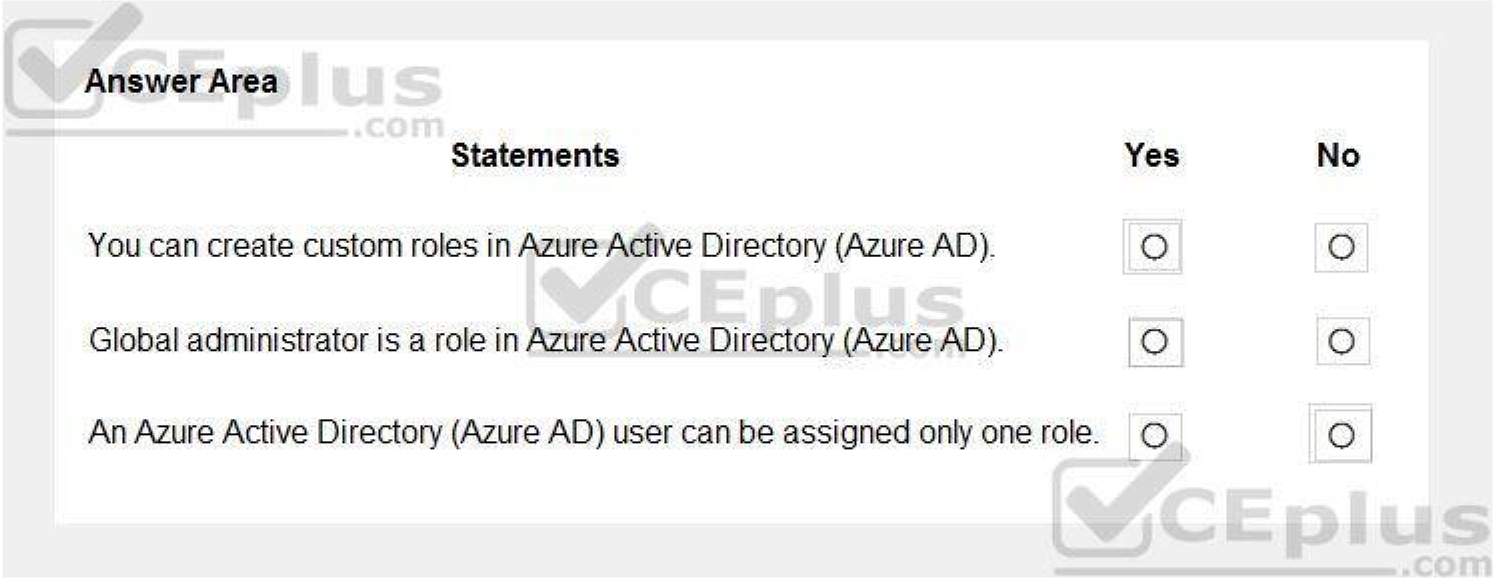
QUESTION 12

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

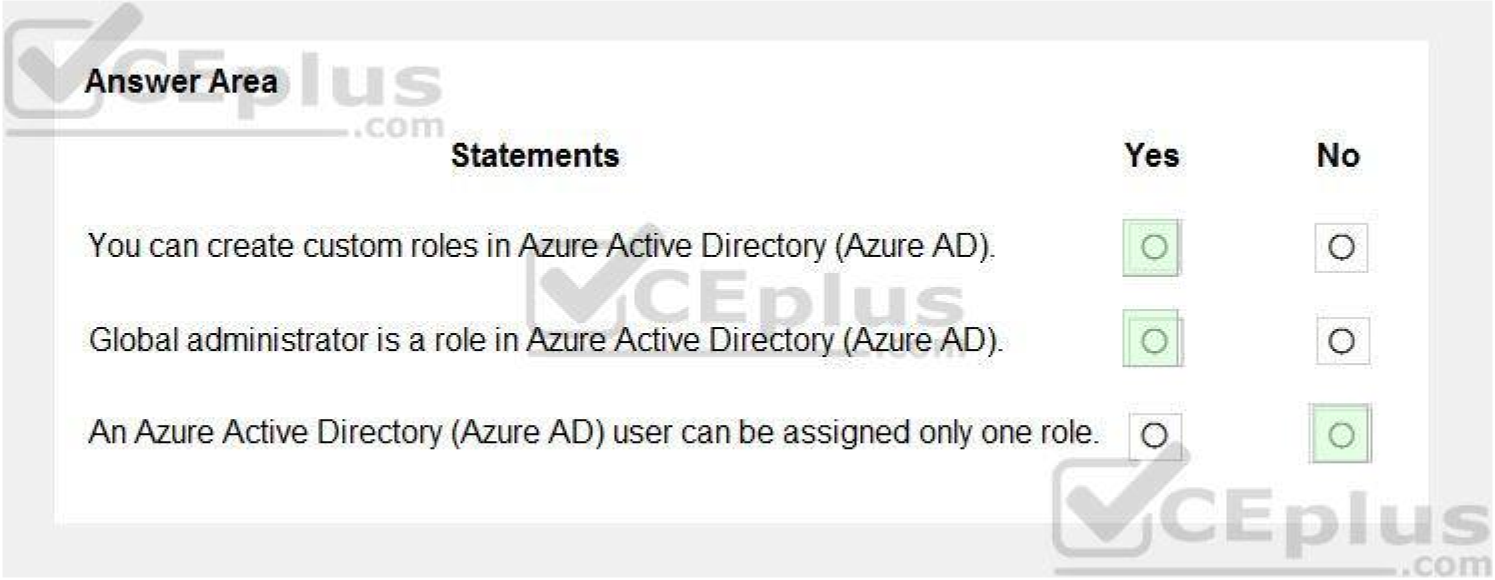
Hot Area:



Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Answer Area:



Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	[✓ ○]	○
Global administrator is a role in Azure Active Directory (Azure AD).	[✓ ○]	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	[✓ ○]

Section:

Explanation:

Box 1: Yes

Azure AD supports custom roles.

Box 2: Yes

Global Administrator has access to all administrative features in Azure Active Directory.

Box 3: No

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

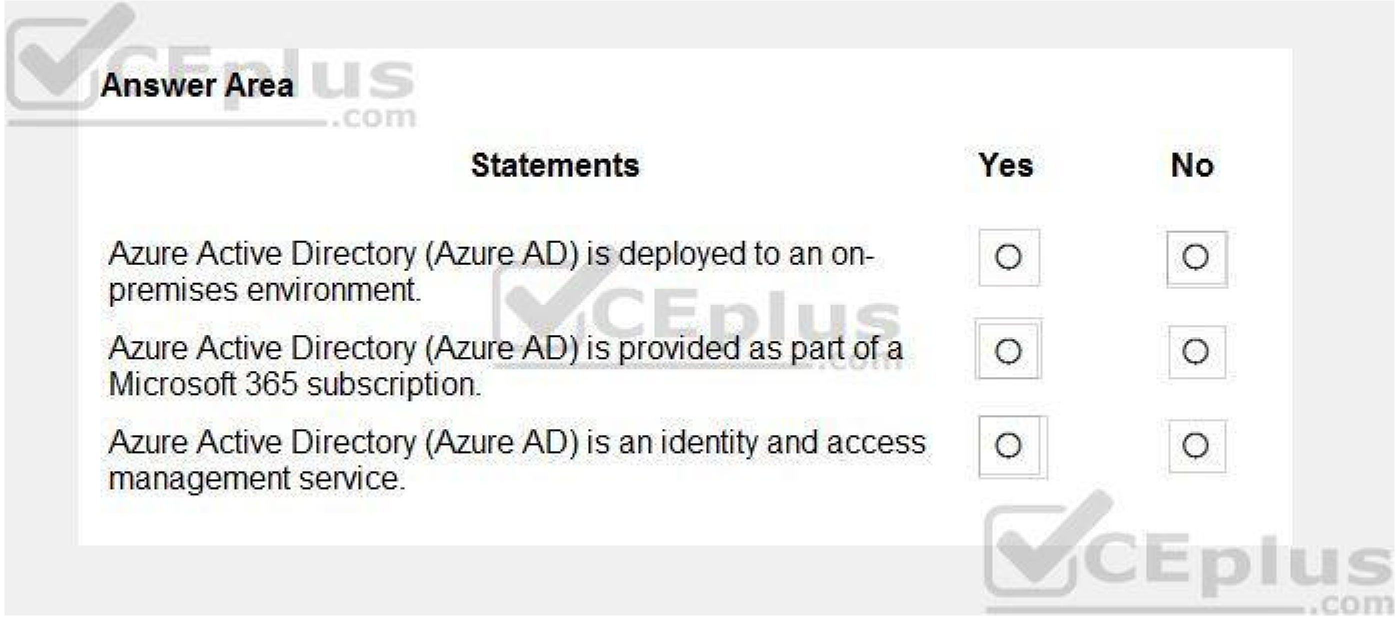
QUESTION 13

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

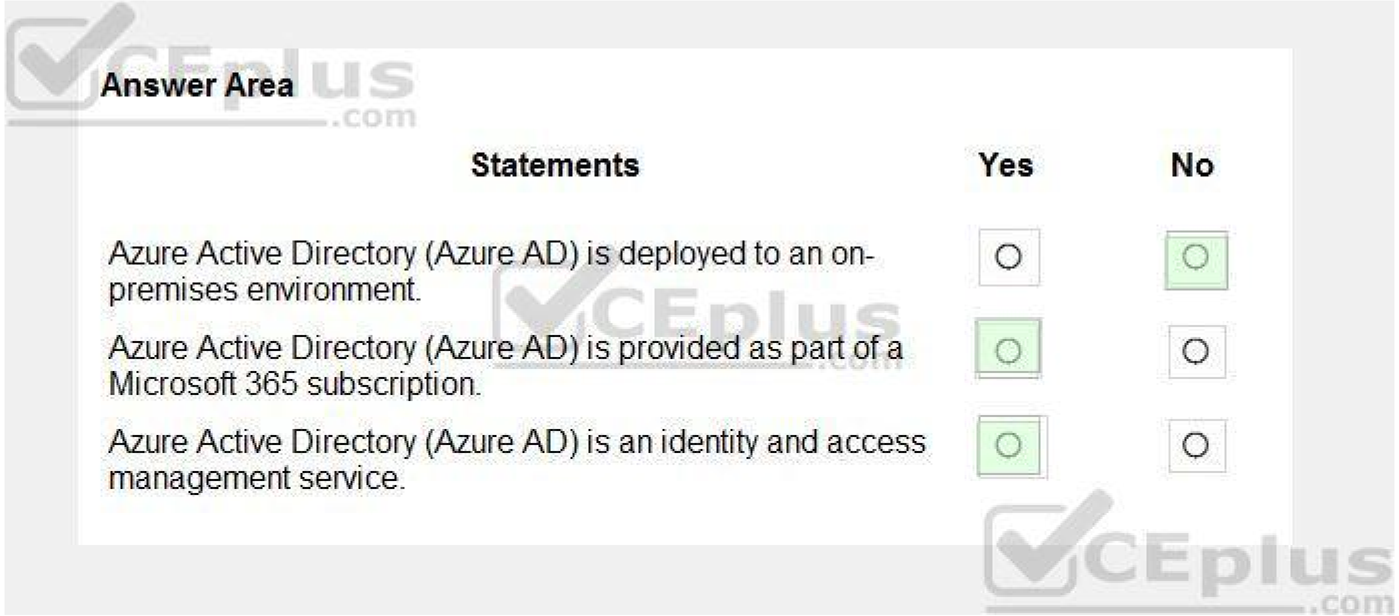
Hot Area:



Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	○	○
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	○	○
Azure Active Directory (Azure AD) is an identity and access management service.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	○	[✓ ○]
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	[✓ ○]	○
Azure Active Directory (Azure AD) is an identity and access management service.	[✓ ○]	○

Section:
Explanation:
Box 1: No
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.
Box 2: Yes
Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.
Box 3: Yes
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

QUESTION 14
What is a use case for implementing information barrier policies in Microsoft 365?

A. to restrict unauthenticated access to Microsoft 365
B. to restrict Microsoft Teams chats between certain groups within an organization
C. to restrict Microsoft Exchange Online email between certain groups within an organization
D. to restrict data sharing to external email recipients

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide

QUESTION 15
What can you use to provision Azure resources across multiple subscriptions in a consistent manner?

A. Azure Defender
B. Azure Blueprints
C. Azure Sentinel
D. Azure Policy

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

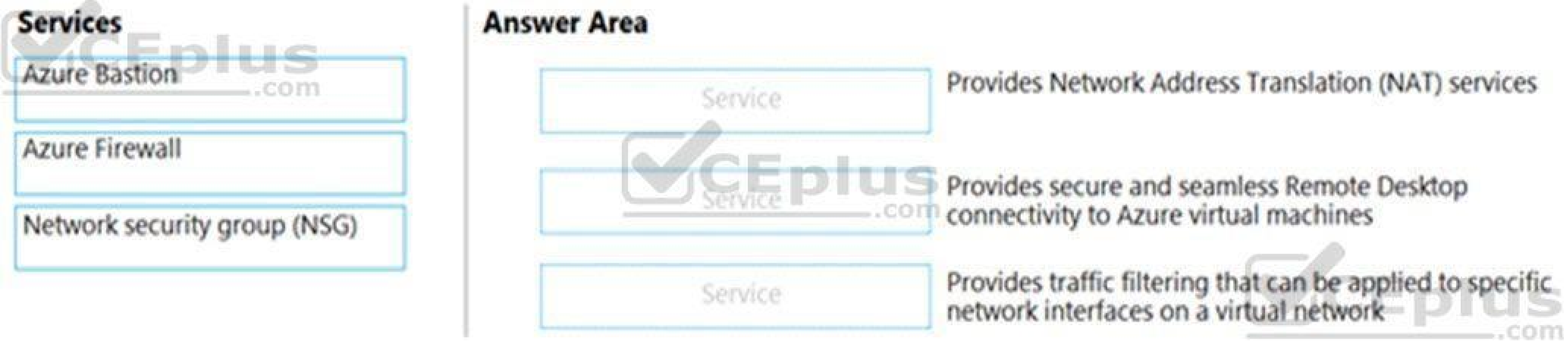
QUESTION 16
Which Microsoft 365 compliance center feature can you use to identify all the documents on a Microsoft SharePoint Online site that contain a specific key word?

A. Audit
B. Compliance Manager
C. Content Search
D. Alerts

Correct Answer: C
Section:
Explanation:
The Content Search tool in the Security & Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations, and instant messaging conversations in Skype for Business. The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide

QUESTION 17
DRAG DROP
Match the Azure networking service to the appropriate description.
To answer, drag the appropriate service from the column on the left to its description on the right. Each service may be used once, more than once, or not at all.
NOTE: Each correct match is worth one point.

Select and Place:



Services

Azure Bastion

Azure Firewall

Network security group (NSG)

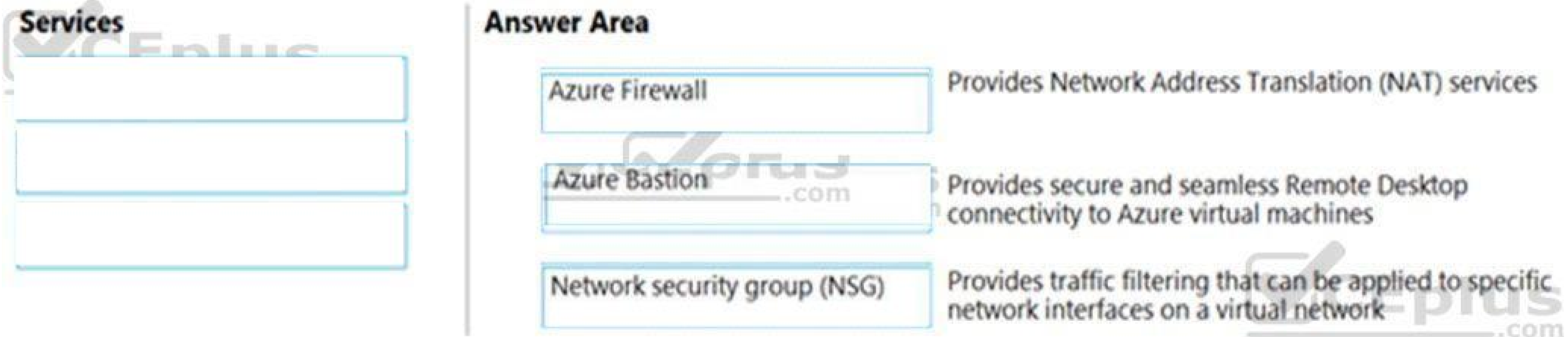
Answer Area

Service | Provides Network Address Translation (NAT) services

Service | Provides secure and seamless Remote Desktop connectivity to Azure virtual machines

Service | Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Correct Answer:



Services

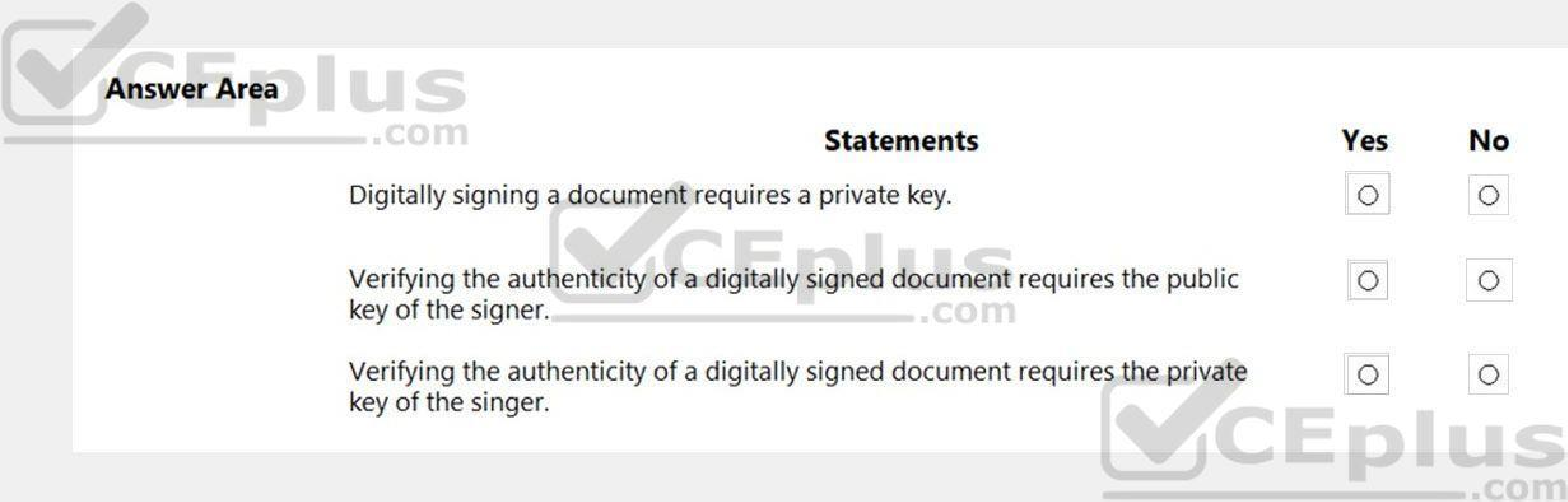
Answer Area

Azure Firewall	Provides Network Address Translation (NAT) services
Azure Bastion	Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Section:
Explanation:
Box 1: Azure Firewall
Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.
Box 2: Azure Bastion
Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.
Box 3: Network security group (NSG)
You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.
Reference:
https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
https://docs.microsoft.com/en-us/azure/firewall/features
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 18
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

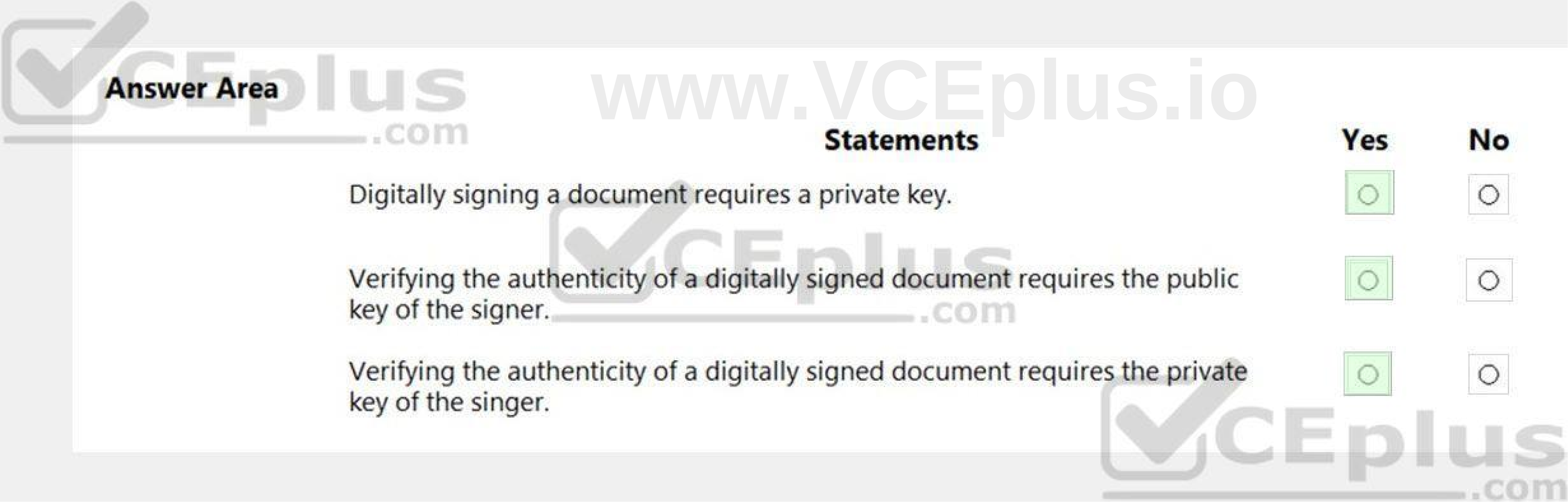
Hot Area:



Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	○	○
Verifying the authenticity of a digitally signed document requires the public key of the signer.	○	○
Verifying the authenticity of a digitally signed document requires the private key of the singer.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	[✓ ○]	○
Verifying the authenticity of a digitally signed document requires the public key of the signer.	[✓ ○]	○
Verifying the authenticity of a digitally signed document requires the private key of the singer.	[✓ ○]	○

Section:

Explanation:

Box 1: Yes

A certificate is required that provides a private and a public key.

Box 2: Yes

The public key is used to validate the private key that is associated with a digital signature.

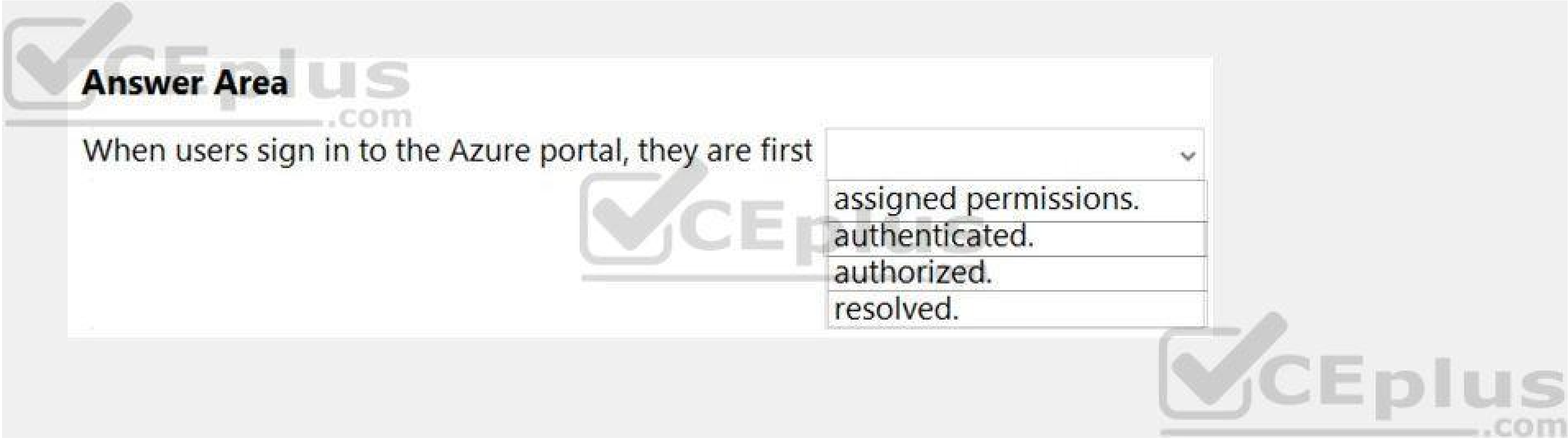
Box 3: Yes

The private key, or rather the password to the private key, validates the identity of the signer.

