MIcrosoft.SC-900.vAug-2024.by.Tina.100q

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

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

Exam A

QUESTION 1

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 2

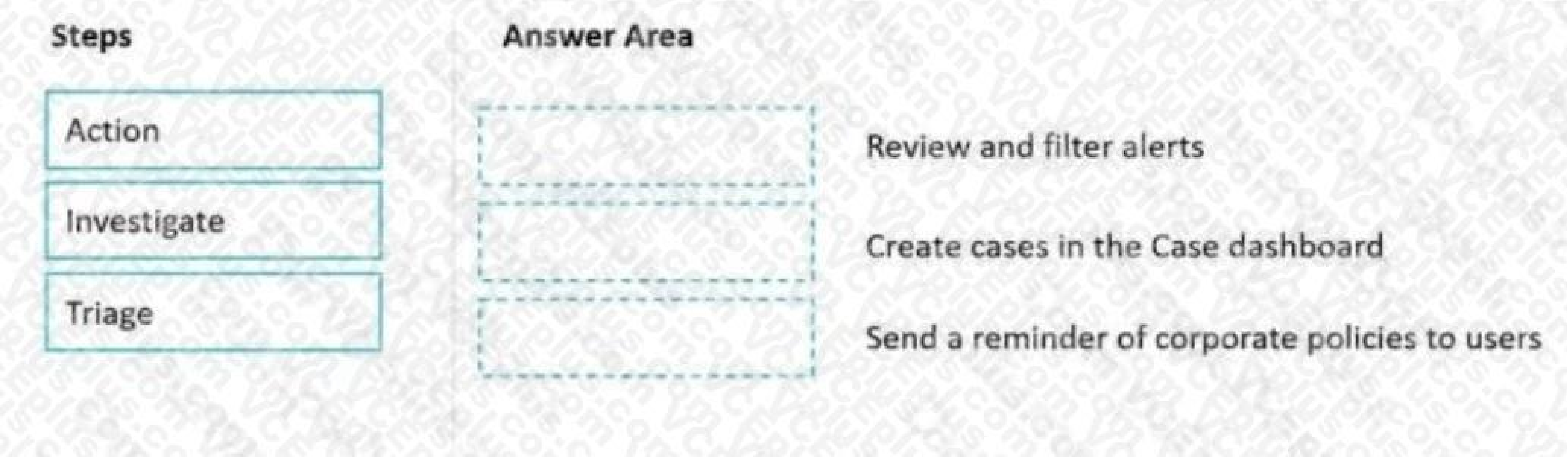
DRAG DROP

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

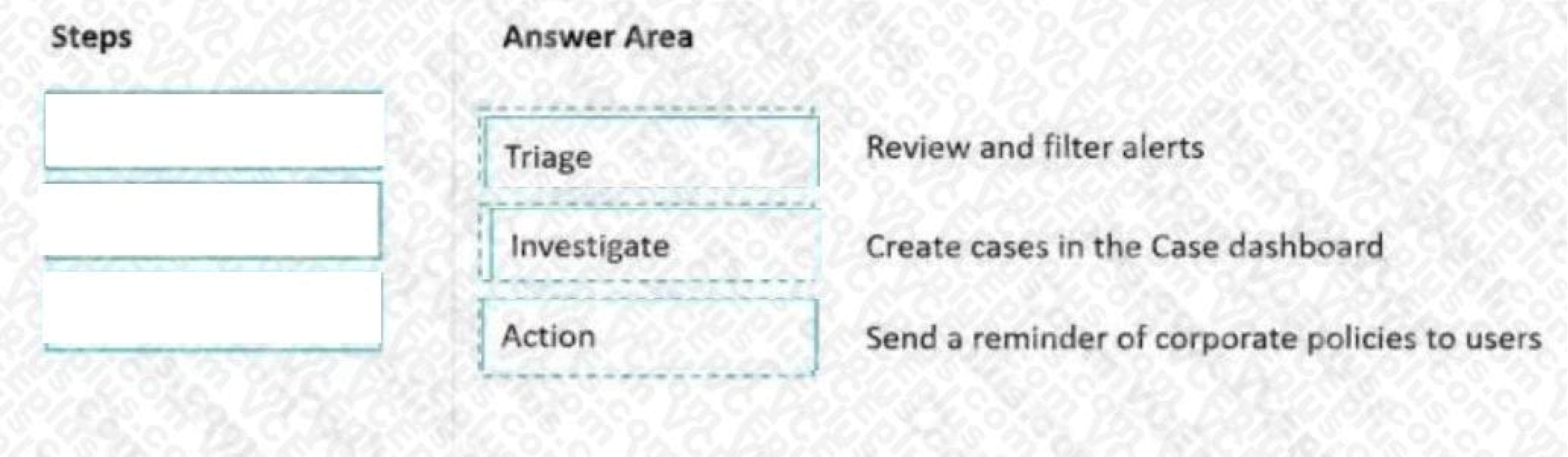
Answer Area

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 3
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 4
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 5
What can you use to provide a user with a two-hour window to complete an administrative task in Azure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Multi-Factor Authentication (MFA)
C. Azure Active Directory (Azure AD) Identity Protection
D. conditional access policies

Correct Answer: D
Section:

QUESTION 6
In a hybrid identity model, what can you use to sync identities between Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD)?

A. Active Directory Federation Services (AD FS)
B. Azure Sentinel
C. Azure AD Connect
D. Azure Ad Privileged Identity Management (PIM)

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

QUESTION 7

What is the purpose of Azure Active Directory (Azure AD) Password Protection?

A. to control how often users must change their passwords

B. to identify devices to which users can sign in without using multi-factor authentication (MFA)

C. to encrypt a password by using globally recognized encryption standards

D. to prevent users from using specific words in their passwords

Correct Answer: D
Section:
Explanation:

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

QUESTION 8

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:

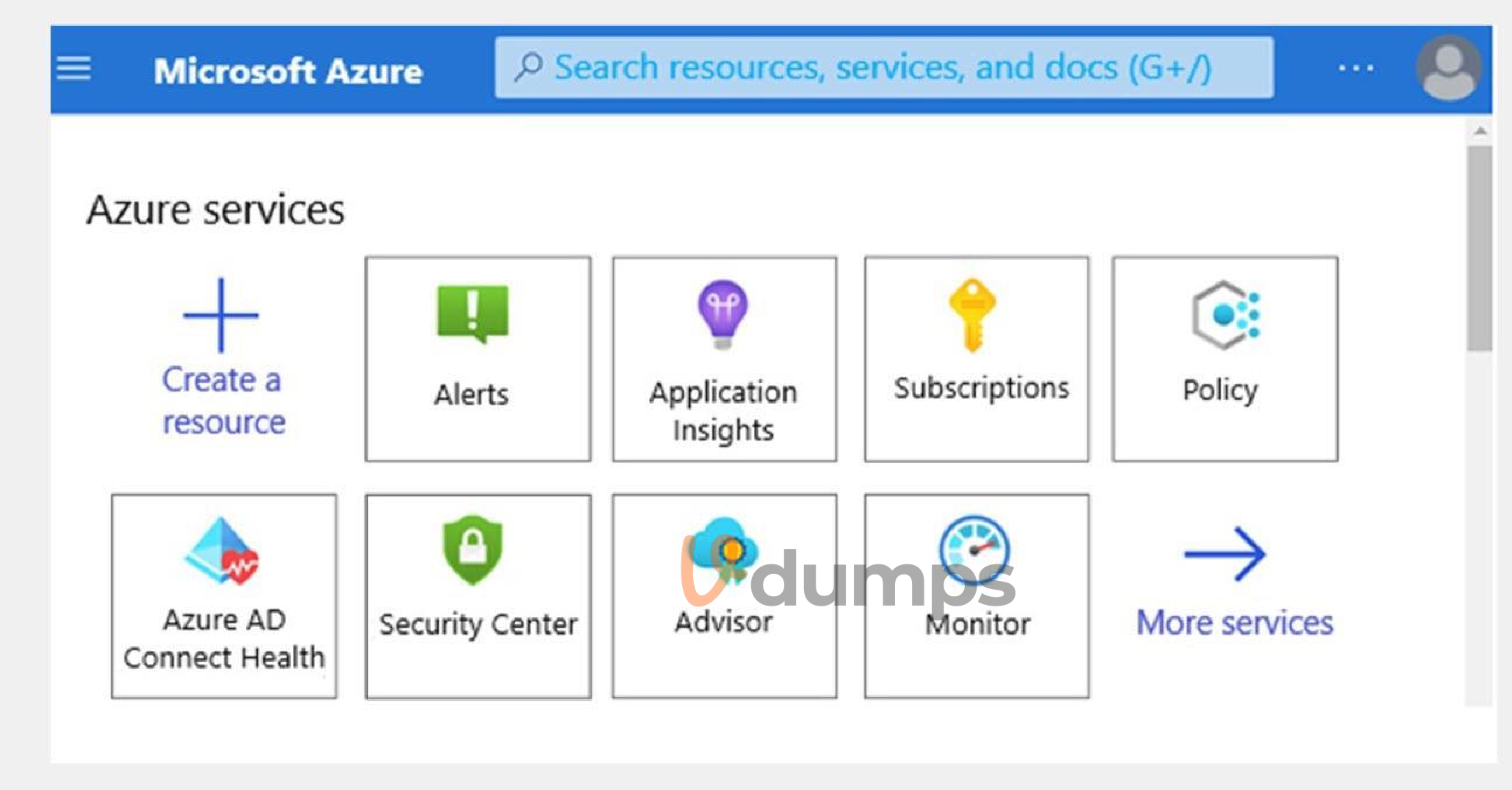
Reference:
https://docs.microsoft.com/en-us/security/zero-trust/

QUESTION 9

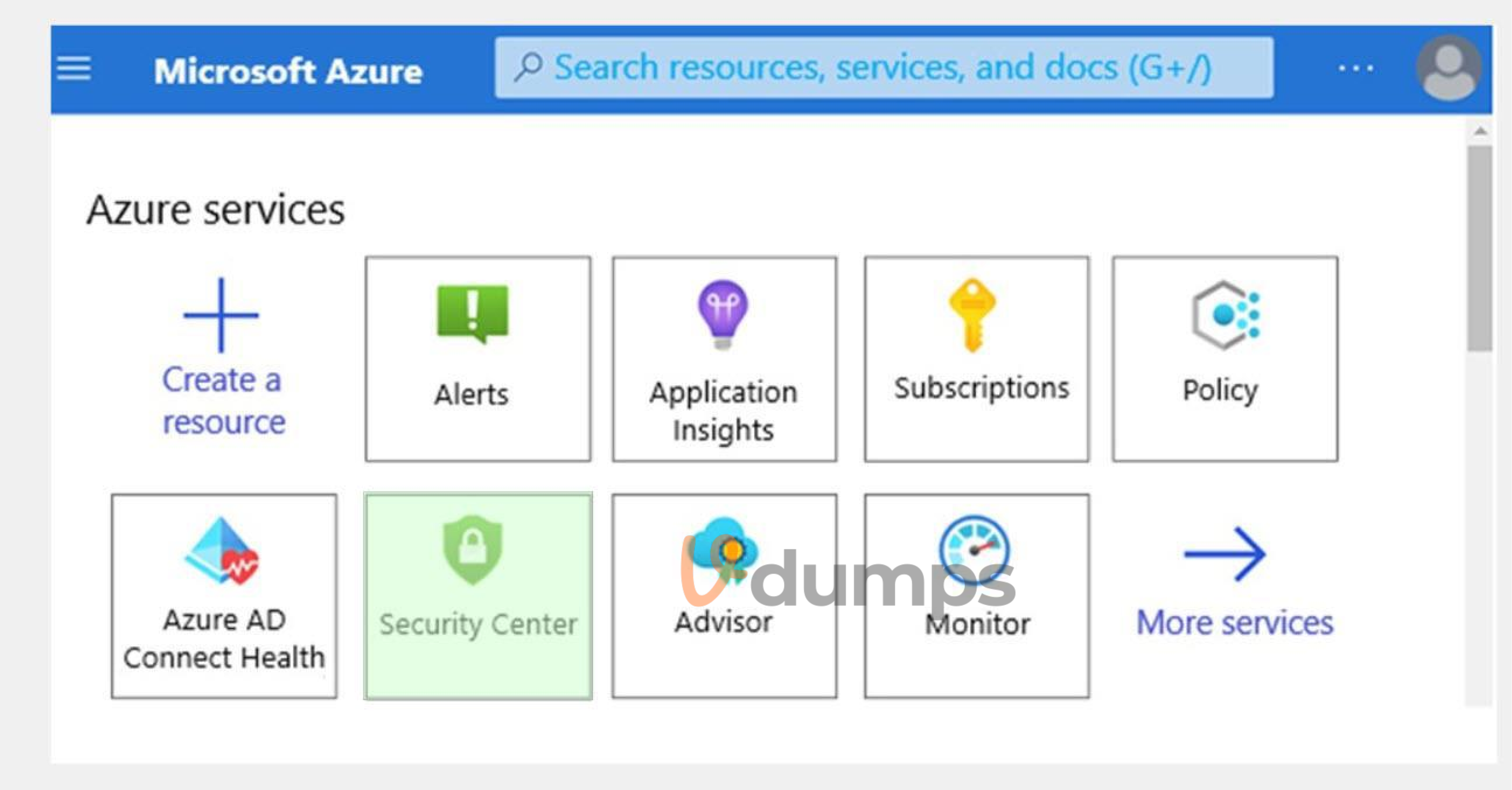
HOTSPOT

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 10

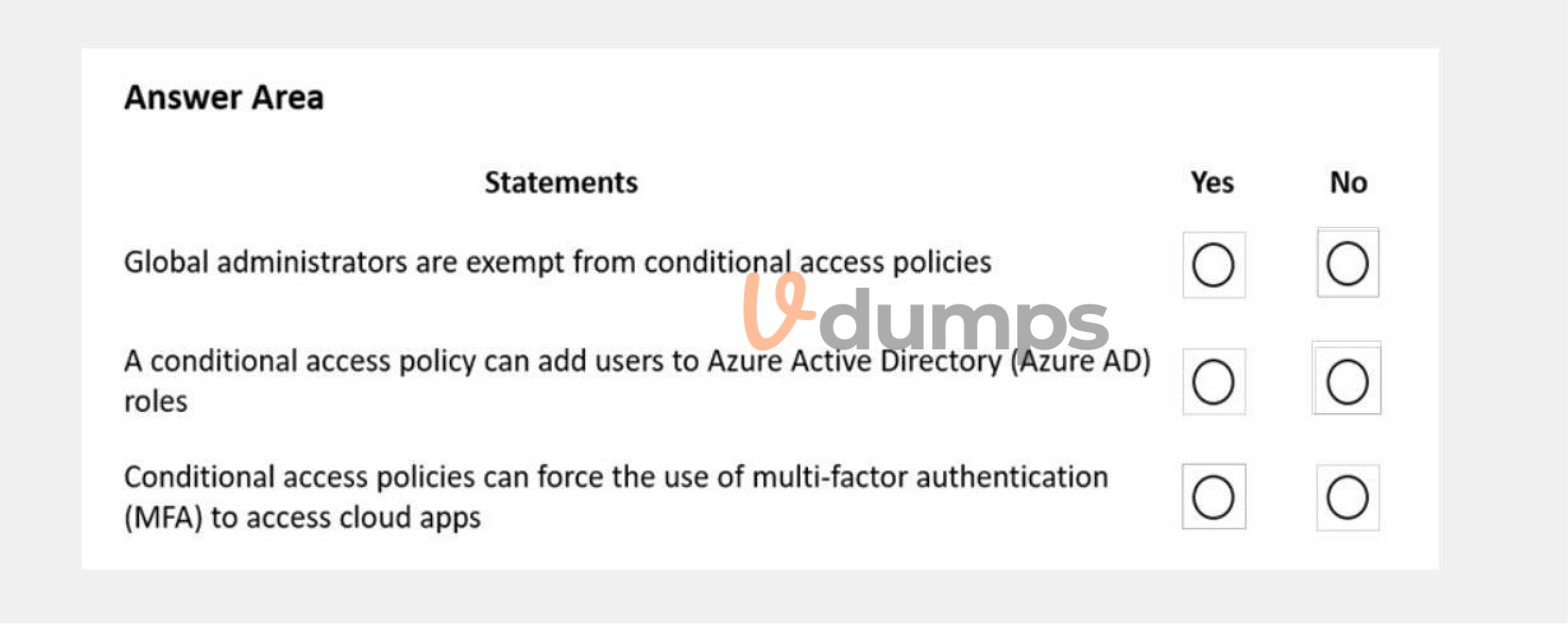
You have an Azure subscription.
You need to implement approval-based, time-bound role activation.
What should you use?

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 11
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.

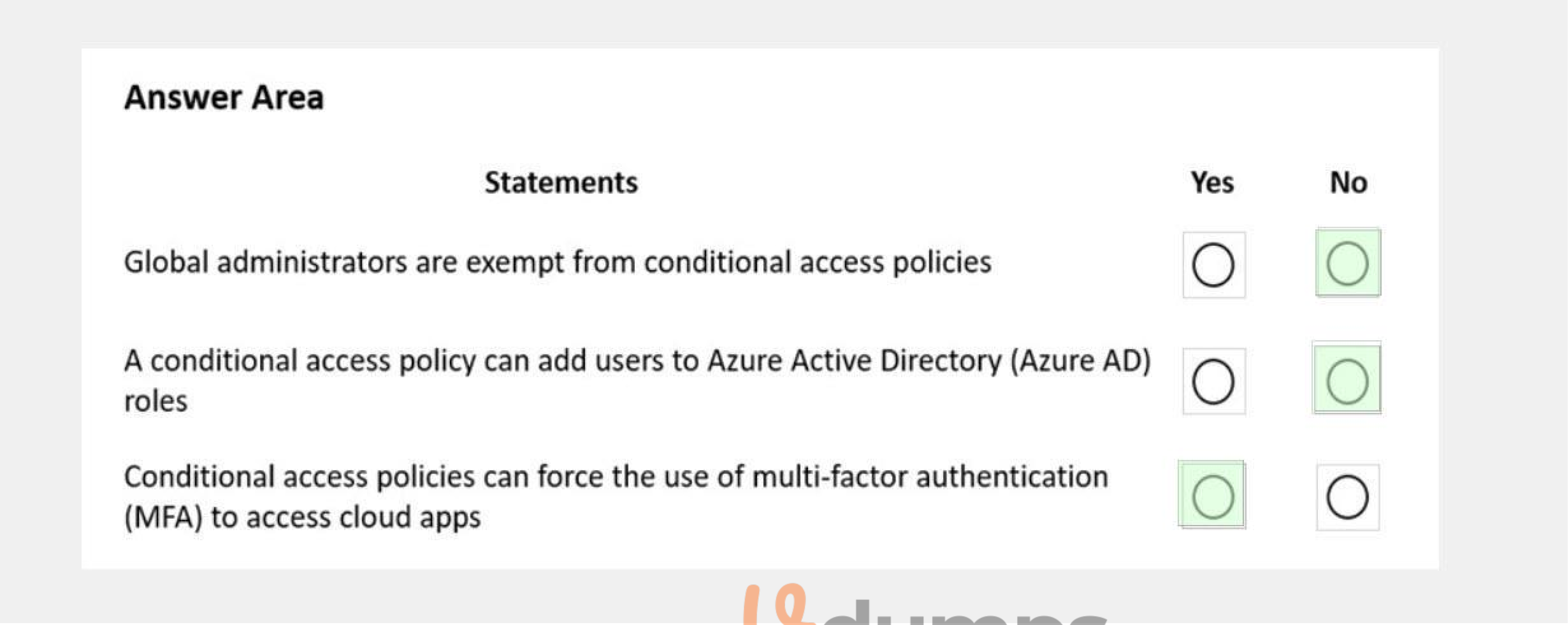
Hot Area:



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 12

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 13
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 14
What can you use to provision Azure resources across multiple subscriptions in a consistent manner?

A. Microsoft Defender for Cloud
B. Azure Blueprints
C. Microsoft Sentinel
D. Azure Policy

Correct Answer: B
Section:

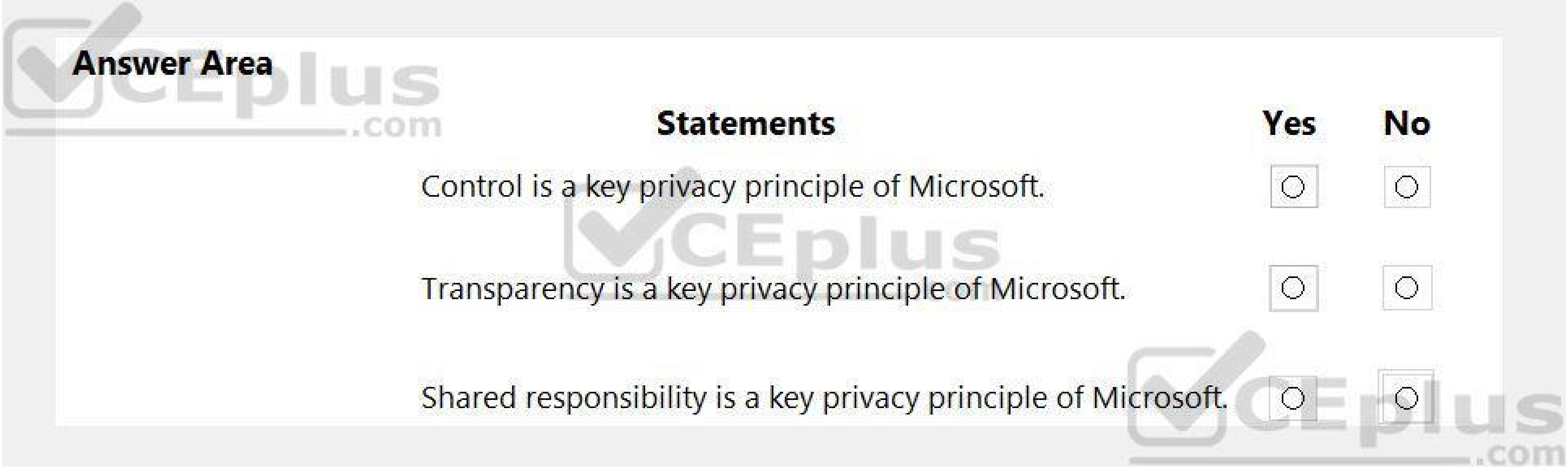
QUESTION 15
You need to keep a copy of all files in a Microsoft SharePoint site for one year, even if users delete the files from the site. What should you apply to the site?

A. a data loss prevention (DLP) policy
B. a retention policy
C. an insider risk policy
D. a sensitivity label policy

Correct Answer: B
Section:

QUESTION 16
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.

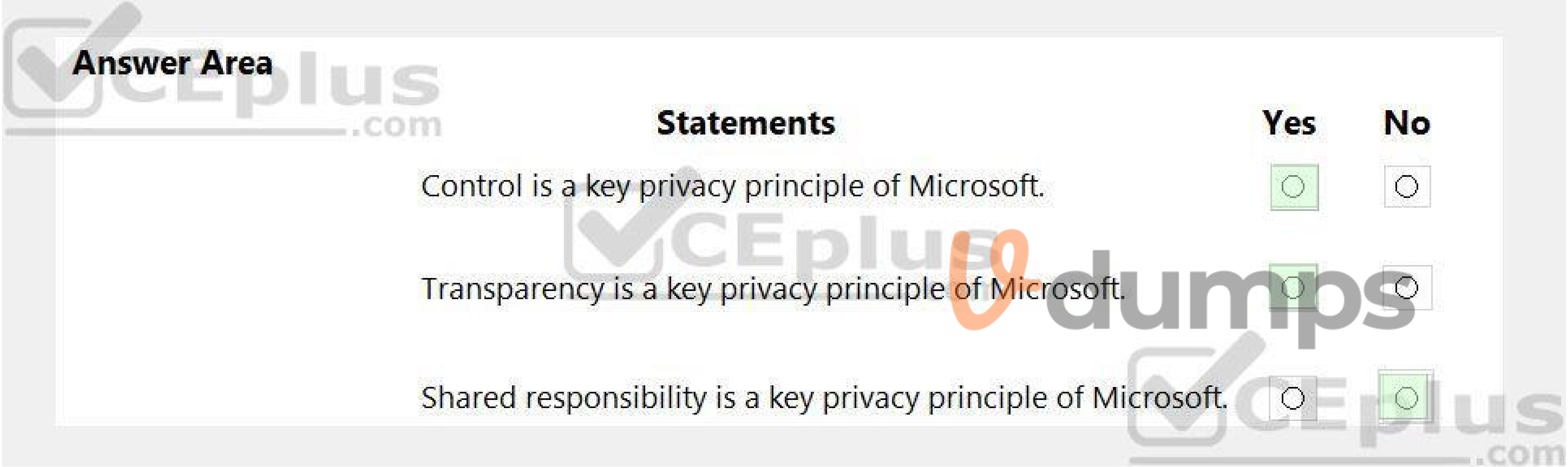
Hot Area:



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:



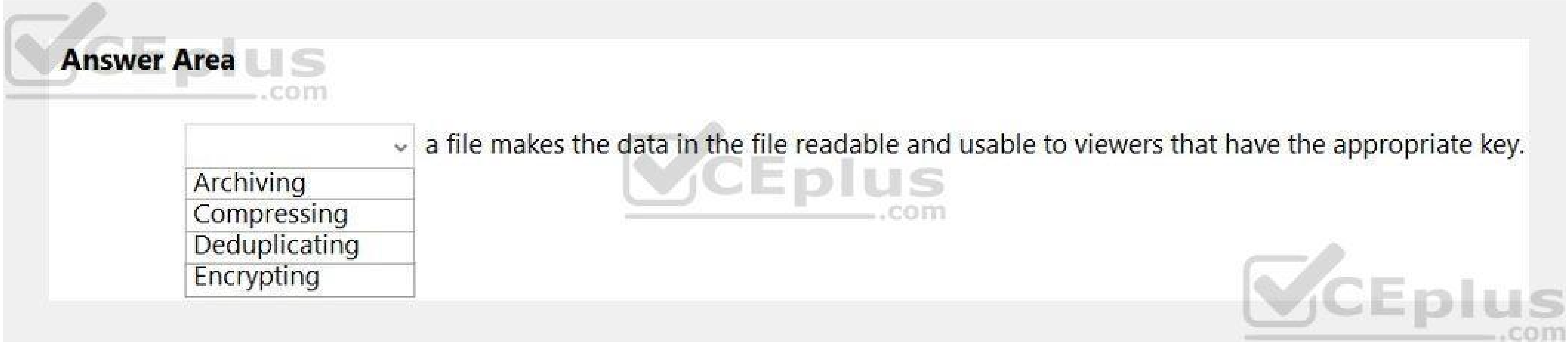
Answer Area

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 17
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

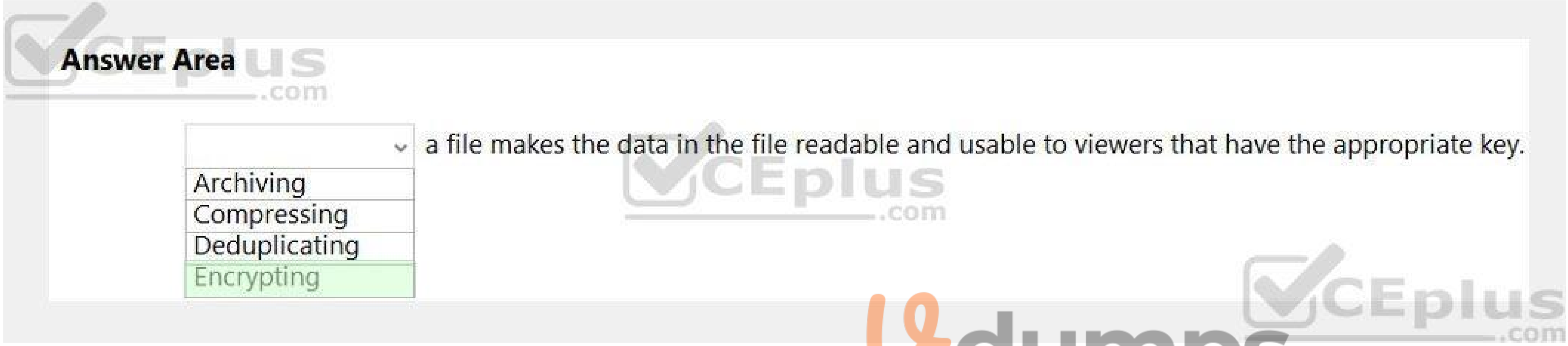


Answer Area

[⌄] 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

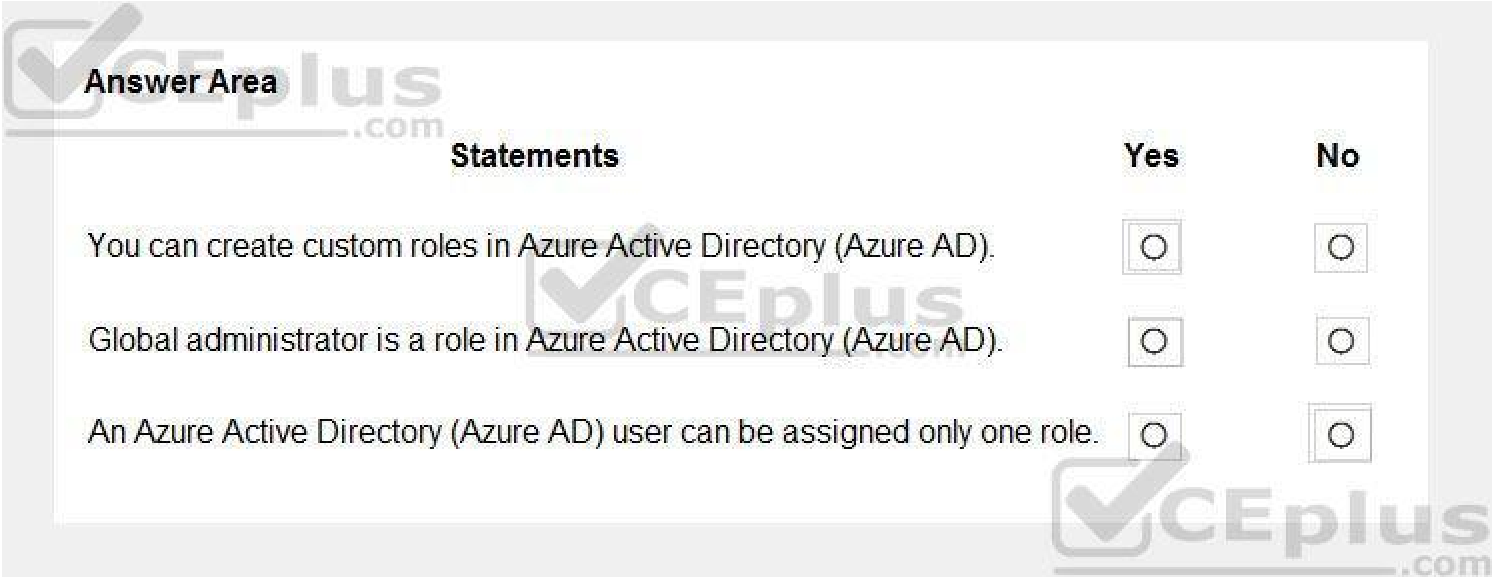
[⌄] a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- [✓ Encrypting]

Section:
Explanation:

QUESTION 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.

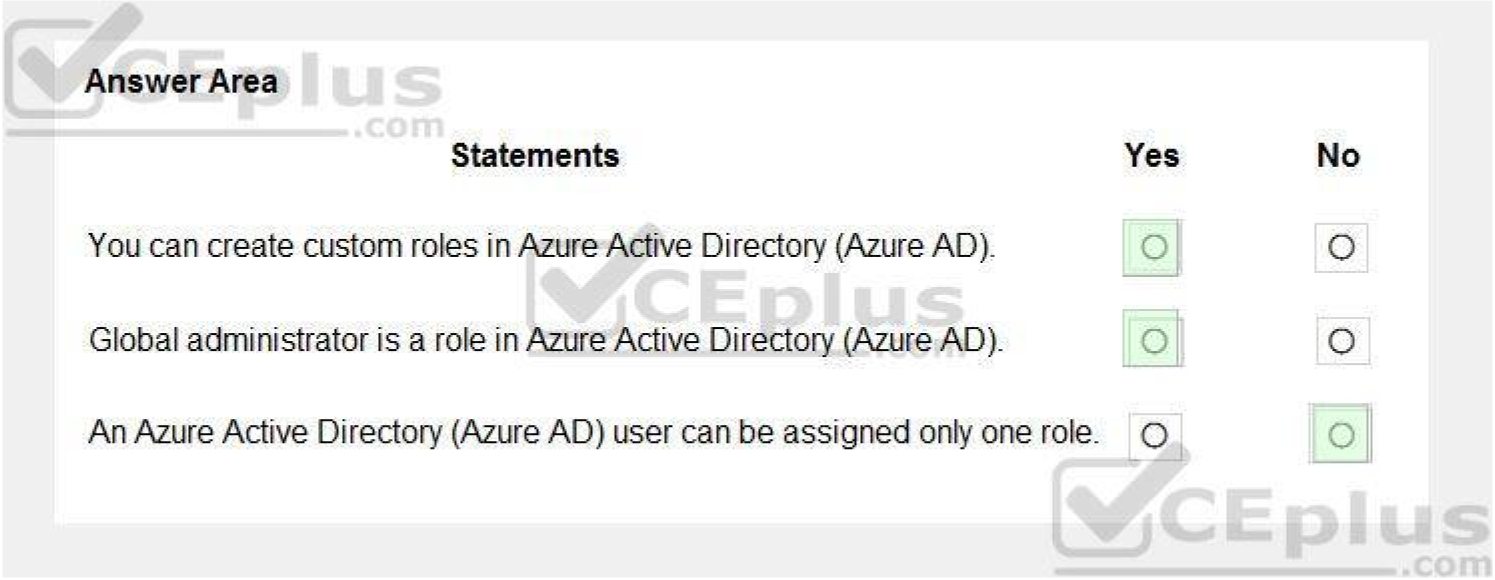
Hot Area:



Answer Area

Statements	Yes	No
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

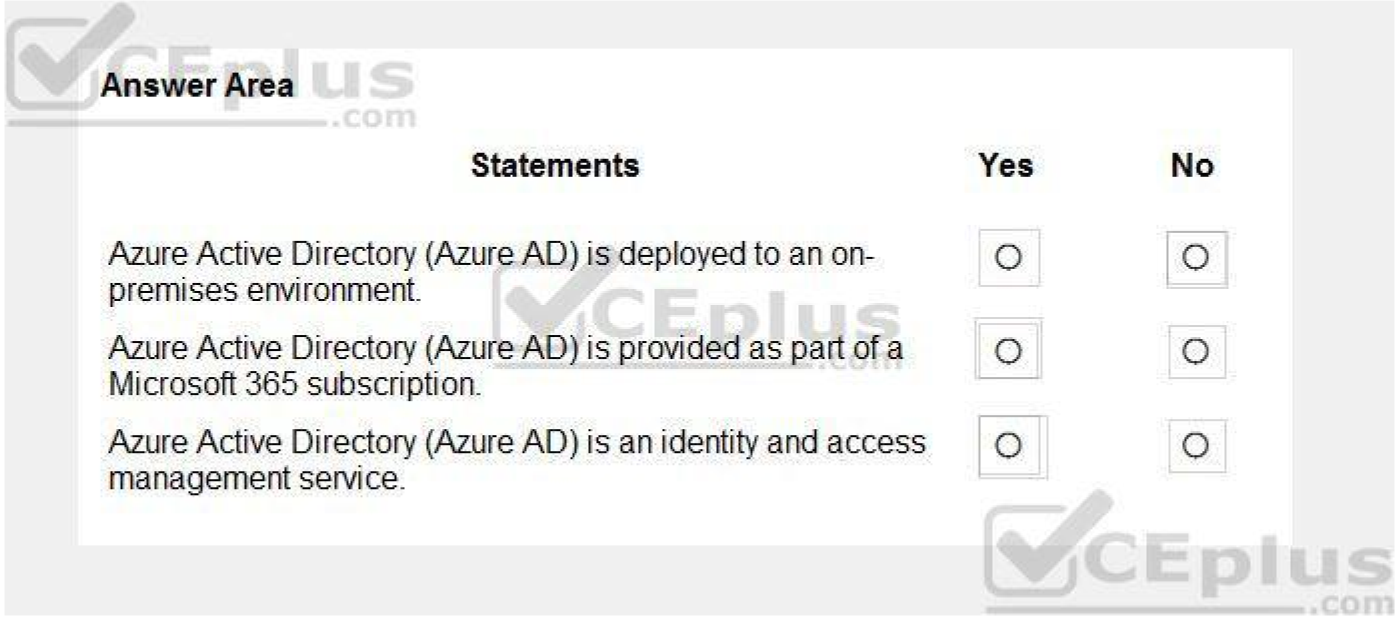
QUESTION 19

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.

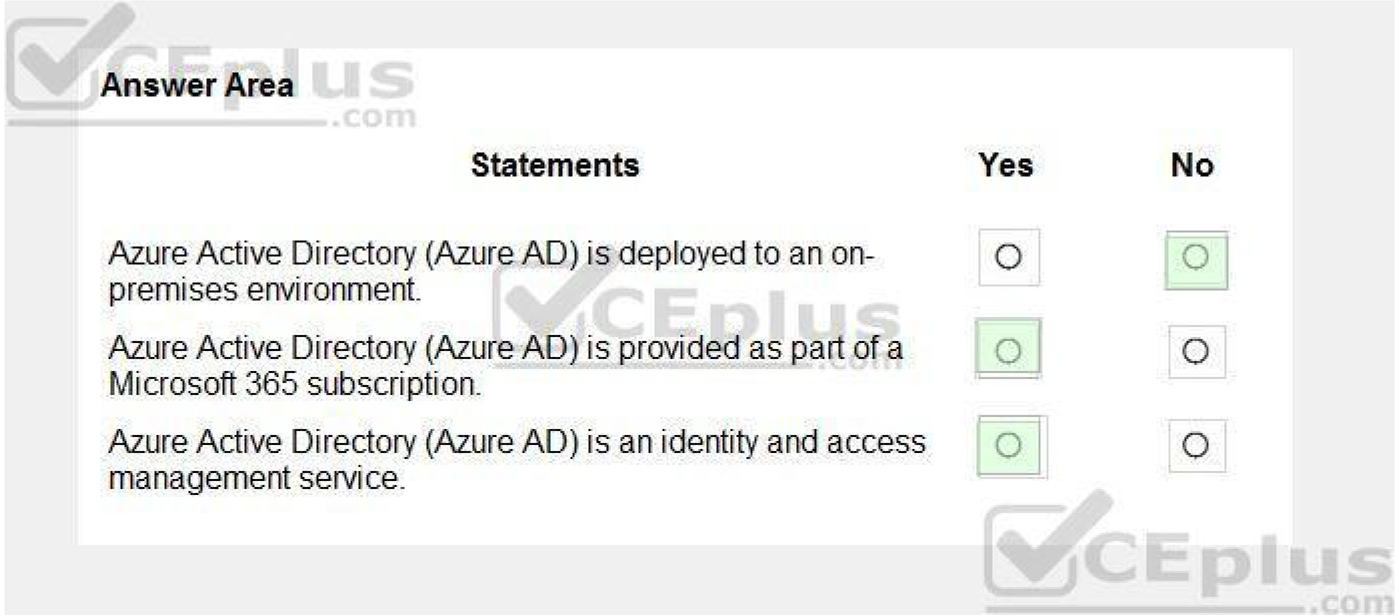
Hot Area:



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:

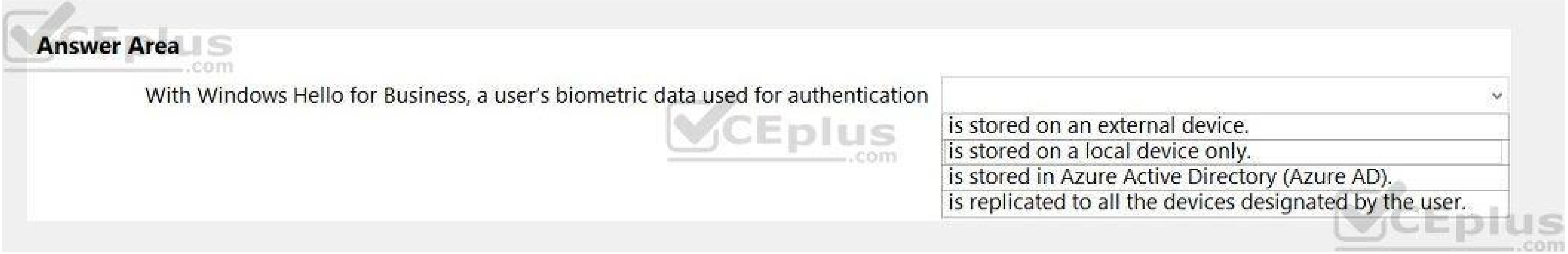
https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

QUESTION 20

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

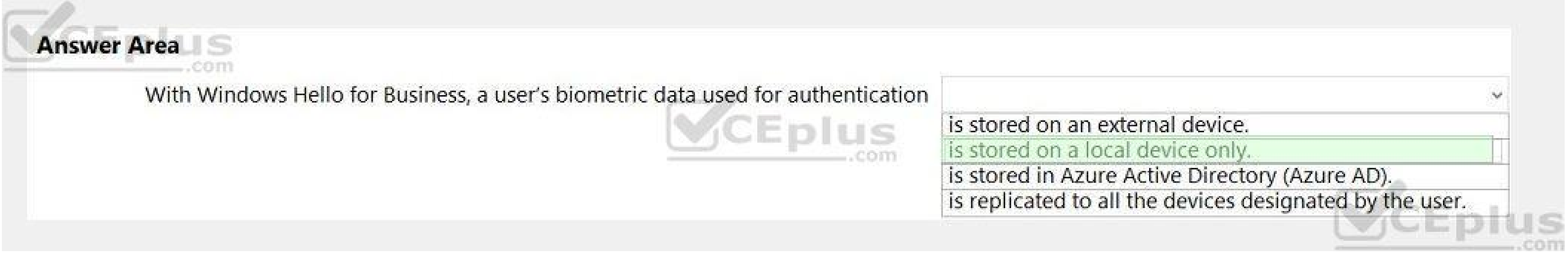


Answer Area

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

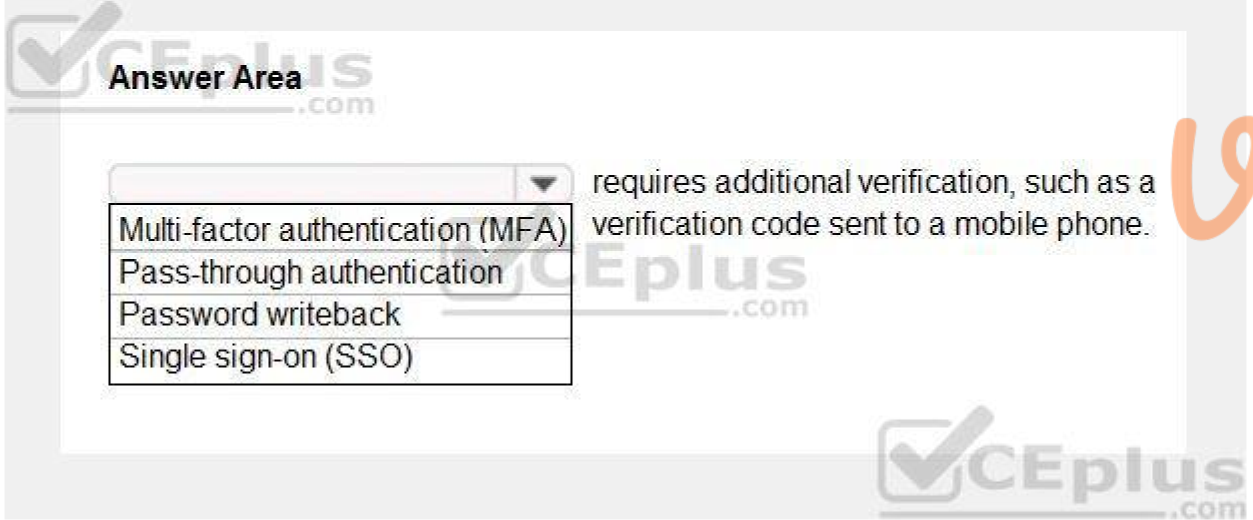
With Windows Hello for Business, a user's biometric data used for authentication

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

Hot Area:

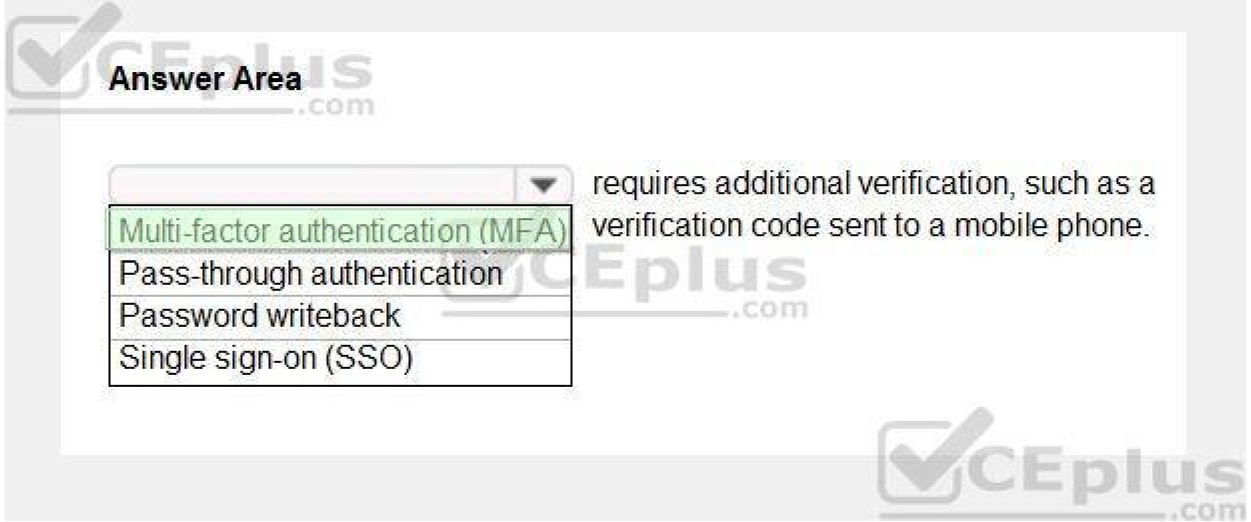


Answer Area

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

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

Answer Area:



Answer Area

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

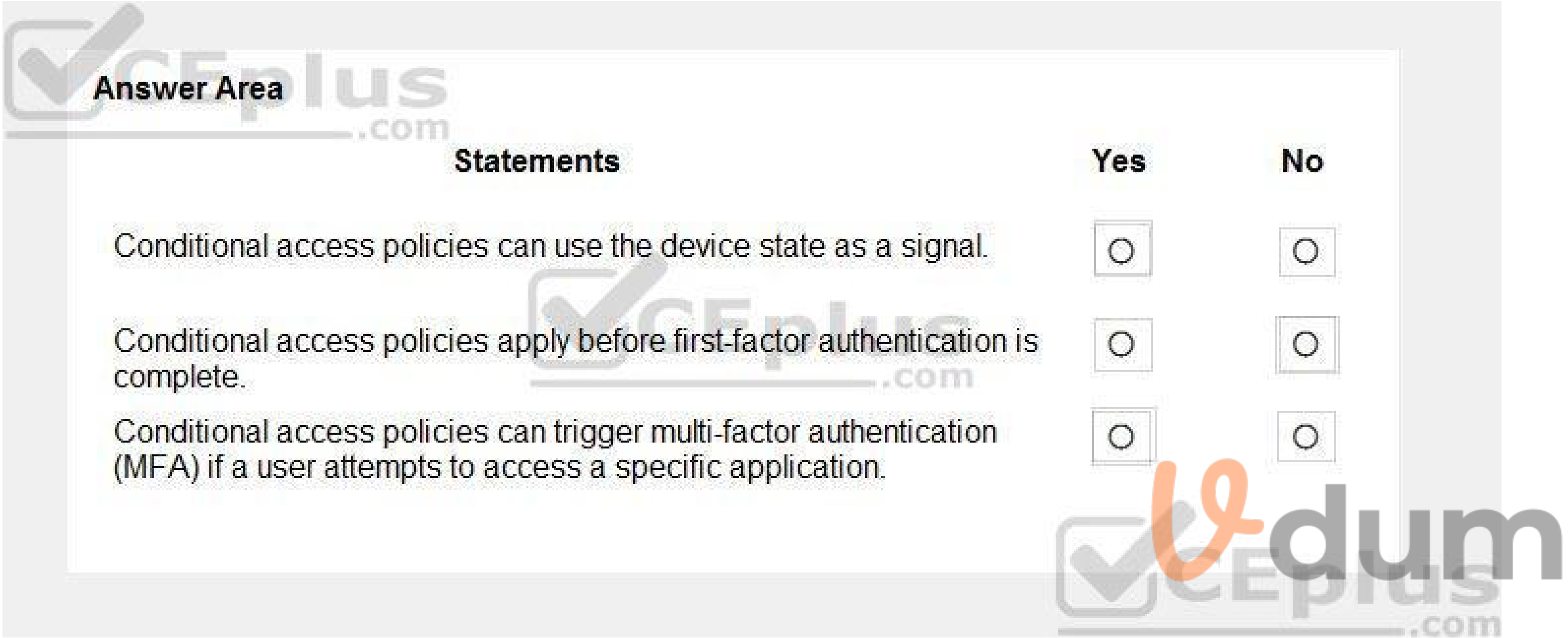
- [✓ Multi-factor authentication (MFA)]
- Pass-through authentication
- Password writeback
- Single sign-on (SSO)

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 22
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.

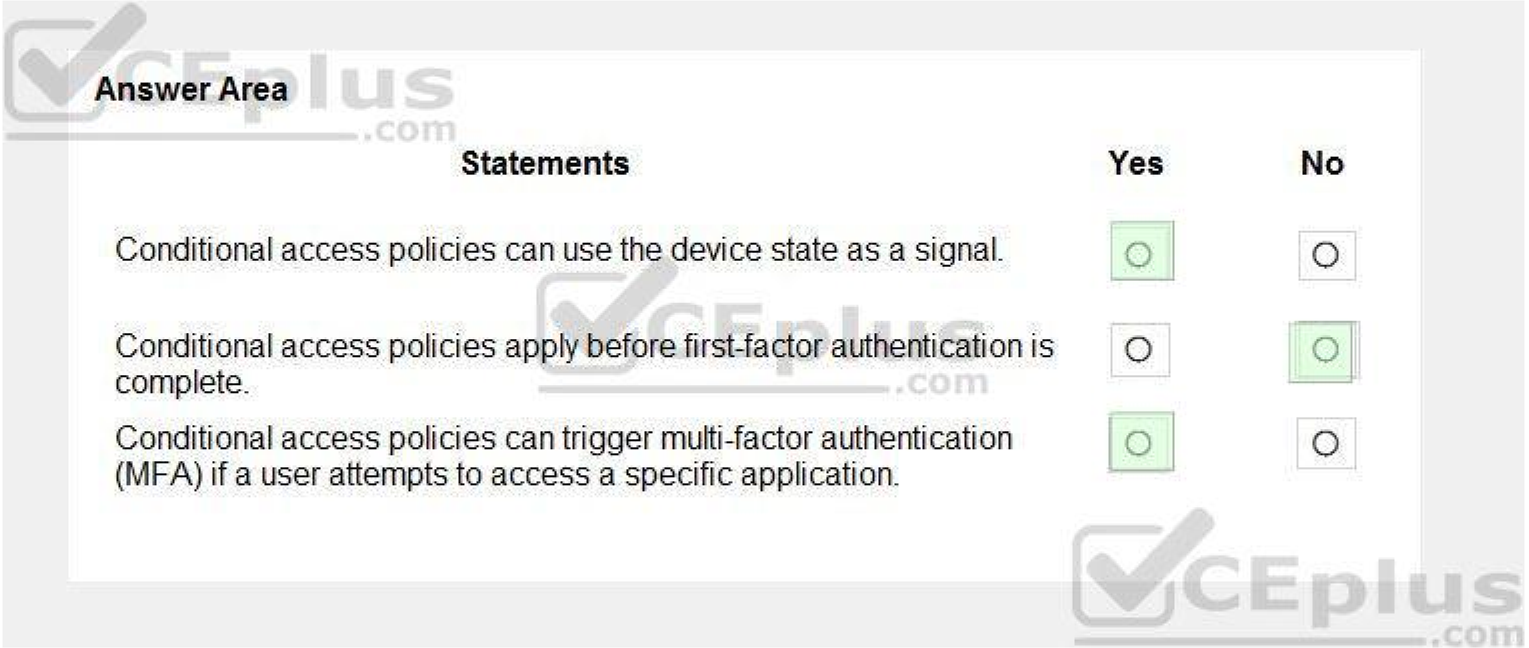
Hot Area:



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

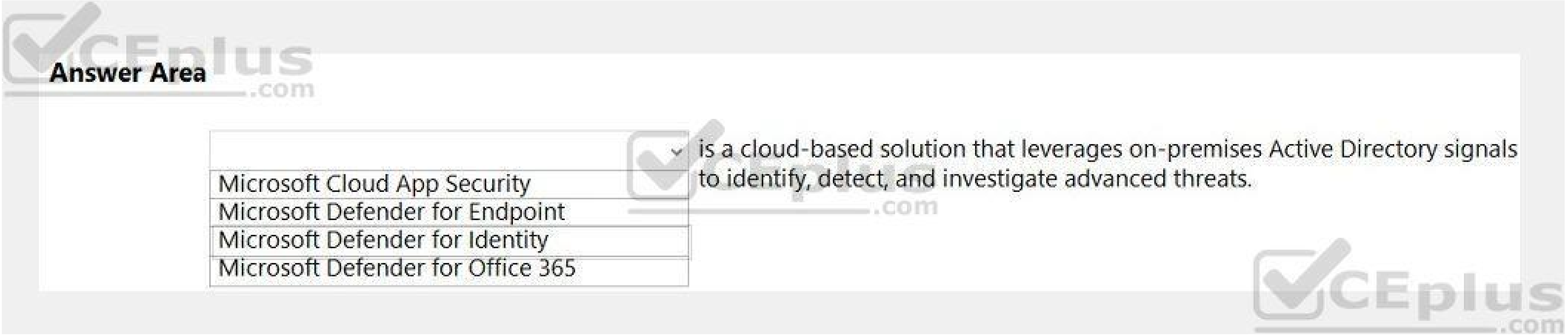
Statements	Yes	No
Conditional access policies can use the device state as a signal.	[✓ ○]	○
Conditional access policies apply before first-factor authentication is complete.	○	[✓ ○]
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.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

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 23
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

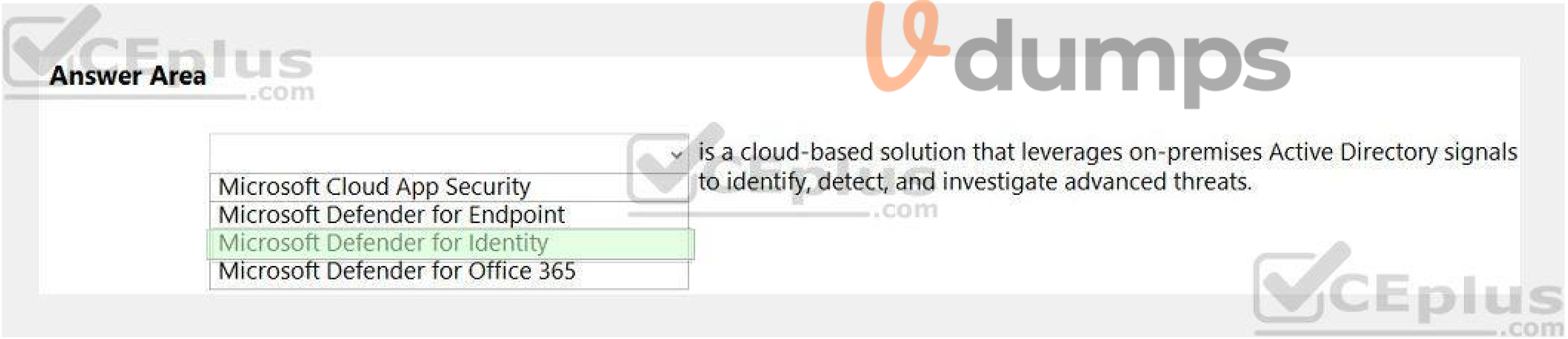


Answer Area

- 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

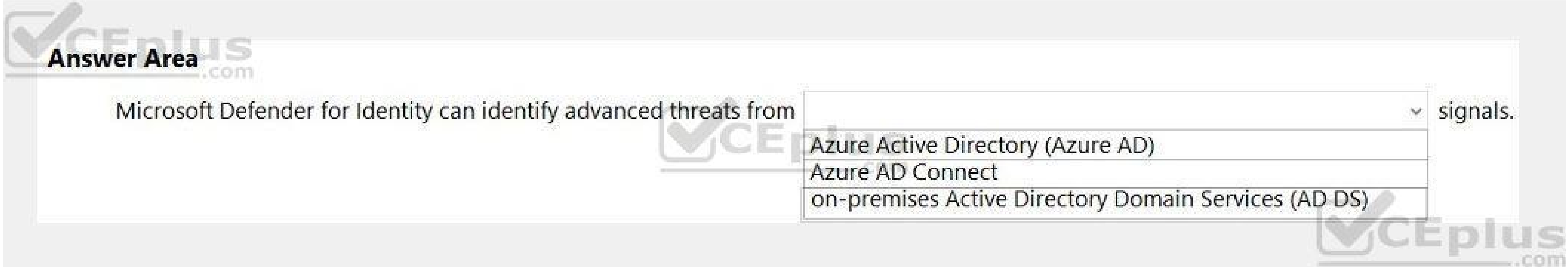
- Microsoft Cloud App Security
- Microsoft Defender for Endpoint
- [✓ Microsoft Defender for Identity]
- Microsoft Defender for Office 365