Reference:
https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512
https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/fin-ops/organization-administration/electronic-signature-overview

QUESTION 19
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

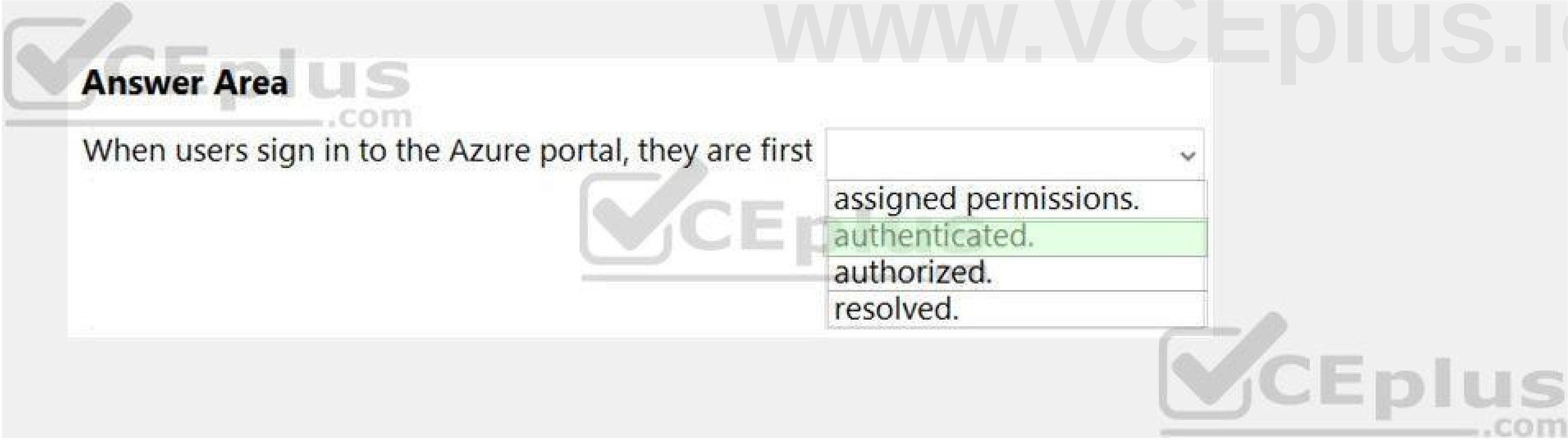


Answer Area

When users sign in to the Azure portal, they are first

- assigned permissions.
- authenticated.
- authorized.
- resolved.

Answer Area:



Answer Area

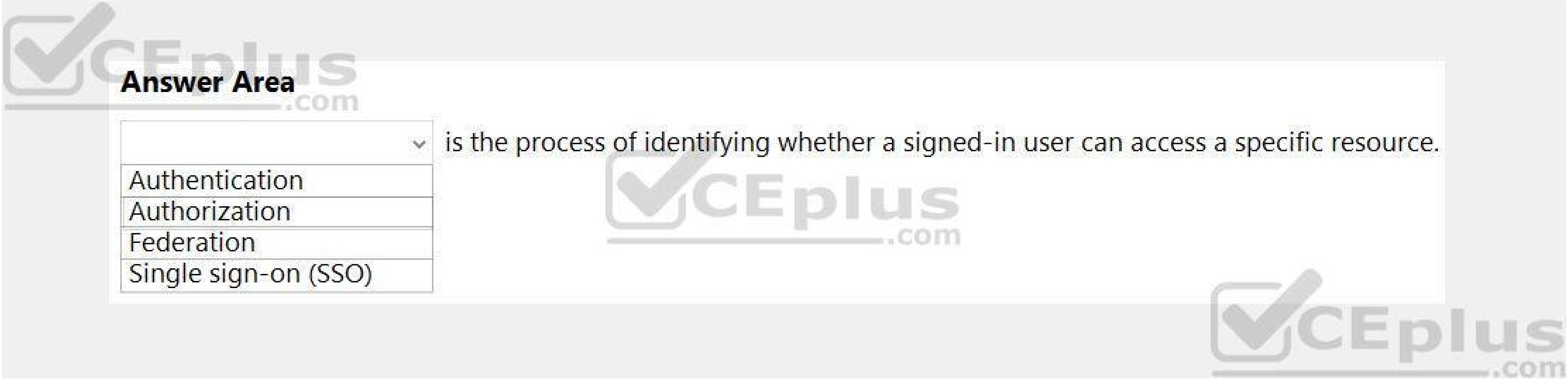
When users sign in to the Azure portal, they are first

- assigned permissions.
- [✓ authenticated.]
- authorized.
- resolved.

Section:
Explanation:

QUESTION 20
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

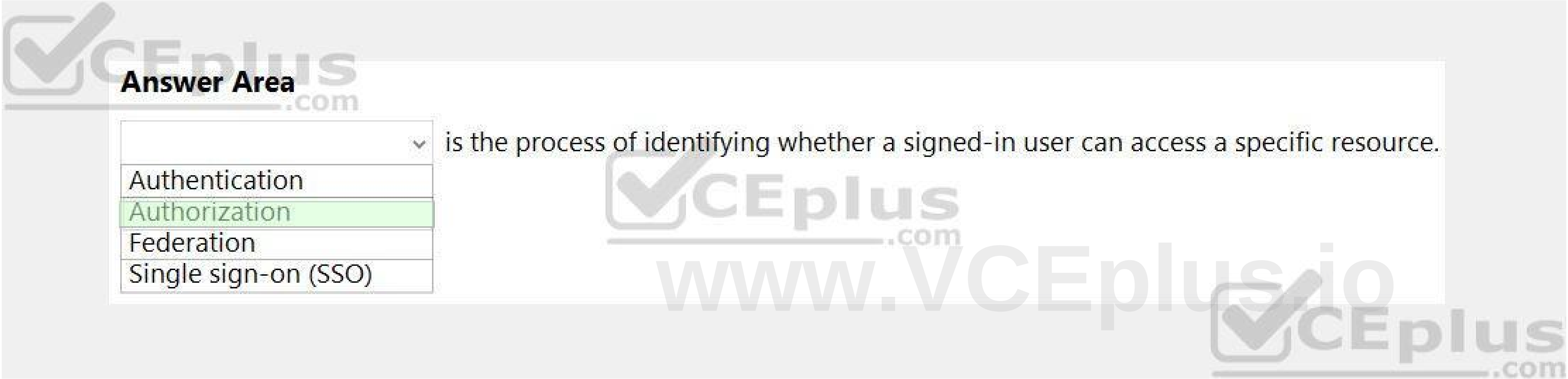


Answer Area

[ ] is the process of identifying whether a signed-in user can access a specific resource.

- Authentication
- Authorization
- Federation
- Single sign-on (SSO)

Answer Area:



Answer Area

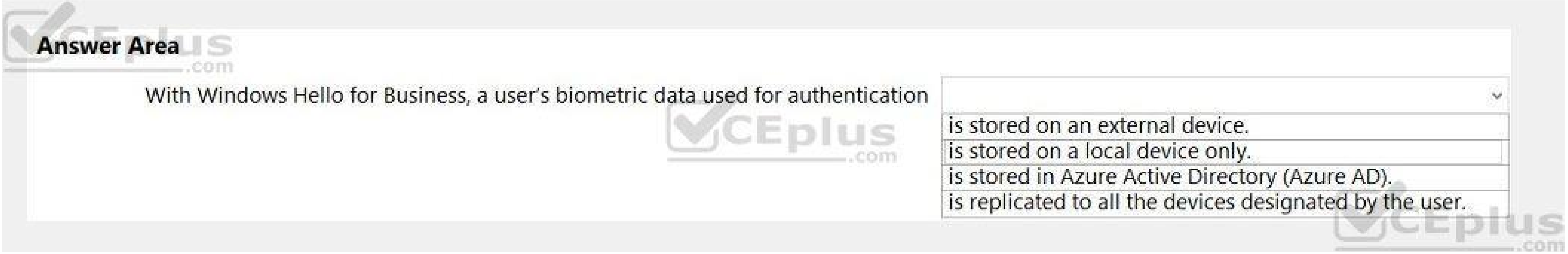
[ ] is the process of identifying whether a signed-in user can access a specific resource.

- Authentication
- [✓ Authorization]
- Federation
- Single sign-on (SSO)

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization

QUESTION 21
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

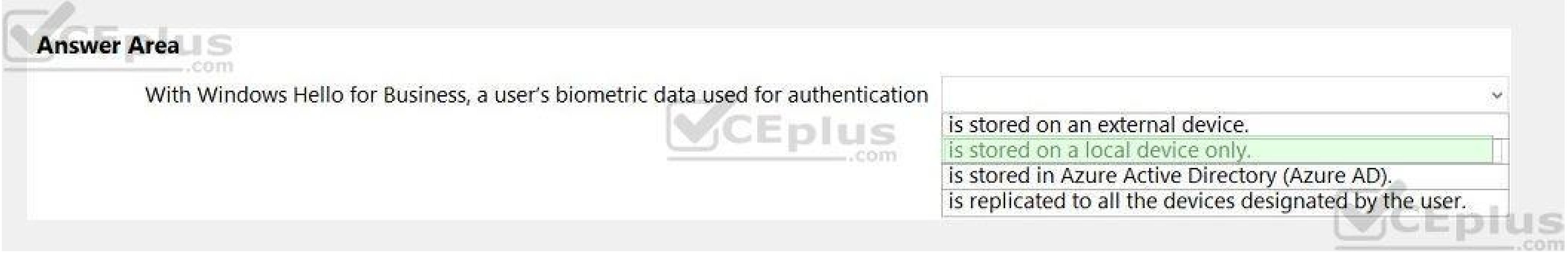


Answer Area

With Windows Hello for Business, a user's biometric data used for authentication [ ]

- is stored on an external device.
- is stored on a local device only.
- is stored in Azure Active Directory (Azure AD).
- is replicated to all the devices designated by the user.

Answer Area:



Answer Area

With Windows Hello for Business, a user's biometric data used for authentication

- is stored on an external device.
- [✓ is stored on a local device only.]
- is stored in Azure Active Directory (Azure AD).
- is replicated to all the devices designated by the user.

Section:

Explanation:

Biometrics templates are stored locally on a device.

Reference:

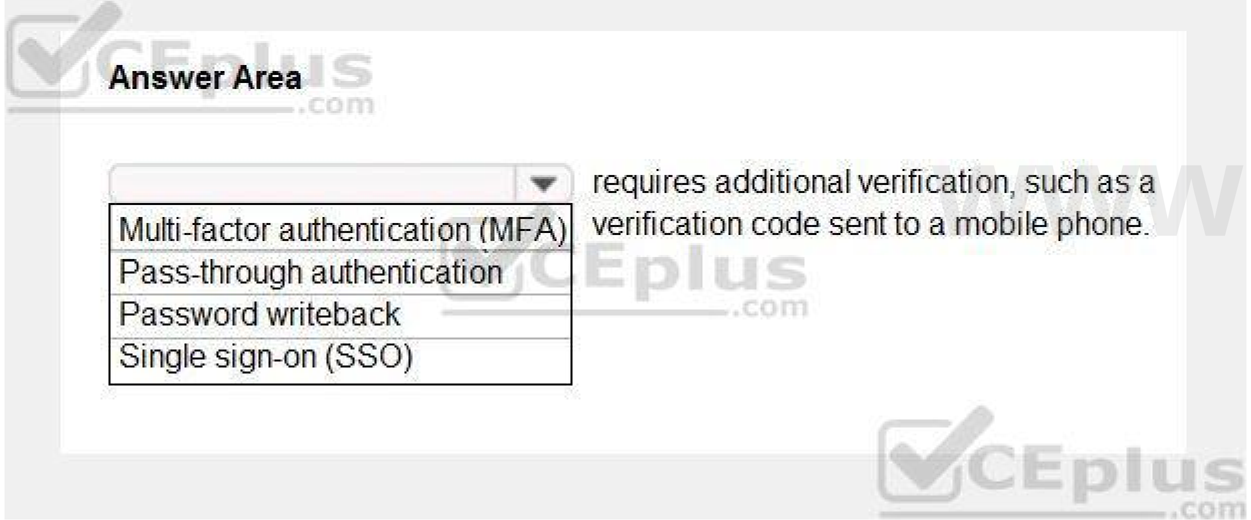
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

QUESTION 22

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

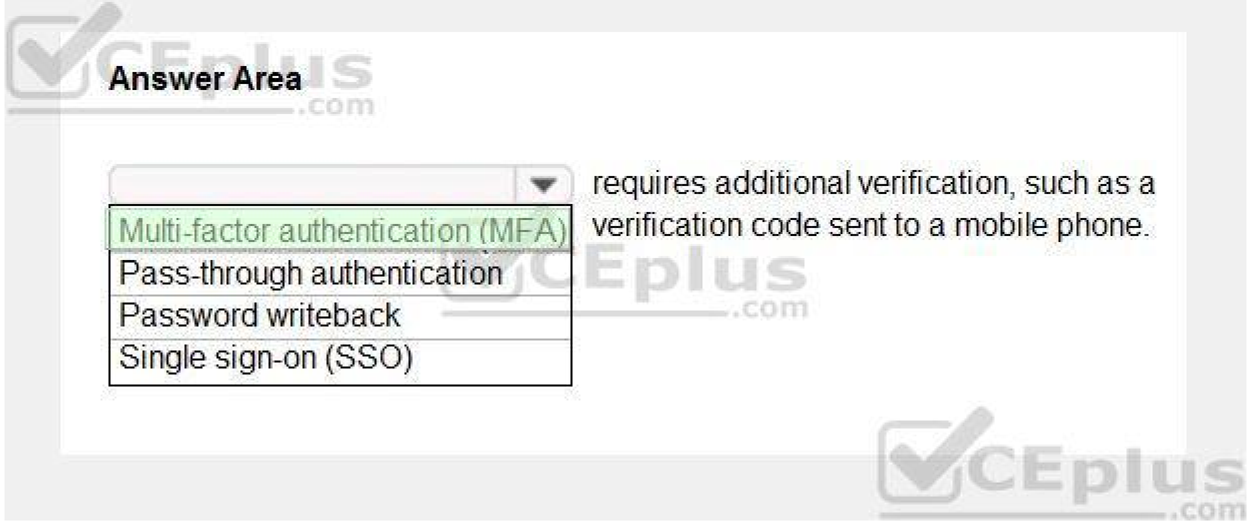


Answer Area

- Multi-factor authentication (MFA)
- Pass-through authentication
- Password writeback
- Single sign-on (SSO)

requires additional verification, such as a verification code sent to a mobile phone.

Answer Area:



Answer Area

- [✓ Multi-factor authentication (MFA)]
- Pass-through authentication
- Password writeback
- Single sign-on (SSO)

requires additional verification, such as a verification code sent to a mobile phone.

Section:

Explanation:

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

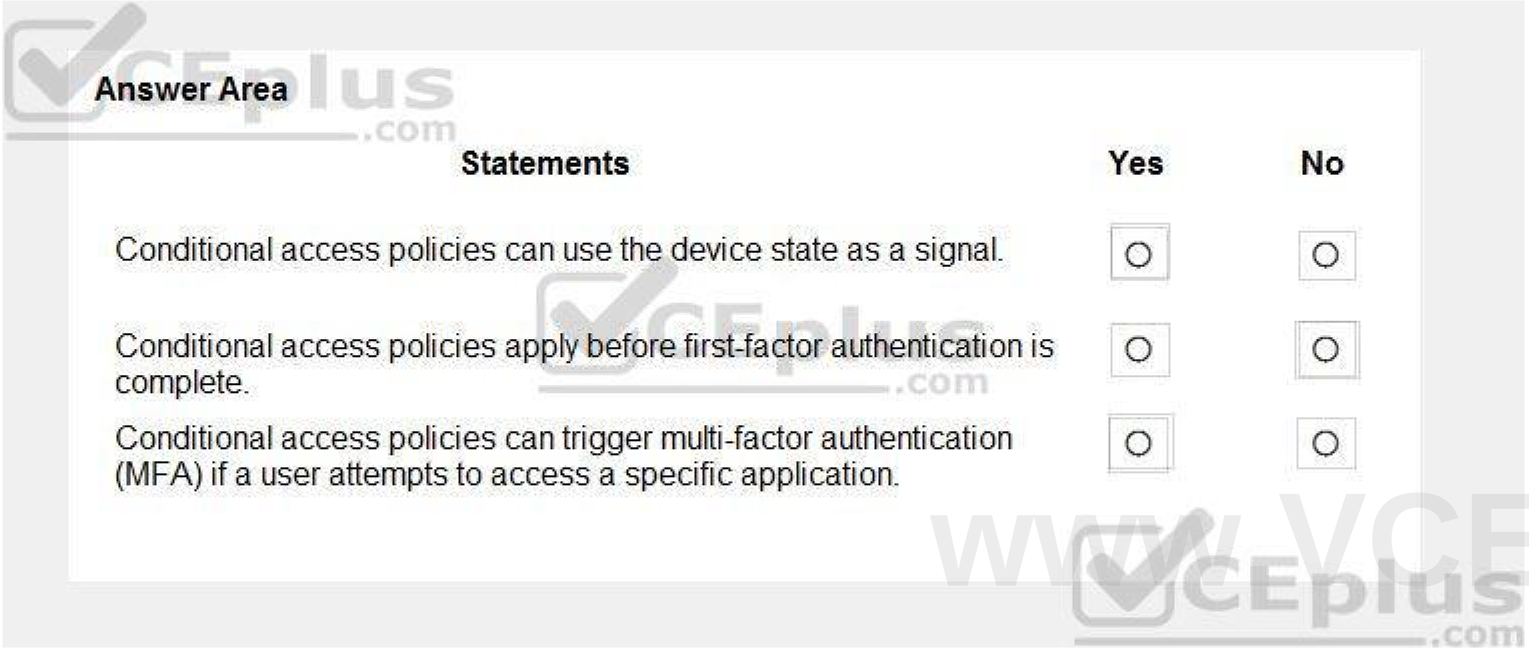
QUESTION 23

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

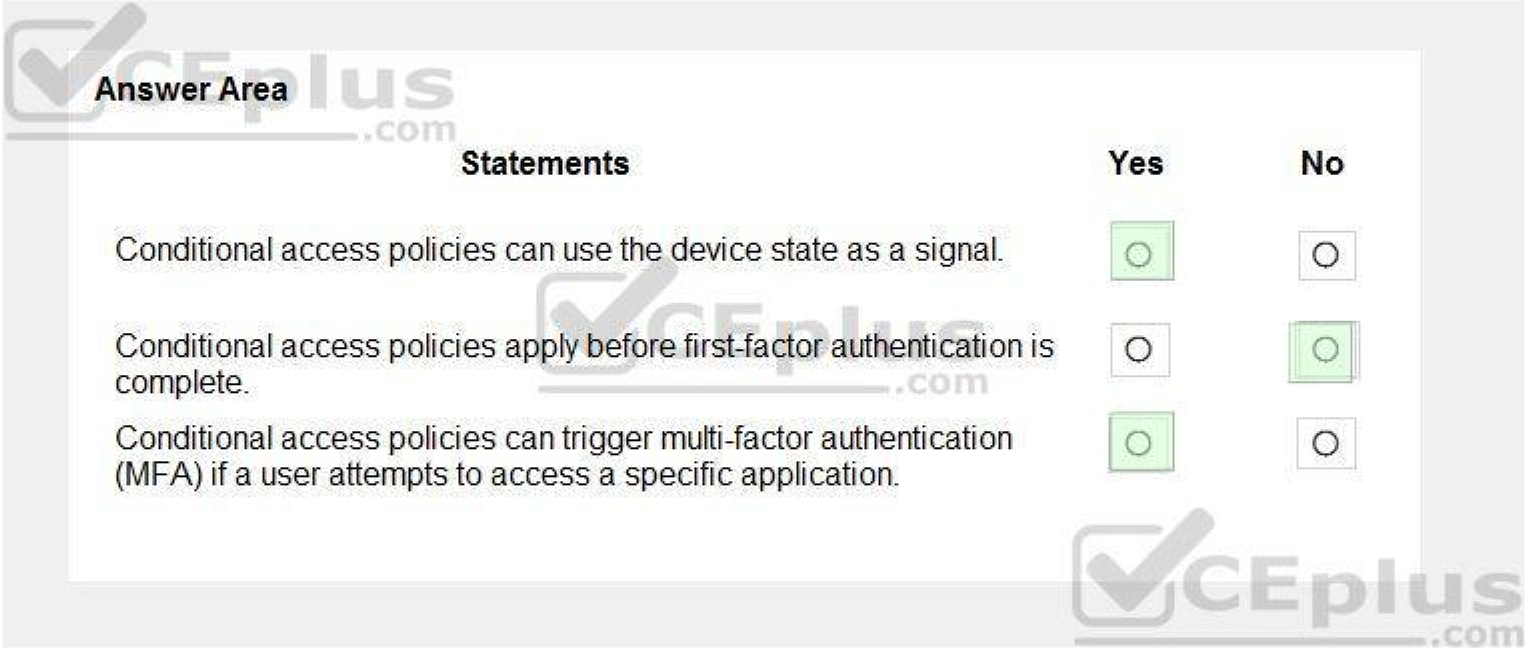
Hot Area:



Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	○	○
Conditional access policies apply before first-factor authentication is complete.	○	○
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	[✓ ○]	○
Conditional access policies apply before first-factor authentication is complete.	○	[✓ ○]
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	[✓ ○]	○

Section:

Explanation:

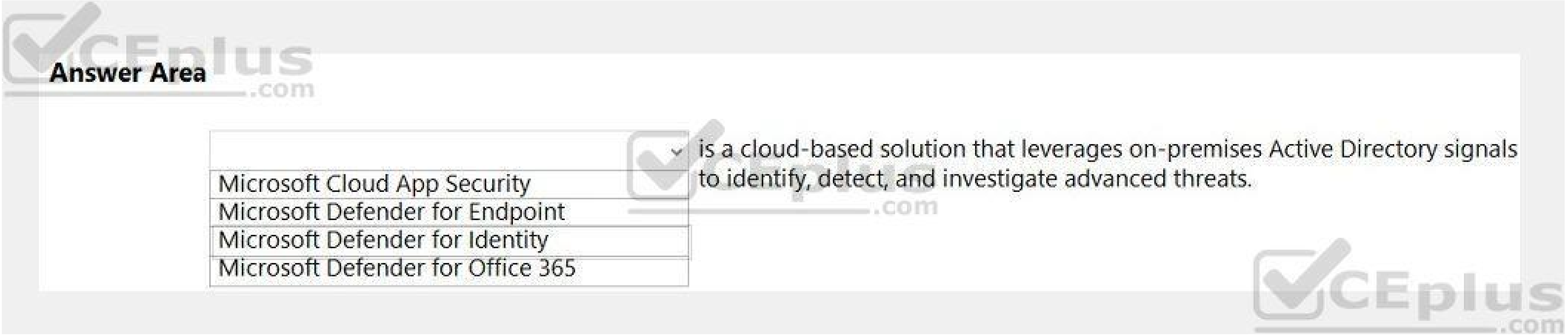
Box 1: Yes

Box 2: No

Conditional Access policies are enforced after first-factor authentication is completed.
Box 3: Yes
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

QUESTION 24
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

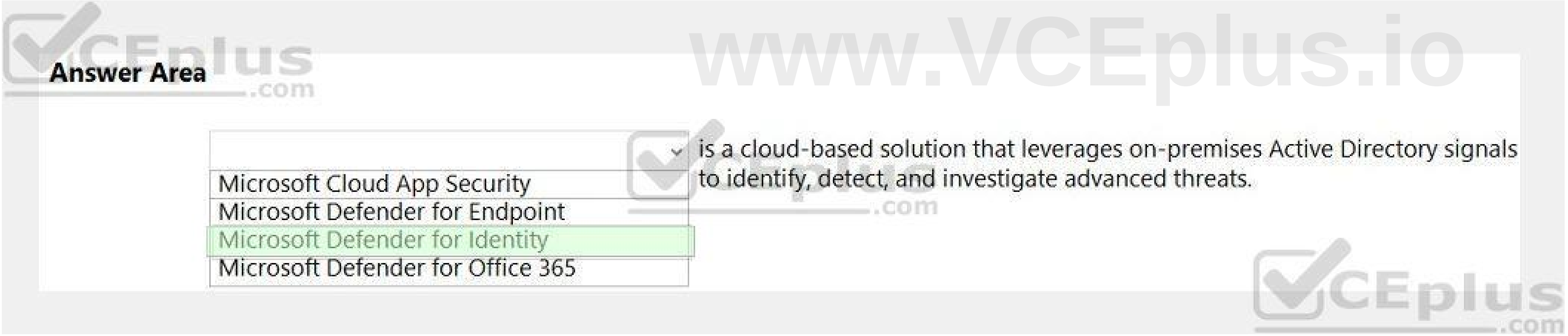


Answer Area

- Microsoft Cloud App Security
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Answer Area:



Answer Area

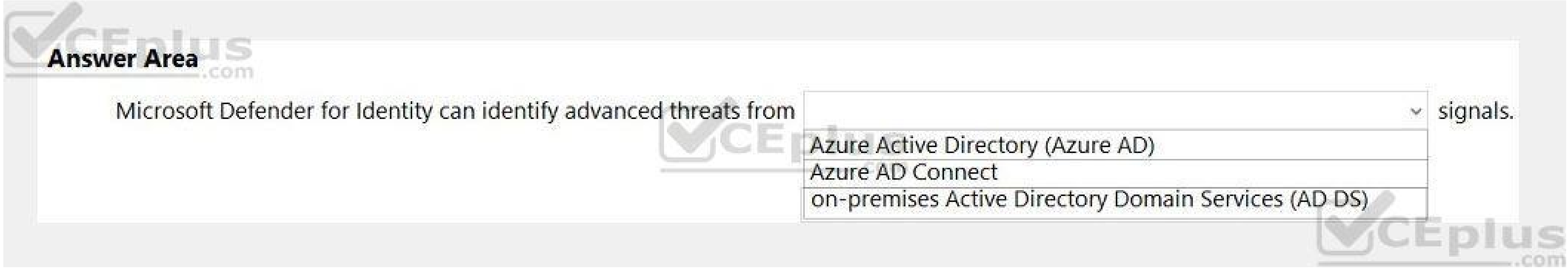
- Microsoft Cloud App Security
- Microsoft Defender for Endpoint
- [✓ Microsoft Defender for Identity]
- Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is

QUESTION 25
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

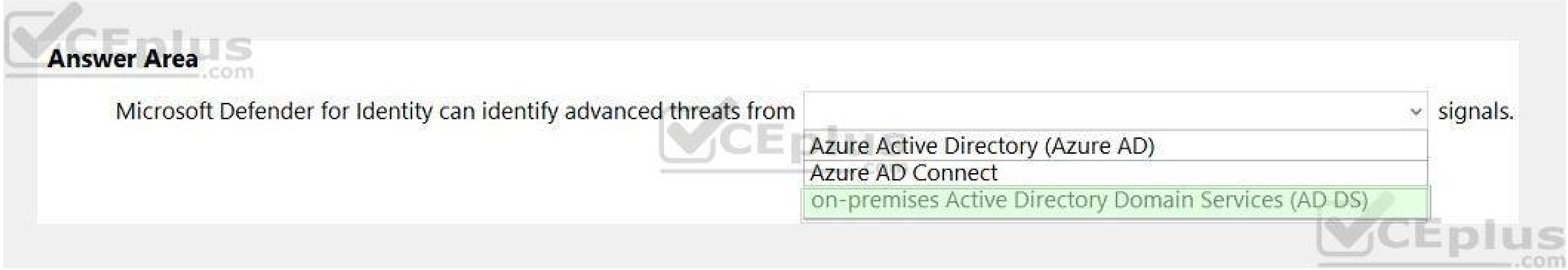


Answer Area

Microsoft Defender for Identity can identify advanced threats from ▾ signals.