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 24
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

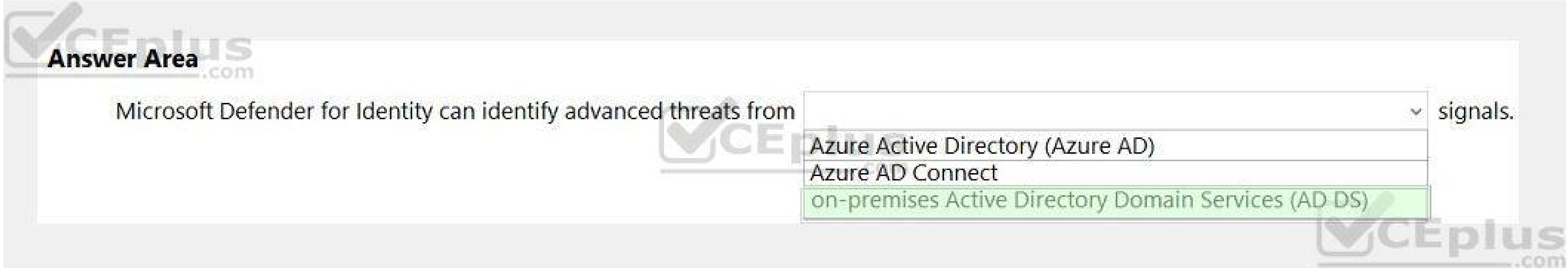


Answer Area

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:

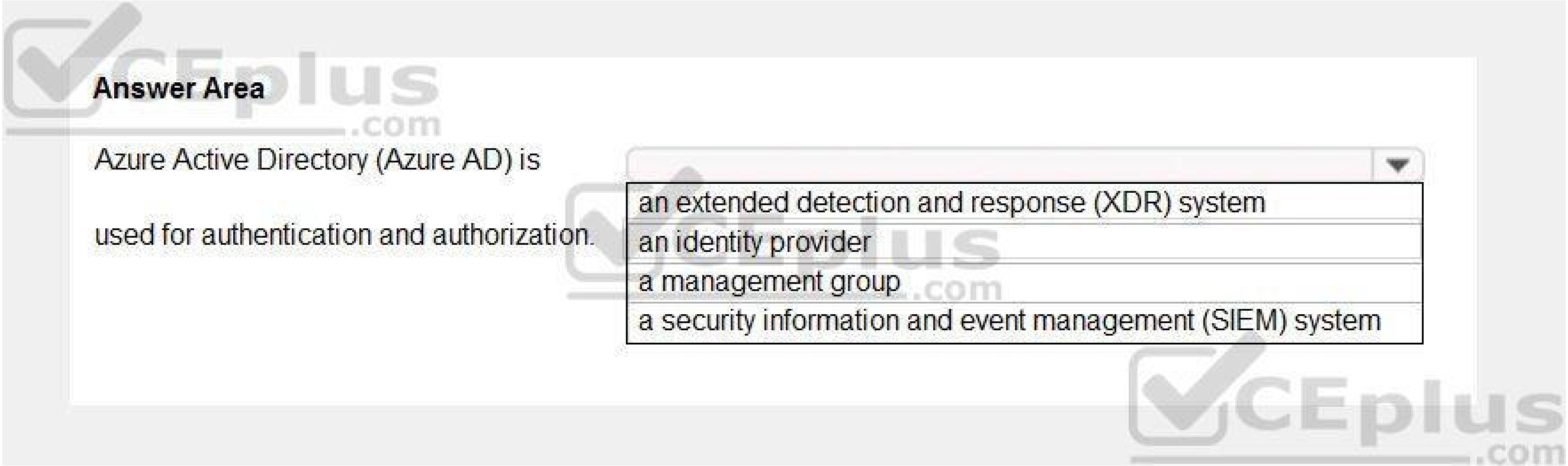
https://docs.microsoft.com/en-us/defender-for-identity/what-is

QUESTION 25

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

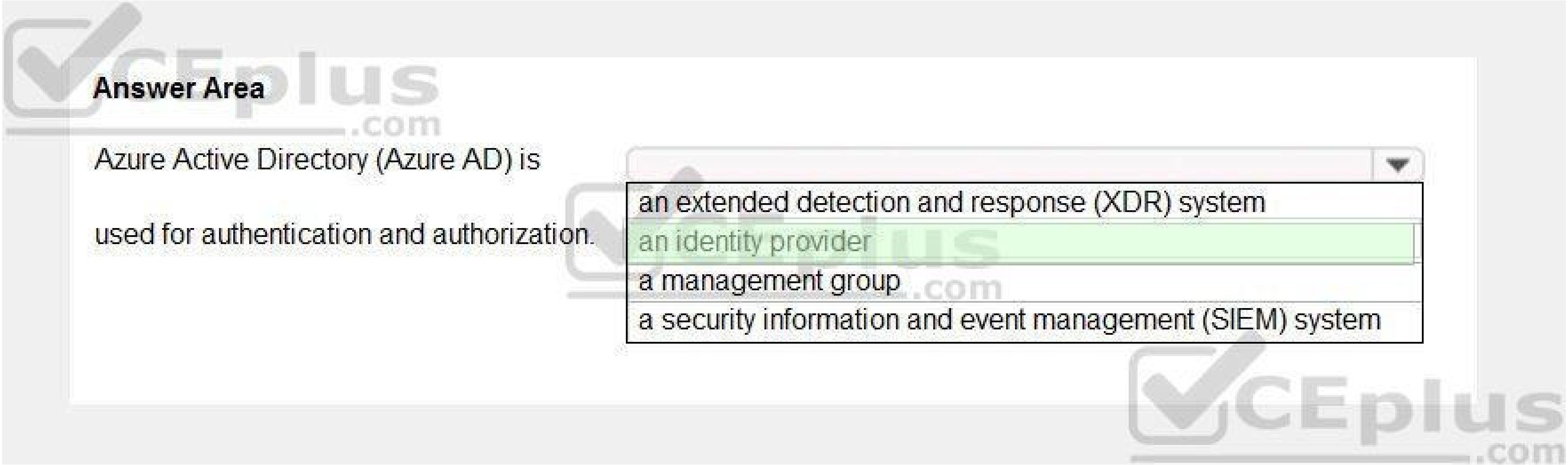


Answer Area

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

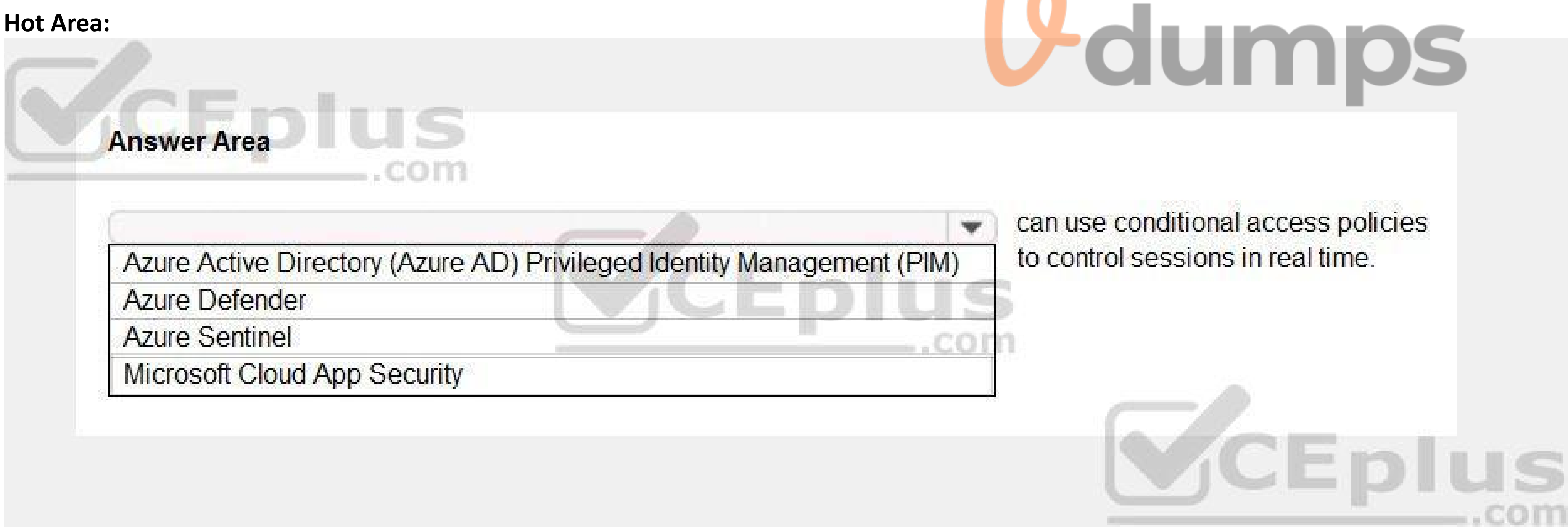
Azure Active Directory (Azure AD) is ▾ used for authentication and authorization.

- 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 26
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

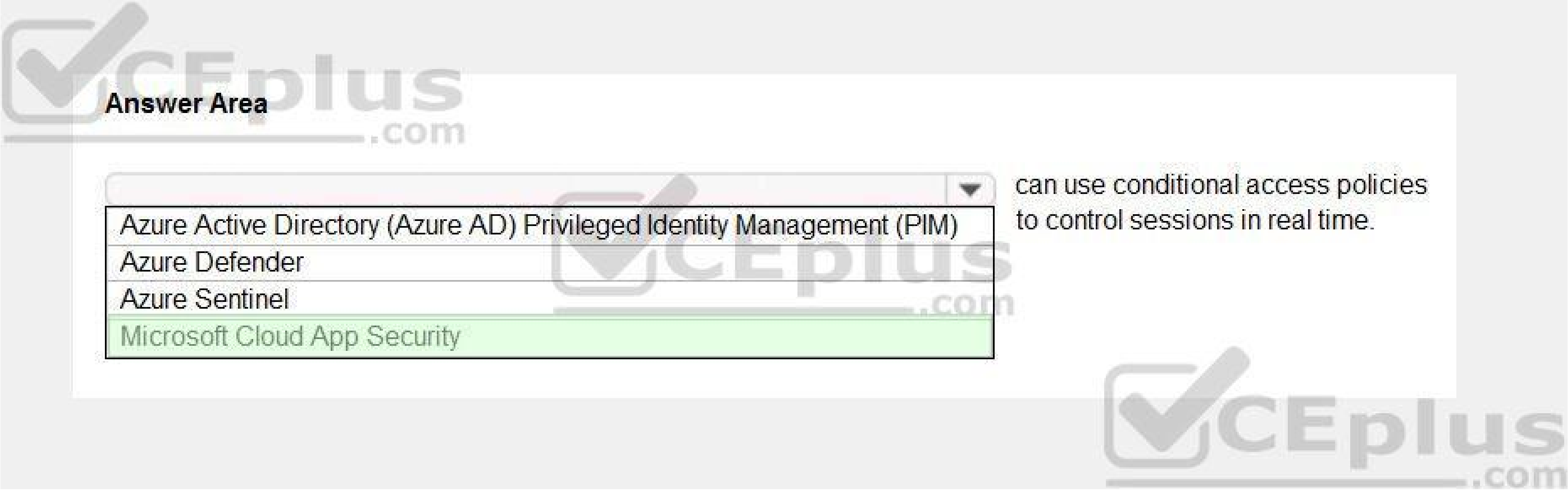


Answer Area

▾ 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

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]

Section:

Explanation:

Reference:

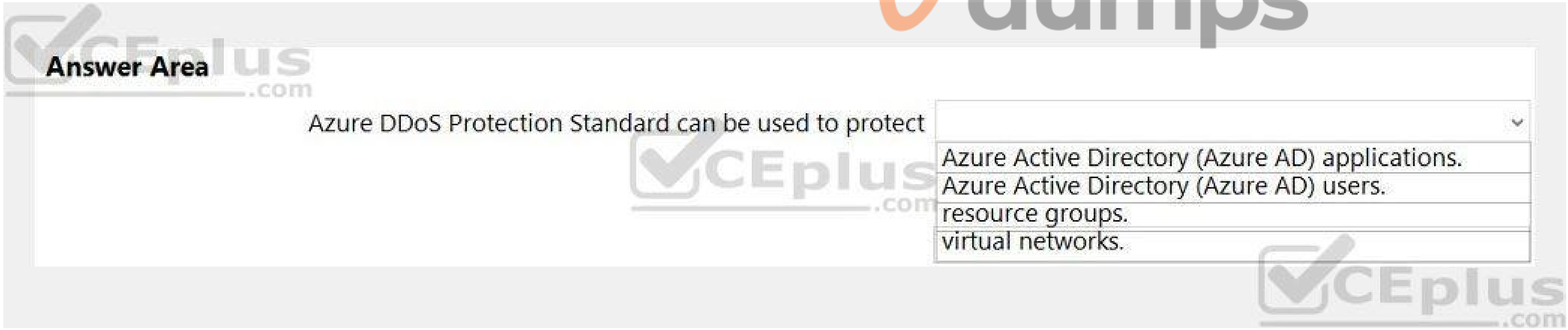
https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

QUESTION 27

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

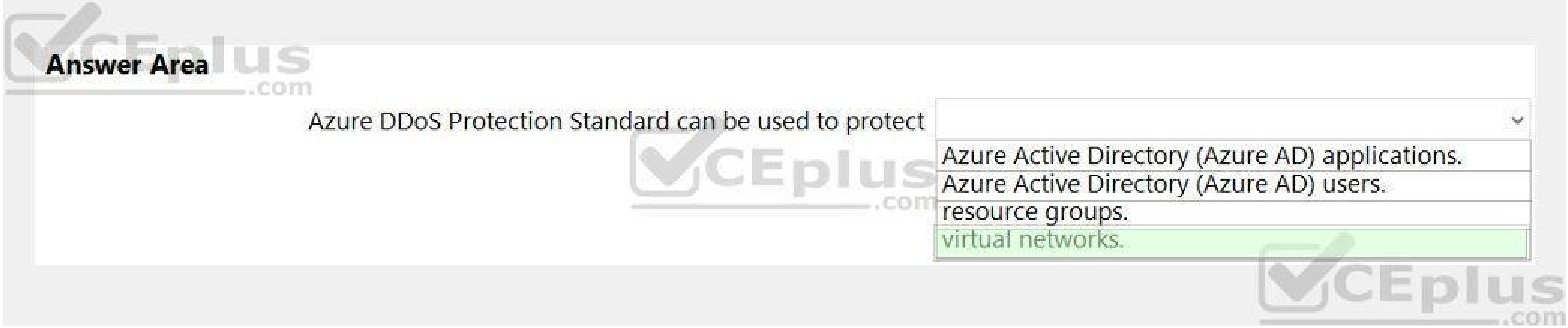


Answer Area

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

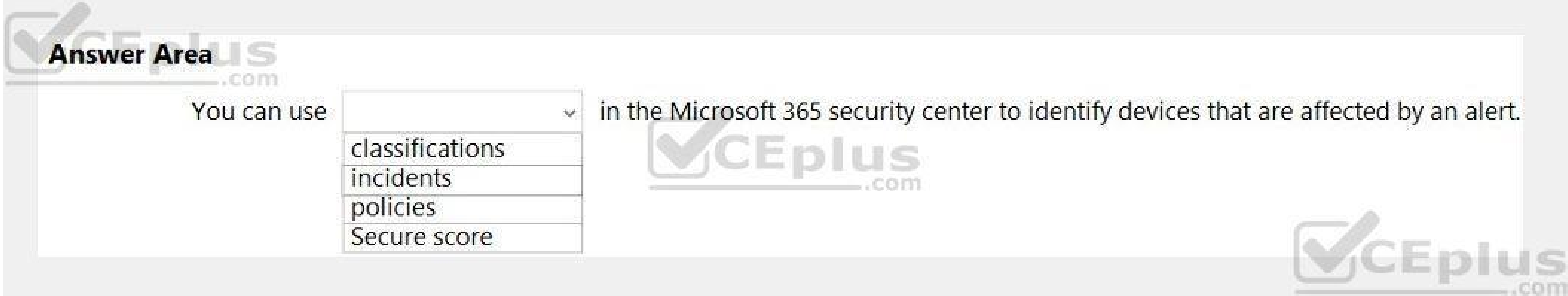
- Azure Active Directory (Azure AD) applications.
- Azure Active Directory (Azure AD) users.
- resource groups.
- [✓ virtual networks.]

Section:

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

QUESTION 28
HOTSPOT
Select the answer that correctly completes the sentence.

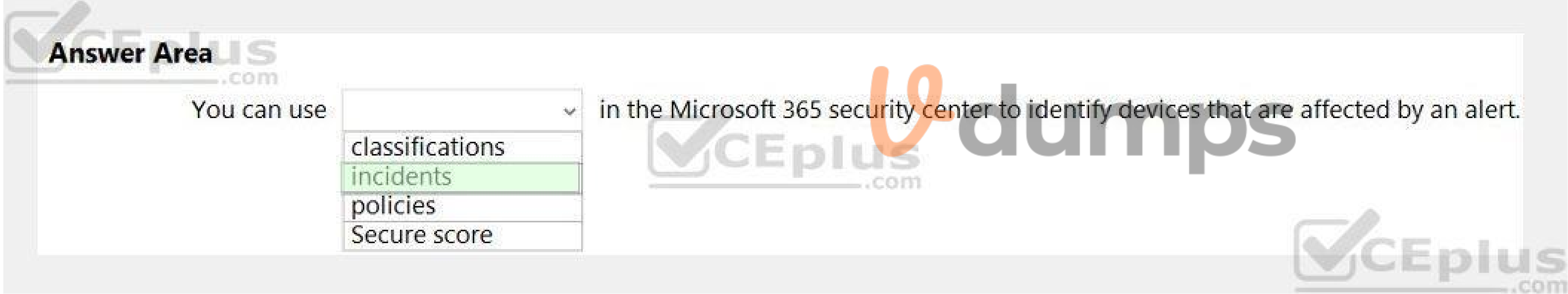
Hot Area:



Answer Area

You can use [classifications / incidents / policies / Secure score] in the Microsoft 365 security center to identify devices that are affected by an alert.

Answer Area:



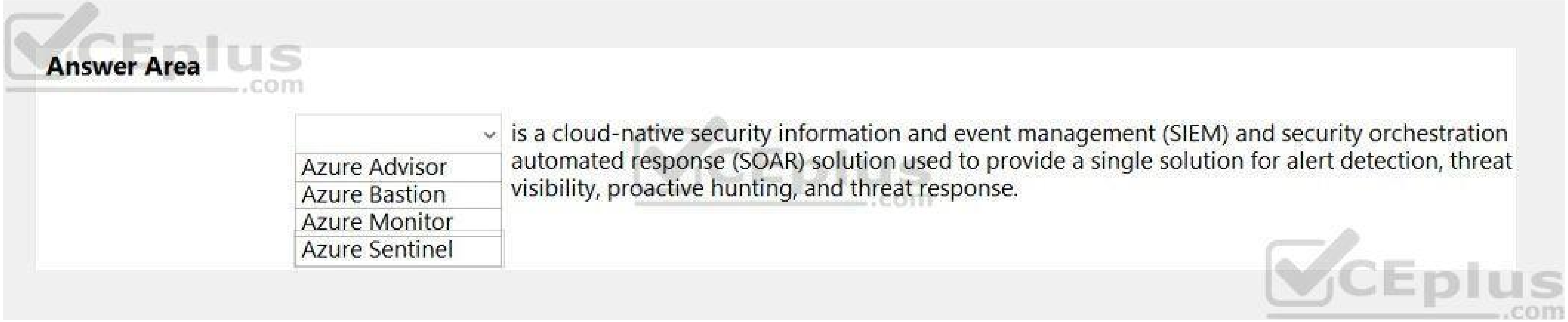
Answer Area

You can use [classifications / [✓ incidents] / policies / Secure score] in the Microsoft 365 security center to identify devices that are affected by an alert.

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

QUESTION 29
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

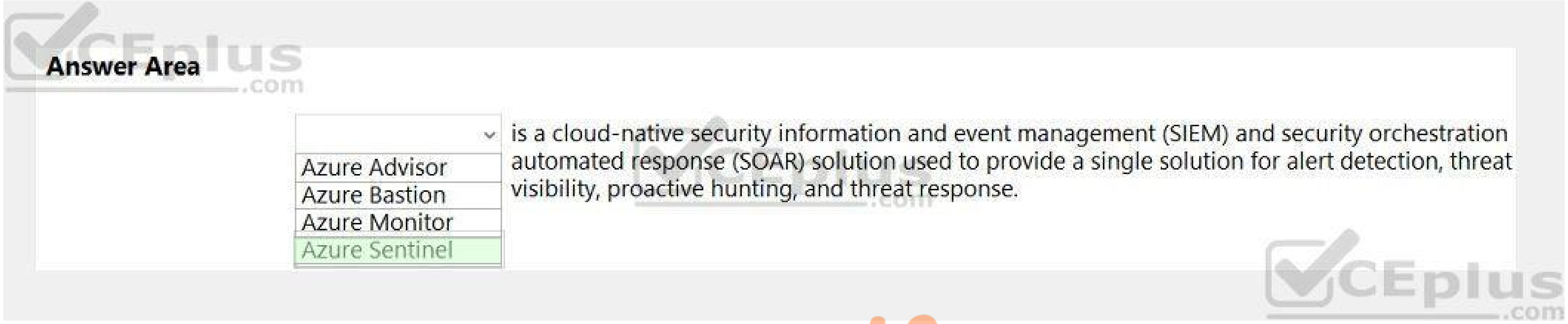


Answer Area

- Azure Advisor
- Azure Bastion
- Azure Monitor
- Azure Sentinel

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

- Azure Advisor
- Azure Bastion
- Azure Monitor
- [✓ Azure Sentinel]

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

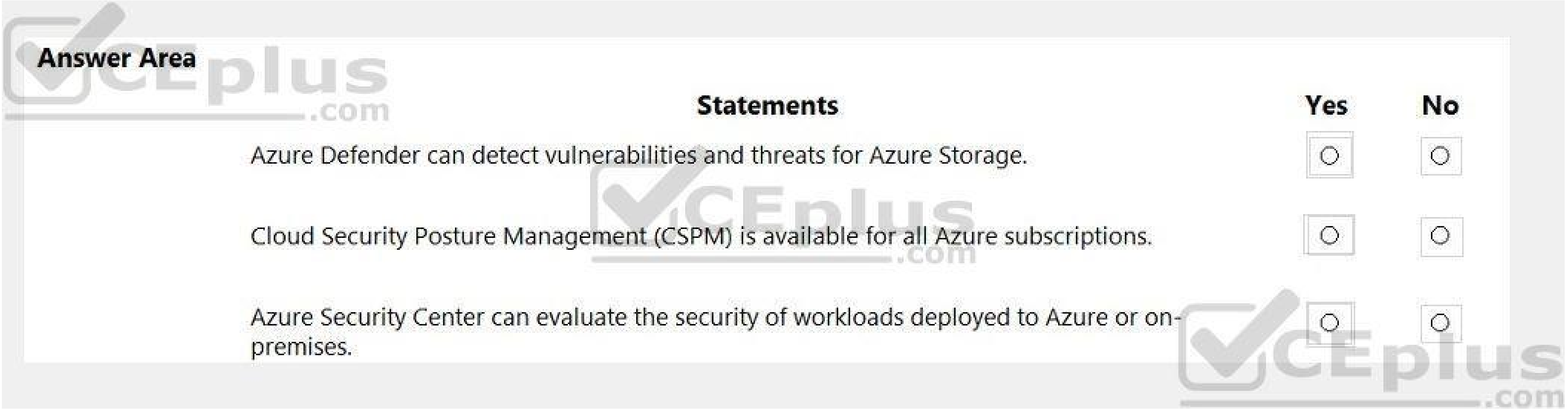
QUESTION 30

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.