- Azure Active Directory (Azure AD)
- Azure AD Connect
- on-premises Active Directory Domain Services (AD DS)

Answer Area:



Answer Area

Microsoft Defender for Identity can identify advanced threats from ▾ signals.

- Azure Active Directory (Azure AD)
- Azure AD Connect
- [✓ on-premises Active Directory Domain Services (AD DS)]

Section:

Explanation:

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Reference:

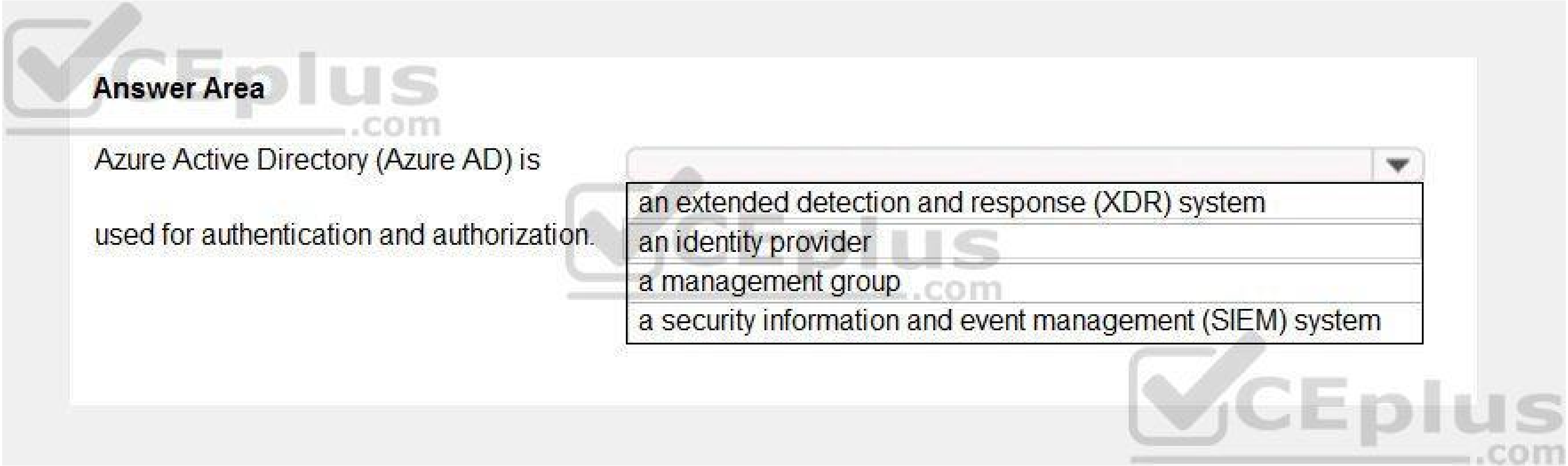
https://docs.microsoft.com/en-us/defender-for-identity/what-is

QUESTION 26

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

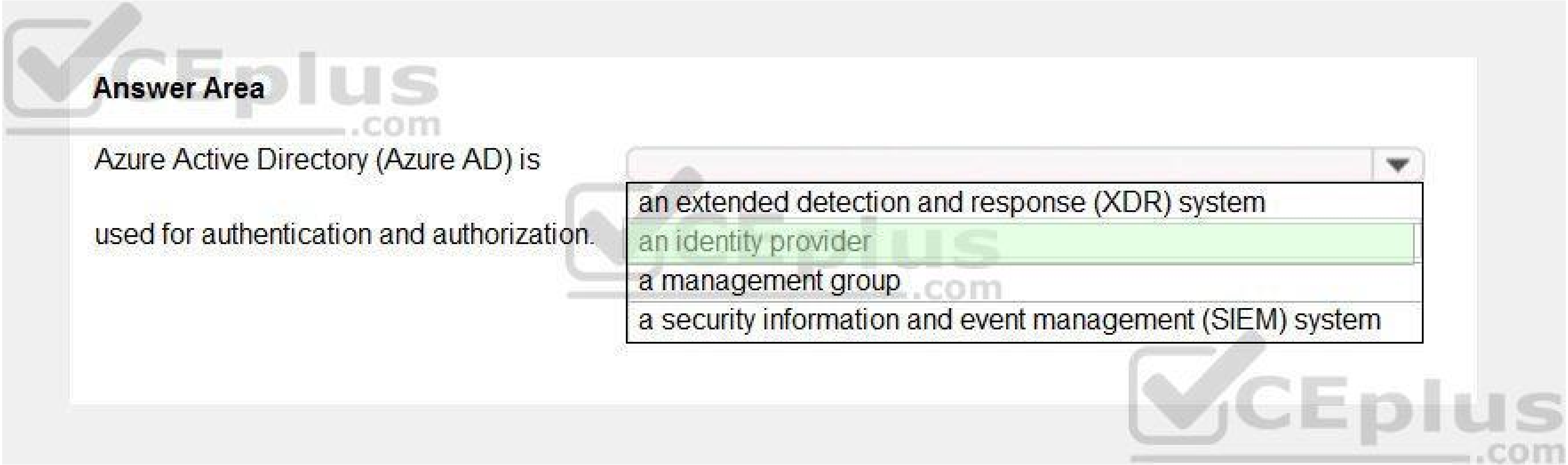


Answer Area

Azure Active Directory (Azure AD) is ▾ used for authentication and authorization.

- an extended detection and response (XDR) system
- an identity provider
- a management group
- a security information and event management (SIEM) system

Answer Area:



Answer Area

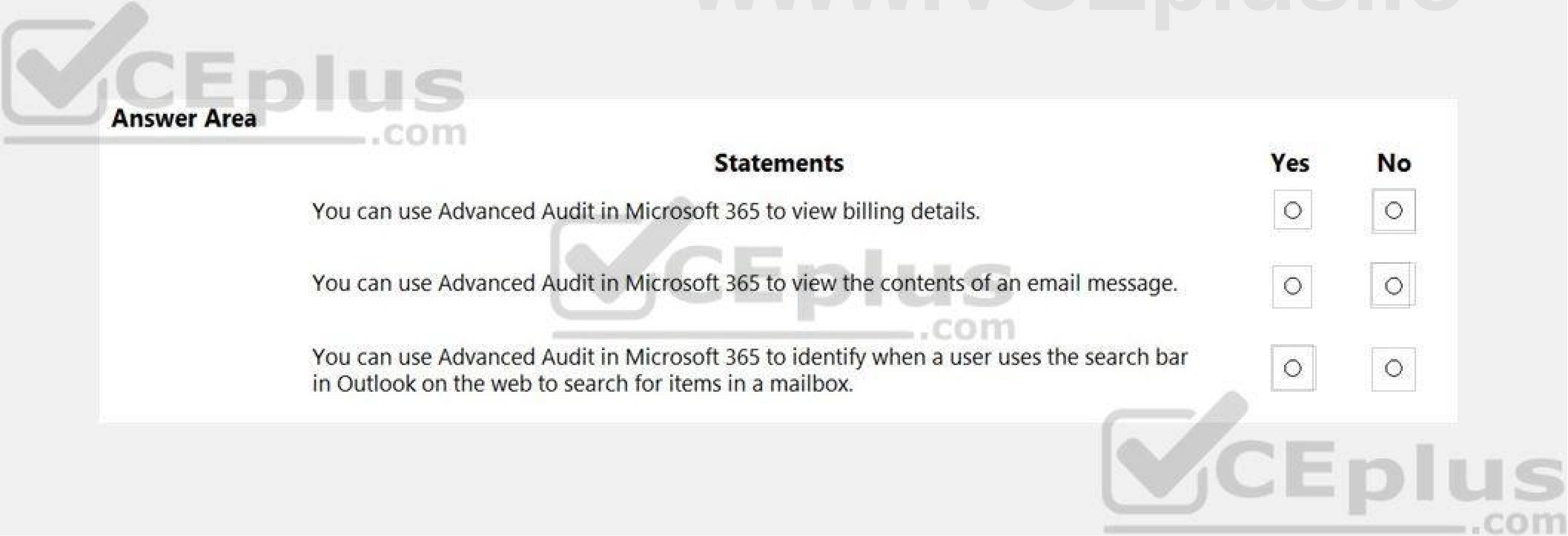
Azure Active Directory (Azure AD) is used for authentication and authorization.

- an extended detection and response (XDR) system
- [✓ an identity provider]
- a management group
- a security information and event management (SIEM) system

Section:
Explanation:
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

QUESTION 27
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

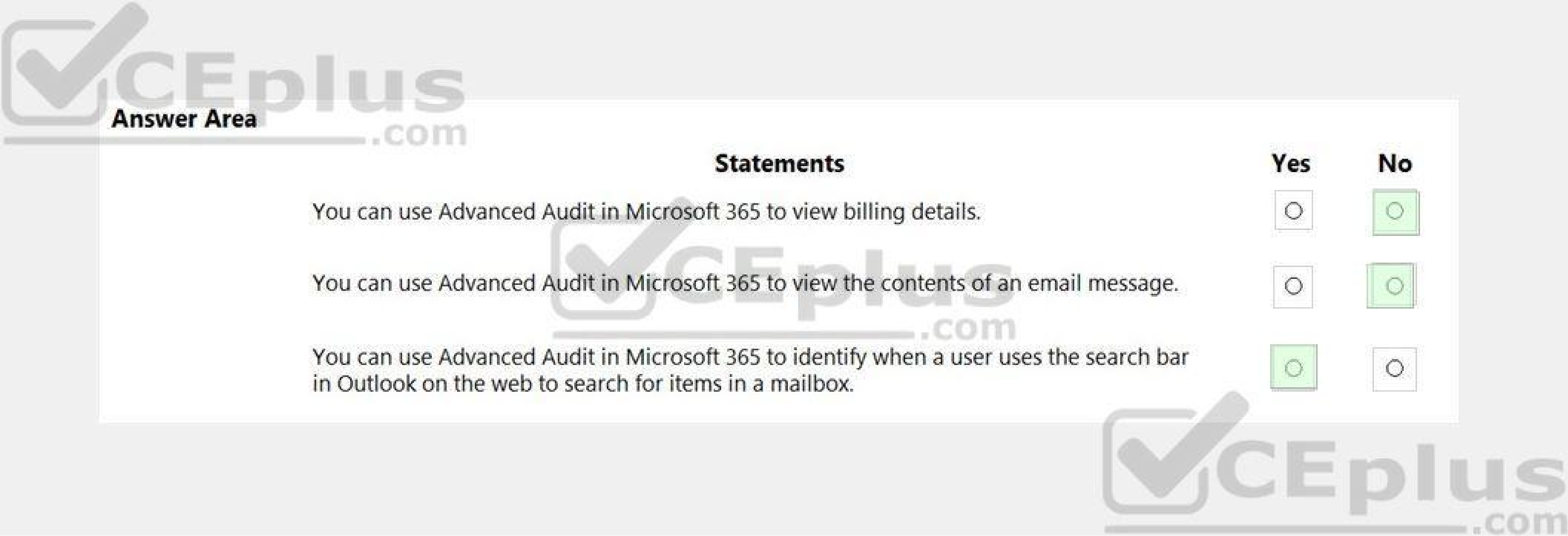
Hot Area:



Answer Area

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

Answer Area:



Answer Area

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	[✓ ○]
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	[✓ ○]
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	[✓ ○]	○

Section:

Explanation:

Box 1: No

Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.

Box 2: No

Box 3: Yes

Reference:

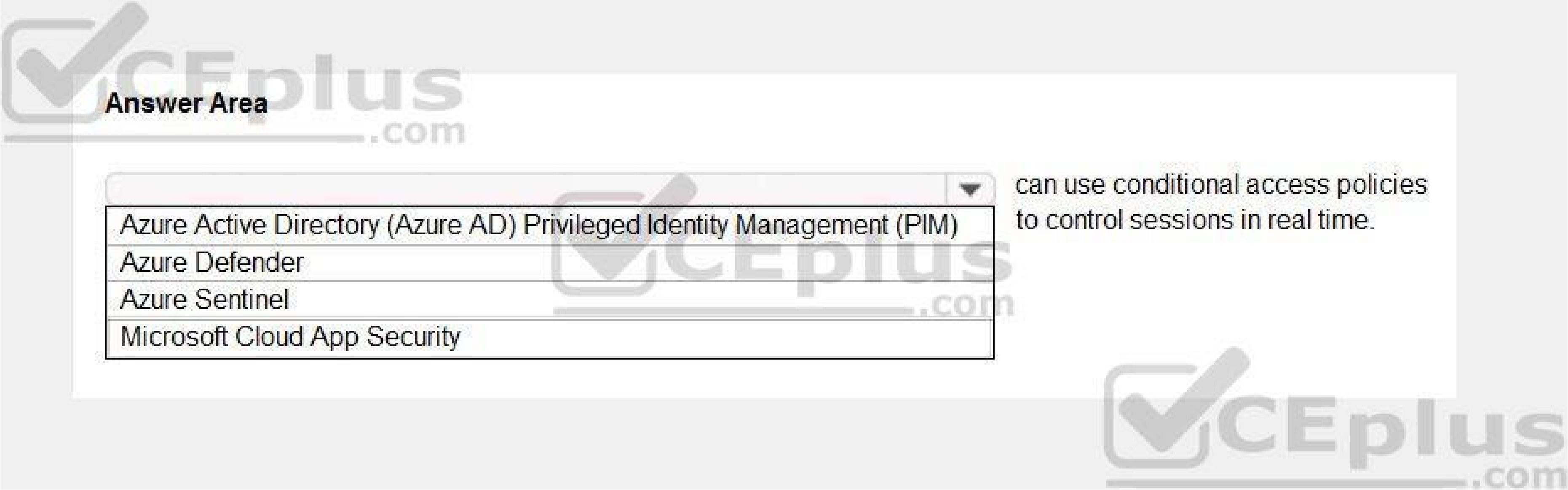
https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide

QUESTION 28

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

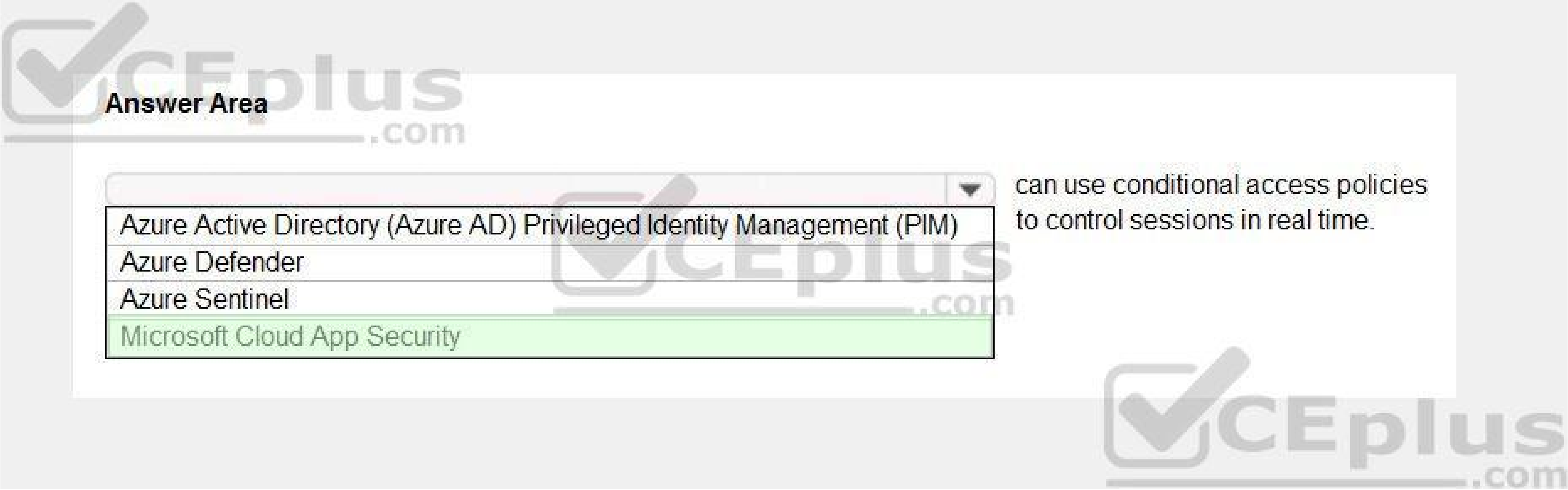


Answer Area

[▼] can use conditional access policies to control sessions in real time.

- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Azure Defender
- Azure Sentinel
- Microsoft Cloud App Security

Answer Area:



Answer Area

- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Azure Defender
- Azure Sentinel
- [✓ Microsoft Cloud App Security]

can use conditional access policies to control sessions in real time.

Section:

Explanation:

Reference:

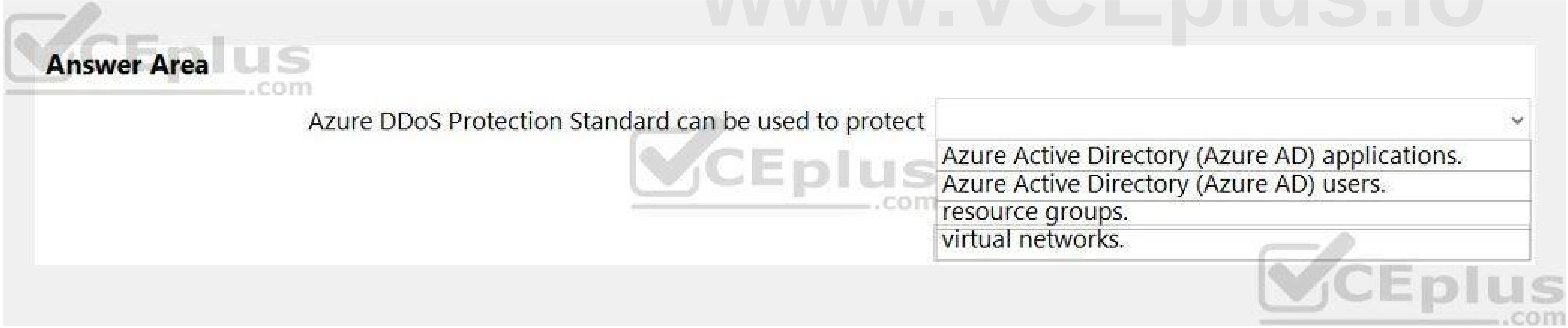
https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

QUESTION 29

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

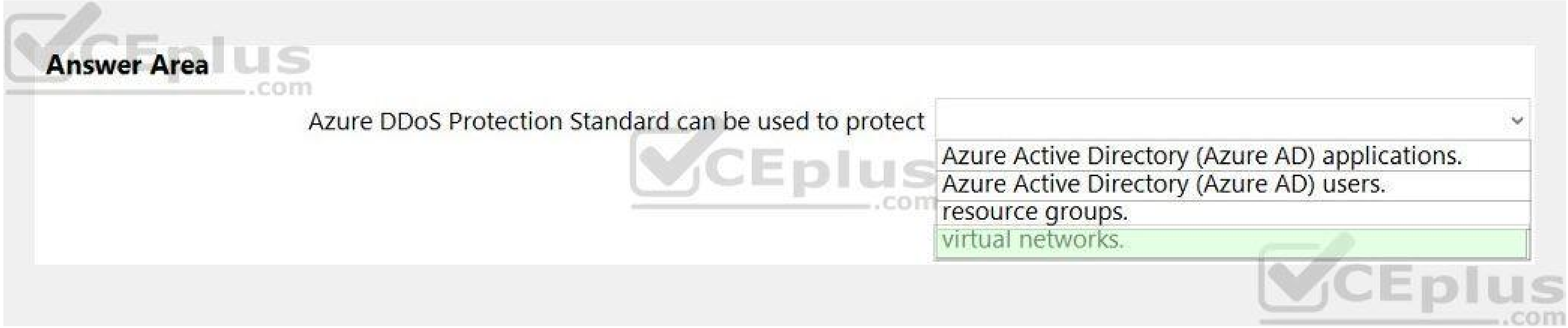


Answer Area

Azure DDoS Protection Standard can be used to protect

- Azure Active Directory (Azure AD) applications.
- Azure Active Directory (Azure AD) users.
- resource groups.
- virtual networks.

Answer Area:



Answer Area

Azure DDoS Protection Standard can be used to protect

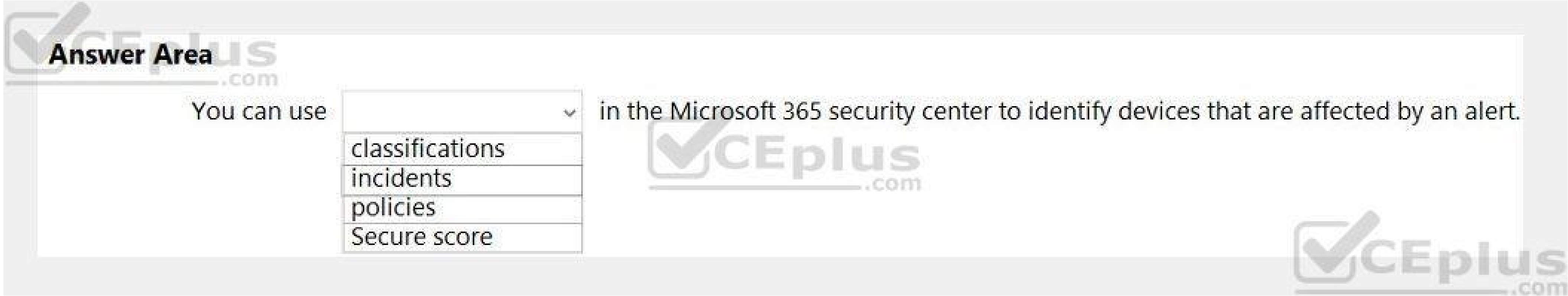
- Azure Active Directory (Azure AD) applications.
- Azure Active Directory (Azure AD) users.
- resource groups.
- [✓ virtual networks.]