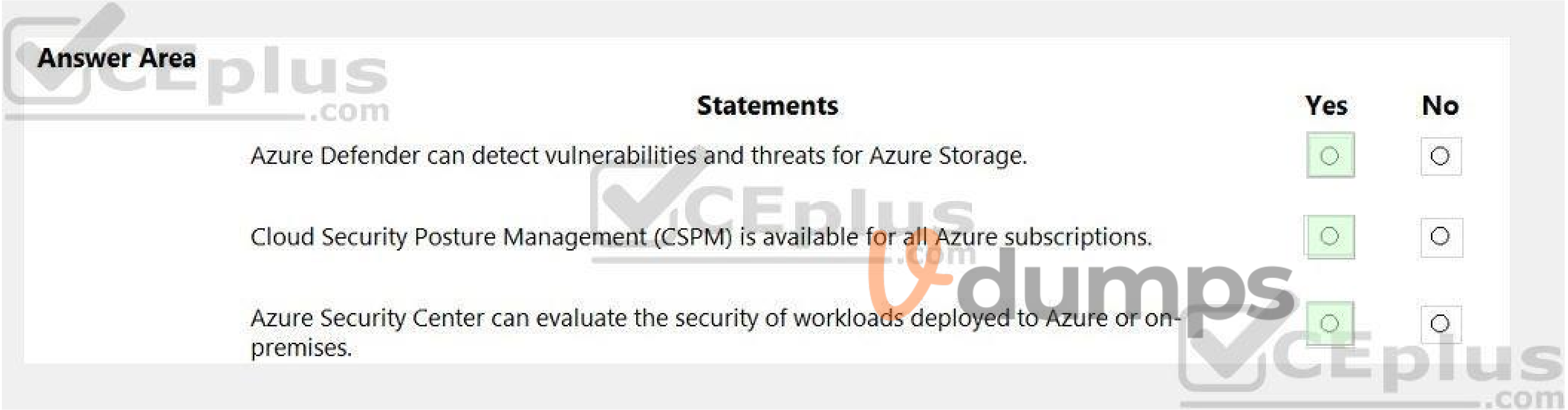
Hot Area:



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

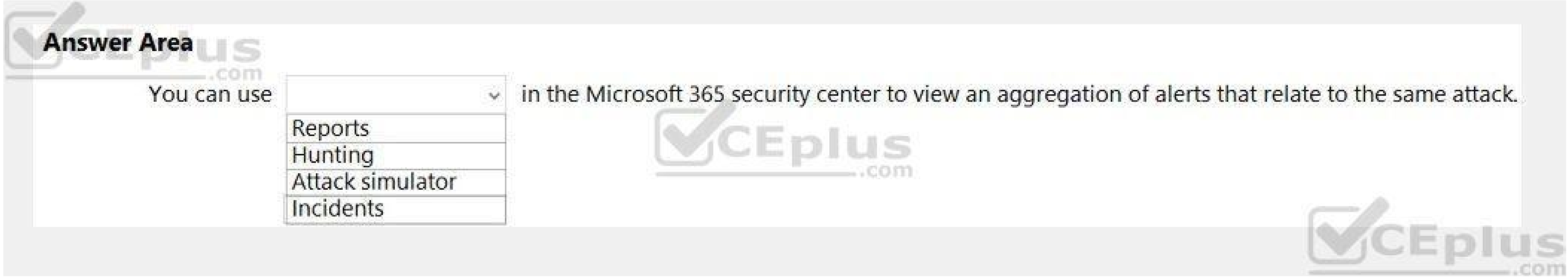
https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction

QUESTION 31

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

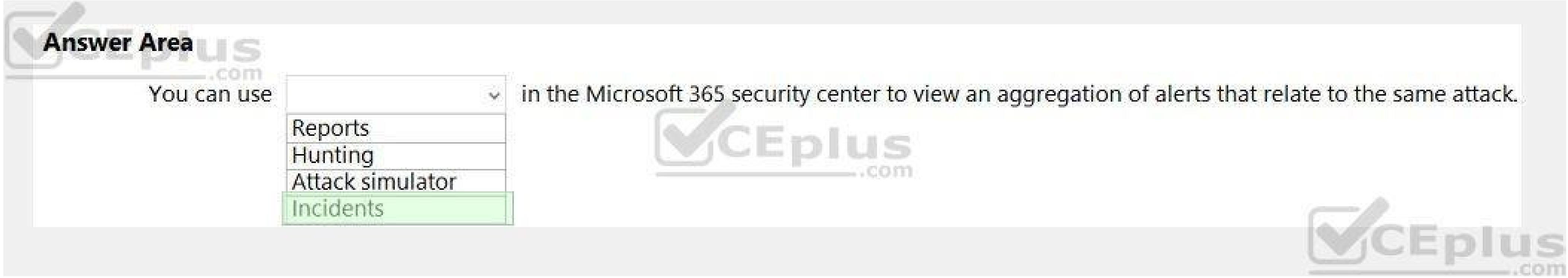


Answer Area

You can use [dropdown] 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 [dropdown] 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

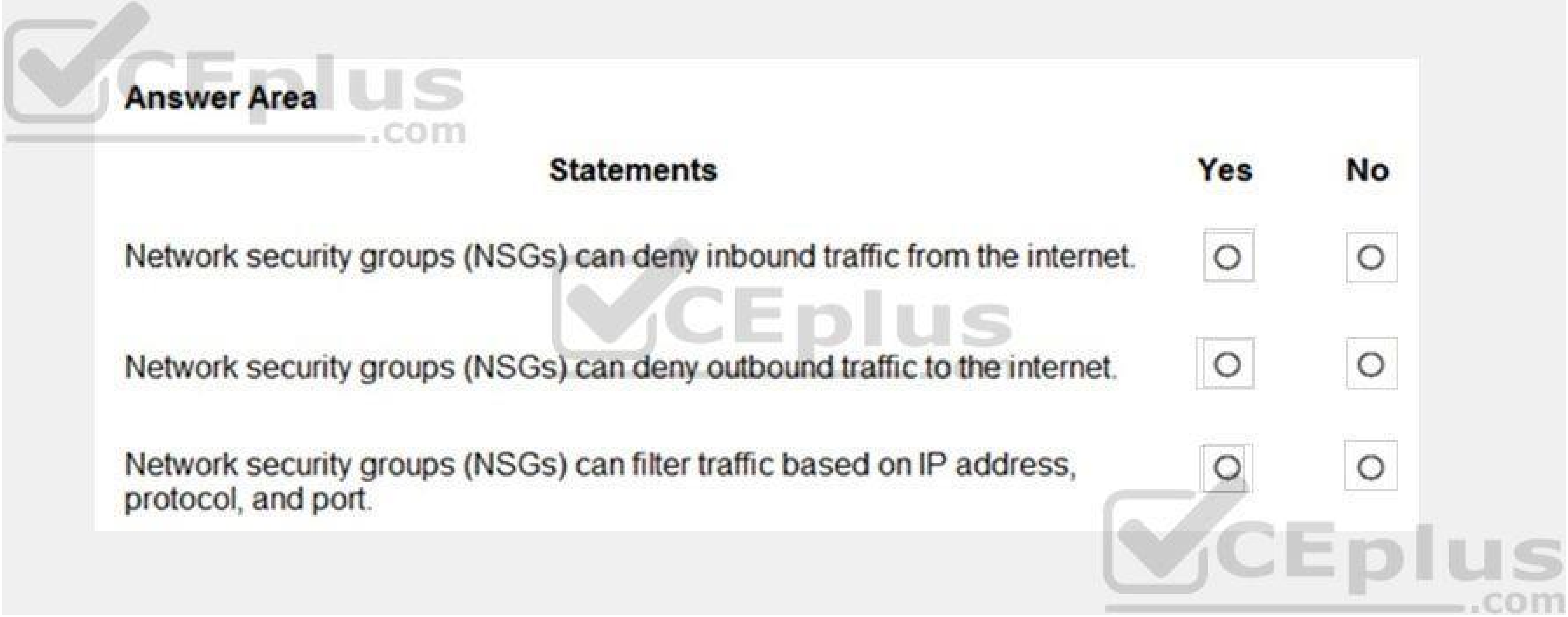
QUESTION 32

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.

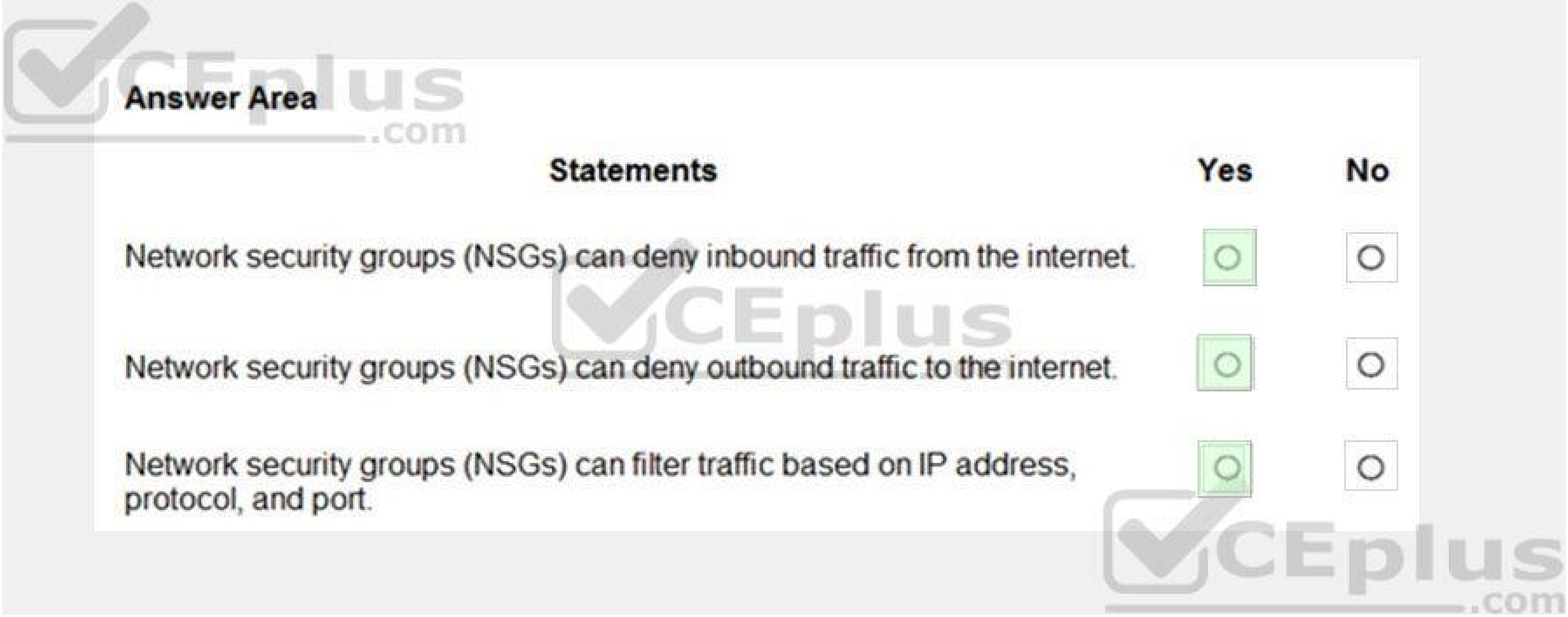
Hot Area:



Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	○	○
Network security groups (NSGs) can deny outbound traffic to the internet.	○	○
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	[✓ ○]	○
Network security groups (NSGs) can deny outbound traffic to the internet.	[✓ ○]	○
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	[✓ ○]	○

Section:

Explanation:

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

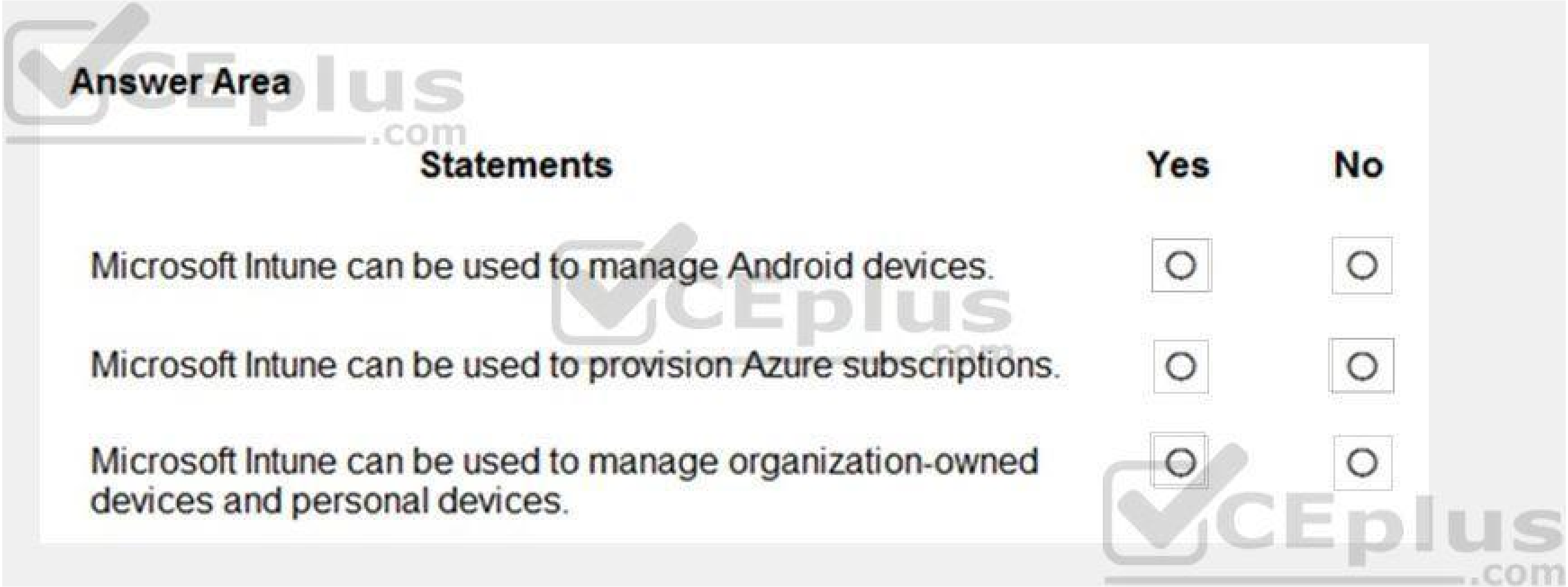
QUESTION 33

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.

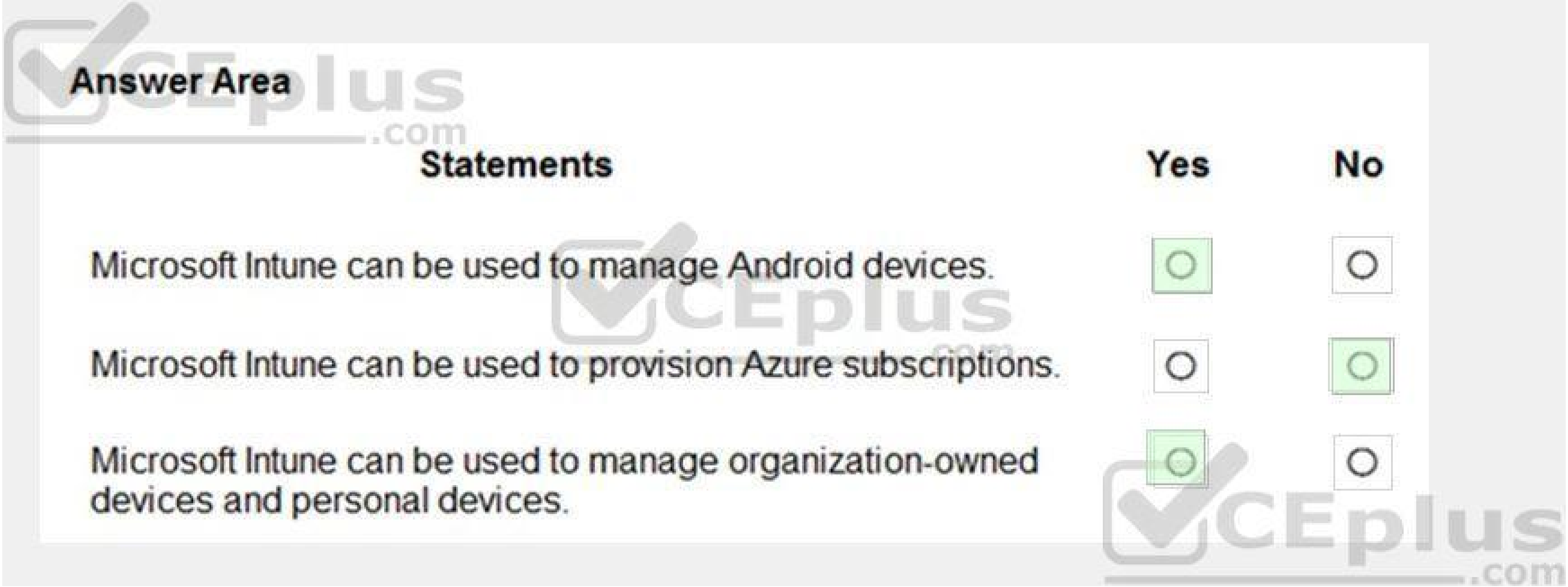
Hot Area:



Answer Area

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

Answer Area:



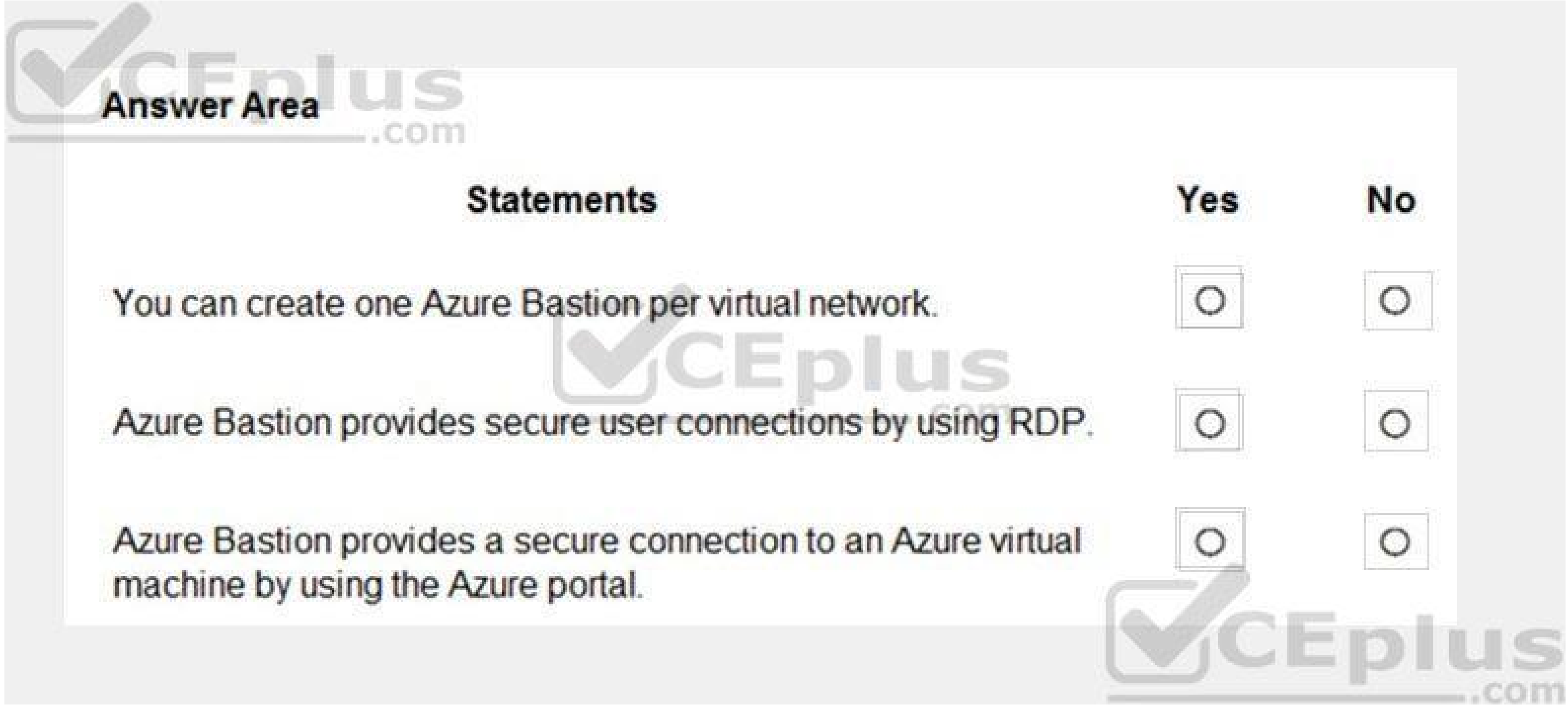
Answer Area

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	[✓ ○]	○
Microsoft Intune can be used to provision Azure subscriptions.	○	[✓ ○]
Microsoft Intune can be used to manage organization-owned devices and personal devices.	[✓ ○]	○

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management

QUESTION 34
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.

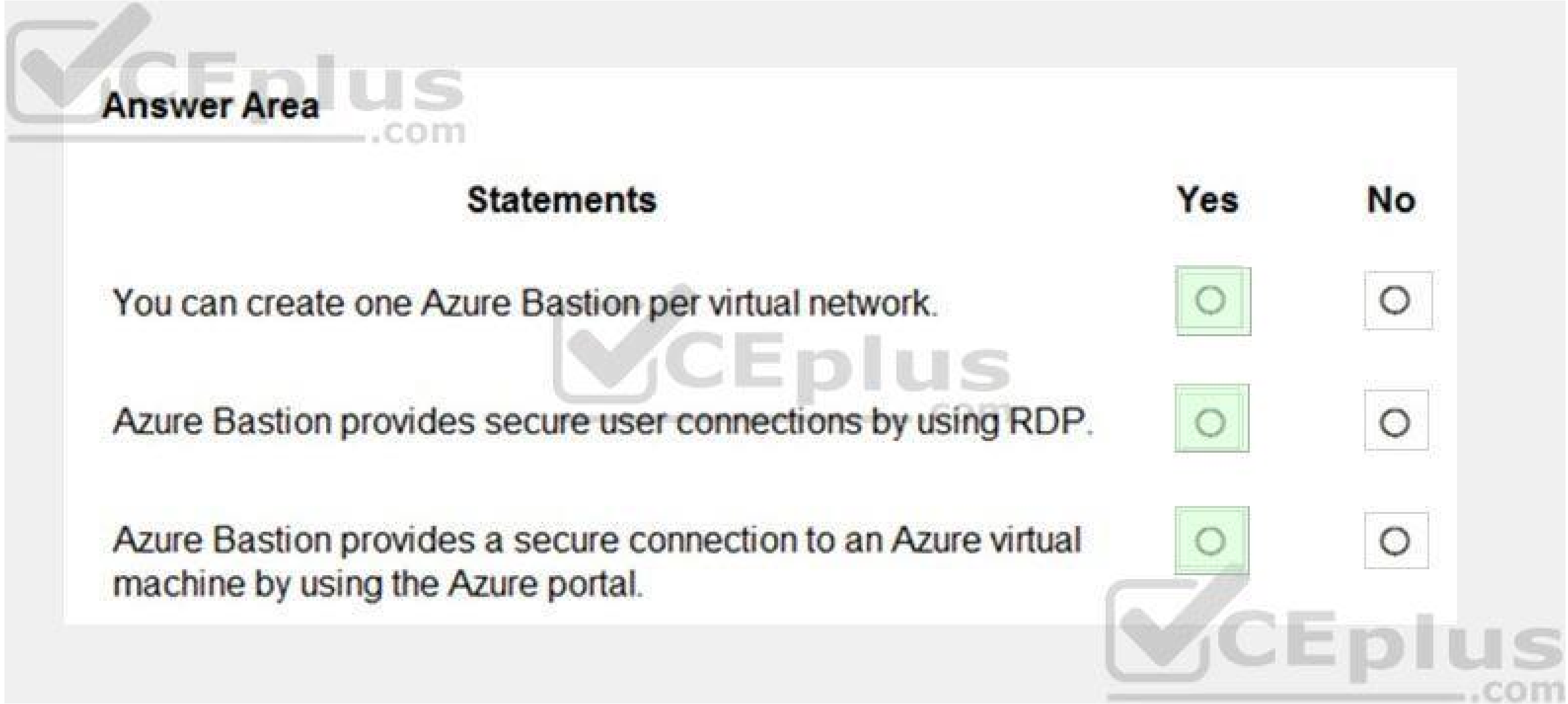
Hot Area:



Answer Area

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

Answer Area:



Answer Area

Statements	Yes	No
You can create one Azure Bastion per virtual network.	[✓ ○]	○
Azure Bastion provides secure user connections by using RDP.	[✓ ○]	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	[✓ ○]	○

Section:

Explanation:

Reference:

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

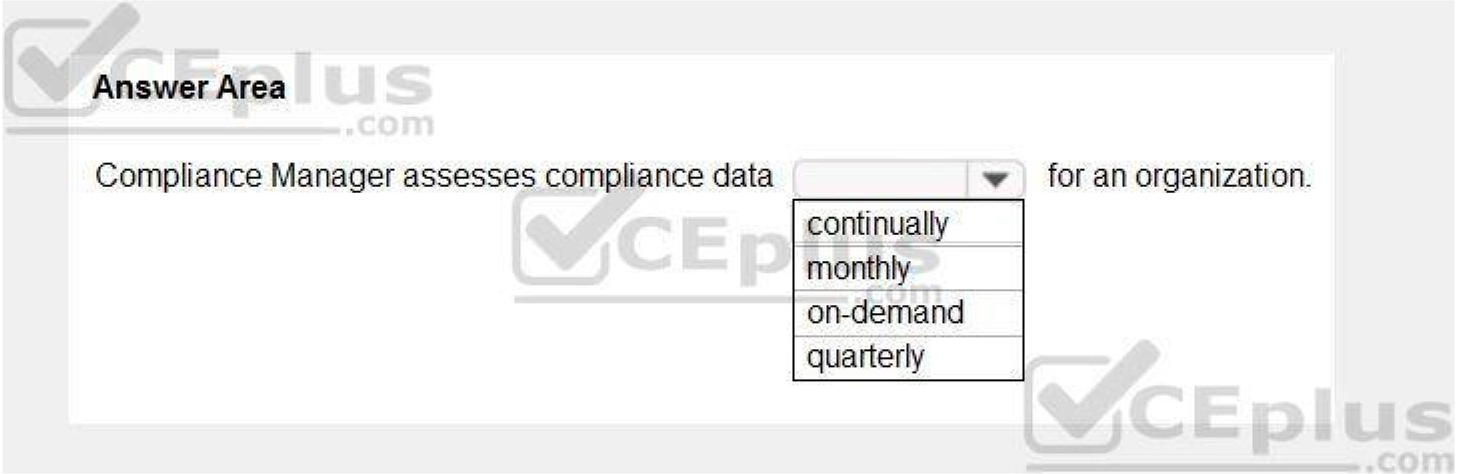
https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal

QUESTION 35

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

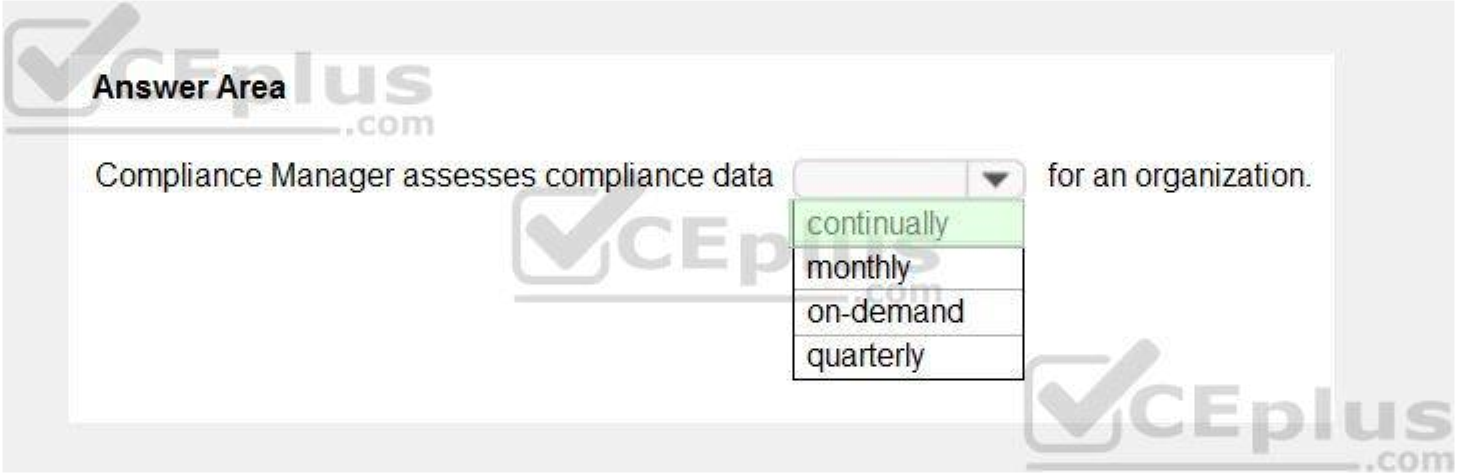


Answer Area

Compliance Manager assesses compliance data [▼] for an organization.

- continually
- monthly
- on-demand
- quarterly

Answer Area:



Answer Area

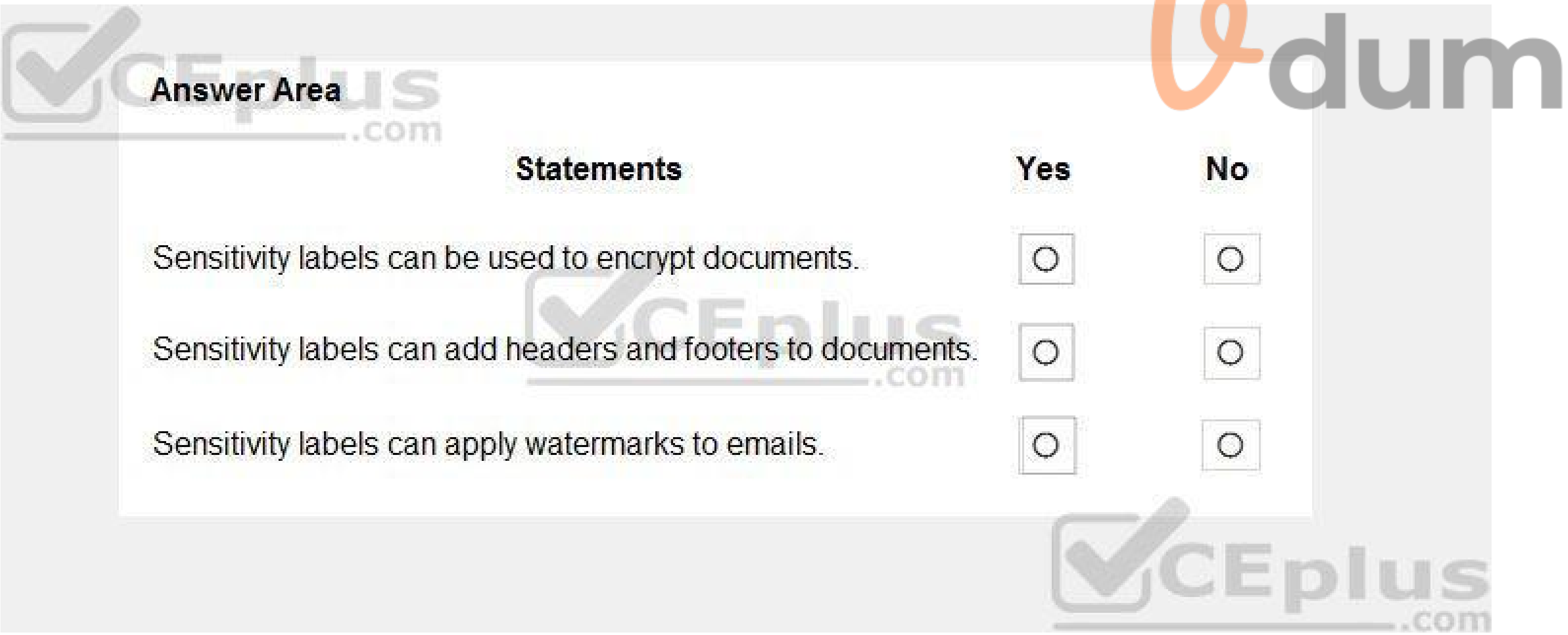
Compliance Manager assesses compliance data [continually ▾] for an organization.

- continually
- monthly
- on-demand
- quarterly

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#how-compliance-manager-continuously-assesses-controls

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.

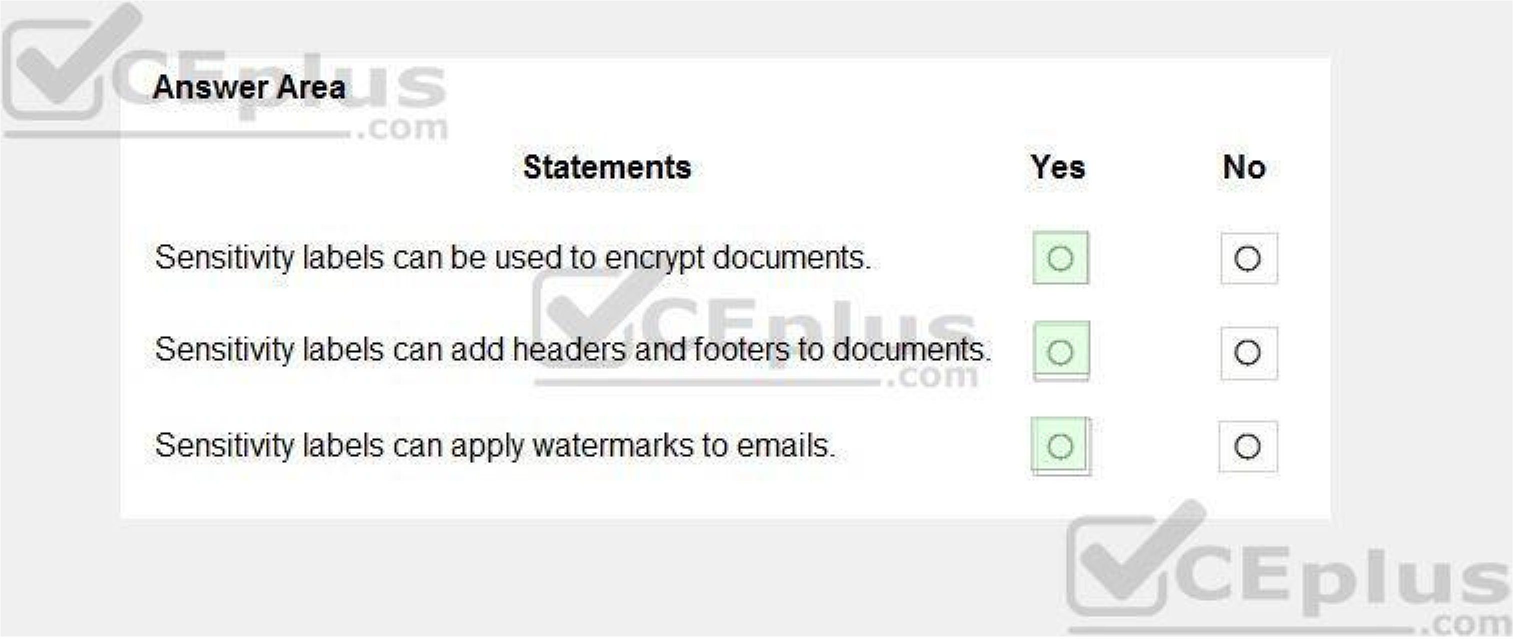
Hot Area:



Answer Area

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	○	○
Sensitivity labels can add headers and footers to documents.	○	○
Sensitivity labels can apply watermarks to emails.	○	○

Answer Area:



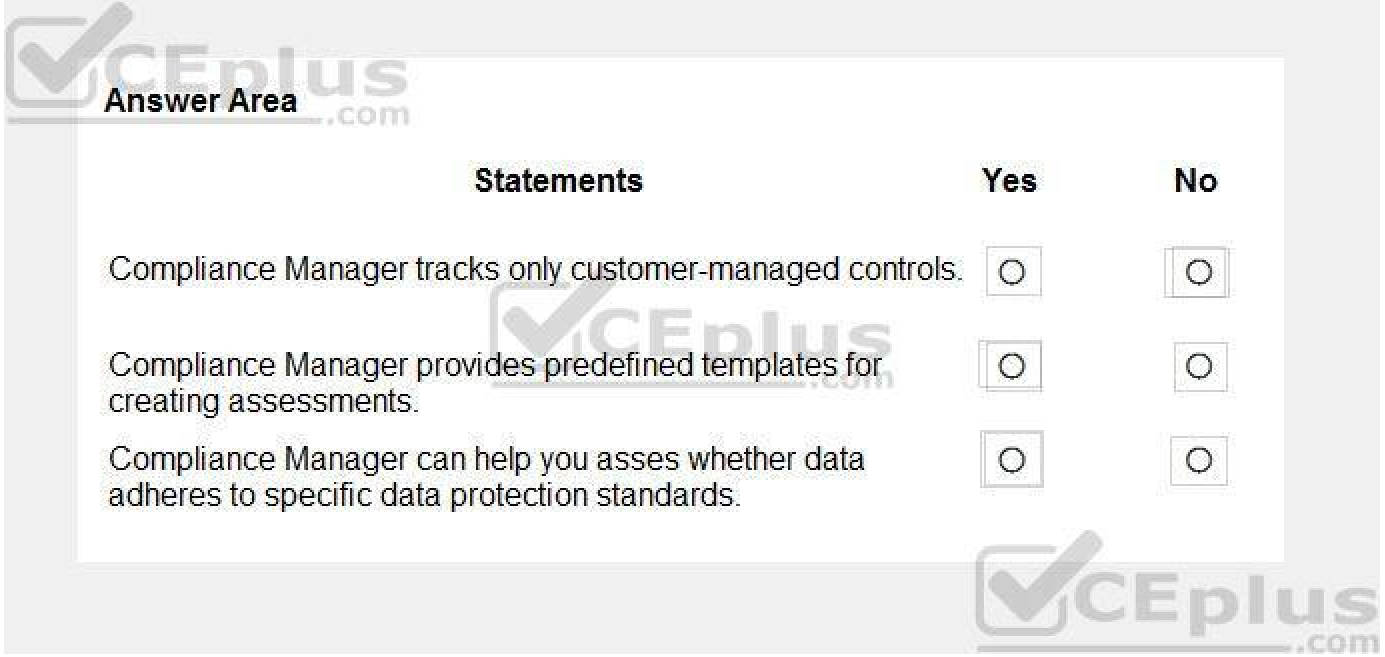
Answer Area

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	[✓ ○]	○
Sensitivity labels can add headers and footers to documents.	[✓ ○]	○
Sensitivity labels can apply watermarks to emails.	[✓ ○]	○

Section:
Explanation:
Box 1: Yes
You can use sensitivity labels to provide protection settings that include encryption of emails and documents to prevent unauthorized people from accessing this data.
Box 2: Yes
You can use sensitivity labels to mark the content when you use Office apps, by adding watermarks, headers, or footers to documents that have the label applied. Box 3: Yes
You can use sensitivity labels to mark the content when you use Office apps, by adding headers, or footers to email that have the label applied.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

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.

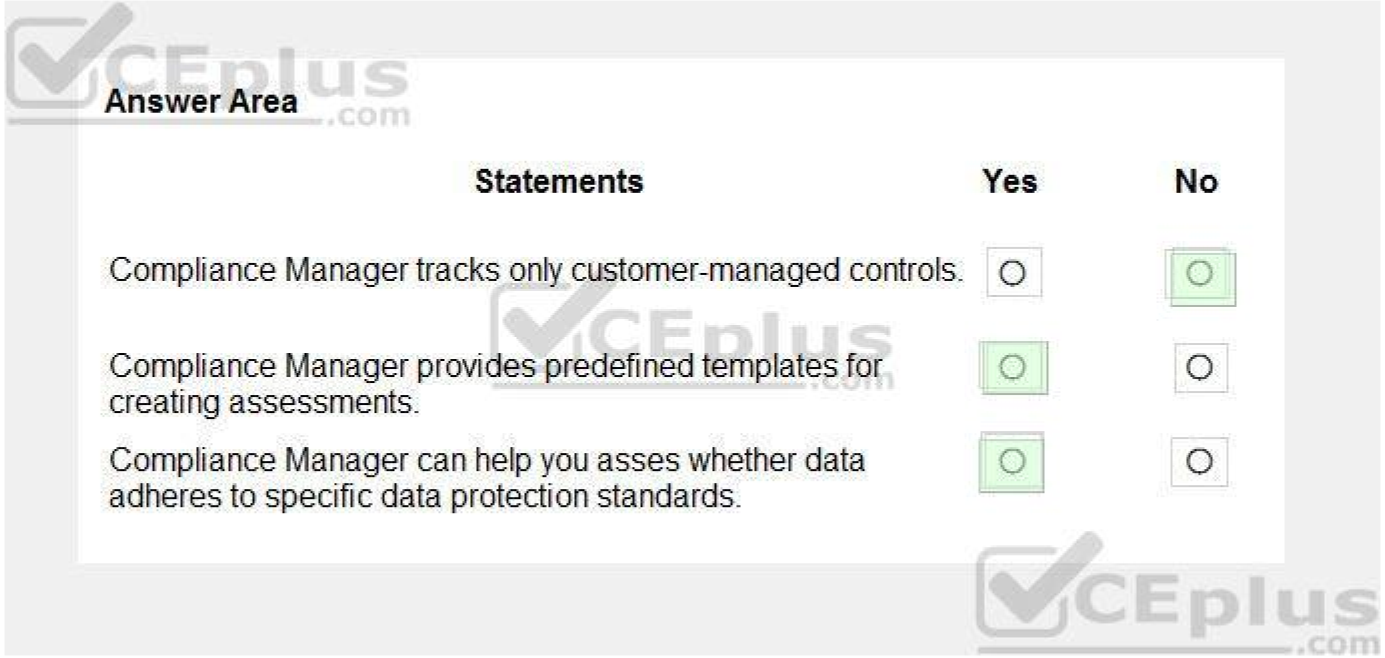
Hot Area:



Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	○	○
Compliance Manager provides predefined templates for creating assessments.	○	○
Compliance Manager can help you asses whether data adheres to specific data protection standards.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	○	[✓ ○]
Compliance Manager provides predefined templates for creating assessments.	[✓ ○]	○
Compliance Manager can help you asses whether data adheres to specific data protection standards.	[✓ ○]	○

Section:

Explanation:

Box 1: No

Compliance Manager tracks Microsoft managed controls, customer-managed controls, and shared controls.

Box 2: Yes

Box 3: Yes

Reference:

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

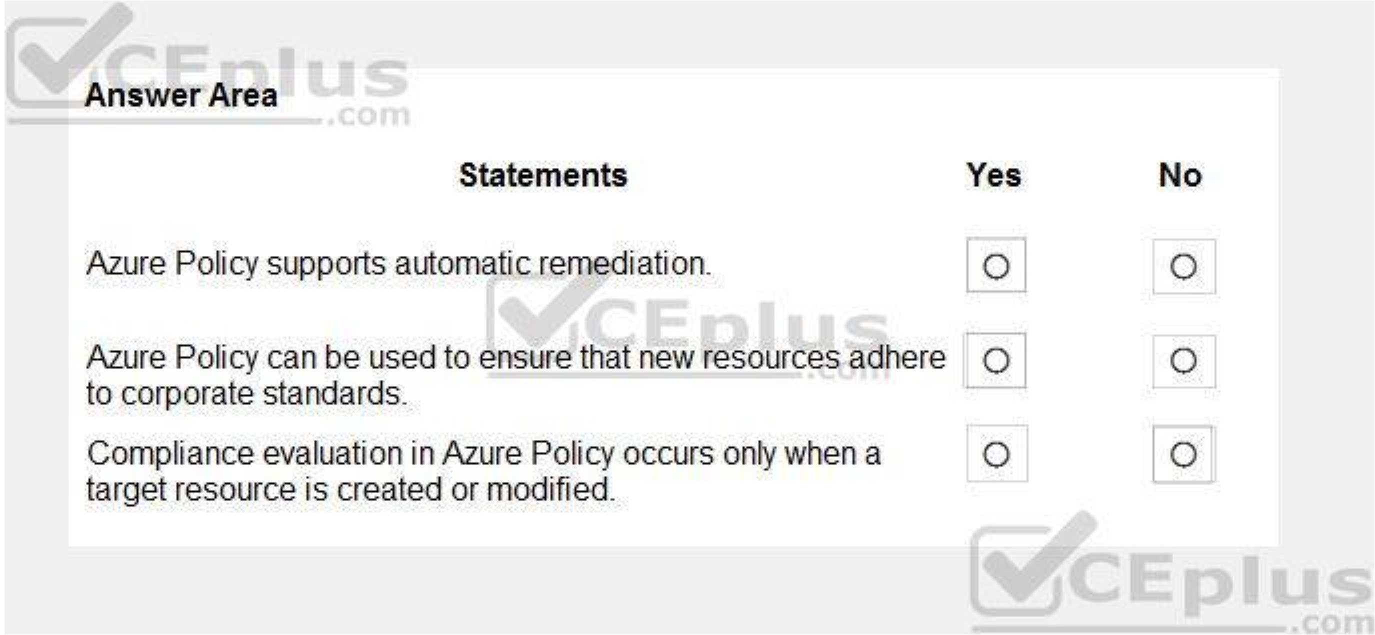
QUESTION 38

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.

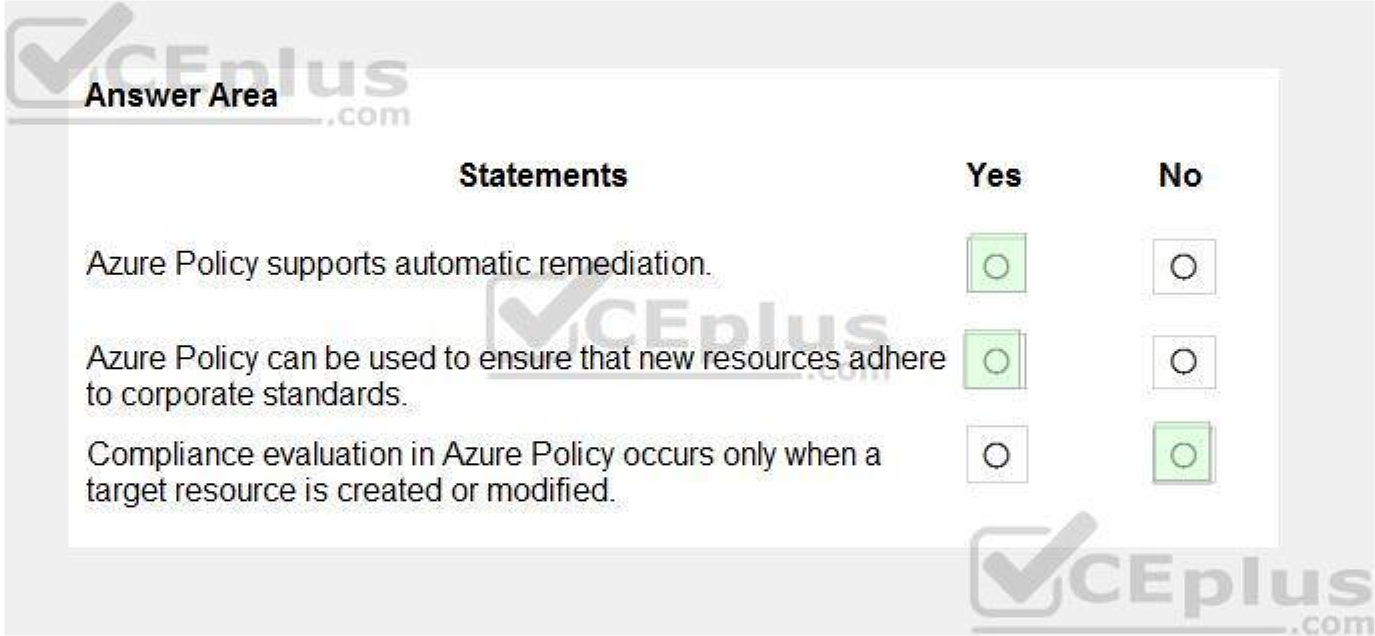
Hot Area:



Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	○	○
Azure Policy can be used to ensure that new resources adhere to corporate standards.	○	○
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	○	○

Answer Area:



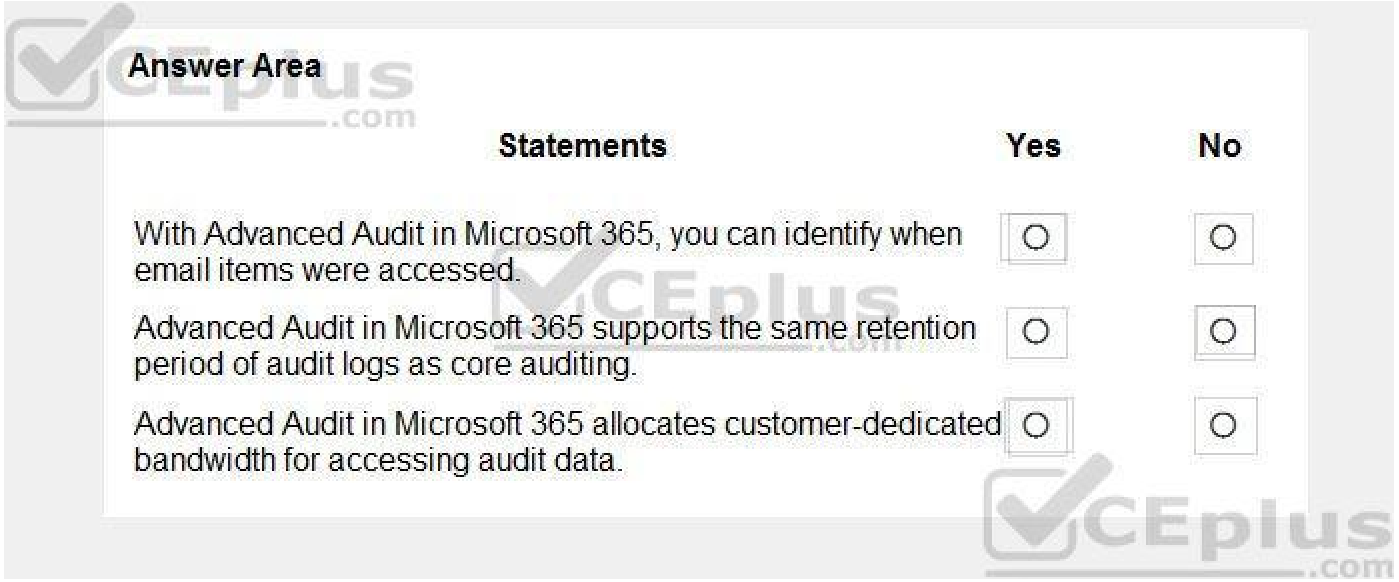
Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	[✓ ○]	○
Azure Policy can be used to ensure that new resources adhere to corporate standards.	[✓ ○]	○
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	○	[✓ ○]

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 39
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.

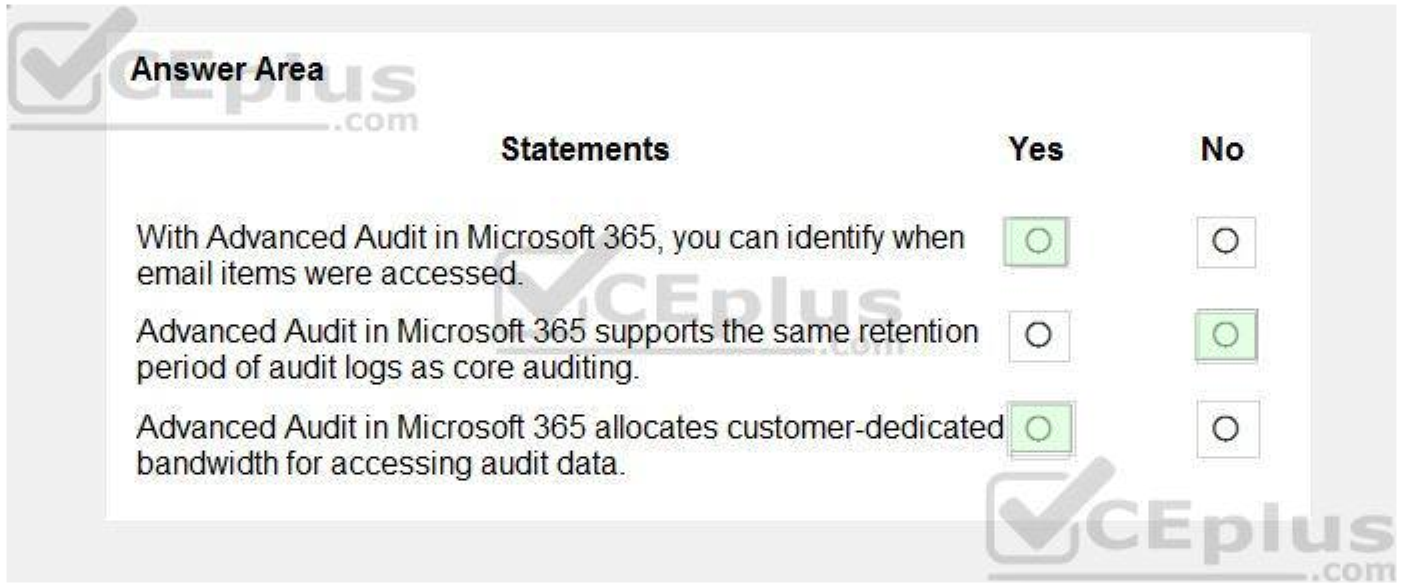
Hot Area:



Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	○	○
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	○	○
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	○	○

Answer Area:



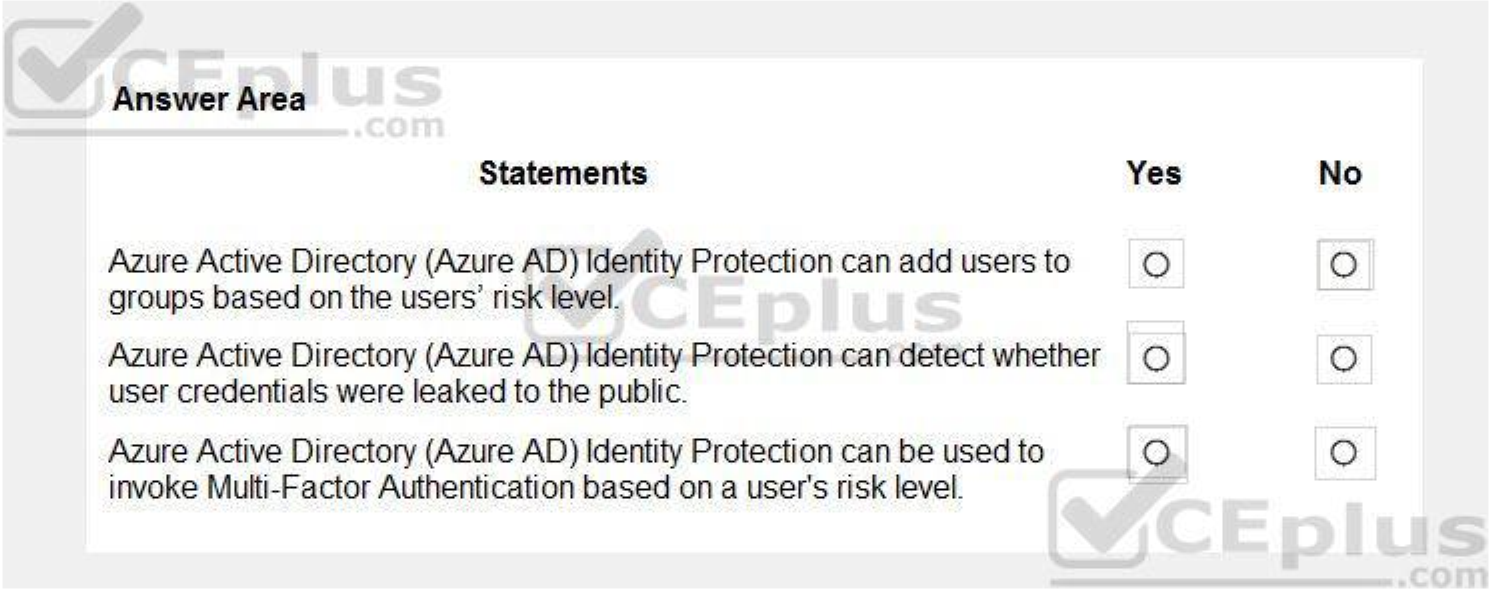
Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	[✓ ○]	○
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	○	[✓ ○]
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	[✓ ○]	○

Section:
Explanation:
Box 1: Yes
The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients.
Box 2: No
Basic Audit retains audit records for 90 days.
Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint, or AzureActiveDirectory for the Workload property (which indicates the service in which the activity occurred) for one year.
Box 3: yes
Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-solutions-overview?view=o365-worldwide#licensing-requirements
https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#advanced-audit

QUESTION 40
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.

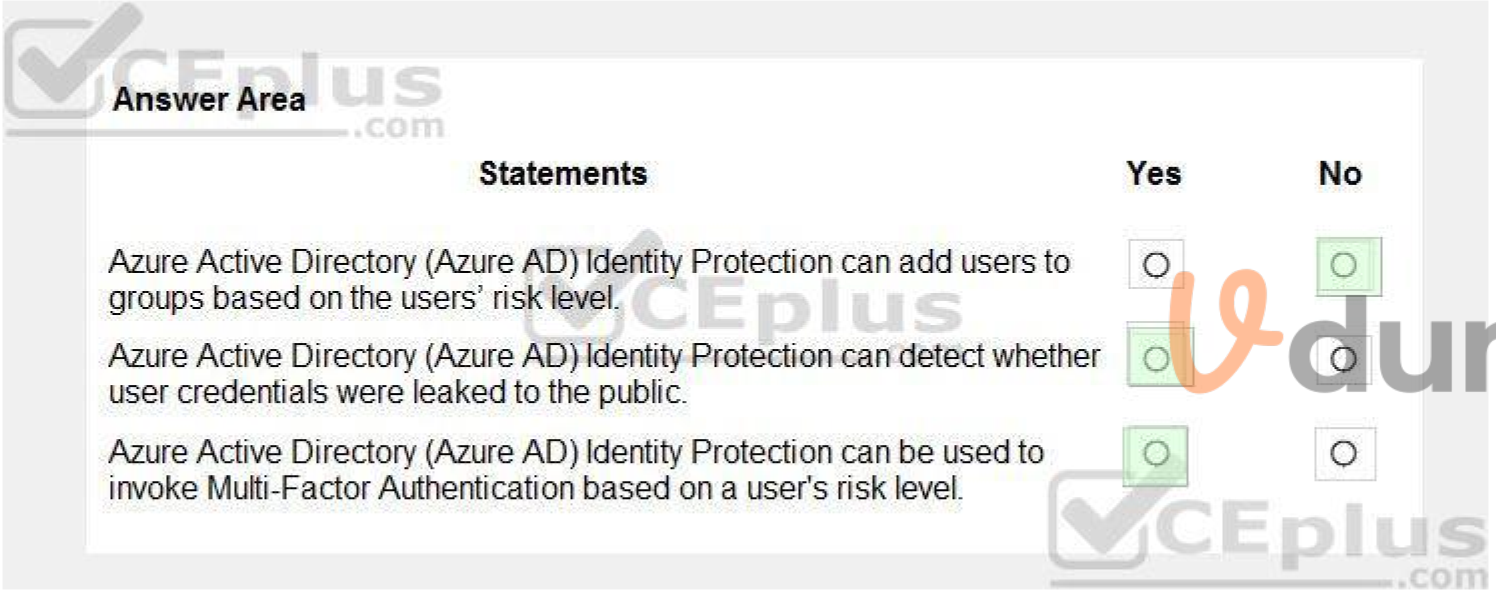
Hot Area:



Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	○	○
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	○	○
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	○	[✓ ○]
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	[✓ ○]	○
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	[✓ ○]	○

Section:
Explanation:
Box 1: No
Box 2: Yes
Leaked Credentials indicates that the user's valid credentials have been leaked.
Box 3: Yes
Multi-Factor Authentication can be required based on conditions, one of which is user risk.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

QUESTION 41

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?

A. Microsoft Secure Score
B. Productivity Score
C. Secure score in Azure Security Center

D. Compliance score

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

QUESTION 42
What do you use to provide real-time integration between Azure Sentinel and another security source?

A. Azure AD Connect
B. a Log Analytics workspace
C. Azure Information Protection
D. a data connector

Correct Answer: D
Section:
Explanation:
To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App Security, etc.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/overview

QUESTION 43
Which Microsoft portal provides information about how Microsoft cloud services comply with regulatory standard, such as International Organization for Standardization (ISO)?

A. the Microsoft Endpoint Manager admin center
B. Azure Cost Management + Billing
C. Microsoft Service Trust Portal
D. the Azure Active Directory admin center

Correct Answer: C
Section:
Explanation:
The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

QUESTION 44
In the shared responsibility model for an Azure deployment, what is Microsoft solely responsible for managing?