Section:

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

QUESTION 30
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

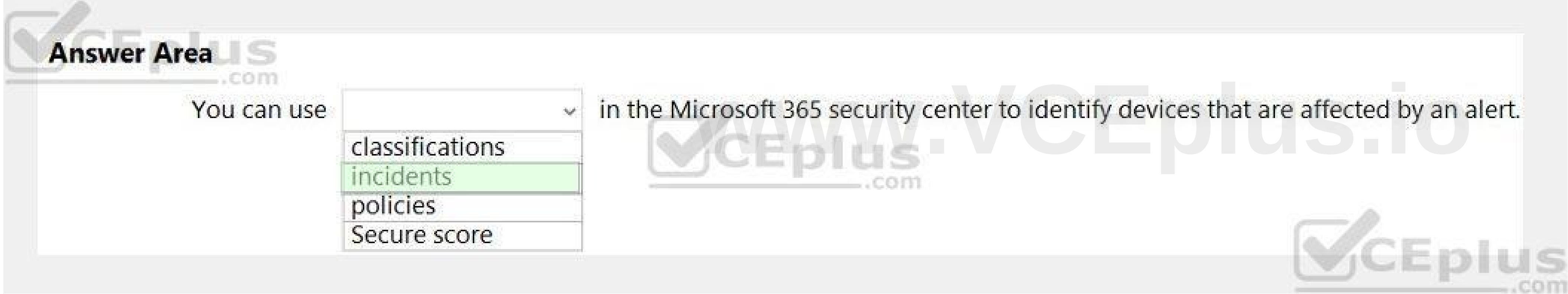


Answer Area

You can use [ ] in the Microsoft 365 security center to identify devices that are affected by an alert.

- classifications
- incidents
- policies
- Secure score

Answer Area:



Answer Area

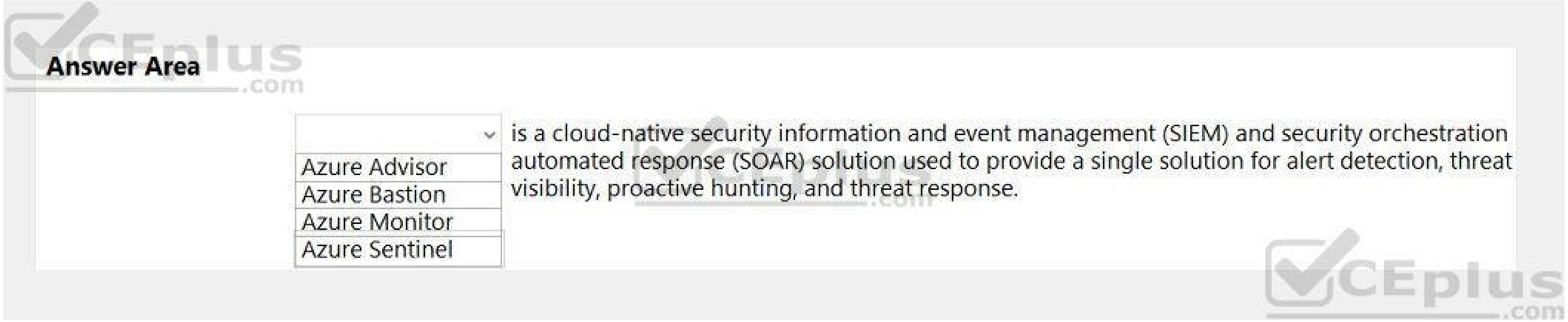
You can use [ ] in the Microsoft 365 security center to identify devices that are affected by an alert.

- classifications
- incidents
- policies
- Secure score

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

QUESTION 31
HOTSPOT
Select the answer that correctly completes the sentence.

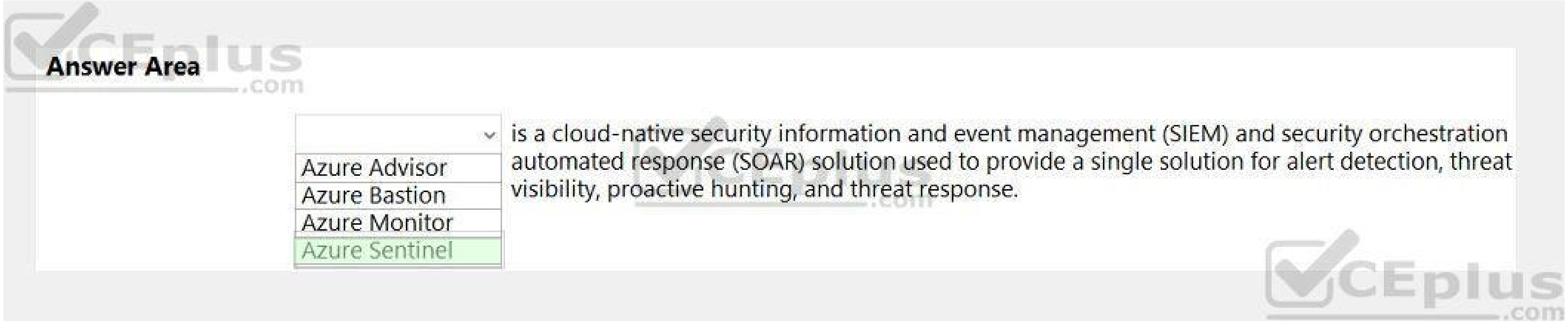
Hot Area:



Answer Area

is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Answer Area:



Answer Area

is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Section:

Explanation:

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/overview

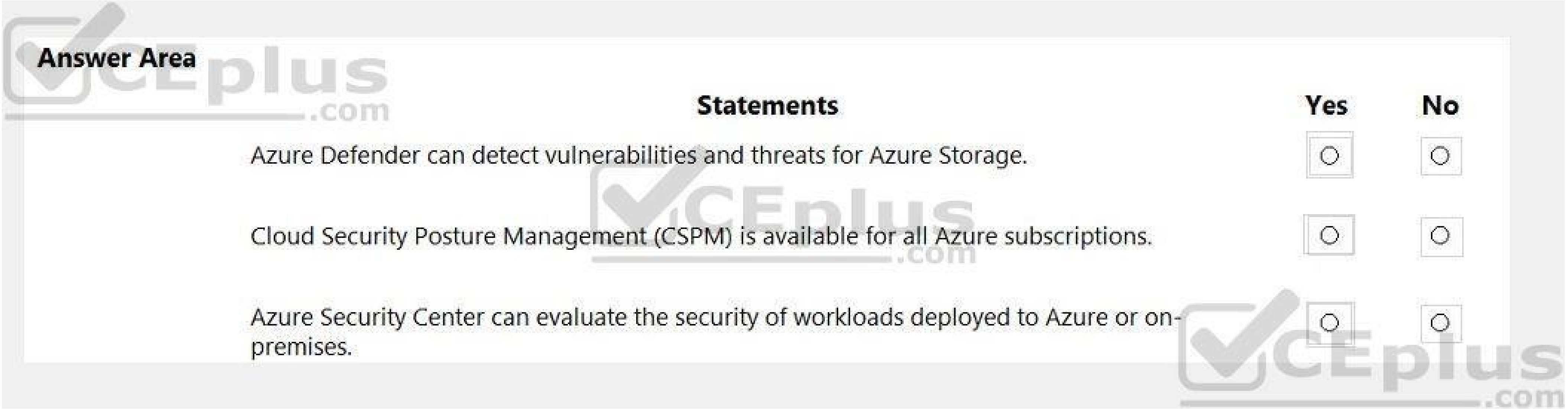
QUESTION 32

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

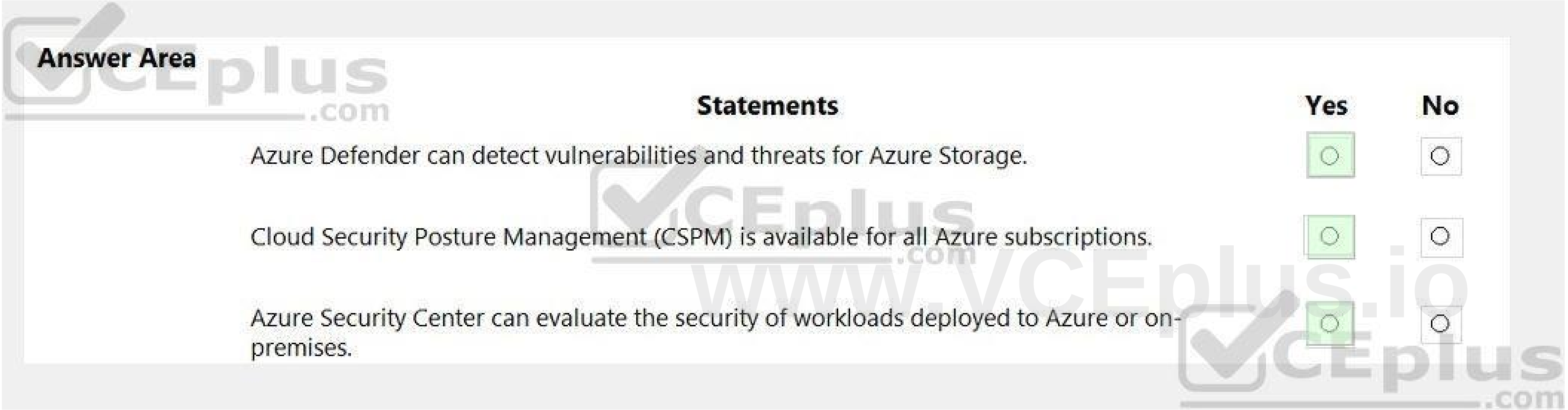
Hot Area:



Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	○	○

Answer Area:



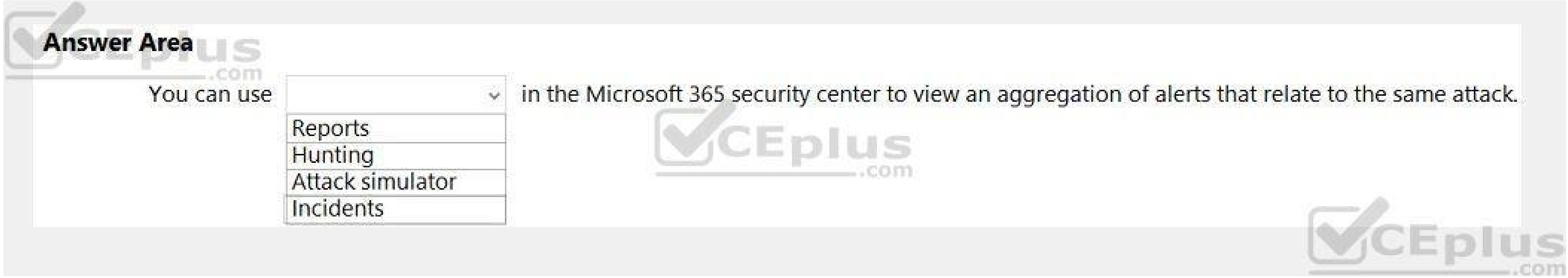
Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	[✓ ○]	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	[✓ ○]	○
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	[✓ ○]	○

Section:
Explanation:
Box 1: Yes
Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more
Box 2: Yes
Cloud security posture management (CSPM) is available for free to all Azure users.
Box 3: Yes
Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender
https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction
https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction

QUESTION 33
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

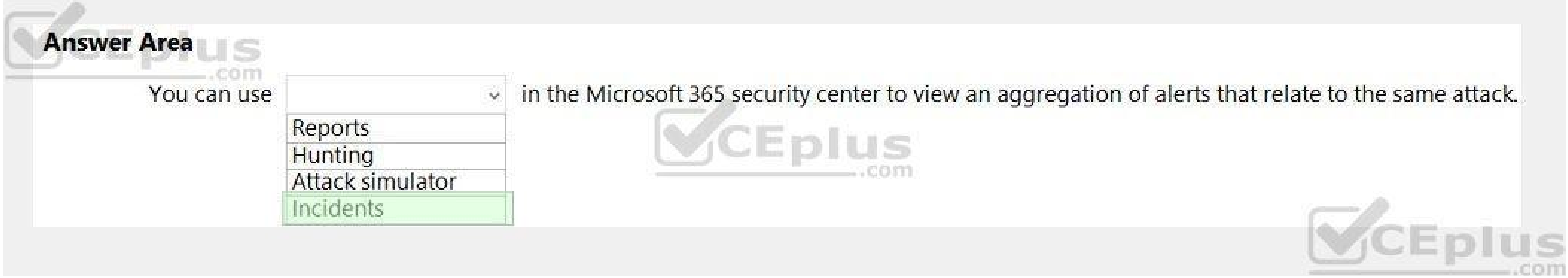


Answer Area

You can use ⌄ in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

- Reports
- Hunting
- Attack simulator
- Incidents

Answer Area:



Answer Area

You can use ⌄ in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

- Reports
- Hunting
- Attack simulator
- [✓ Incidents]

Section:

Explanation:

Reference:

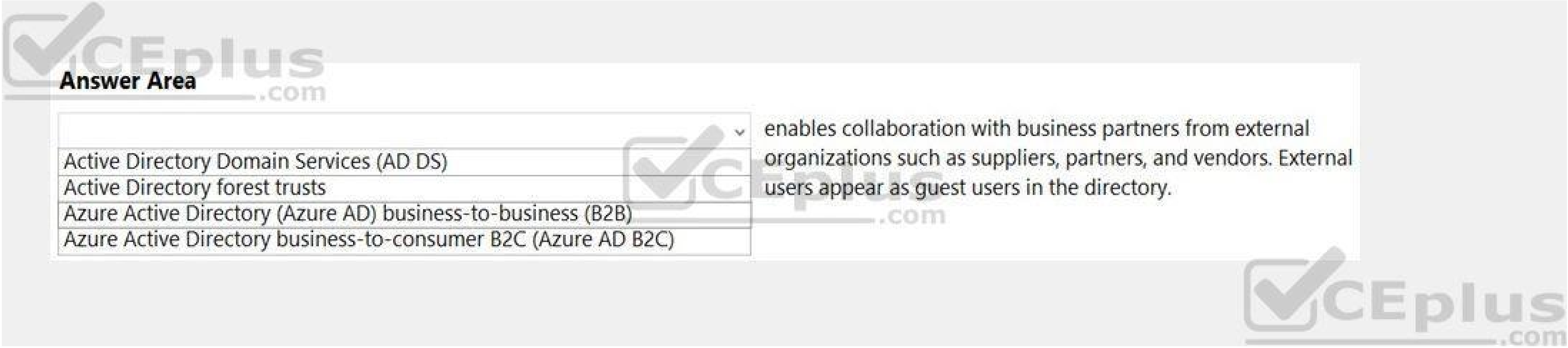
https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide

QUESTION 34

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

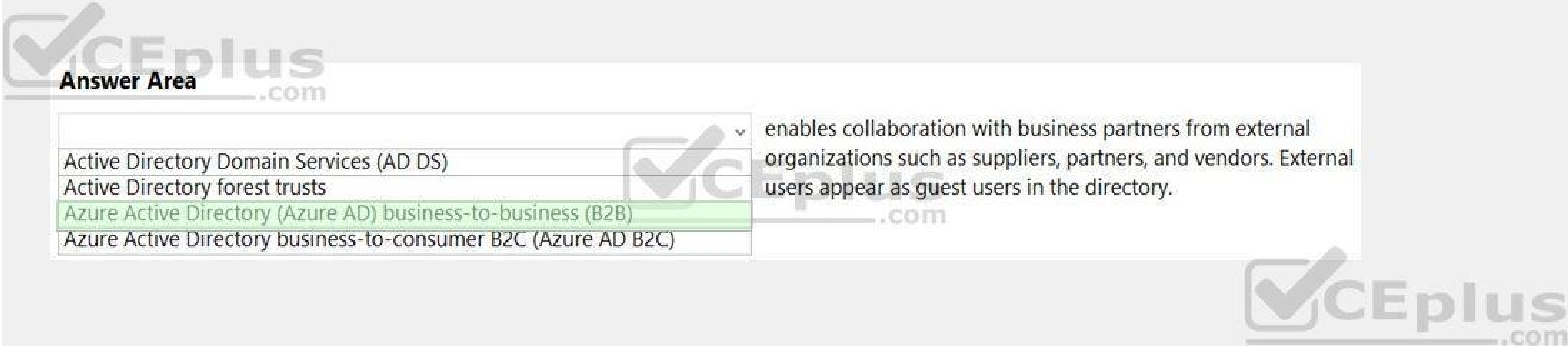


Answer Area

⌄ enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

- Active Directory Domain Services (AD DS)
- Active Directory forest trusts
- Azure Active Directory (Azure AD) business-to-business (B2B)
- Azure Active Directory business-to-consumer B2C (Azure AD B2C)

Answer Area:



Answer Area

[dropdown] enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

- Active Directory Domain Services (AD DS)
- Active Directory forest trusts
- [✓ Azure Active Directory (Azure AD) business-to-business (B2B)]
- Azure Active Directory business-to-consumer B2C (Azure AD B2C)

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

QUESTION 35

In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

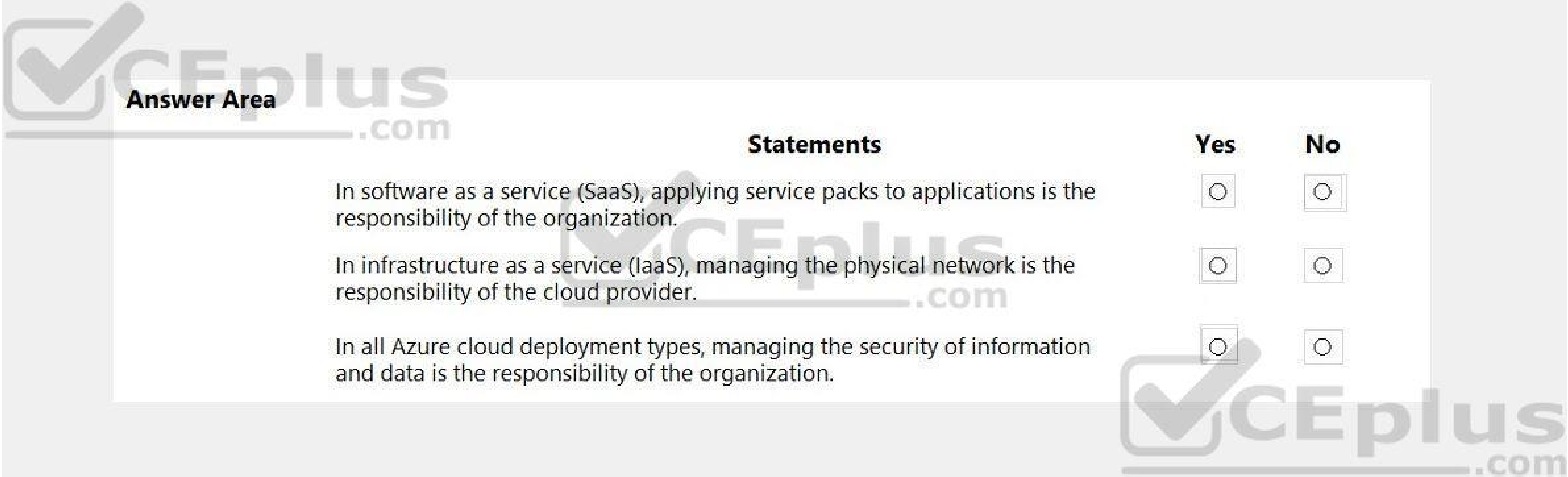
A. Plan
B. Manage
C. Adopt
D. Govern
E. Define Strategy

Correct Answer: A, E
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview

QUESTION 36

HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

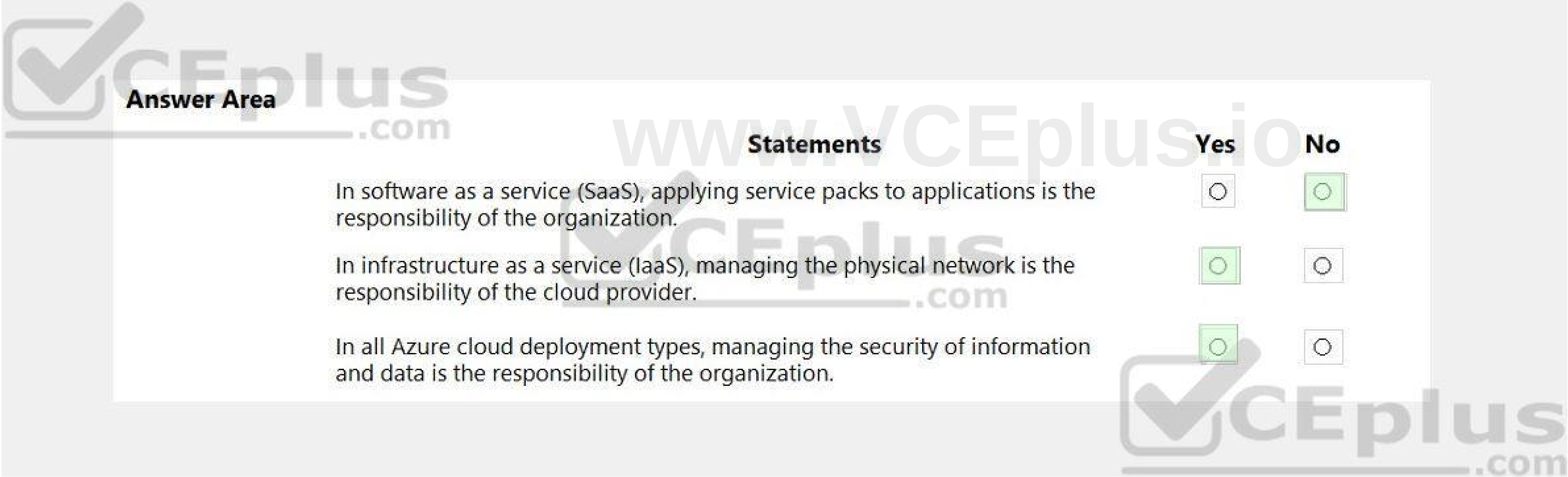
Hot Area:



Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	○	○
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	○	○
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	○	○

Answer Area:



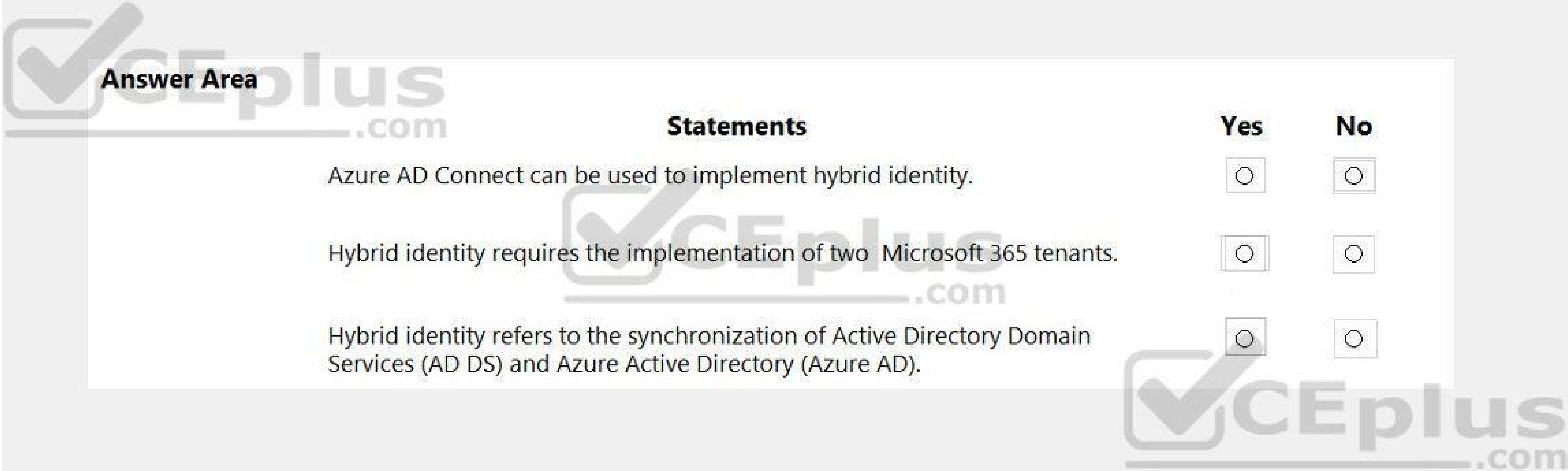
Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	○	[✓ ○]
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	[✓ ○]	○
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	[✓ ○]	○

Section:
Explanation:

QUESTION 37
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

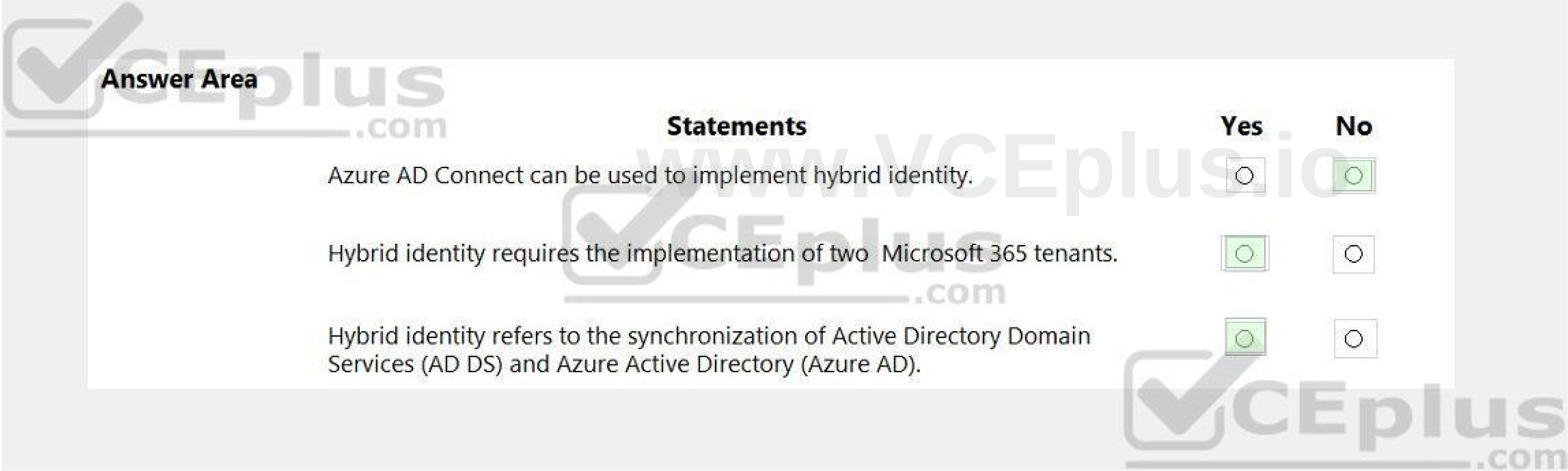
Hot Area:



Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	○	○
Hybrid identity requires the implementation of two Microsoft 365 tenants.	○	○
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	○	○

Answer Area:



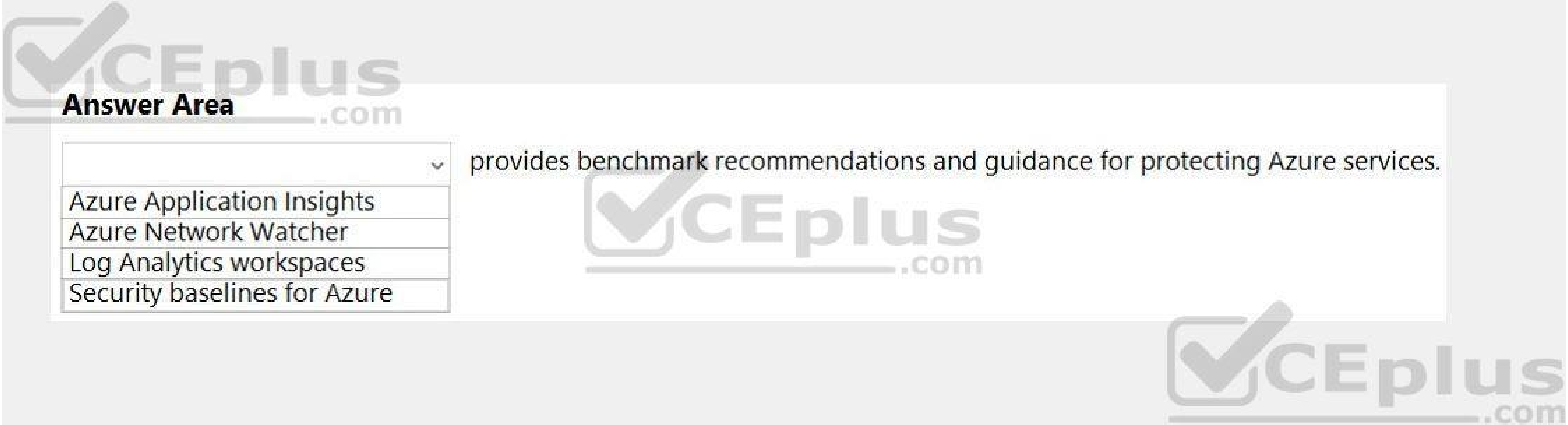
Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	○	[✓ ○]
Hybrid identity requires the implementation of two Microsoft 365 tenants.	[✓ ○]	○
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	[✓ ○]	○

Section:
Explanation:

QUESTION 38
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

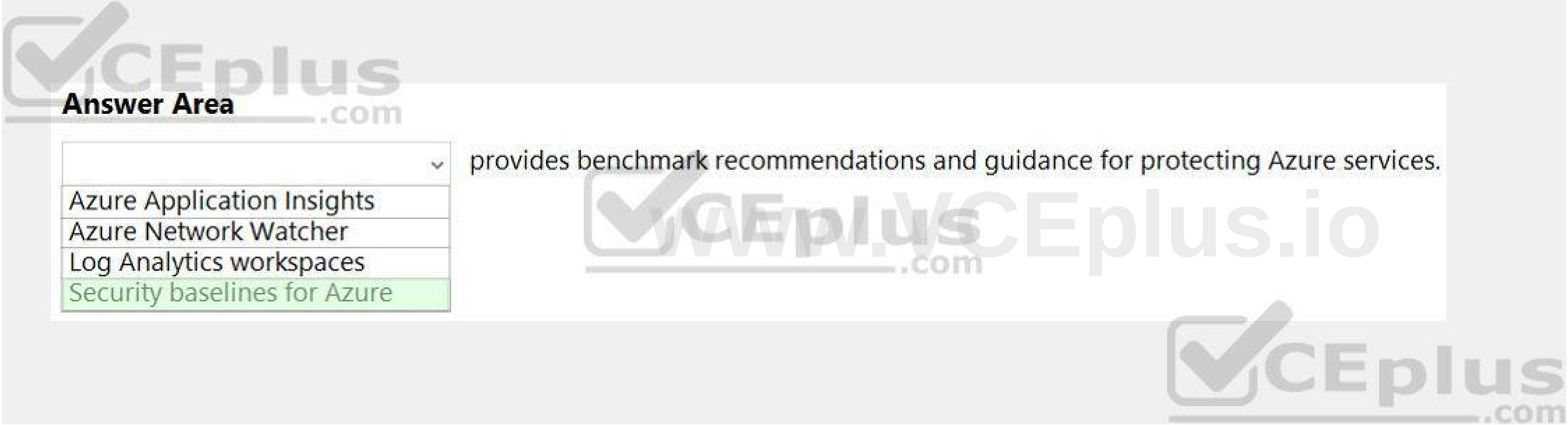


Answer Area

[ ] provides benchmark recommendations and guidance for protecting Azure services.

- Azure Application Insights
- Azure Network Watcher
- Log Analytics workspaces
- Security baselines for Azure

Answer Area:



Answer Area

[ ] provides benchmark recommendations and guidance for protecting Azure services.

- Azure Application Insights
- Azure Network Watcher
- Log Analytics workspaces
- Security baselines for Azure

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cloud-services-security-baseline

QUESTION 39
Which Microsoft 365 feature can you use to restrict users from sending email messages that contain lists of customers and their associated credit card numbers?

A. retention policies
B. data loss prevention (DLP) policies
C. conditional access policies
D. information barriers

Correct Answer: B
Section:
Explanation:

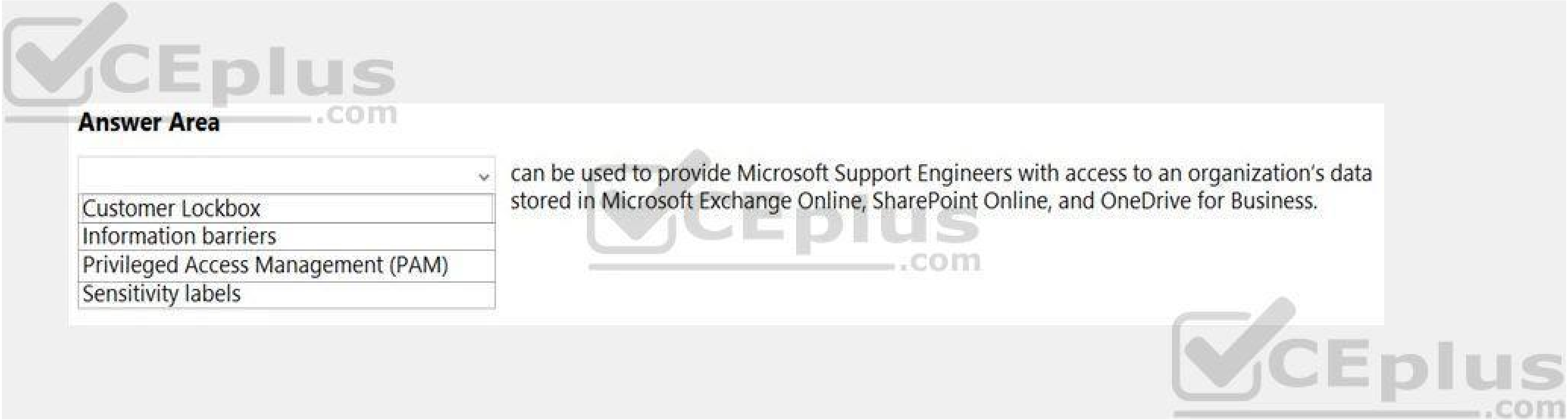
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

QUESTION 40

HOTSPOT

Select the answer that correctly completes the sentence.

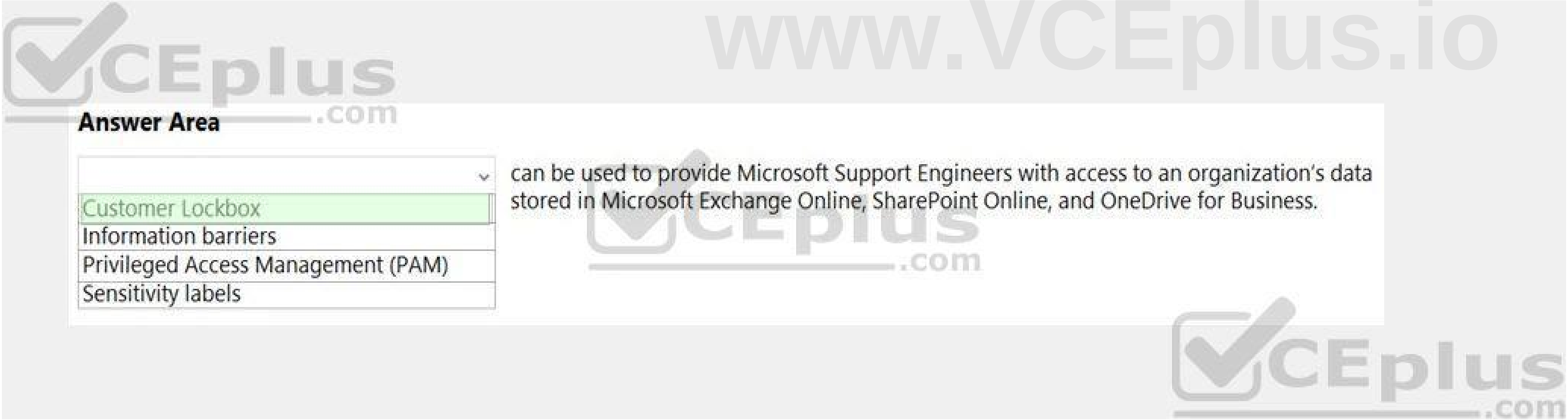
Hot Area:



Answer Area

Customer Lockbox Information barriers Privileged Access Management (PAM) Sensitivity labels	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Answer Area:



Answer Area

[✓ Customer Lockbox] Information barriers Privileged Access Management (PAM) Sensitivity labels	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Section:

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

QUESTION 41

In a Core eDiscovery workflow, what should you do before you can search for content?

A. Create an eDiscovery hold.

B. Run Express Analysis.

C. Configure attorney-client privilege detection.

D. Export and download results.

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide

QUESTION 42
Which Microsoft portal provides information about how Microsoft manages privacy, compliance, and security?

A. Microsoft Service Trust Portal
B. Compliance Manager
C. Microsoft 365 compliance center
D. Microsoft Support

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

QUESTION 43
What can you protect by using the information protection solution in the Microsoft 365 compliance center?

A. computers from zero-day exploits
B. users from phishing attempts
C. files from malware and viruses
D. sensitive data from being exposed to unauthorized users

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

QUESTION 44
What can you specify in Microsoft 365 sensitivity labels?

A. how long files must be preserved
B. when to archive an email message
C. which watermark to add to files
D. where to store files

Correct Answer: C
Section:
Explanation:
Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

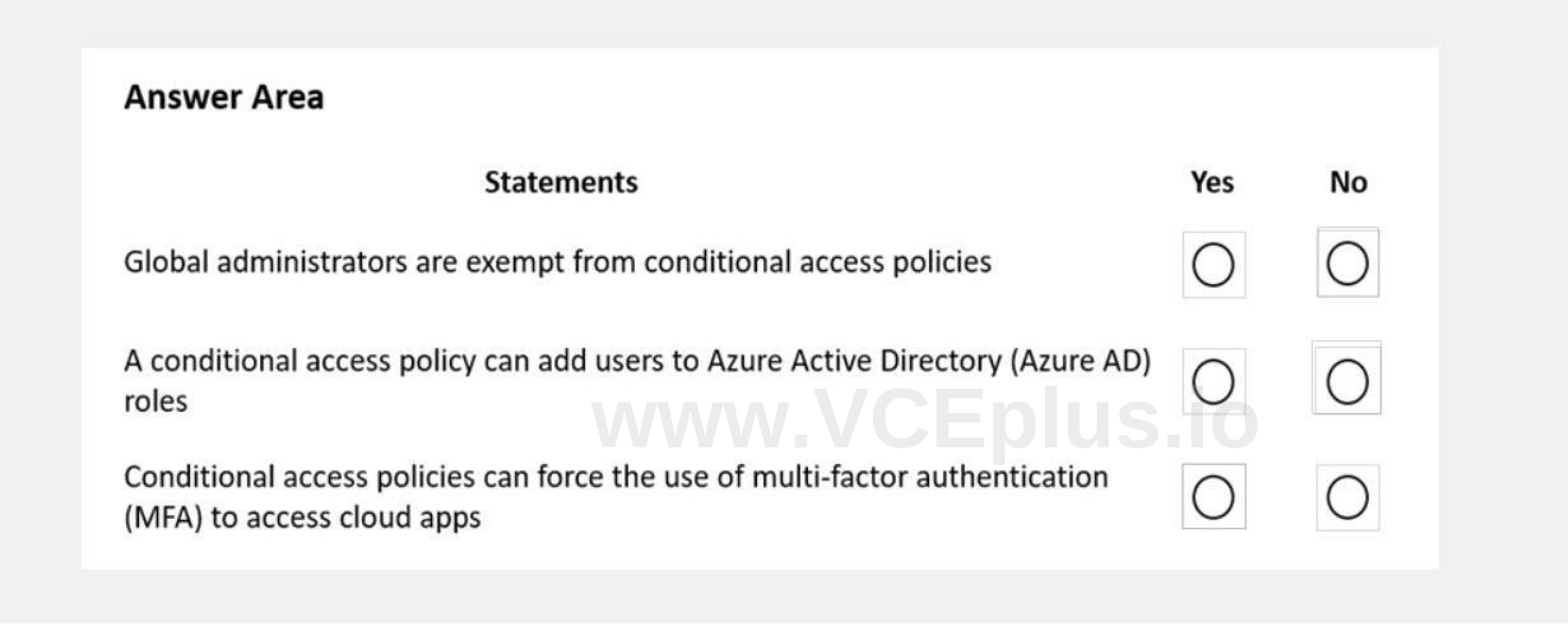
QUESTION 45

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

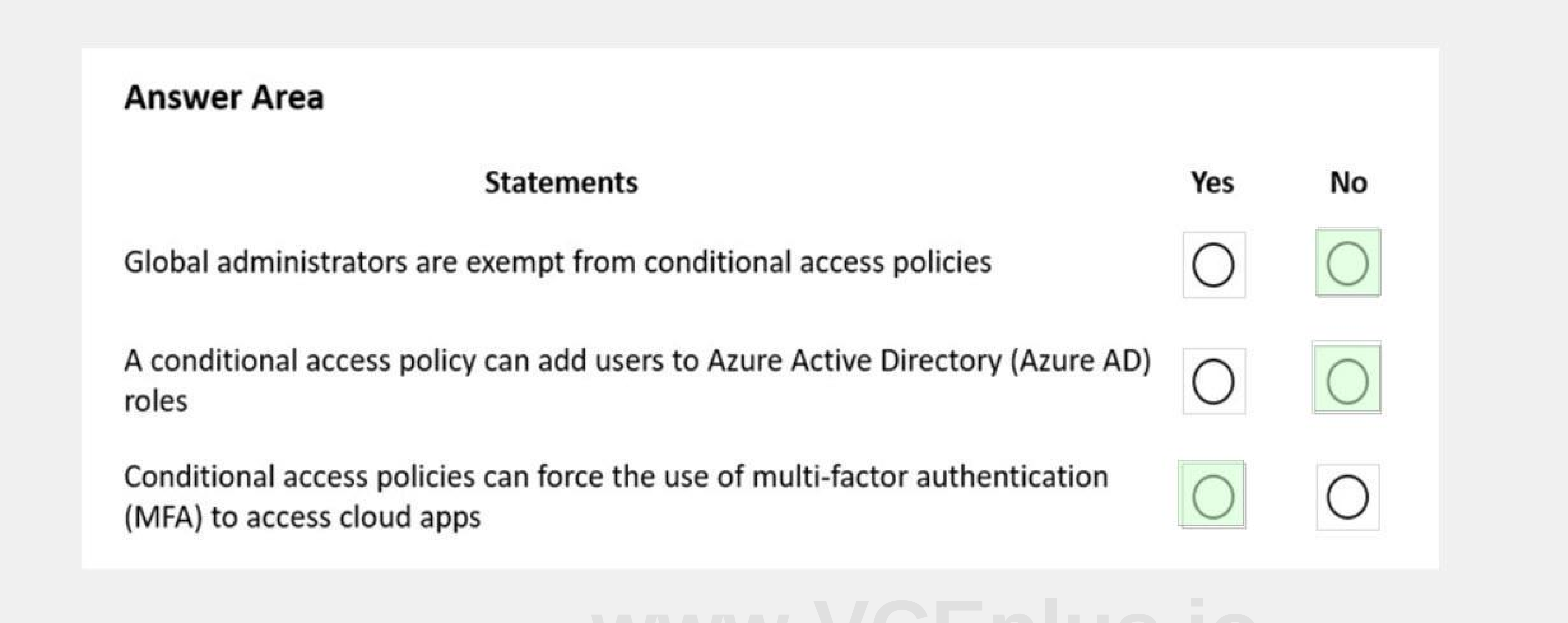
Hot Area:



Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	○
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	○
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	○	○

Answer Area:



Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	[✓ ○]
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	[✓ ○]
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	[✓ ○]	○

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa

QUESTION 46

When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. All users must authenticate from a registered device.
B. Administrators must always use Azure Multi-Factor Authentication (MFA).
C. Azure Multi-Factor Authentication (MFA) registration is required for all users.
D. All users must authenticate by using passwordless sign-in.
E. All users must authenticate by using Windows Hello.

Correct Answer: B, C
Section:
Explanation:
Security defaults make it easy to protect your organization with the following preconfigured security settings:
Requiring all users to register for Azure AD Multi-Factor Authentication.
Requiring administrators to do multi-factor authentication.
Blocking legacy authentication protocols.
Requiring users to do multi-factor authentication when necessary. Protecting privileged activities like access to the Azure portal.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

QUESTION 47
Which type of identity is created when you register an application with Active Directory (Azure AD)?

A. a user account
B. a user-assigned managed identity
C. a system-assigned managed identity
D. a service principal

Correct Answer: D
Section:
Explanation:
When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.
Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

QUESTION 48
Which three tasks can be performed by using Azure Active Directory (Azure AD) Identity Protection? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Configure external access for partner organizations.
B. Export risk detection to third-party utilities.
C. Automate the detection and remediation of identity based-risks.
D. Investigate risks that relate to user authentication.
E. Create and automatically assign sensitivity labels to data.

Correct Answer: B, C, D
Section:

QUESTION 49
You have a Microsoft 365 E3 subscription.
You plan to audit user activity by using the unified audit log and Basic Audit.
For how long will the audit records be retained?

A. 15 days
B. 30 days
C. 90 days
D. 180 days

Correct Answer: C
Section:

QUESTION 50
To which type of resource can Azure Bastion provide secure access?