A. the management of mobile devices
B. the permissions for the user data stored in Azure
C. the creation and management of user accounts
D. the management of the physical hardware

Correct Answer: D
Section:

QUESTION 45
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 46
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:

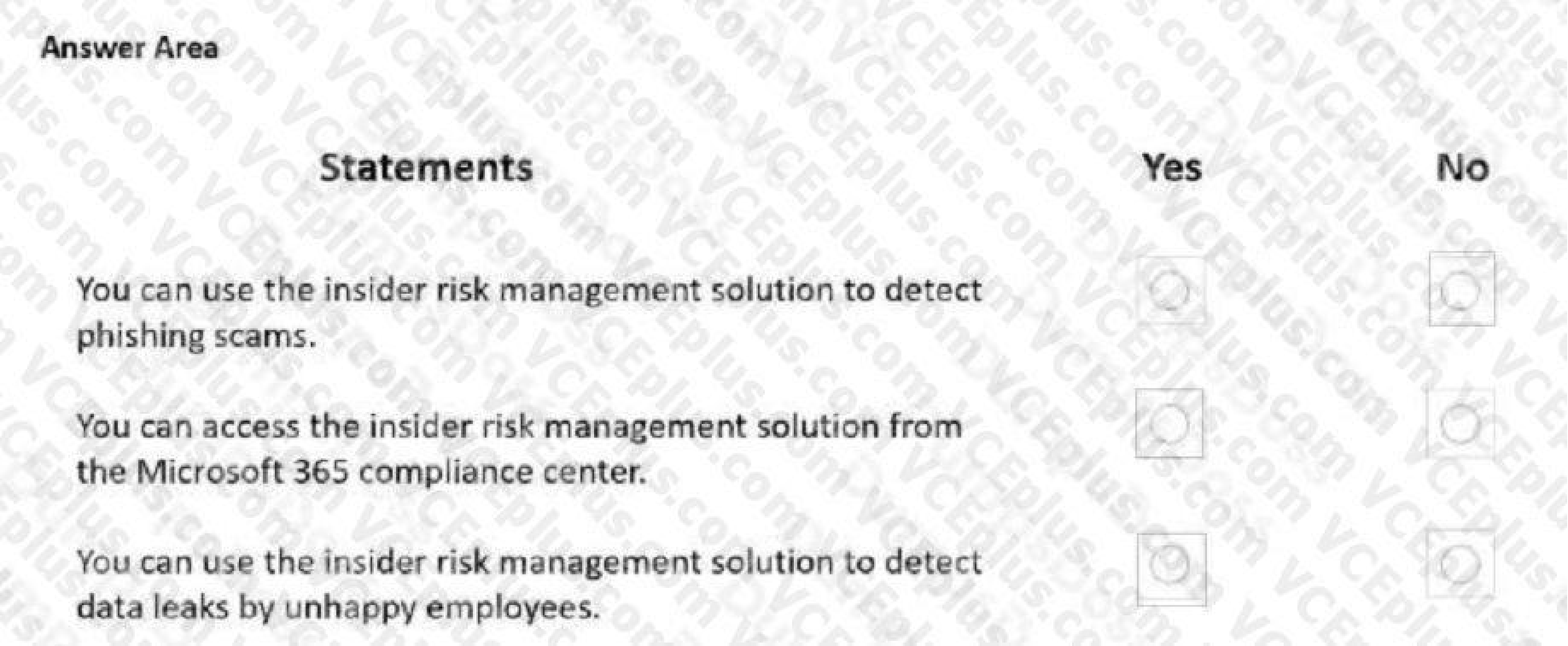
QUESTION 47
To which type of resource can Azure Bastion provide secure access?

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 48
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.

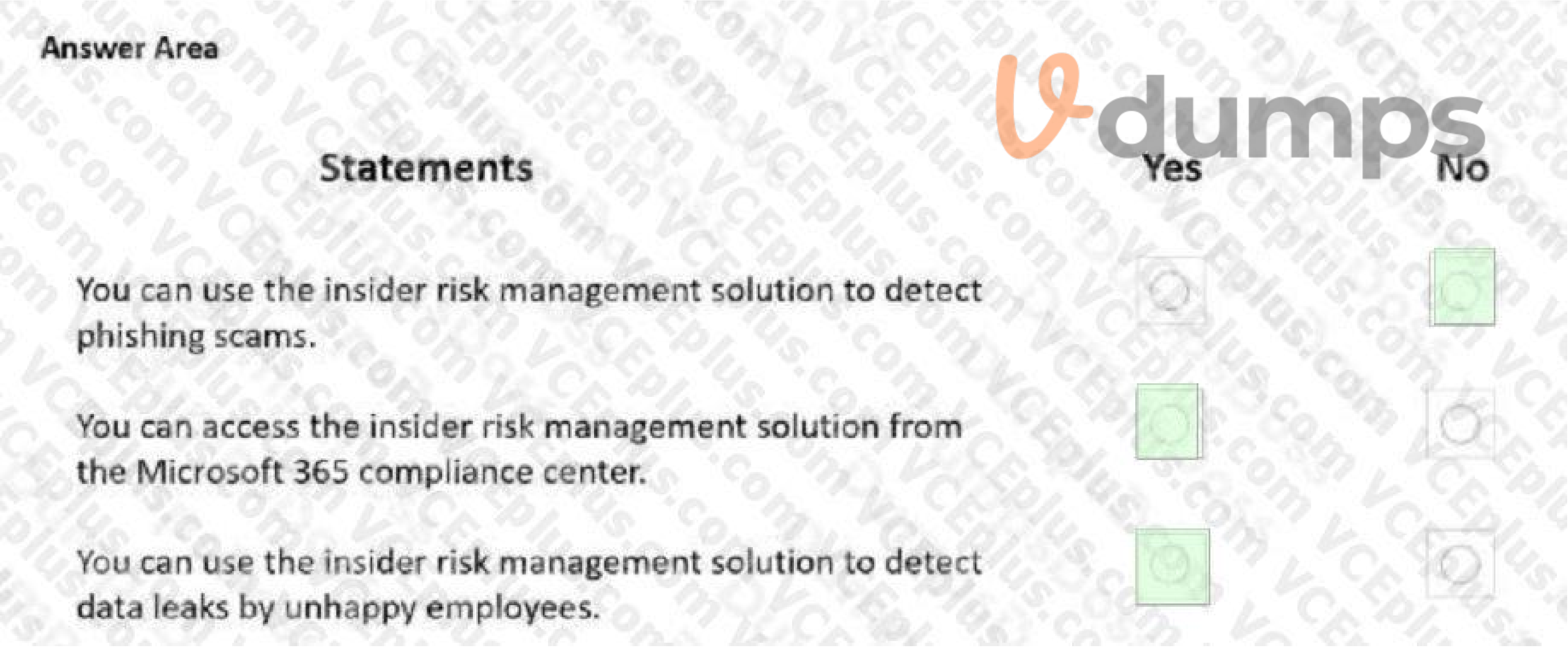
Hot Area:



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 49
What is an assessment in Compliance Manager?

A. A grouping of controls from a specific regulation, standard or policy.
B. Recommended guidance to help organizations align with their corporate standards.
C. A dictionary of words that are not allowed in company documents.
D. A policy initiative that includes multiple policies.

Correct Answer: A
Section:
Explanation:

QUESTION 50
You need to create a data loss prevention (DLP) policy. What should you use?

A. the Microsoft 365 admin center
B. the Microsoft Endpoint Manager admin center
C. the Microsoft 365 Defender portal
D. the Microsoft 365 Compliance center

Correct Answer: A
Section:

QUESTION 51
What are customers responsible for when evaluating security in a software as a service (SaaS) cloud services model?

A. applications
B. network controls
C. operating systems
D. accounts and identities

Correct Answer: A
Section:
Explanation:

QUESTION 52
Which compliance feature should you use to identify documents that are employee resumes?

A. pre-trained classifiers
B. Content explorer
C. Activity explorer
D. eDiscovery

Correct Answer: A
Section:

QUESTION 53
Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. phone call
B. text message (SMS)
C. email verification
D. Microsoft Authenticator app
E. security question

Correct Answer: A, B, D
Section:

QUESTION 54
What should you use to ensure that the members of an Azure Active Directory group use multi-factor authentication (MFA) when they sign in?

A. Azure Active Directory (Azure AD) Identity Protection
B. a conditional access policy
C. Azure role-based access control (Azure RBAC)
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Correct Answer: B
Section:
Explanation:
The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.

QUESTION 55
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 56
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 57
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 58
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:

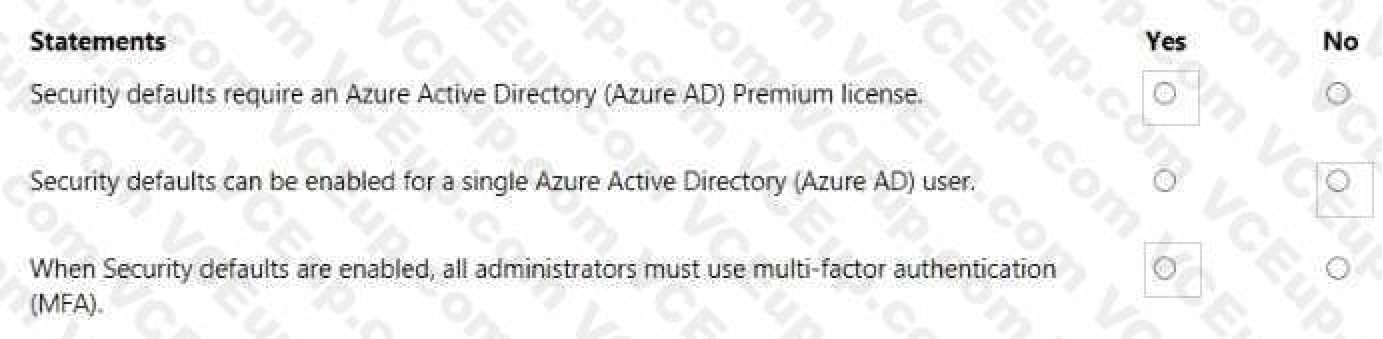
QUESTION 59
What is a characteristic of a sensitivity label in Microsoft 365?

A. persistent
B. encrypted
C. restricted to predefined categories

Correct Answer: B
Section:

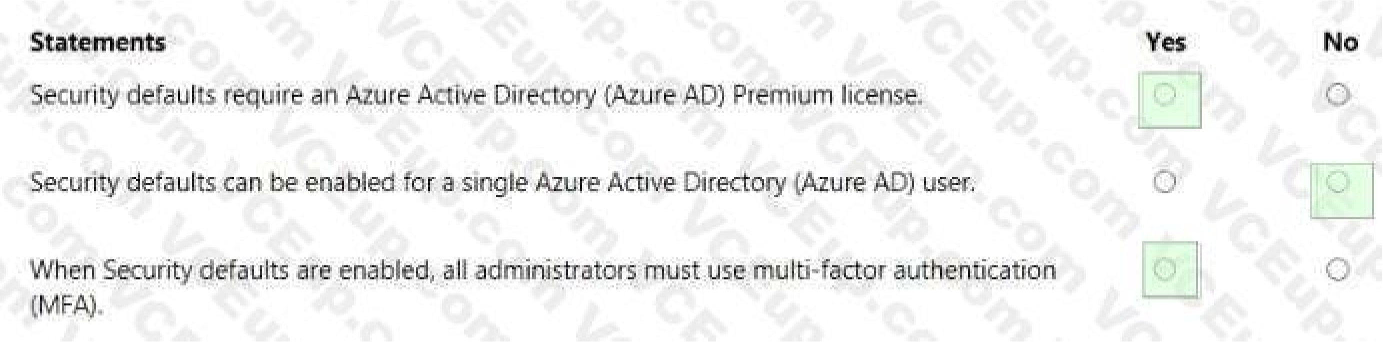
QUESTION 60
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point

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:

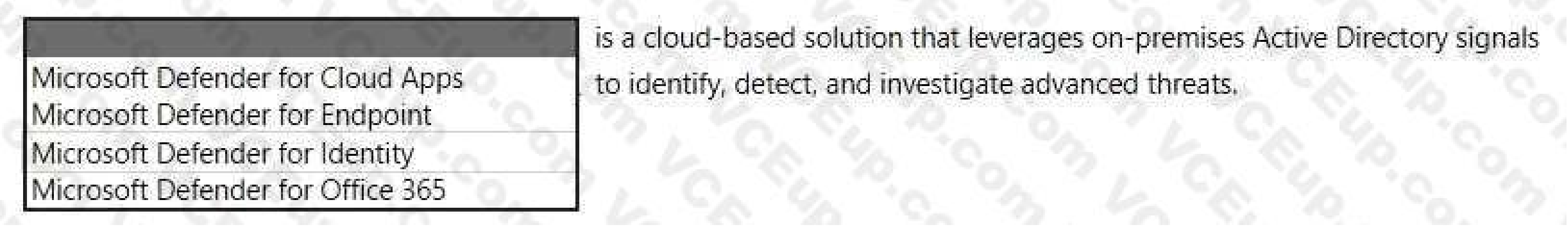
Explanation:

QUESTION 61

HOTSPOT

Select the answer that correctly completes the sentence.

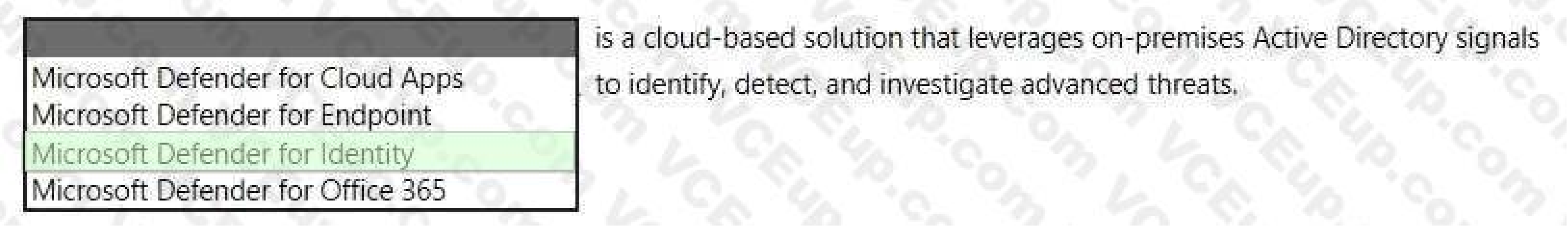
Hot Area:



- 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 62

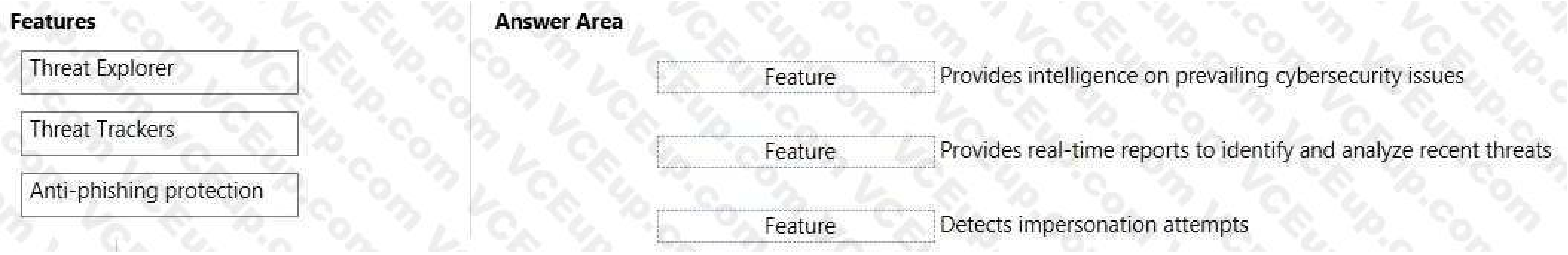
DRAG DROP

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

Threat Explorer

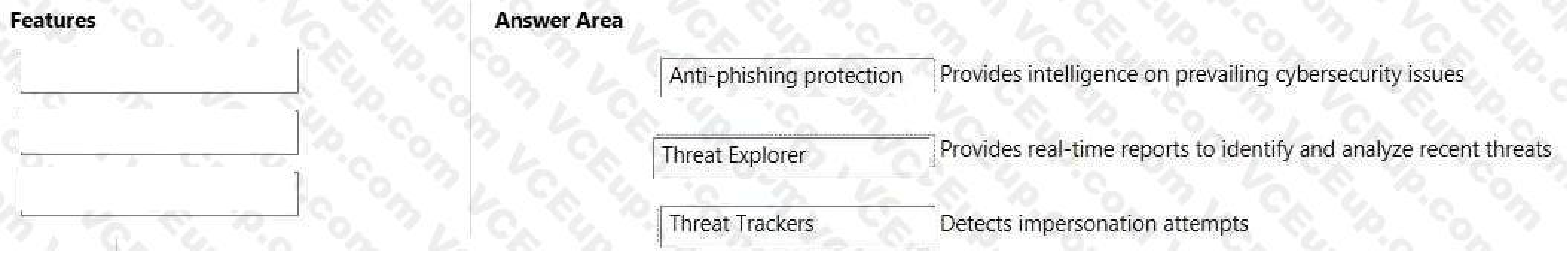
Threat Trackers

Anti-phishing protection

Answer Area

Feature	Provides intelligence on prevailing cybersecurity issues
Feature	Provides real-time reports to identify and analyze recent threats
Feature	Detects impersonation attempts

Correct Answer:



Features

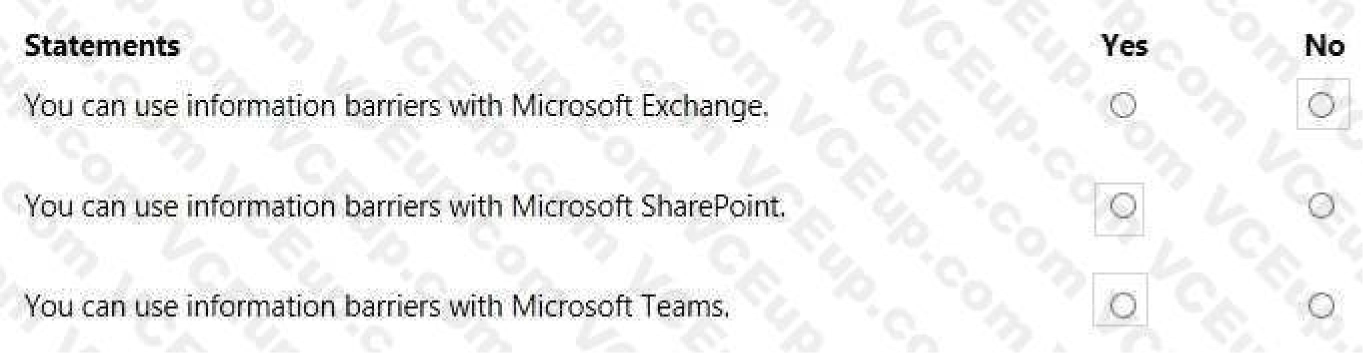
Answer Area

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:

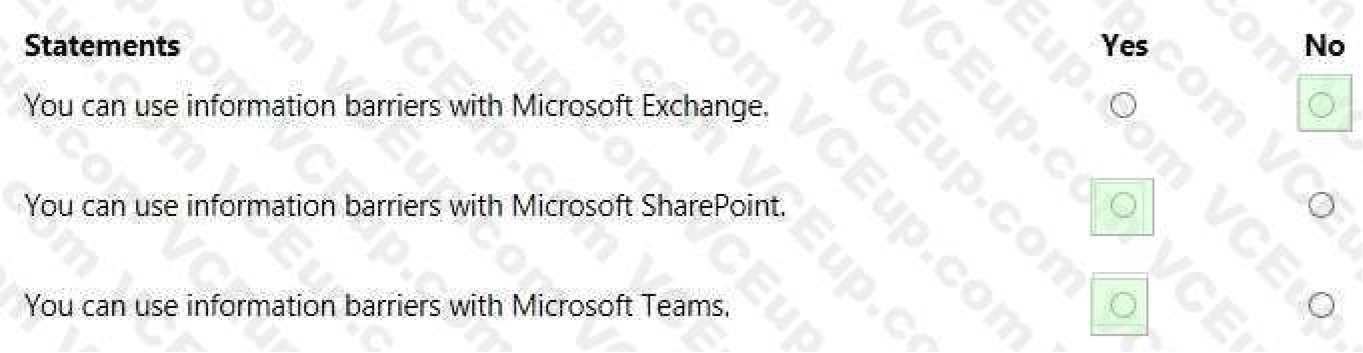
QUESTION 63
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



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:

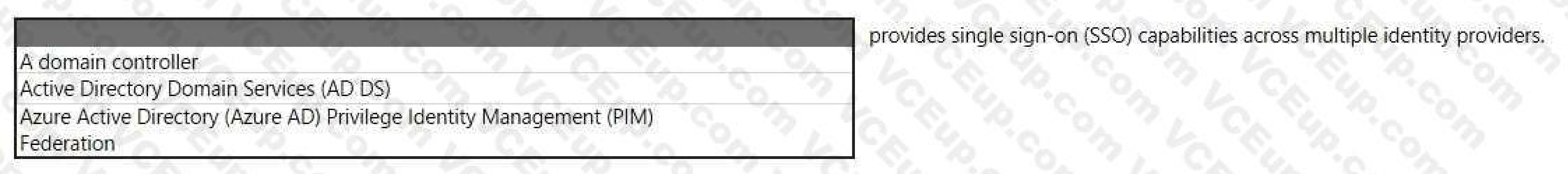


Statements	Yes	No
You can use information barriers with Microsoft Exchange.	○	[✓ ○]
You can use information barriers with Microsoft SharePoint.	[✓ ○]	○
You can use information barriers with Microsoft Teams.	[✓ ○]	○

Section:
Explanation:

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

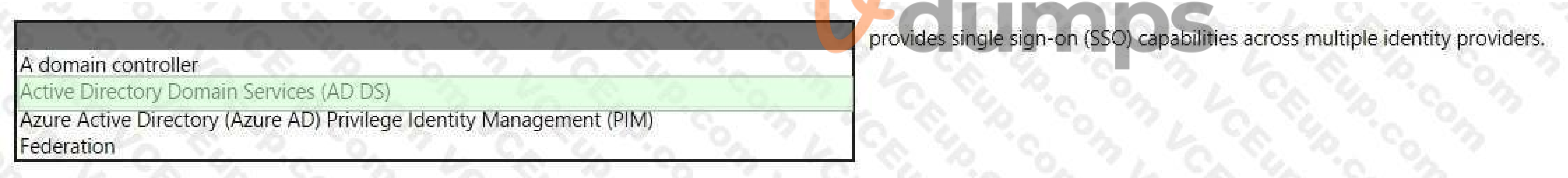
Hot Area:



- 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:



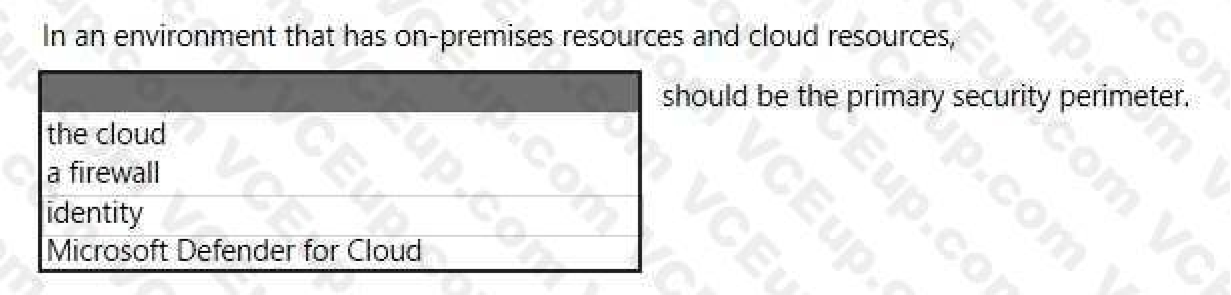
- A domain controller
- [✓ Active Directory Domain Services (AD DS)]
- Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
- Federation

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

Section:
Explanation:

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

Hot Area:

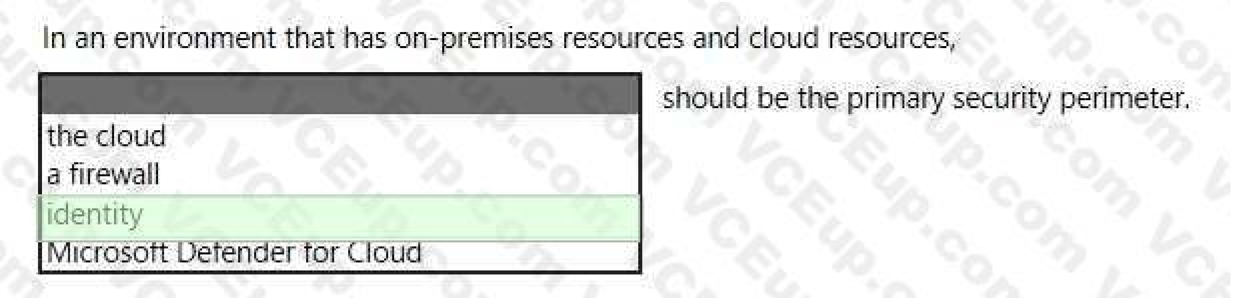


In an environment that has on-premises resources and cloud resources,

- the cloud
- a firewall
- identity
- Microsoft Defender for Cloud

should be the primary security perimeter.

Answer Area:



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

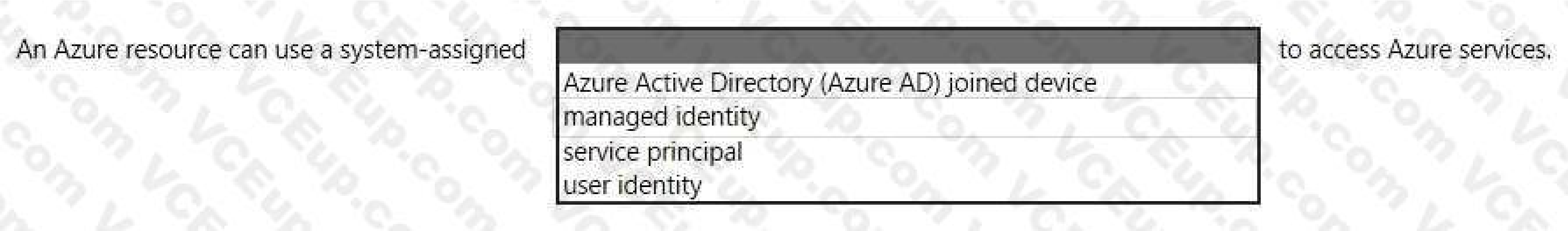
should be the primary security perimeter.

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

Section:
Explanation:

QUESTION 66
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

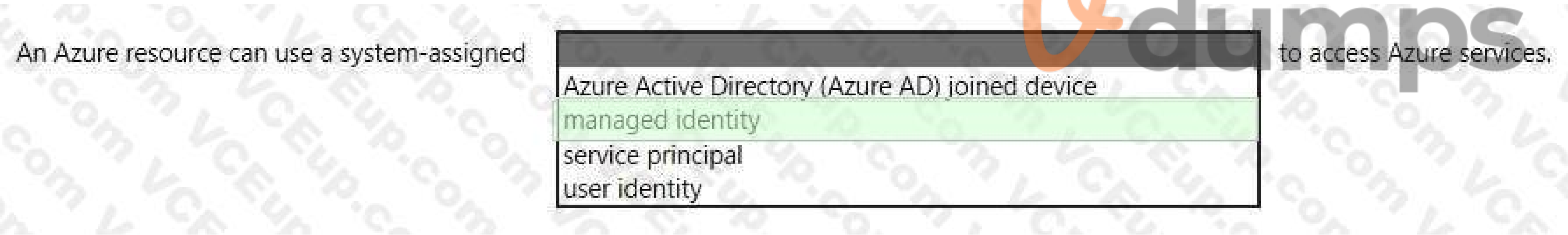


An Azure resource can use a system-assigned

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

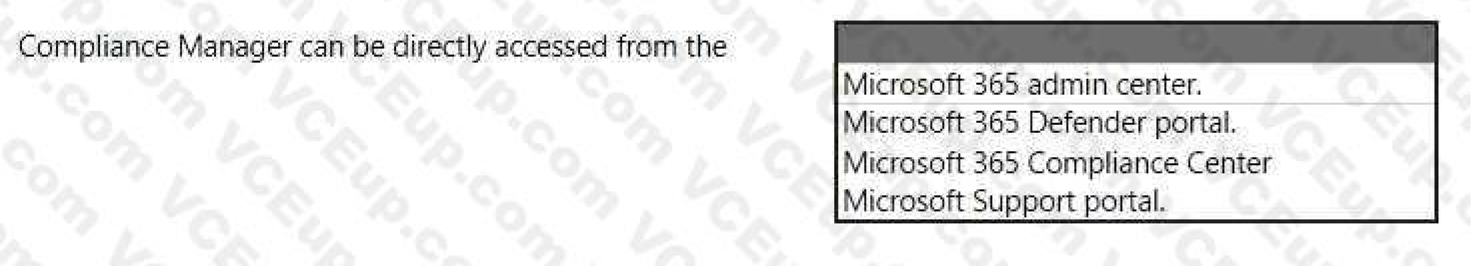
to access Azure services.