A. Azure Files
B. Azure SQL Managed Instances

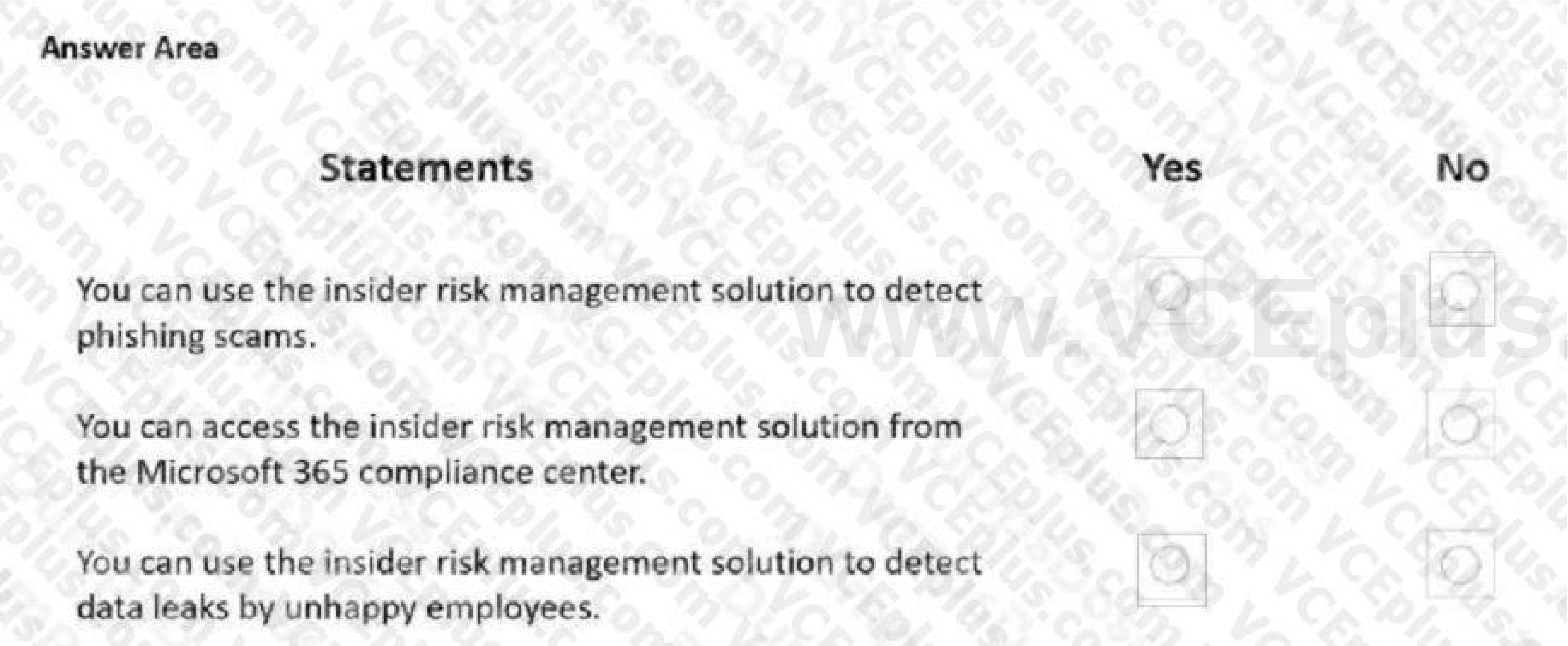
C. Azure virtual machines

D. Azure App Service

Correct Answer: C
Section:
Explanation:
Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.
Reference: https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

QUESTION 51
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

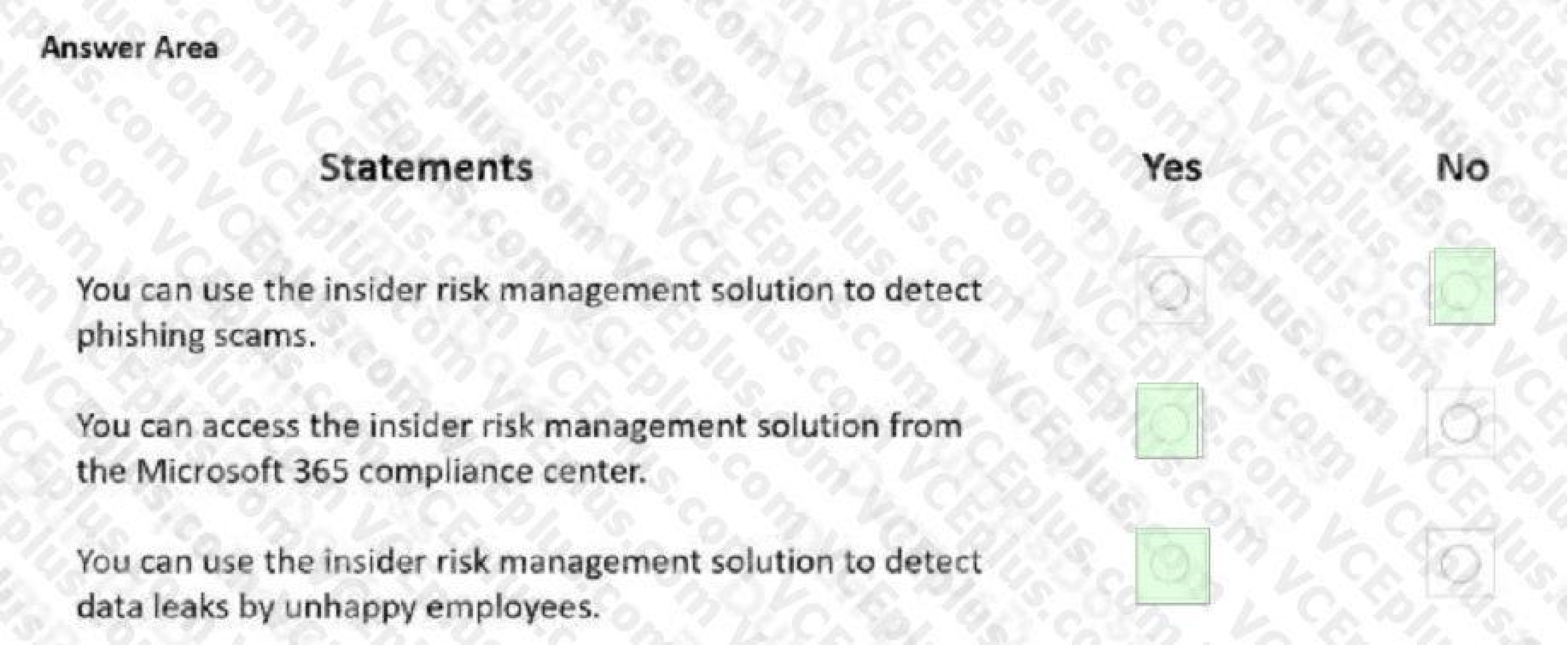
Hot Area:



Answer Area

Statements	Yes	No
You can use the insider risk management solution to detect phishing scams.	○	○
You can access the insider risk management solution from the Microsoft 365 compliance center.	○	○
You can use the insider risk management solution to detect data leaks by unhappy employees.	○	○

Answer Area:



Answer Area

Statements	Yes	No
You can use the insider risk management solution to detect phishing scams.	○	●
You can access the insider risk management solution from the Microsoft 365 compliance center.	●	○
You can use the insider risk management solution to detect data leaks by unhappy employees.	●	○

Section:
Explanation:
Box 1: Yes
Phishing scams are external threats.
Box 2: Yes
Insider risk management is a compliance solution in Microsoft 365.
Box 3: No
Insider risk management helps minimize internal risks from users. These include: Leaks of sensitive data and data spillage Confidentiality violations Intellectual property (IP) theft Fraud Insider trading Regulatory compliance violationsReference:https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365- worldwidehttps://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance- center?view=o365-worldwide

QUESTION 52
What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

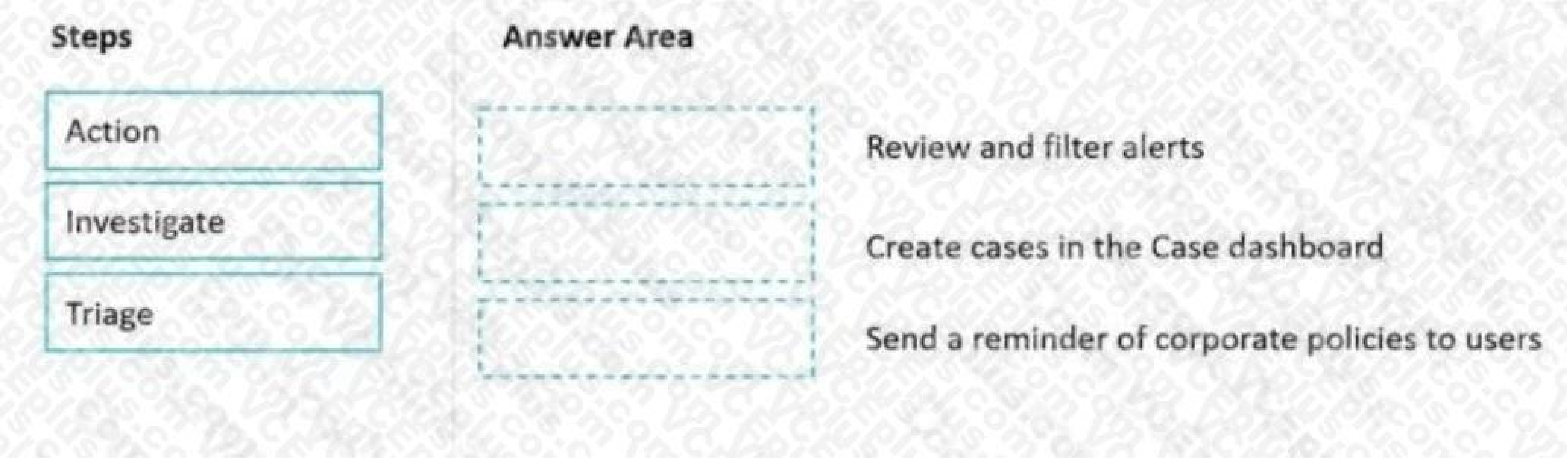
A. to discover and control the use of shadow IT
B. to provide secure connections to Azure virtual machines
C. to protect sensitive information hosted anywhere in the cloud
D. to provide pass-through authentication to on-premises applications
E. to prevent data leaks to noncompliant apps and limit access to regulated data

Correct Answer: A, C, E
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

QUESTION 53
DRAG DROP
Match the Microsoft 365 insider risk management workflow step to the appropriate task.
To answer, drag the appropriate step from the column on the left to its task on the right. Each step may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:



Steps

Action

Investigate

Triage

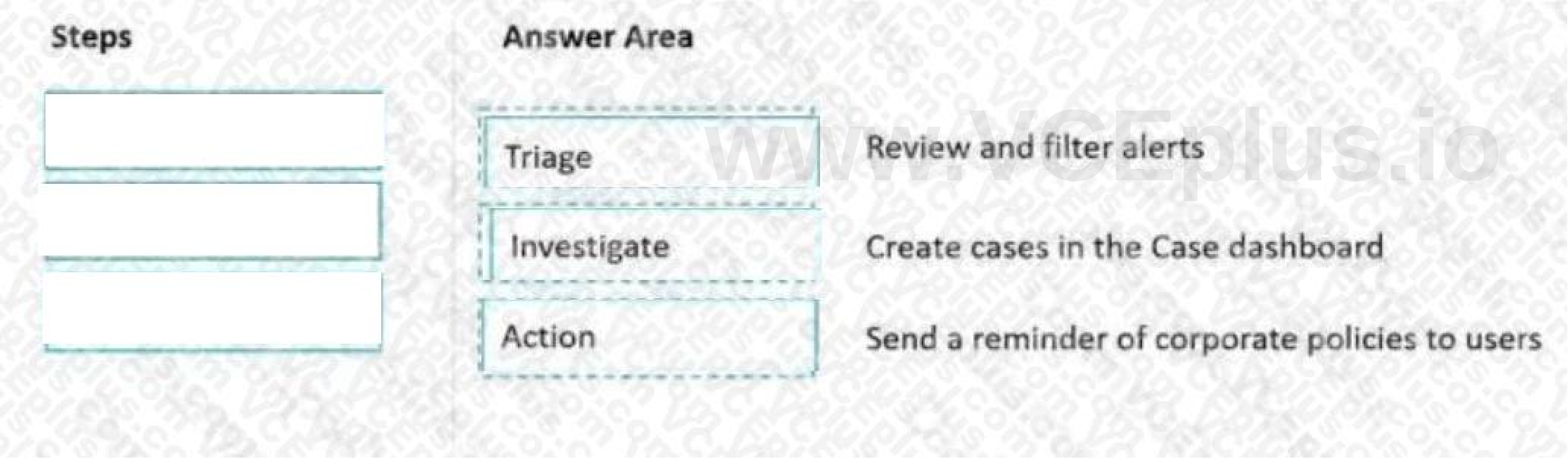
Answer Area

Review and filter alerts

Create cases in the Case dashboard

Send a reminder of corporate policies to users

Correct Answer:



Steps

Answer Area

Triage — Review and filter alerts

Investigate — Create cases in the Case dashboard

Action — Send a reminder of corporate policies to users

Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide

QUESTION 54
What can you use to view the Microsoft Secure Score for Devices?

A. Microsoft Defender for Cloud Apps
B. Microsoft Defender for Endpoint
C. Microsoft Defender for Identity
D. Microsoft Defender for Office 365

Correct Answer: B

Section:
Explanation:
Microsoft Secure Score for Devices
Artikel
12.05.2022
3 Minuten Lesedauer
Applies to:
Microsoft Defender for Endpoint Plan 2
Microsoft Defender Vulnerability Management
Microsoft 365 Defender
Some information relates to pre-released product which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here. To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com). Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on. Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.
Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. It reflects the collective security configuration state of your devices across the following categories:
Application
Operating system
Network
Accounts
Security controls
Select a category to go to the Security recommendations page and view the relevant recommendations. Turn on the Microsoft Secure Score connector
Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your Microsoft Secure Score data. Changes might take up to a few hours to reflect in the dashboard.
In the navigation pane, go to Settings > Endpoints > General > Advanced features Scroll down to Microsoft Secure Score and toggle the setting to On. Select Save preferences.
How it works
Microsoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured. Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management. The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:
Compare collected configurations to the collected benchmarks to discover misconfigured assets Map configurations to vulnerabilities that can be remediated or partially remediated (risk reduction) Collect and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams) Collect and monitor changes of security control configuration state from all assets

QUESTION 55
Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a network interface
B. an Azure App Service web app
C. a virtual network
D. a virtual network subnet
E. a resource group

Correct Answer: A, D
Section:
Explanation:

QUESTION 56
Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

A. Windows 10 and iOS only

B. Windows 10 and Android only
C. Windows 10, Android, and iOS
D. Windows 10 only

Correct Answer: A
Section:

QUESTION 57
Which two cards are available in the Microsoft 365 Defender portal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Users at risk
B. Compliance Score
C. Devices at risk
D. Service Health
E. User Management

Correct Answer: B, C
Section:

QUESTION 58
Which service includes the Attack simul-ation training feature?

A. Microsoft Defender for Cloud Apps
B. Microsoft Defender for Office 365
C. Microsoft Defender for Identity
D. Microsoft Defender for SQL

Correct Answer: B
Section:

QUESTION 59
You need to connect to an Azure virtual machine by using Azure Bastion. What should you use?

A. an SSH client
B. PowerShell remoting
C. the Azure portal
D. the Remote Desktop Connection client

Correct Answer: D
Section:

QUESTION 60
Which Microsoft Defender for Cloud metric displays the overall security health of an Azure subscription?

A. resource health
B. secure score
C. the status of recommendations

D. completed controls

Correct Answer: B
Section:

QUESTION 61
Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

A. Windows 10 and newer only
B. Windows 10 and newer and Android only
C. Windows 10 and newer and macOS only
D. Windows 10 and newer, Android, and macOS

Correct Answer: C
Section:

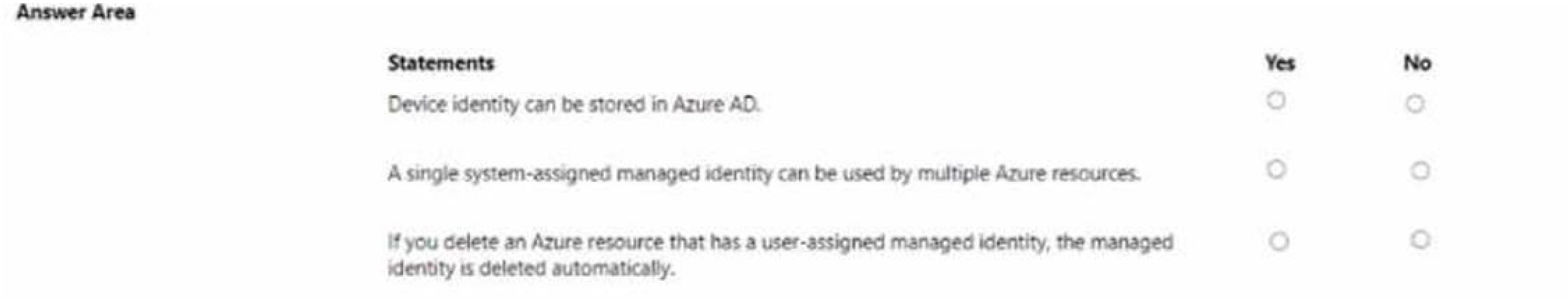
QUESTION 62
What is a function of Conditional Access session controls?

A. prompting multi-factor authentication (MFA)
B. enable limited experiences, such as blocking download of sensitive information
C. enforcing device compliance
D. enforcing client app compliance

Correct Answer: A
Section:
Explanation:

QUESTION 63
HOTSPOT
For each of the following statements, select Yes if the statement is true Otherwise, select No.
NOTE Each correct selection is worth one point.

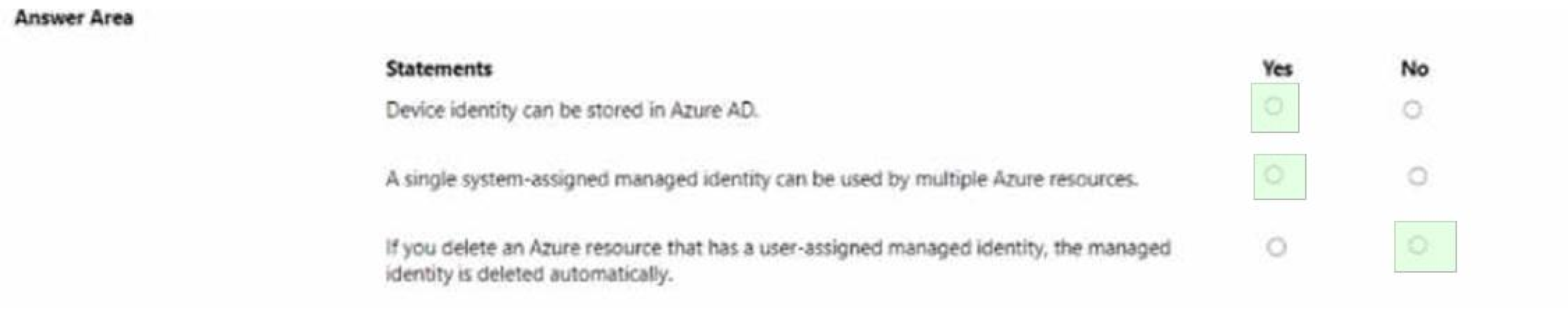
Hot Area:



Answer Area

Statements	Yes	No
Device identity can be stored in Azure AD.	○	○
A single system-assigned managed identity can be used by multiple Azure resources.	○	○
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	○	○

Answer Area:



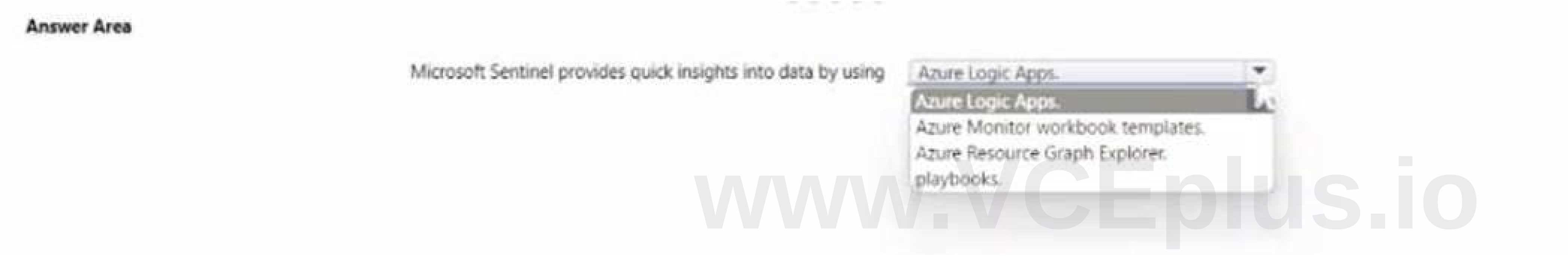
Answer Area

Statements	Yes	No
Device identity can be stored in Azure AD.	[✓ ○]	○
A single system-assigned managed identity can be used by multiple Azure resources.	[✓ ○]	○
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	○	[✓ ○]

Section:
Explanation:

QUESTION 64
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

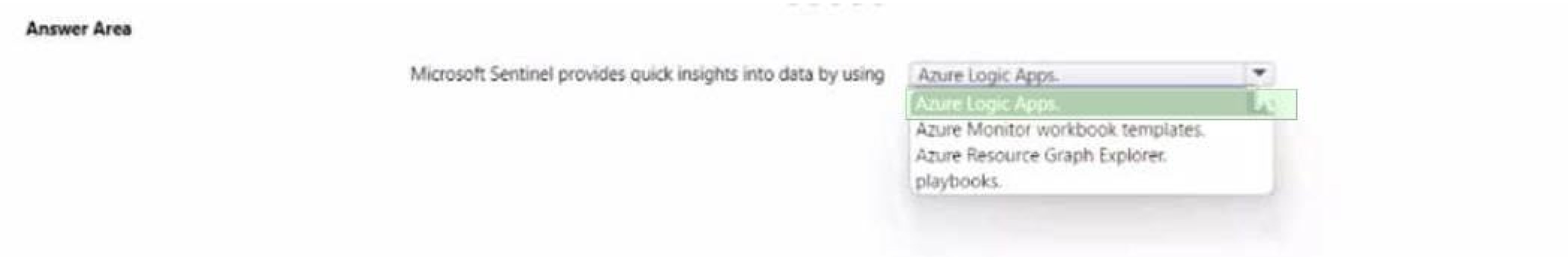


Answer Area

Microsoft Sentinel provides quick insights into data by using Azure Logic Apps. ▾

Azure Logic Apps.
Azure Monitor workbook templates.
Azure Resource Graph Explorer.
playbooks.

Answer Area:



Answer Area

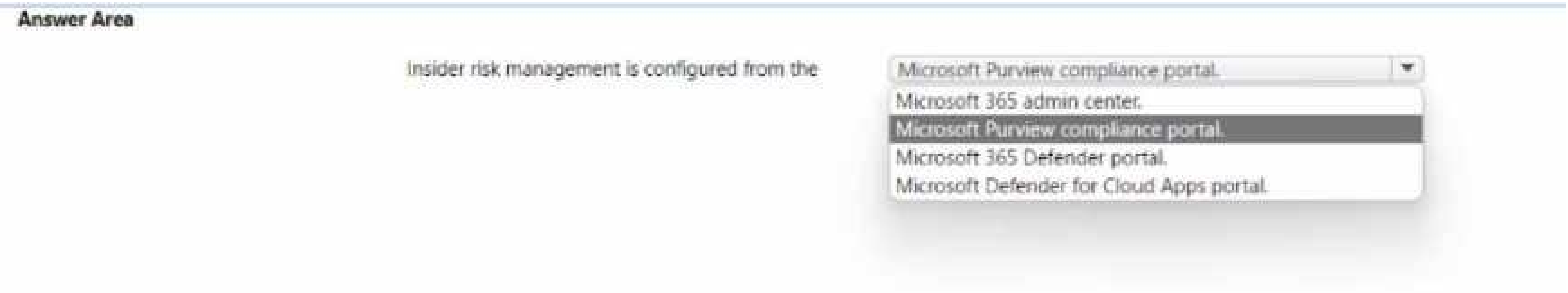
Microsoft Sentinel provides quick insights into data by using Azure Logic Apps. ▾

[✓ Azure Logic Apps.]
Azure Monitor workbook templates.
Azure Resource Graph Explorer.
playbooks.

Section:
Explanation:

QUESTION 65
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

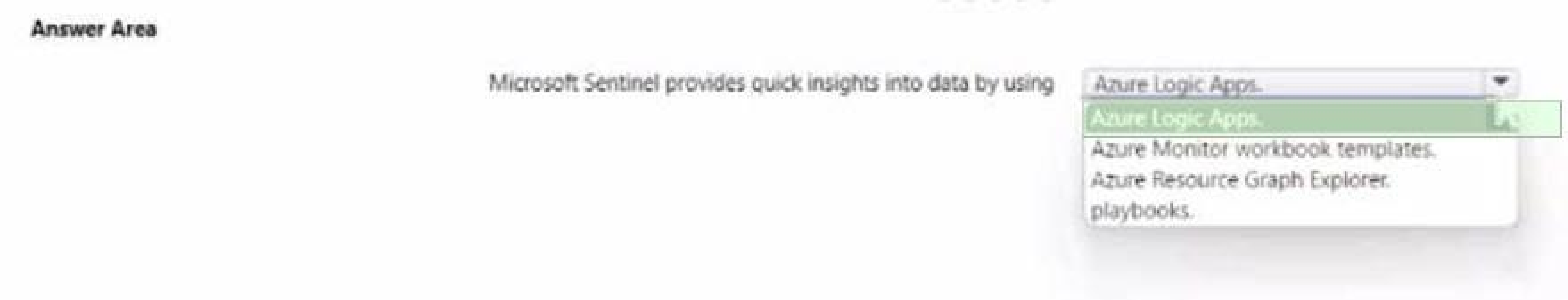


Answer Area

Insider risk management is configured from the Microsoft Purview compliance portal.

Microsoft 365 admin center.
Microsoft Purview compliance portal.
Microsoft 365 Defender portal.
Microsoft Defender for Cloud Apps portal.

Answer Area:



Answer Area

Microsoft Sentinel provides quick insights into data by using Azure Logic Apps.

Azure Logic Apps.
Azure Monitor workbook templates.
Azure Resource Graph Explorer.
playbooks.

Section:
Explanation:

QUESTION 66
What are two reasons to deploy multiple virtual networks instead of using just one virtual network?
Each correct answer presents a complete solution.
NOTE; Each correct selection is worth one point.

A. to separate the resources for budgeting
B. to meet Governance policies
C. to isolate the resources
D. to connect multiple types of resources

Correct Answer: B, C
Section:

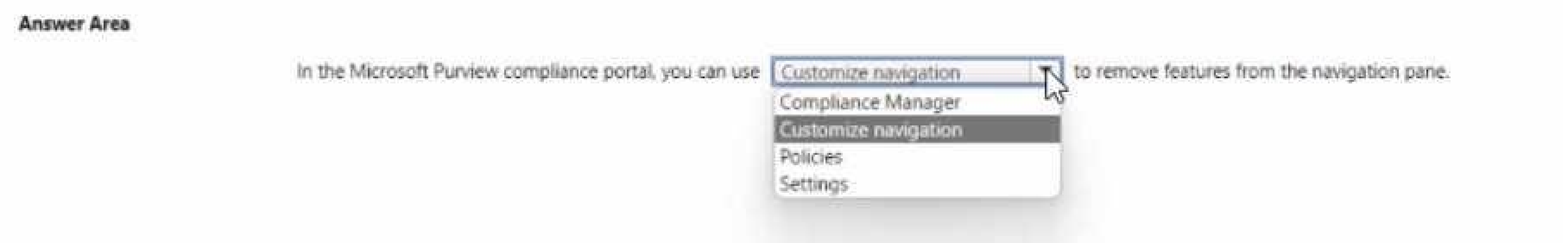
QUESTION 67
What can be created in Active Directory Domain Services (AD DS)?

A. line-of-business (106) applications that require modem authentication
B. mob devices
C. computer accounts
D. software as a service (SaaS) applications that require modem authentication

Correct Answer: D
Section:

QUESTION 68
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

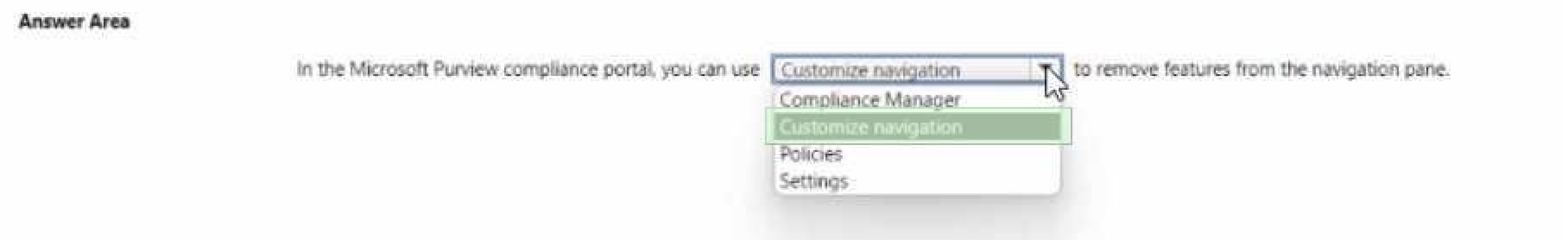


Answer Area

In the Microsoft Purview compliance portal, you can use [Customize navigation ▼] to remove features from the navigation pane.

- Compliance Manager
- Customize navigation
- Policies
- Settings

Answer Area:



Answer Area

In the Microsoft Purview compliance portal, you can use [Customize navigation ▼] to remove features from the navigation pane.

- Compliance Manager
- Customize navigation
- Policies
- Settings

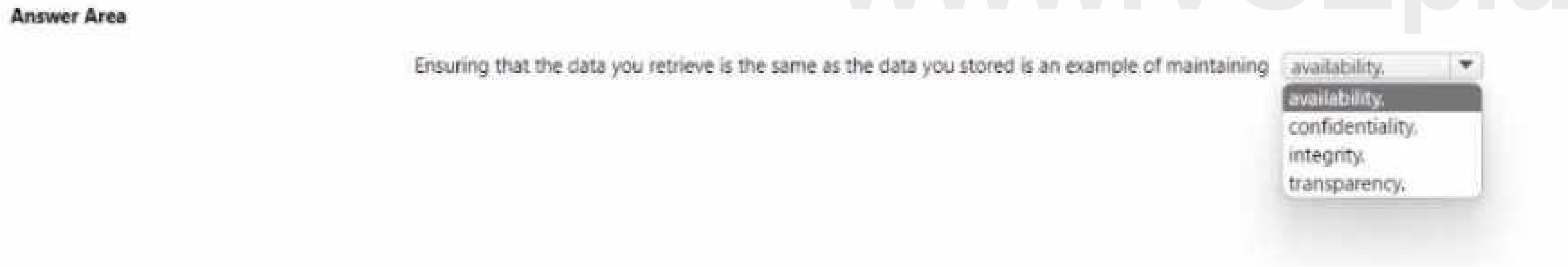
Section:
Explanation:

QUESTION 69

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

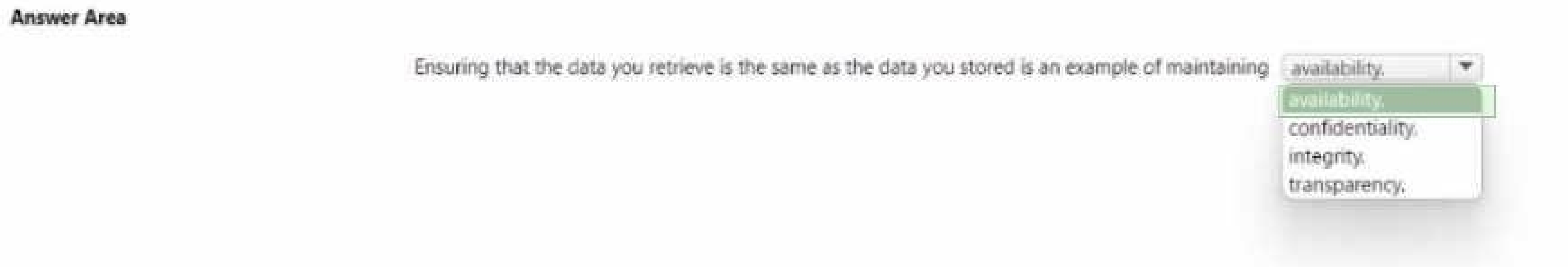


Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining [availability. ▼]

- availability.
- confidentiality.
- integrity.
- transparency.

Answer Area:



Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining [availability. ▼]

- availability.
- confidentiality.
- integrity.
- transparency.

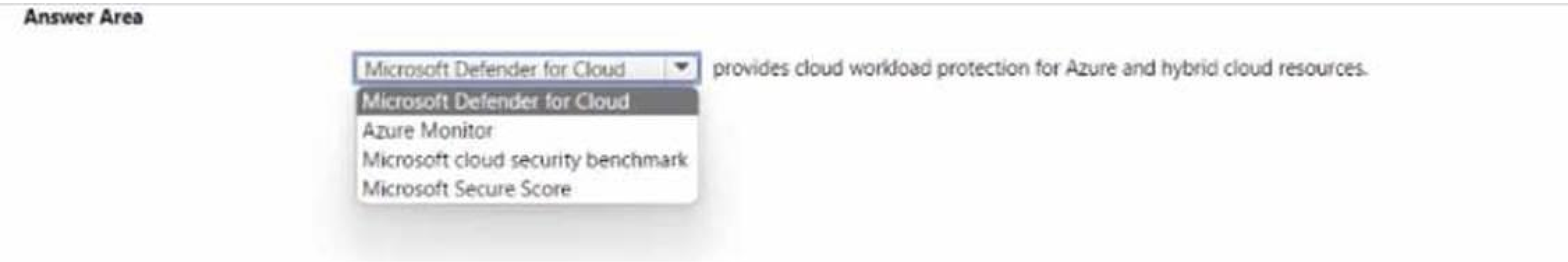
Section:
Explanation:

QUESTION 70

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

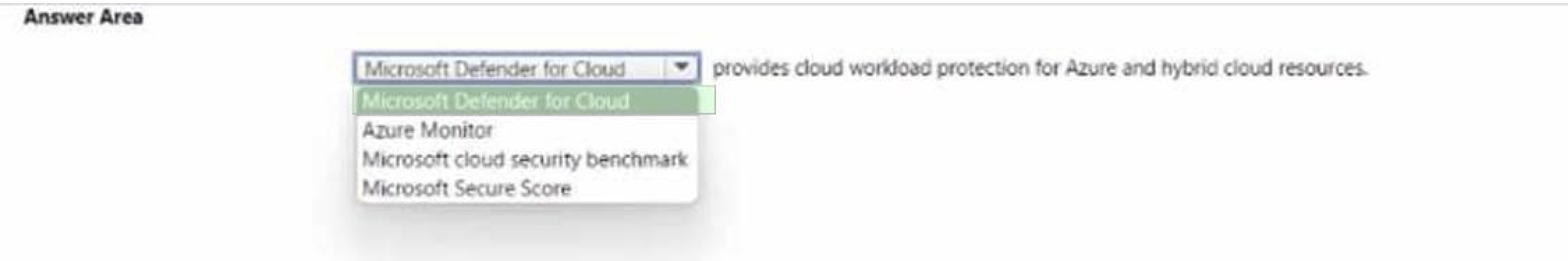


Answer Area

Microsoft Defender for Cloud ▾ provides cloud workload protection for Azure and hybrid cloud resources.

- Microsoft Defender for Cloud
- Azure Monitor
- Microsoft cloud security benchmark
- Microsoft Secure Score

Answer Area:



Answer Area

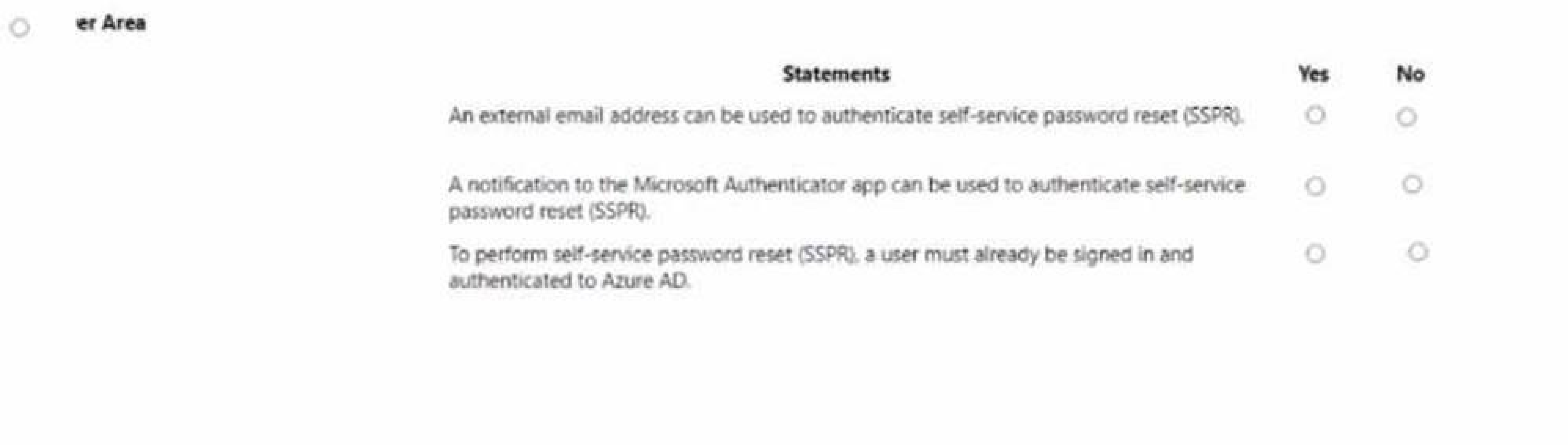
Microsoft Defender for Cloud ▾ provides cloud workload protection for Azure and hybrid cloud resources.

- [✓ Microsoft Defender for Cloud]
- Azure Monitor
- Microsoft cloud security benchmark
- Microsoft Secure Score

Section:
Explanation:

QUESTION 71
HOTSPOT
For each of the following statement, select Yes if the statement is true Otherwise, select No.
NOTE: Each connect selection a worth one point.

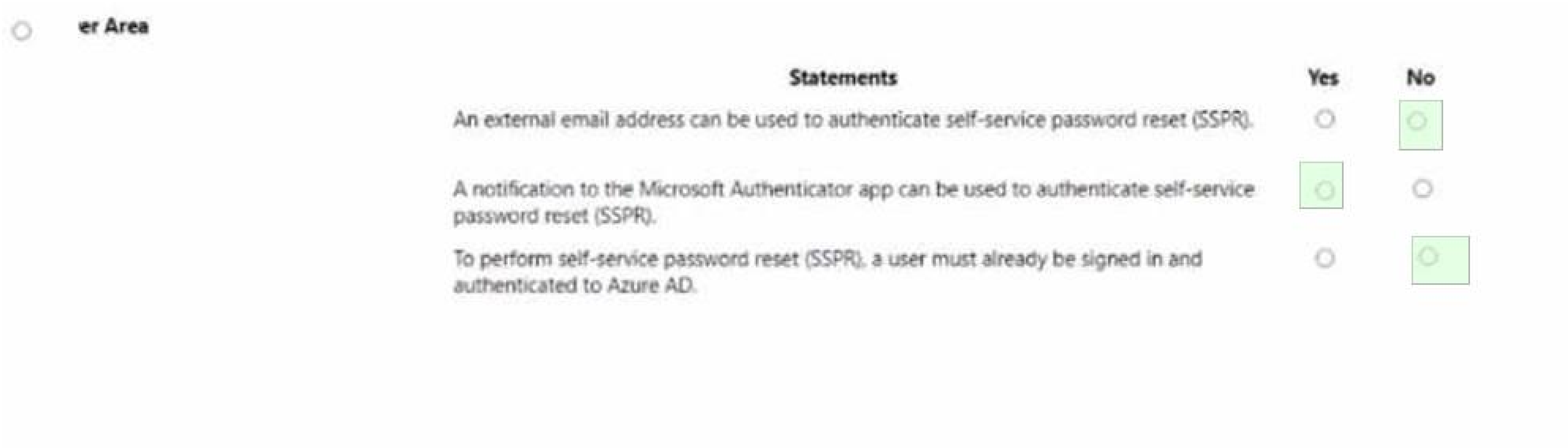
Hot Area:



○ er Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	○	○
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	○	○
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	○	○

Answer Area:



er Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	○	[✓ ○]
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	[✓ ○]	○
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	○	[✓ ○]

Section:
Explanation:

QUESTION 72
Which pillar of identity relates to tracking the resources accessed by a user?

A. auditing
B. authorization
C. authentication
D. administration

Correct Answer: A
Section:

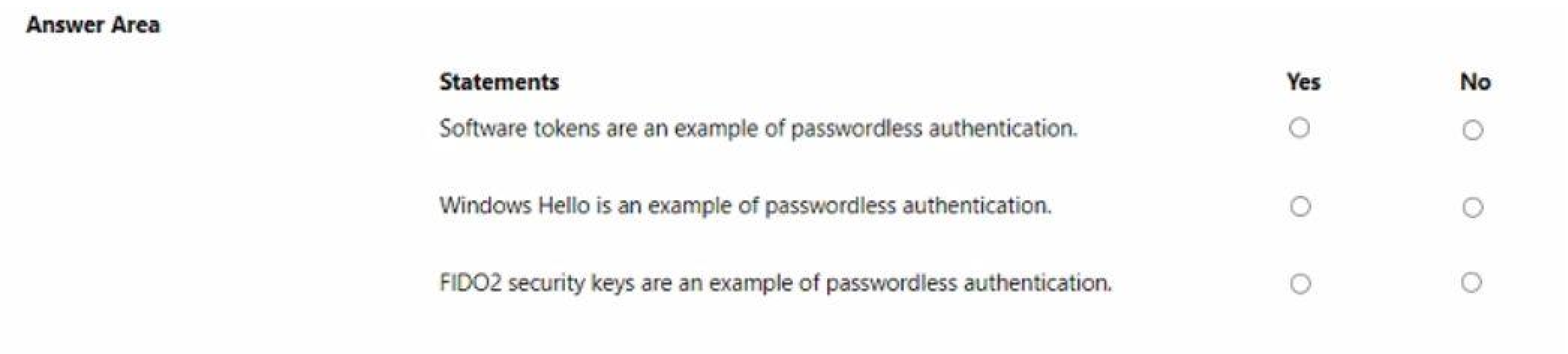
QUESTION 73
Which security feature is available in the free mode of Microsoft Defender for Cloud?

A. vulnerability scanning of virtual machines
B. secure score
C. just-in-time (JIT) VM access to Azure virtual machines
D. threat protection alerts

Correct Answer: C
Section:

QUESTION 74
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

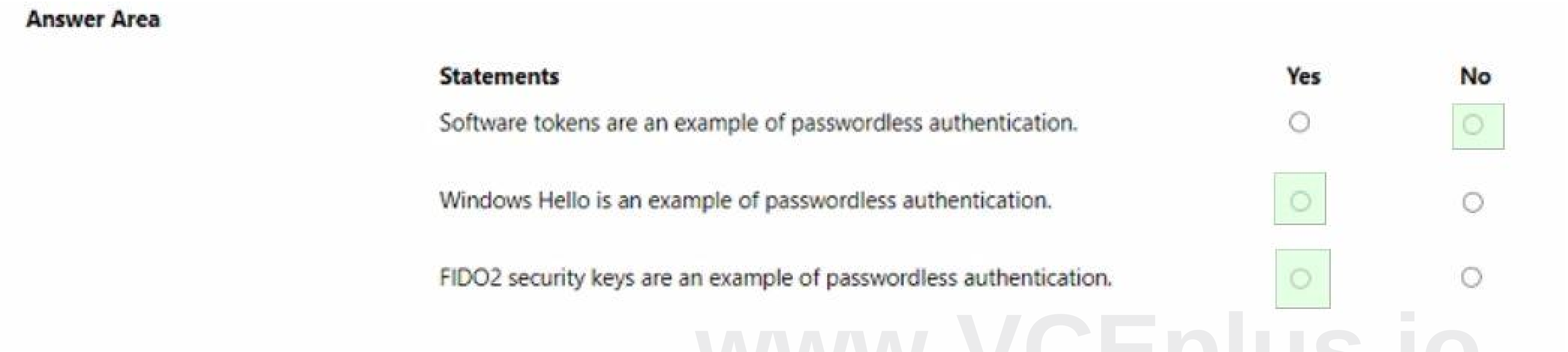
Hot Area:



Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication.	○	○
Windows Hello is an example of passwordless authentication.	○	○
FIDO2 security keys are an example of passwordless authentication.	○	○

Answer Area:



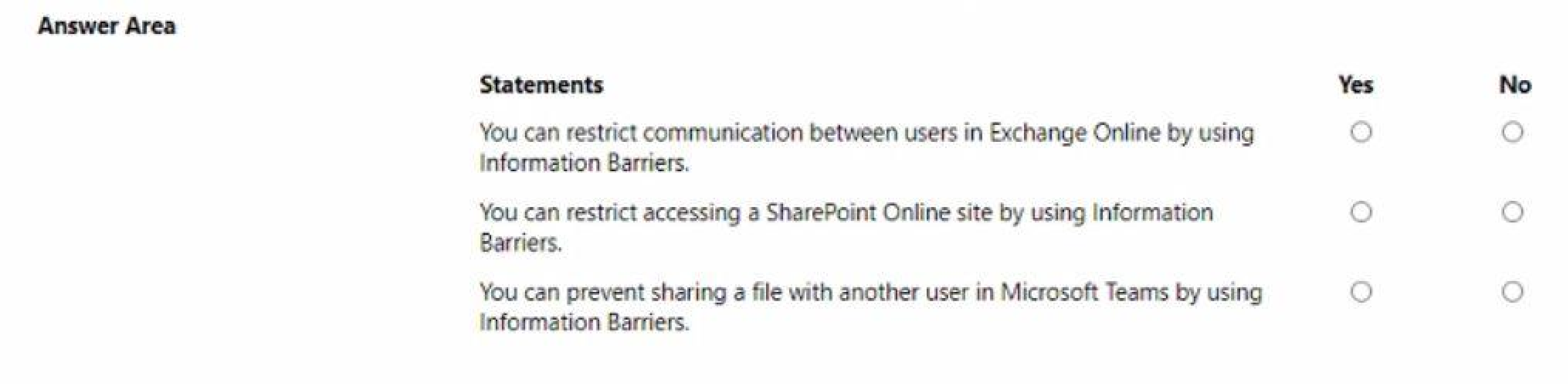
Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication.	○	[✓ ○]
Windows Hello is an example of passwordless authentication.	[✓ ○]	○
FIDO2 security keys are an example of passwordless authentication.	[✓ ○]	○

Section:
Explanation:

QUESTION 75
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

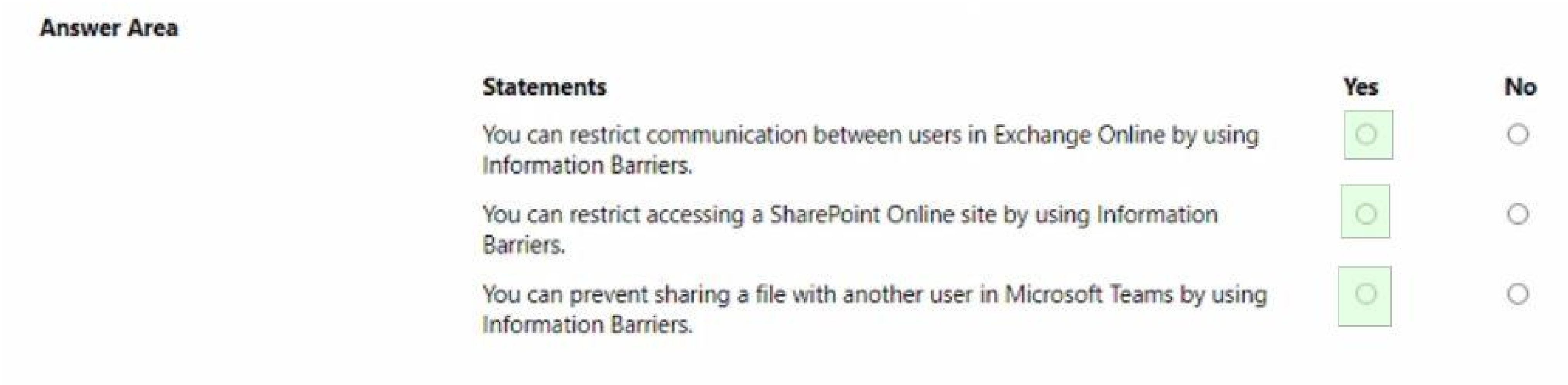
Hot Area:



Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	○	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	○	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	○	○

Answer Area:



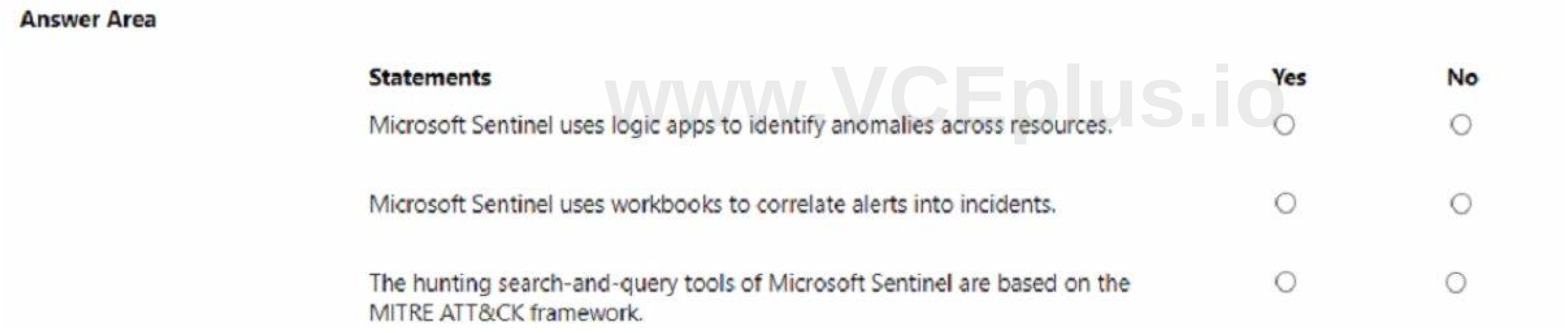
Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	[✓ ○]	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	[✓ ○]	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	[✓ ○]	○

Section:
Explanation:

QUESTION 76
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

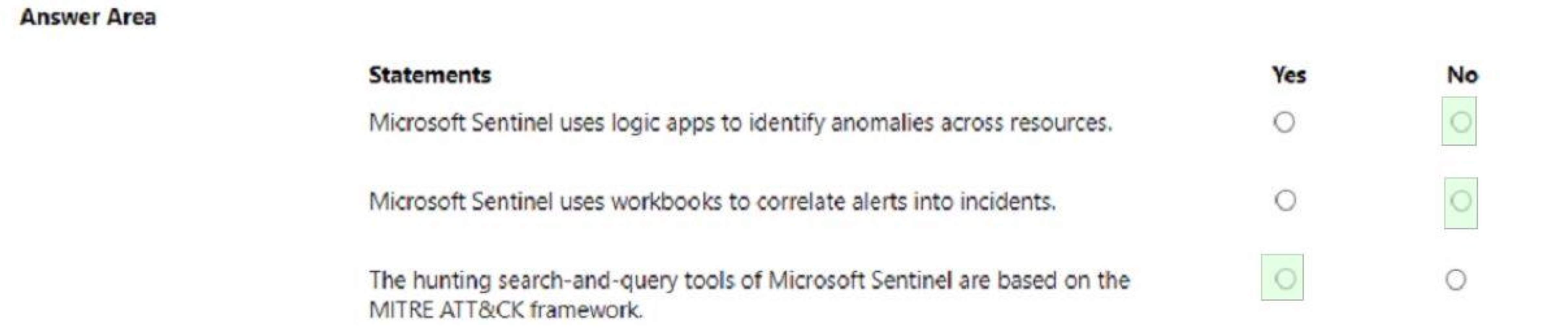
Hot Area:



Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	○	○
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	○	○
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	○	[✓ ○]
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	○	[✓ ○]
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	[✓ ○]	○

Section:

Explanation:

QUESTION 77

What is a characteristic of a sensitivity label in Microsoft 365?