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

Section:
Explanation:

QUESTION 67
HOTSPOT
Select the answer that correctly completes the sentence.

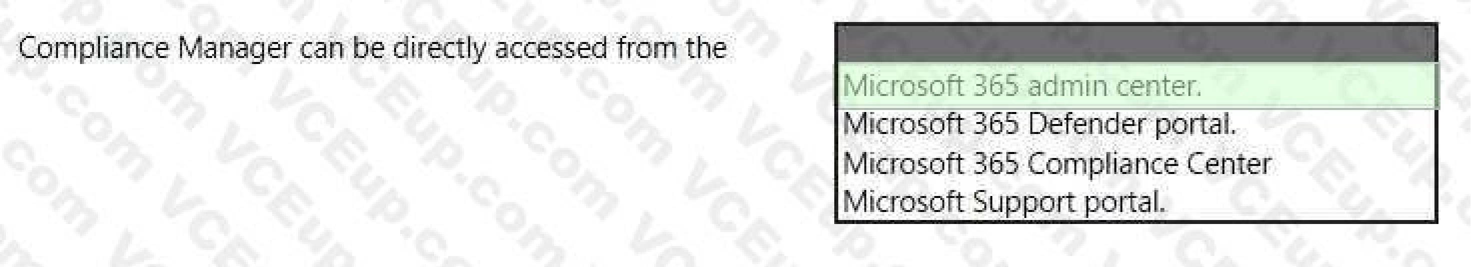
Hot Area:



Compliance Manager can be directly accessed from the

Microsoft 365 admin center.
Microsoft 365 Defender portal.
Microsoft 365 Compliance Center
Microsoft Support portal.

Answer Area:



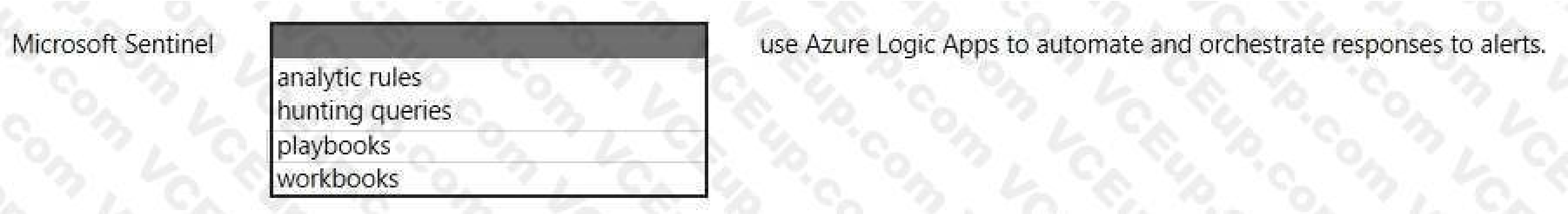
Compliance Manager can be directly accessed from the

[✓ Microsoft 365 admin center.]
Microsoft 365 Defender portal.
Microsoft 365 Compliance Center
Microsoft Support portal.

Section:
Explanation:

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

Hot Area:

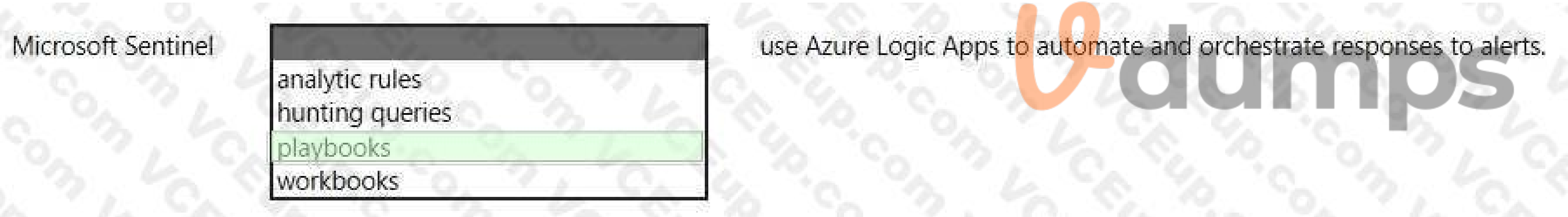


Microsoft Sentinel

analytic rules
hunting queries
playbooks
workbooks

use Azure Logic Apps to automate and orchestrate responses to alerts.

Answer Area:



Microsoft Sentinel

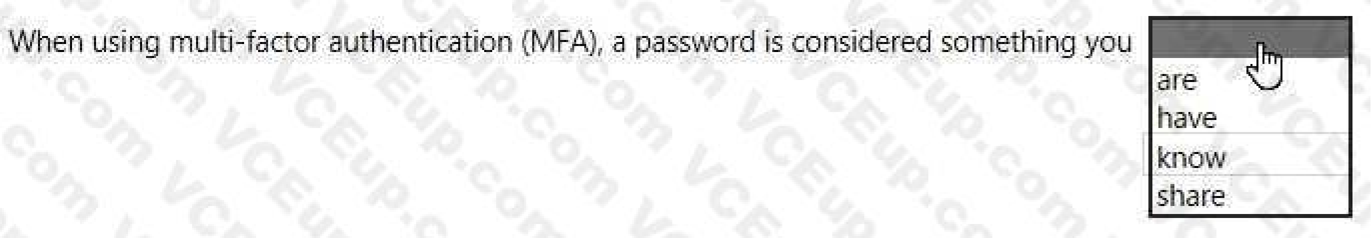
analytic rules
hunting queries
[✓ playbooks]
workbooks

use Azure Logic Apps to automate and orchestrate responses to alerts.

Section:
Explanation:

QUESTION 69
HOTSPOT
Select the answer that correctly completes the sentence.

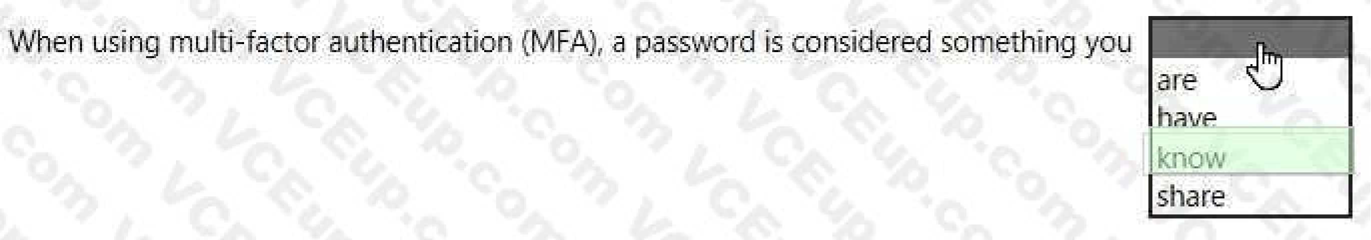
Hot Area:



When using multi-factor authentication (MFA), a password is considered something you

are
have
know
share

Answer Area:



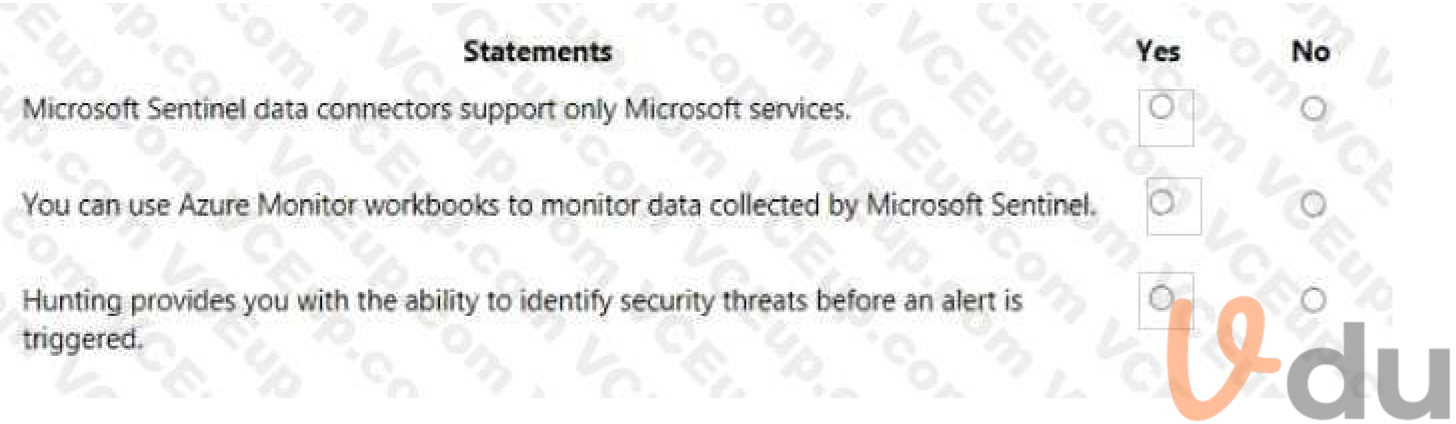
When using multi-factor authentication (MFA), a password is considered something you

- are
- have
- [✓ know]
- share

Section:
Explanation:

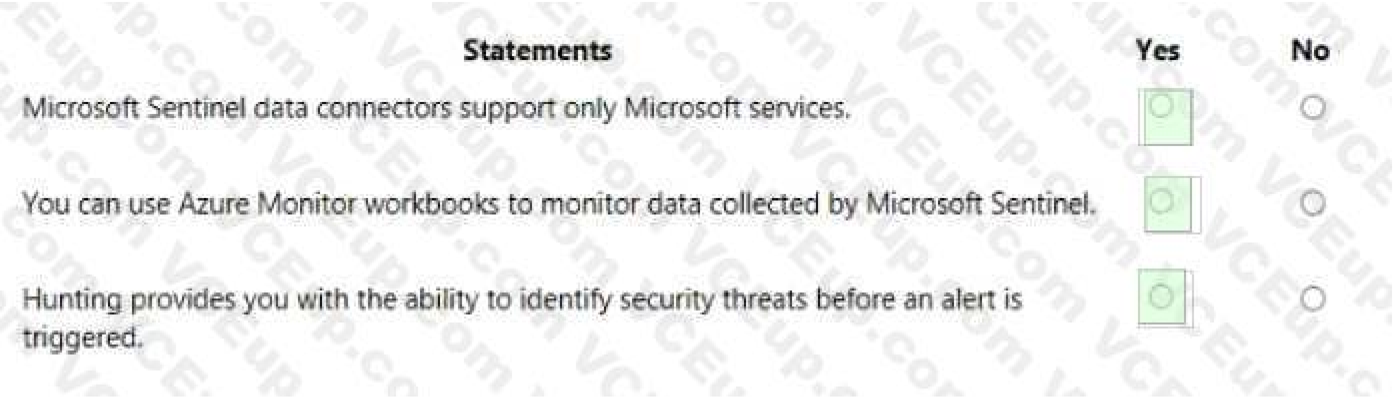
QUESTION 70
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point

Hot Area:



Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	○	○
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	○	○
Hunting provides you with the ability to identify security threats before an alert is triggered.	○	○

Answer Area:

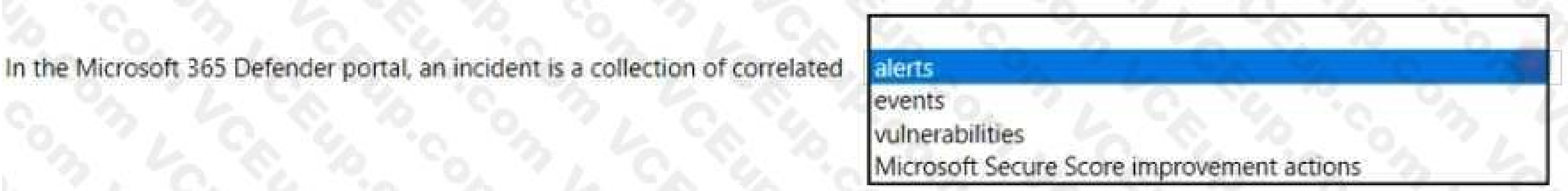


Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	[✓ ○]	○
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	[✓ ○]	○
Hunting provides you with the ability to identify security threats before an alert is triggered.	[✓ ○]	○

Section:
Explanation:

QUESTION 71
HOTSPOT
Select the answer that correctly completes the sentence.

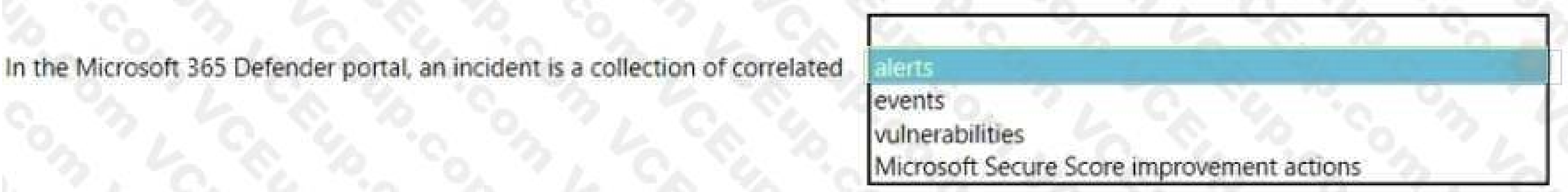
Hot Area:



In the Microsoft 365 Defender portal, an incident is a collection of correlated

- alerts
- events
- vulnerabilities
- Microsoft Secure Score improvement actions

Answer Area:



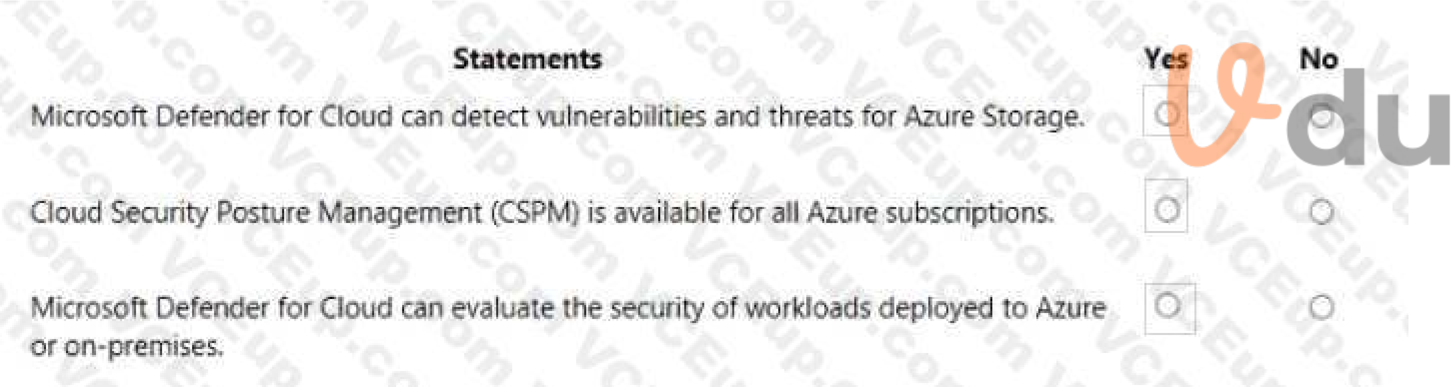
In the Microsoft 365 Defender portal, an incident is a collection of correlated

- [✓ alerts]
- events
- vulnerabilities
- Microsoft Secure Score improvement actions

Section:
Explanation:

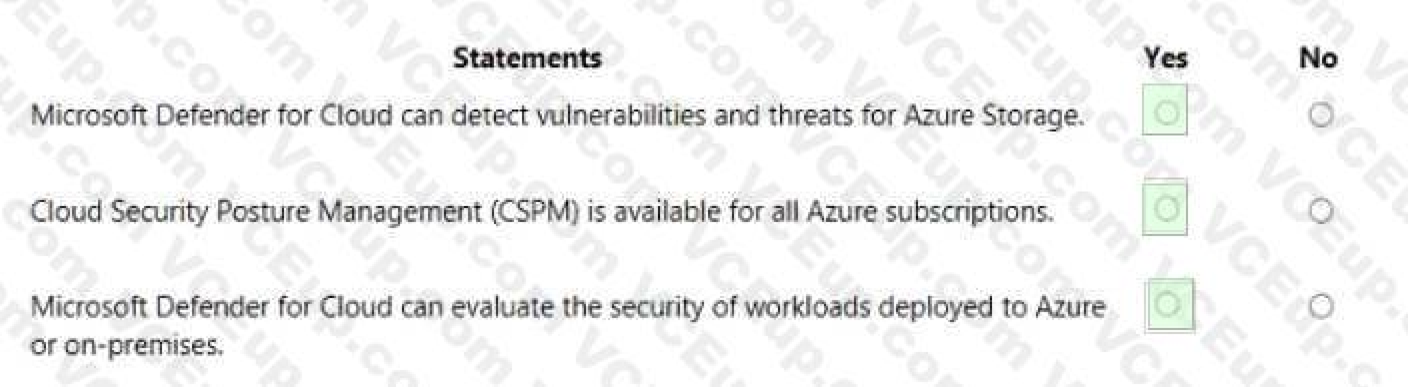
QUESTION 72
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point

Hot Area:



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

Answer Area:



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

Section:
Explanation:

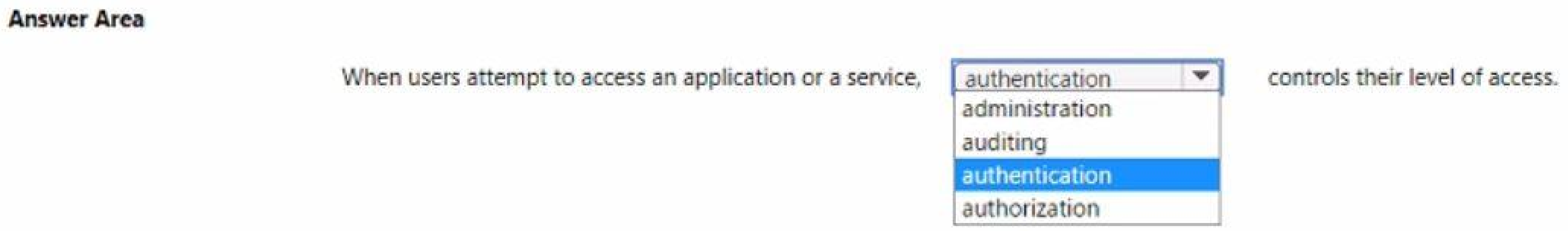
QUESTION 73
When you enable Azure AD Multi-Factor Authentication (MFA), how many factors are required for authentication?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section:

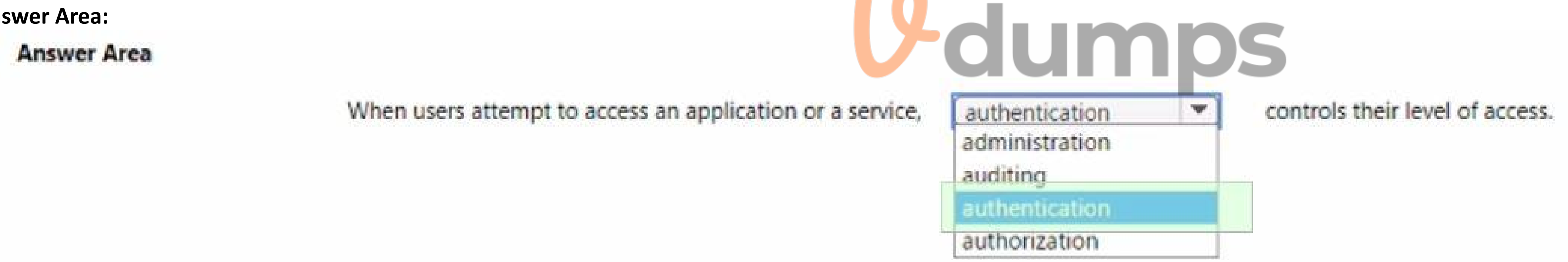
QUESTION 74
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:


Answer Area

When users attempt to access an application or a service, authentication controls their level of access.

Answer Area:


Answer Area

When users attempt to access an application or a service, authentication controls their level of access.

Section:
Explanation:

QUESTION 75
What can you use to ensure that all the users in a specific group must use multi-factor authentication (MFA) to sign in to Azure AD?

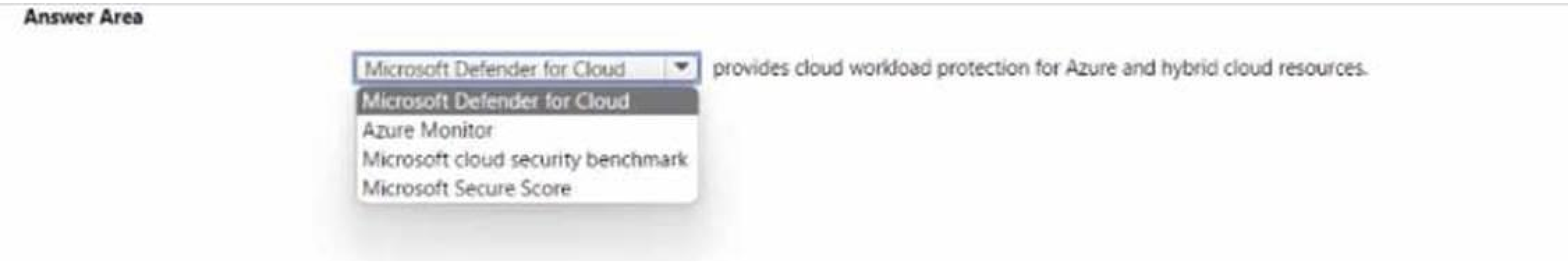
A. Azure Policy
B. a communication compliance policy
C. a Conditional Access policy
D. a user risk policy

Correct Answer: C
Section:

QUESTION 76

HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

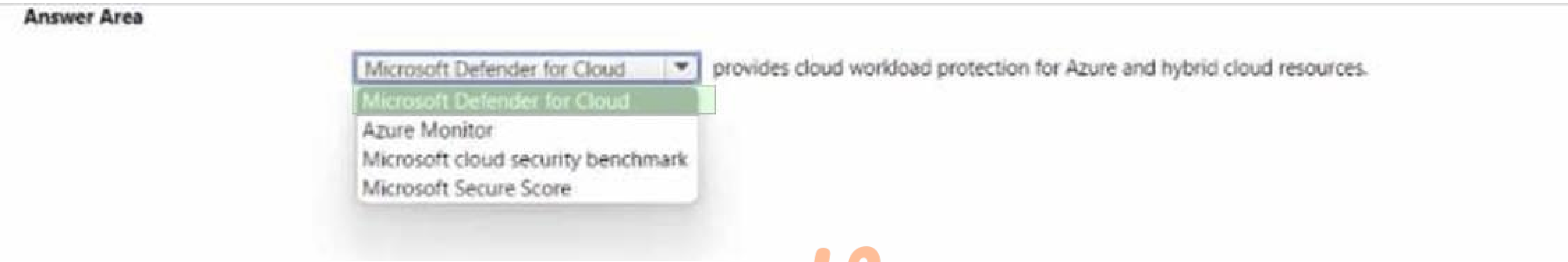


Answer Area

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

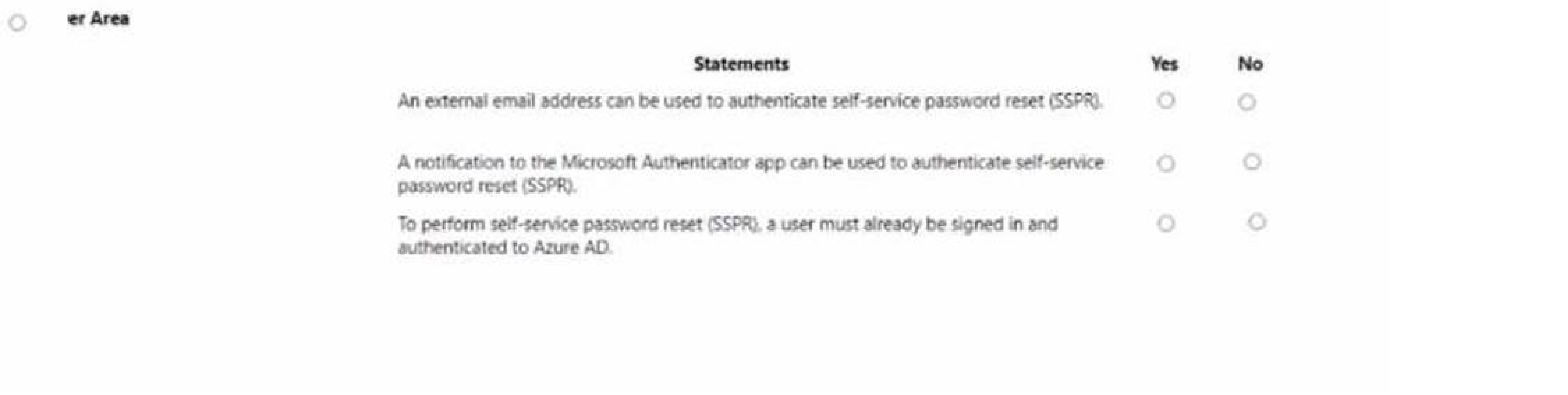
Microsoft Defender for Cloud ▼ provides cloud workload protection for Azure and hybrid cloud resources.

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

Section:
Explanation:

QUESTION 77
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.

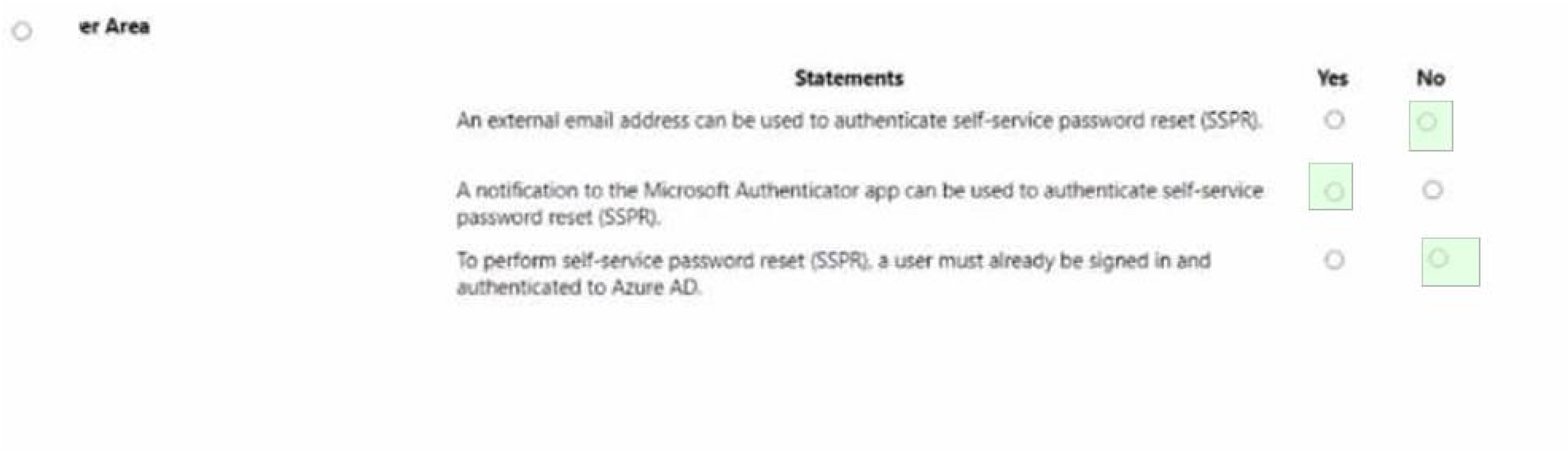
Hot Area:



○ **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:

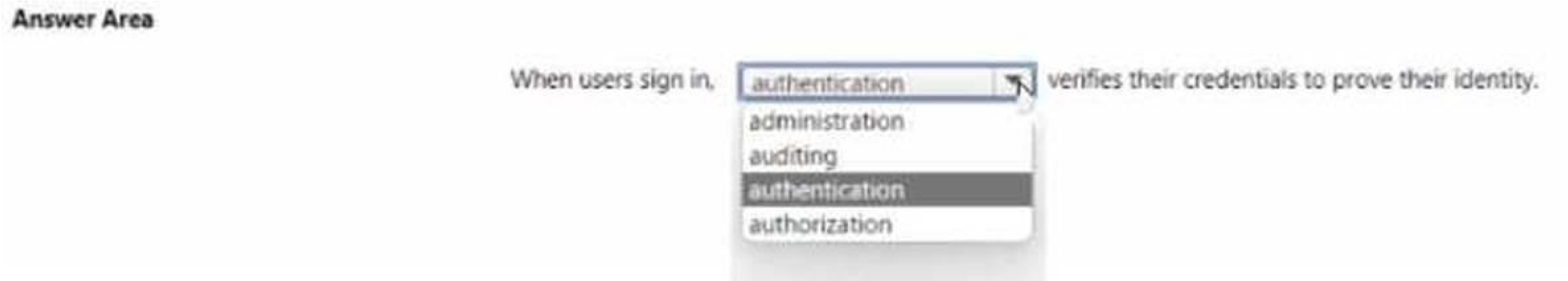
QUESTION 78
Which pillar of identity relates to tracking the resources accessed by a user?

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

Correct Answer: A
Section:

QUESTION 79
HOTSPOT
Select the answer that correctly completes the sentence.

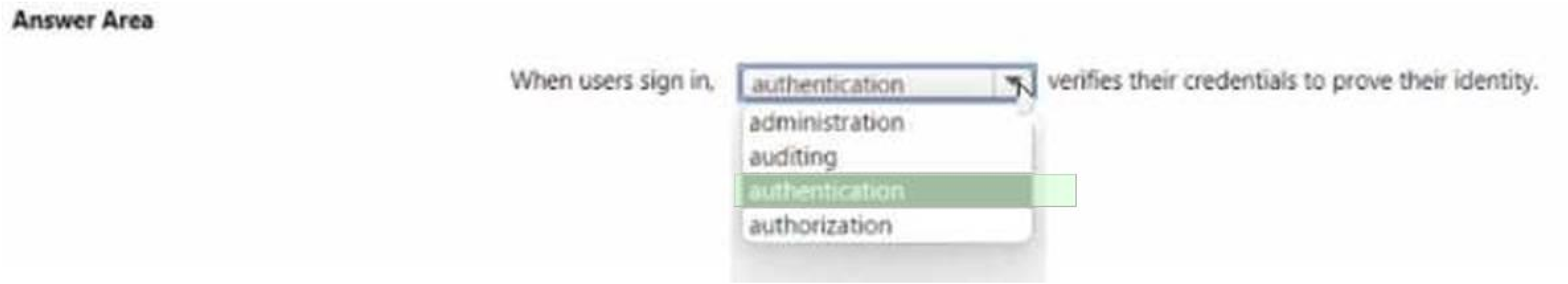
Hot Area:



Answer Area

When users sign in, [authentication ▾] verifies their credentials to prove their identity.

Answer Area:



Answer Area

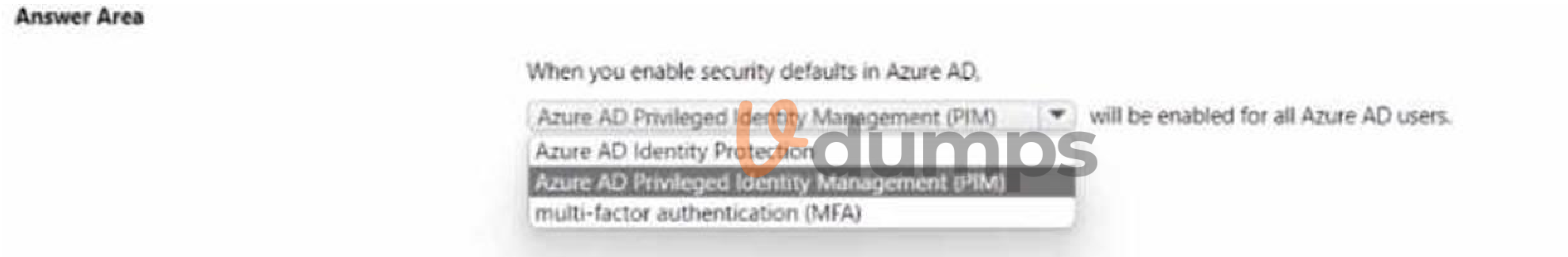
When users sign in, authentication verifies their credentials to prove their identity.

- administration
- auditing
- authentication
- authorization

Section:
Explanation:

QUESTION 80
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

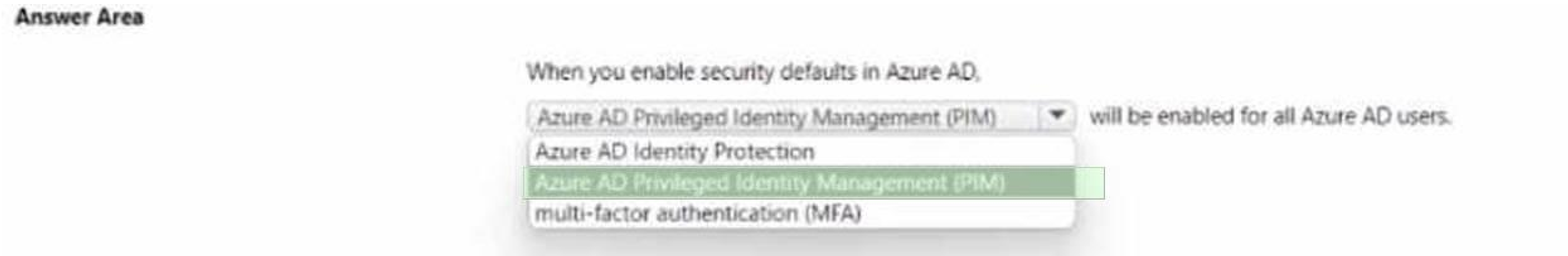


Answer Area

When you enable security defaults in Azure AD, Azure AD Privileged Identity Management (PIM) will be enabled for all Azure AD users.

- Azure AD Identity Protection
- Azure AD Privileged Identity Management (PIM)
- multi-factor authentication (MFA)

Answer Area:

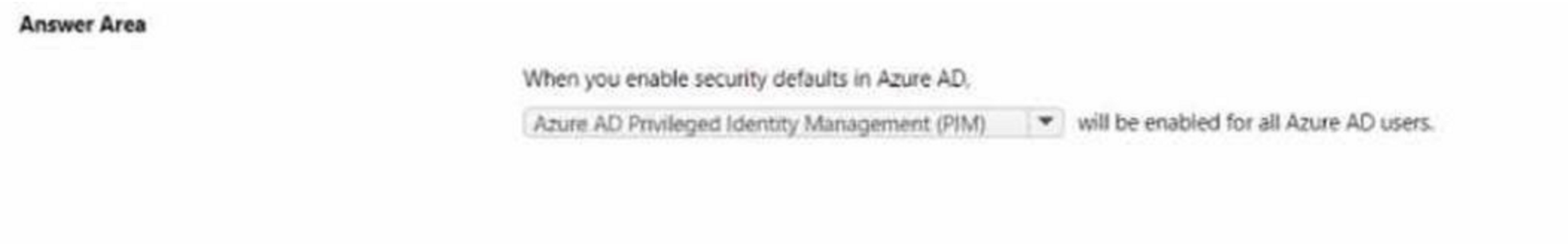


Answer Area

When you enable security defaults in Azure AD, Azure AD Privileged Identity Management (PIM) will be enabled for all Azure AD users.

- Azure AD Identity Protection
- Azure AD Privileged Identity Management (PIM)
- multi-factor authentication (MFA)

Section:
Explanation:



Answer Area

When you enable security defaults in Azure AD,

Azure AD Privileged Identity Management (PIM) ▼ will be enabled for all Azure AD users.

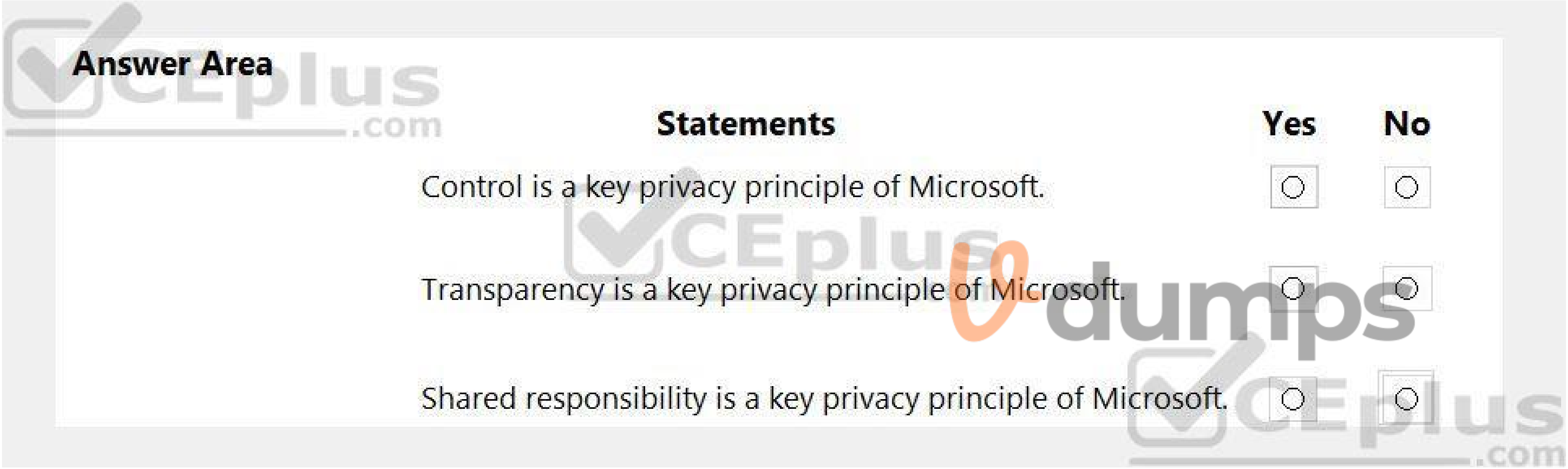
QUESTION 81

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.

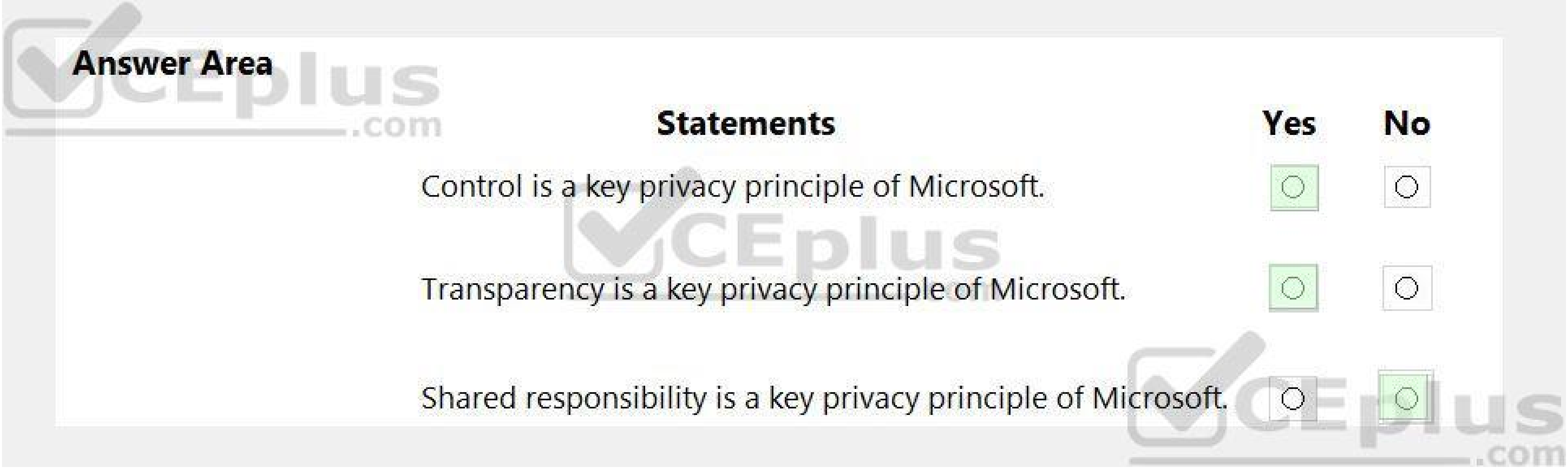
Hot Area:



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 82

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove users that no longer require membership in a group?

A. access reviews

B. managed identities

C. conditional access policies

D. Azure AD Identity Protection

Correct Answer: A

Section:

Explanation:

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

Reference:

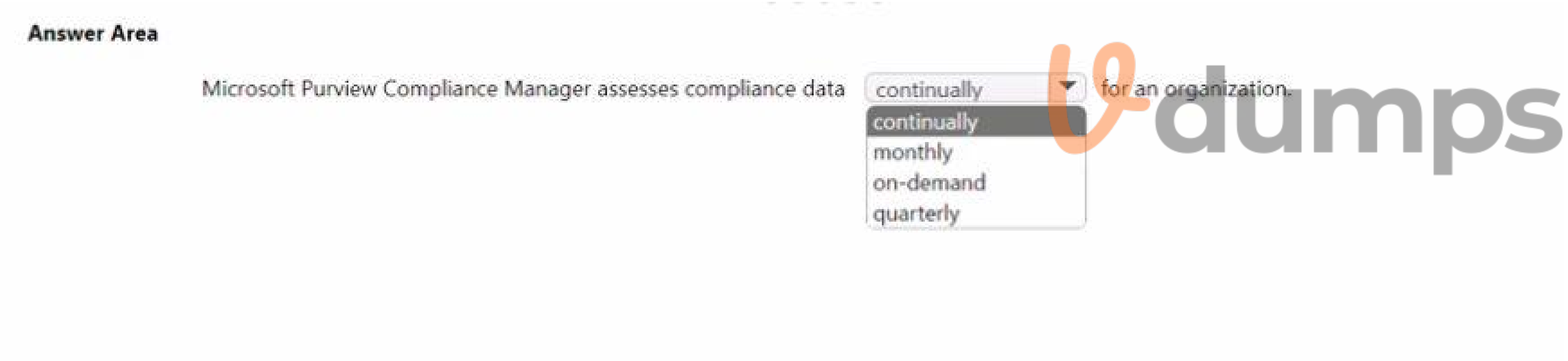
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

QUESTION 83

HOTSPOT

Select the answer that correctly completes the sentence.

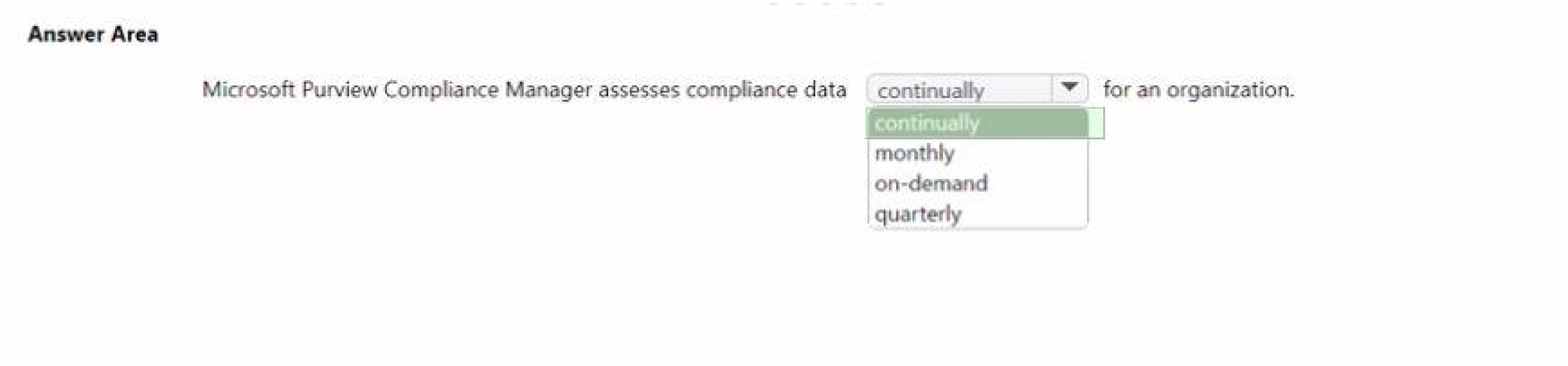
Hot Area:



Answer Area

Microsoft Purview Compliance Manager assesses compliance data continually for an organization.

Answer Area:



Answer Area

Microsoft Purview Compliance Manager assesses compliance data continually for an organization.

Section:

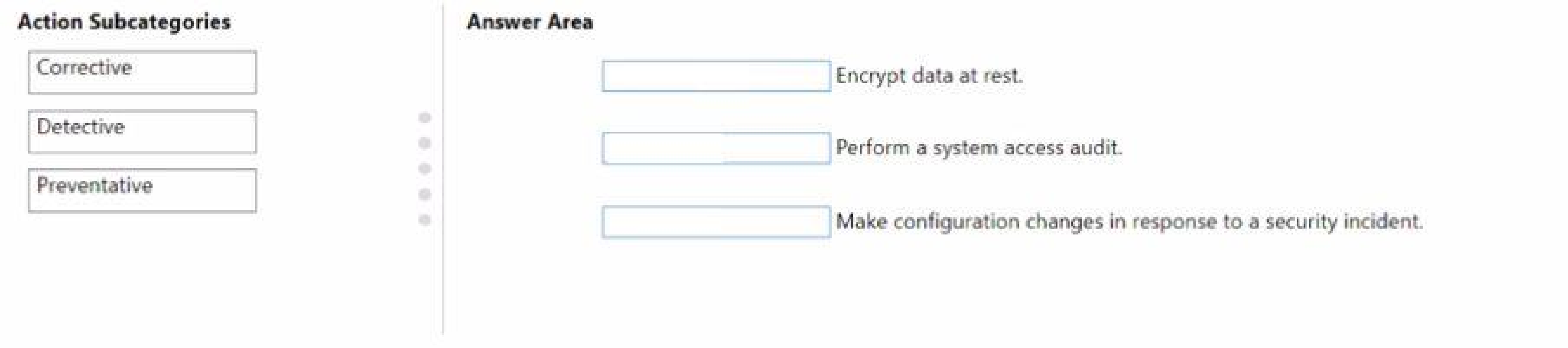
Explanation:

QUESTION 84

DRAG DROP

You are evaluating the compliance score in Microsoft Purview Compliance Manager.
Match the compliance score action subcategories to the appropriate actions.
To answer, drag the appropriate action subcategory from the column on the left to its action on the right. Each action subcategory may be used once, more than once, or not at all.
NOTE: Each correct match is worth one point.

Select and Place:



Action Subcategories

Corrective

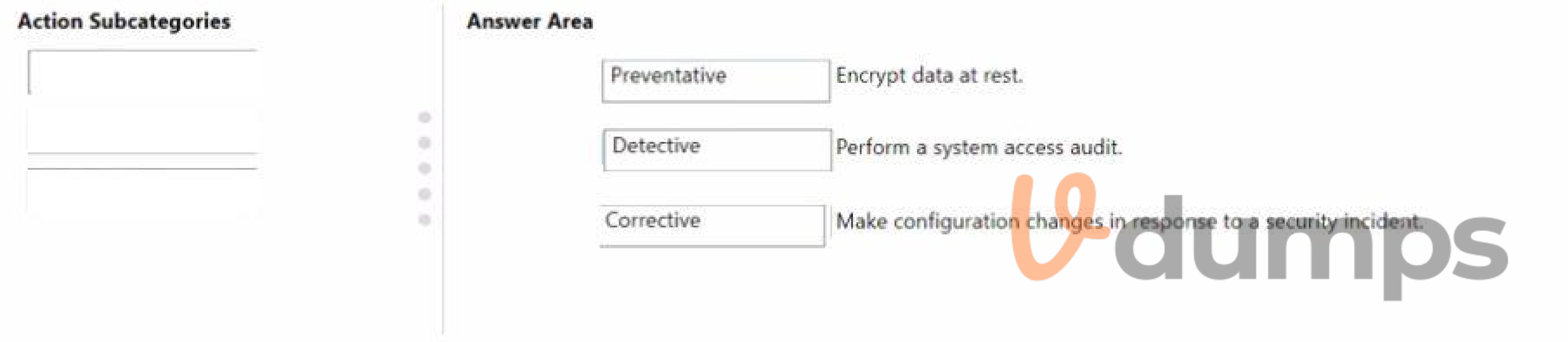
Detective

Preventative

Answer Area

	Encrypt data at rest.
	Perform a system access audit.
	Make configuration changes in response to a security incident.

Correct Answer:



Action Subcategories

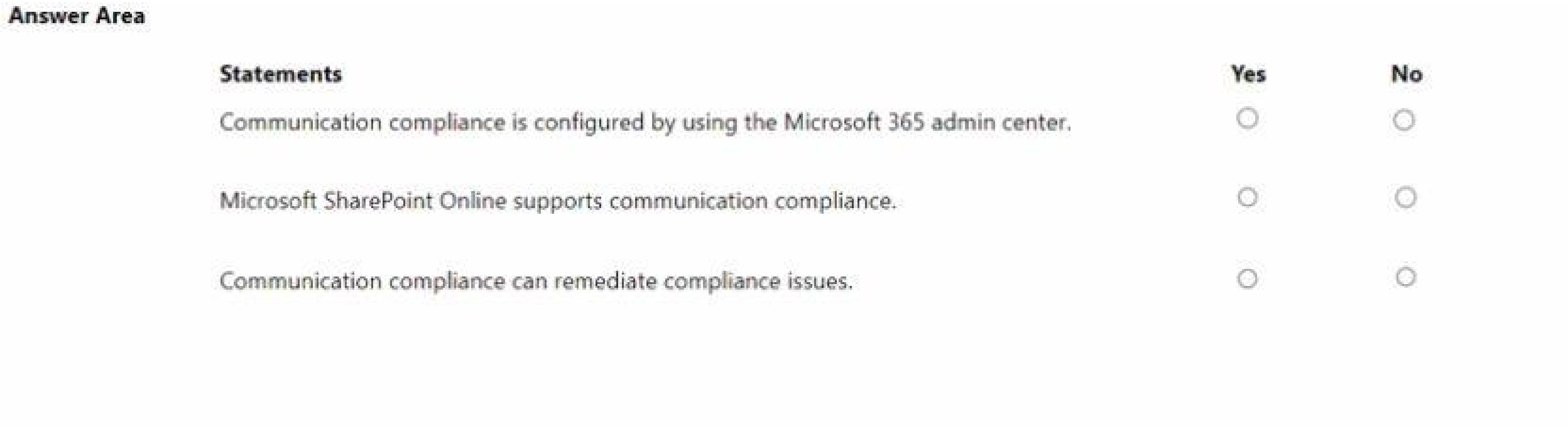
Answer Area

Preventative	Encrypt data at rest.
Detective	Perform a system access audit.
Corrective	Make configuration changes in response to a security incident.

Section:
Explanation:

QUESTION 85
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.

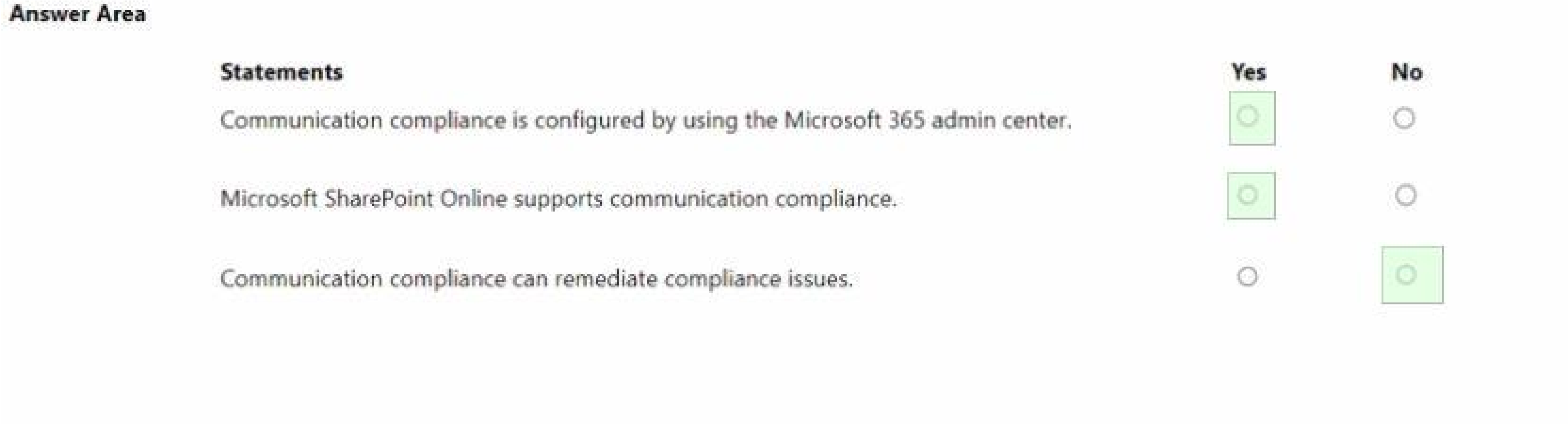
Hot Area:



Answer Area

Statements	Yes	No
Communication compliance is configured by using the Microsoft 365 admin center.	○	○
Microsoft SharePoint Online supports communication compliance.	○	○
Communication compliance can remediate compliance issues.	○	○

Answer Area:



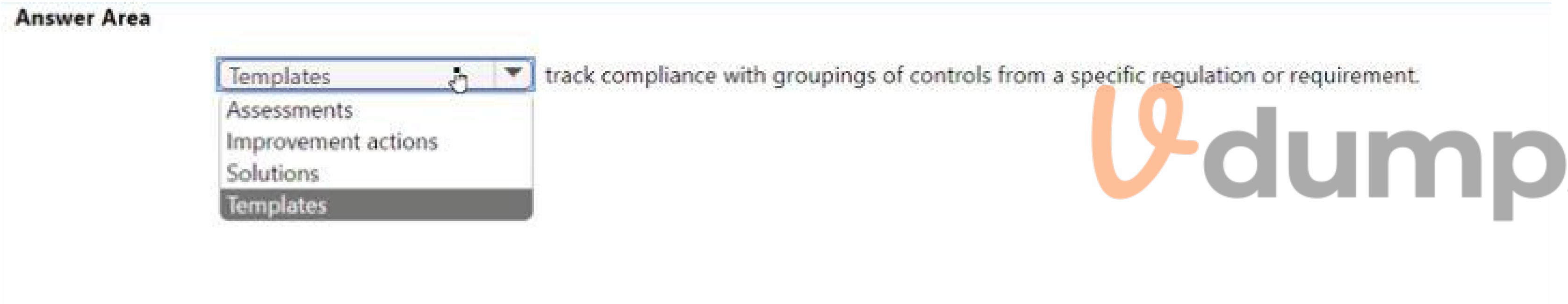
Answer Area

Statements	Yes	No
Communication compliance is configured by using the Microsoft 365 admin center.	[✓ ○]	○
Microsoft SharePoint Online supports communication compliance.	[✓ ○]	○
Communication compliance can remediate compliance issues.	○	[✓ ○]

Section:
Explanation:

QUESTION 86
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

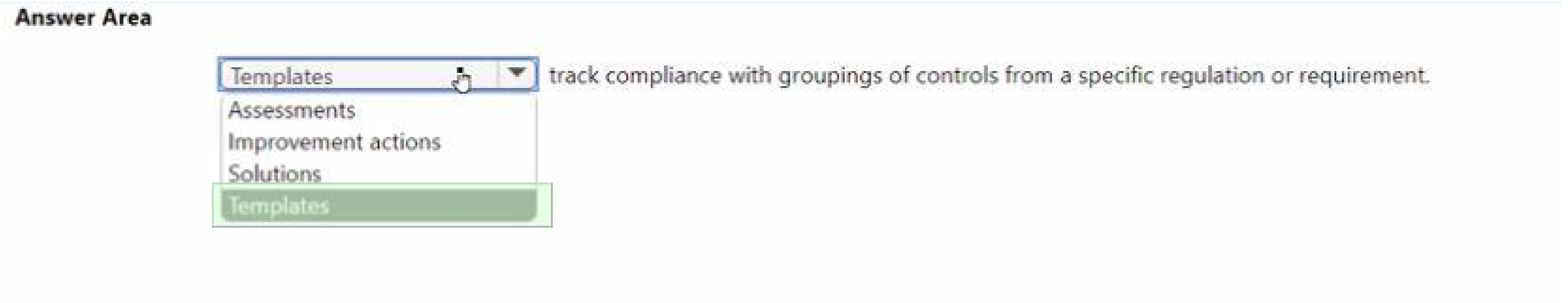


Answer Area

Templates ▾ track compliance with groupings of controls from a specific regulation or requirement.

Assessments
Improvement actions
Solutions
Templates

Answer Area:



Answer Area