A. persistent

B. encrypted

C. restricted to predefined categories

Correct Answer: B

Section:

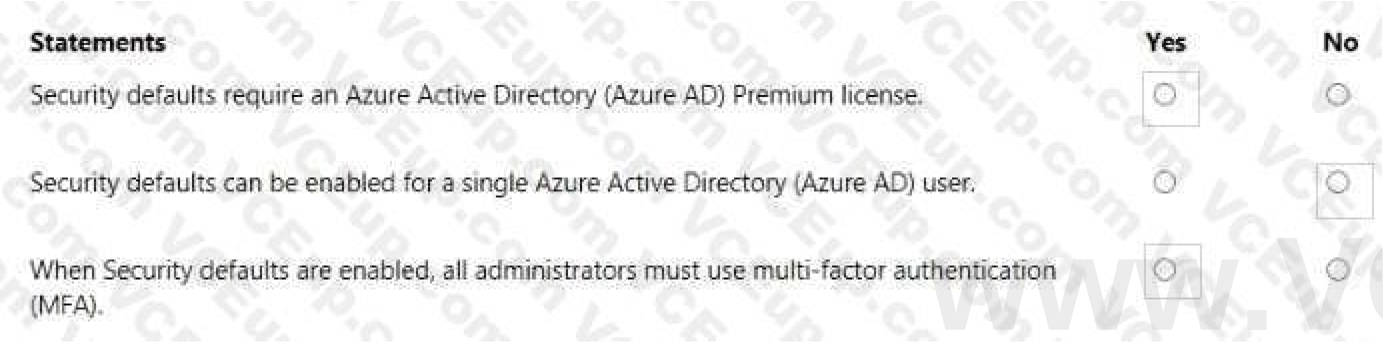
QUESTION 78

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

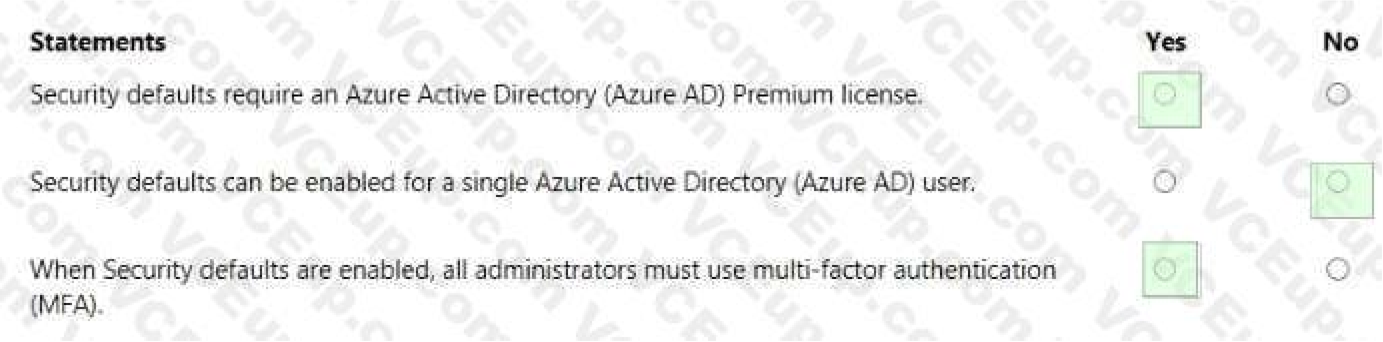
NOTE: Each correct selection is worth one point

Hot Area:



Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	○	○
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	○	○
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	○	○

Answer Area:



Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	[✓ ○]	○
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	○	[✓ ○]
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	[✓ ○]	○

Section:

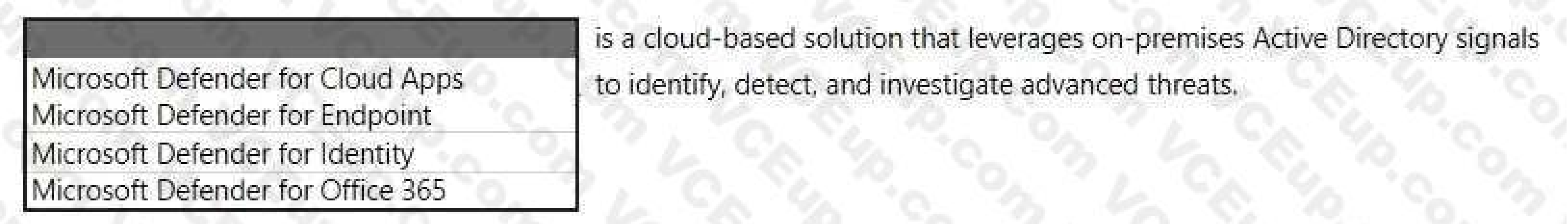
Explanation:

QUESTION 79

HOTSPOT

Select the answer that correctly completes the sentence.

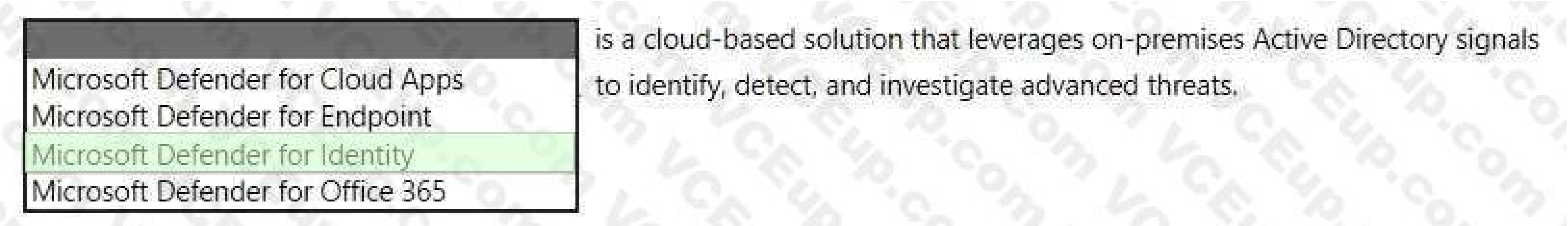
Hot Area:



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

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Answer Area:



- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- [✓ Microsoft Defender for Identity]
- Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Section:

Explanation:

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

QUESTION 80

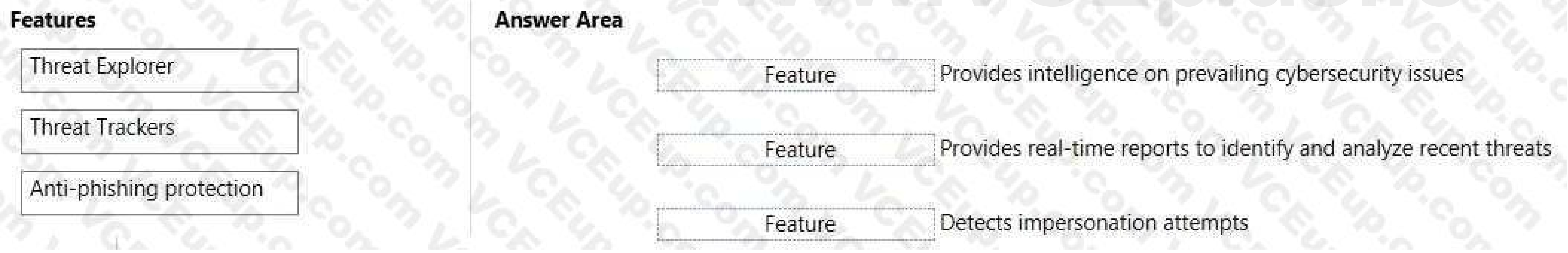
DRAG DROP

Match the Microsoft Defender for Office 365 feature to the correct description.

To answer, drag the appropriate feature from the column on the left to its description on the right. Each feature may be used once, more than once, or not at all.

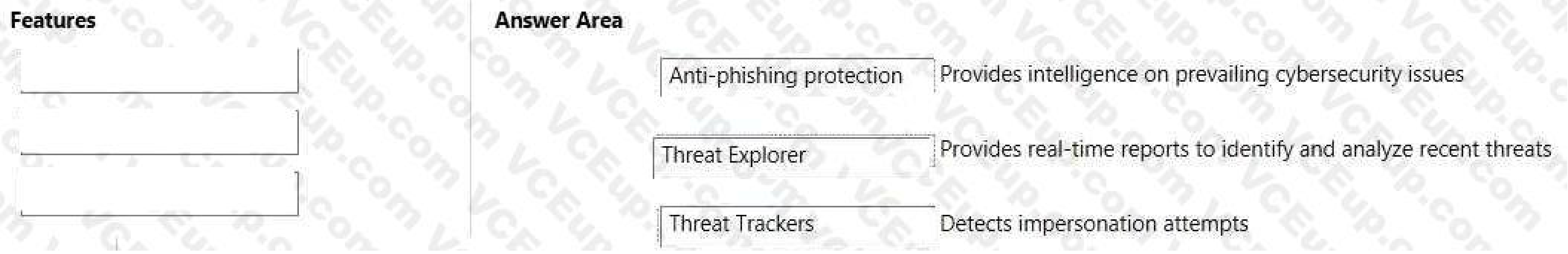
NOTE: Each correct match is worth one point.

Select and Place:



Features	Answer Area	
Threat Explorer	Feature	Provides intelligence on prevailing cybersecurity issues
Threat Trackers	Feature	Provides real-time reports to identify and analyze recent threats
Anti-phishing protection	Feature	Detects impersonation attempts

Correct Answer:



Features	Answer Area	
	Anti-phishing protection	Provides intelligence on prevailing cybersecurity issues
	Threat Explorer	Provides real-time reports to identify and analyze recent threats
	Threat Trackers	Detects impersonation attempts

Section:

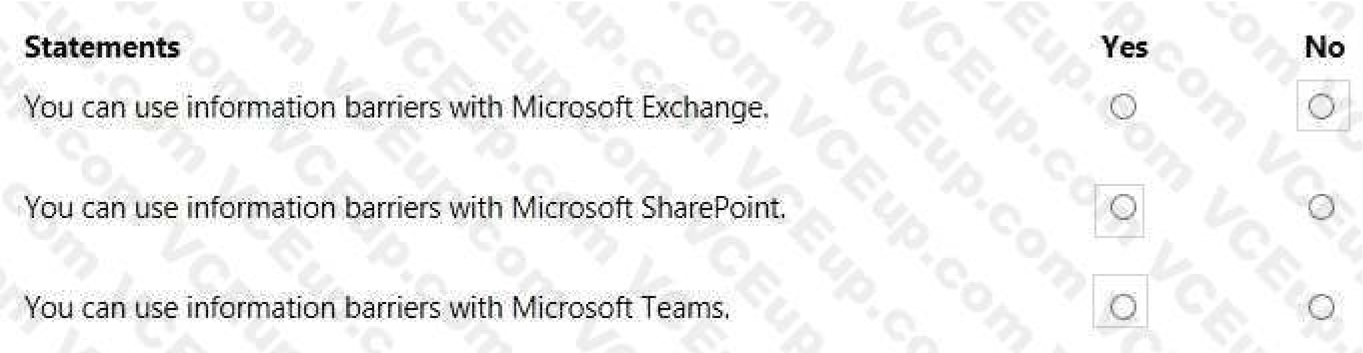
Explanation:

QUESTION 81

HOTSPOT

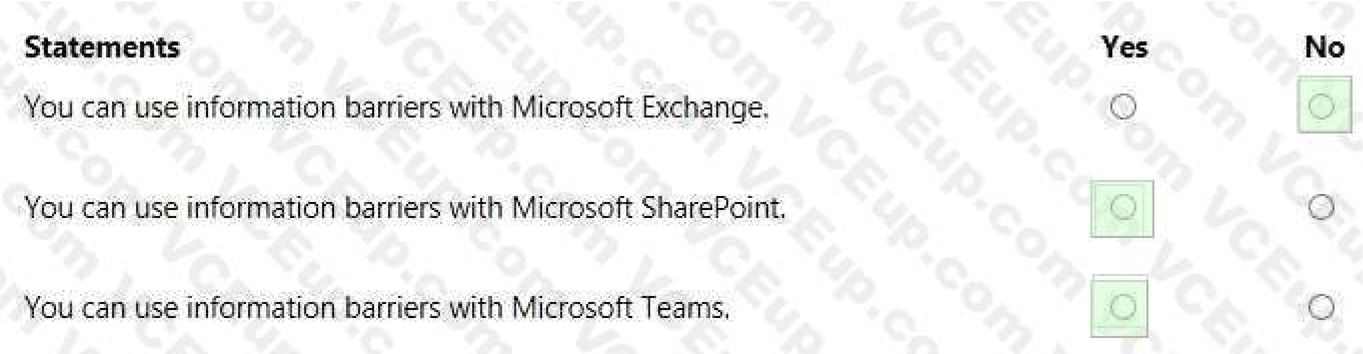
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
You can use information barriers with Microsoft Exchange.	○	○
You can use information barriers with Microsoft SharePoint.	○	○
You can use information barriers with Microsoft Teams.	○	○

Answer Area:

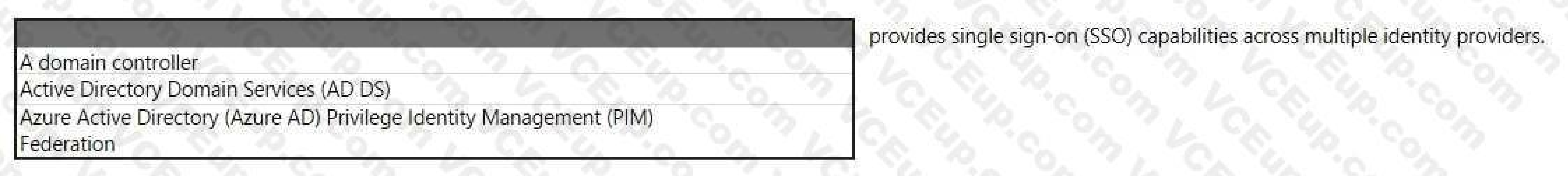


Statements	Yes	No
You can use information barriers with Microsoft Exchange.	○	[✓ ○]
You can use information barriers with Microsoft SharePoint.	[✓ ○]	○
You can use information barriers with Microsoft Teams.	[✓ ○]	○

Section:
Explanation:

QUESTION 82
HOTSPOT
Select the answer that correctly completes the sentence.

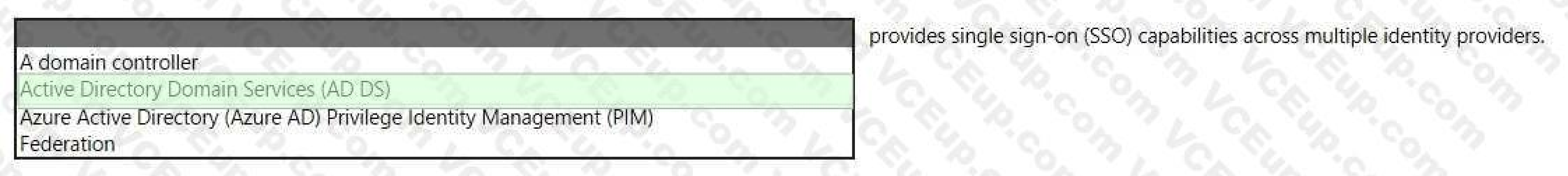
Hot Area:



- A domain controller
- Active Directory Domain Services (AD DS)
- Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
- Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

Answer Area:



- A domain controller
- [✓ Active Directory Domain Services (AD DS)]
- Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
- Federation

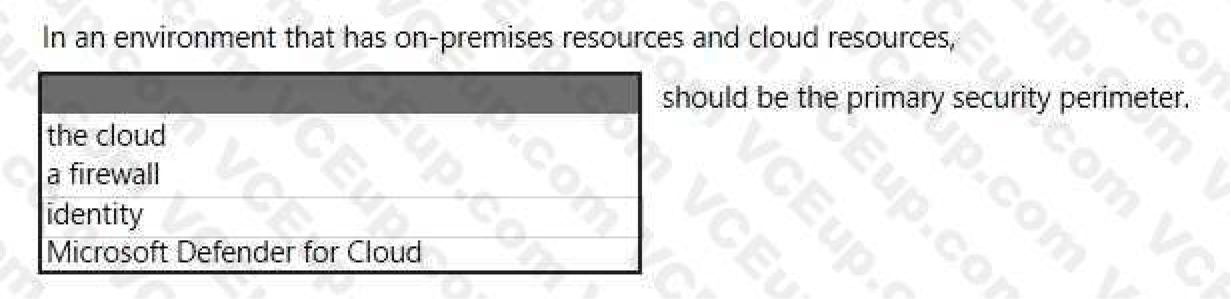
provides single sign-on (SSO) capabilities across multiple identity providers.

Section:
Explanation:

QUESTION 83
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

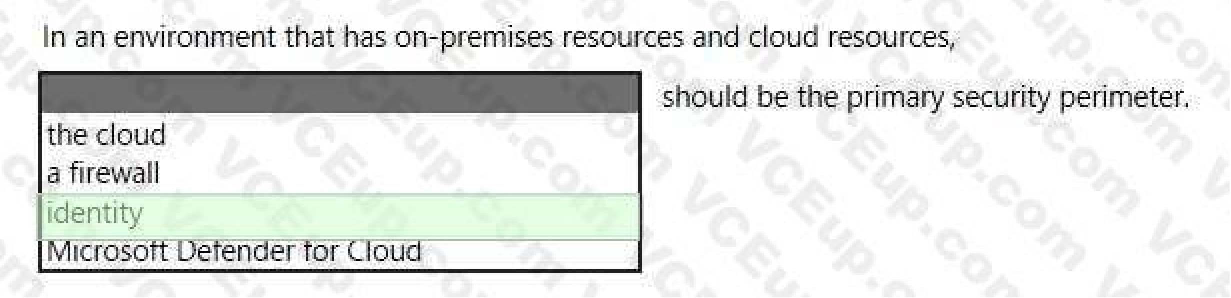


In an environment that has on-premises resources and cloud resources,

should be the primary security perimeter.

the cloud
a firewall
identity
Microsoft Defender for Cloud

Answer Area:



In an environment that has on-premises resources and cloud resources,

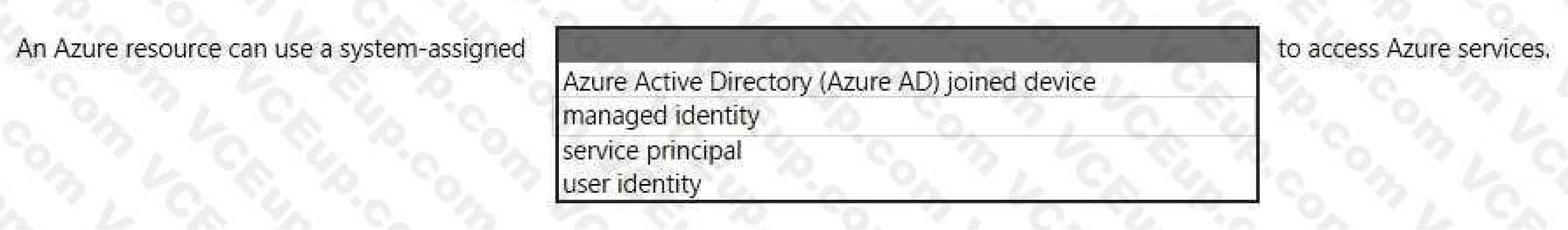
should be the primary security perimeter.

the cloud
a firewall
[✓ identity]
Microsoft Defender for Cloud

Section:
Explanation:

QUESTION 84
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

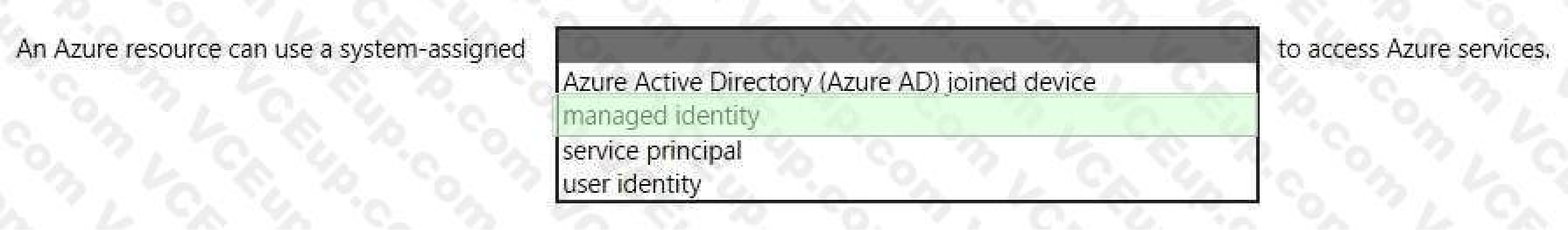


An Azure resource can use a system-assigned

to access Azure services.

Azure Active Directory (Azure AD) joined device
managed identity
service principal
user identity

Answer Area:



An Azure resource can use a system-assigned

to access Azure services.

Azure Active Directory (Azure AD) joined device
[✓ managed identity]
service principal
user identity

Section:
Explanation:

QUESTION 85
When you enable Azure AD Multi-Factor Authentication (MFA), how many factors are required for authentication?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B
Section:

QUESTION 86
Which Microsoft Purview solution can be used to identify data leakage?

A. insider risk management

B. Compliance Manager

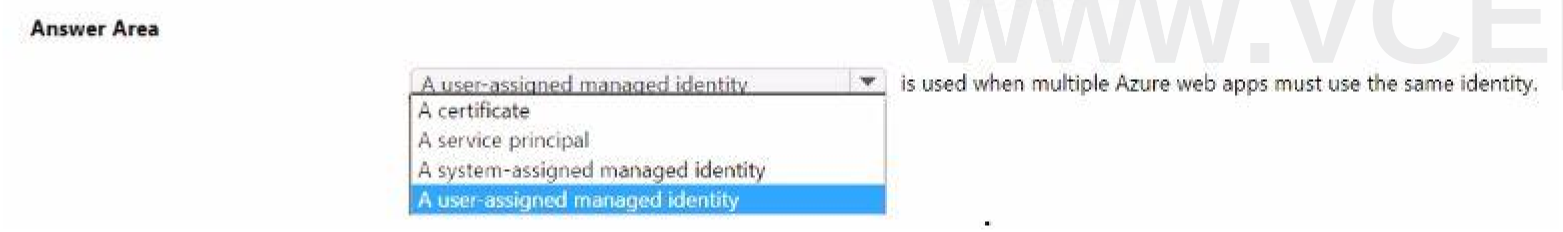
C. communication compliance

D. eDiscovery

Correct Answer: A
Section:

QUESTION 87
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

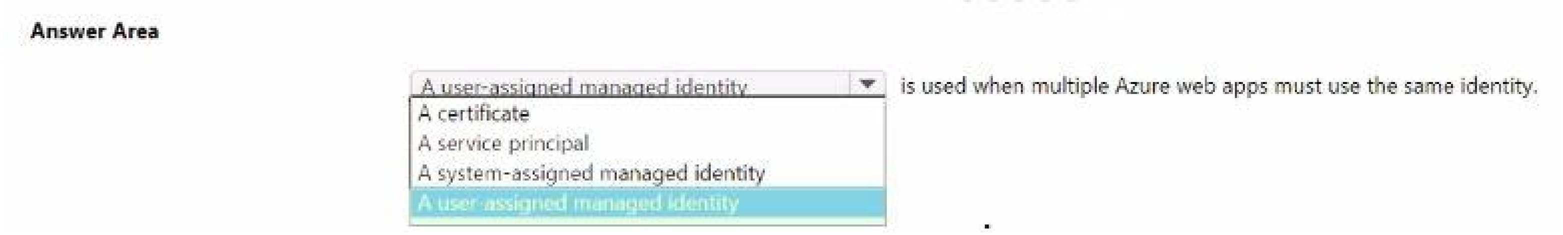


Answer Area

A user-assigned managed identity ▼ is used when multiple Azure web apps must use the same identity.

- A certificate
- A service principal
- A system-assigned managed identity
- A user-assigned managed identity

Answer Area:



Answer Area

A user-assigned managed identity ▼ is used when multiple Azure web apps must use the same identity.

- A certificate
- A service principal
- A system-assigned managed identity
- A user-assigned managed identity

Section:
Explanation: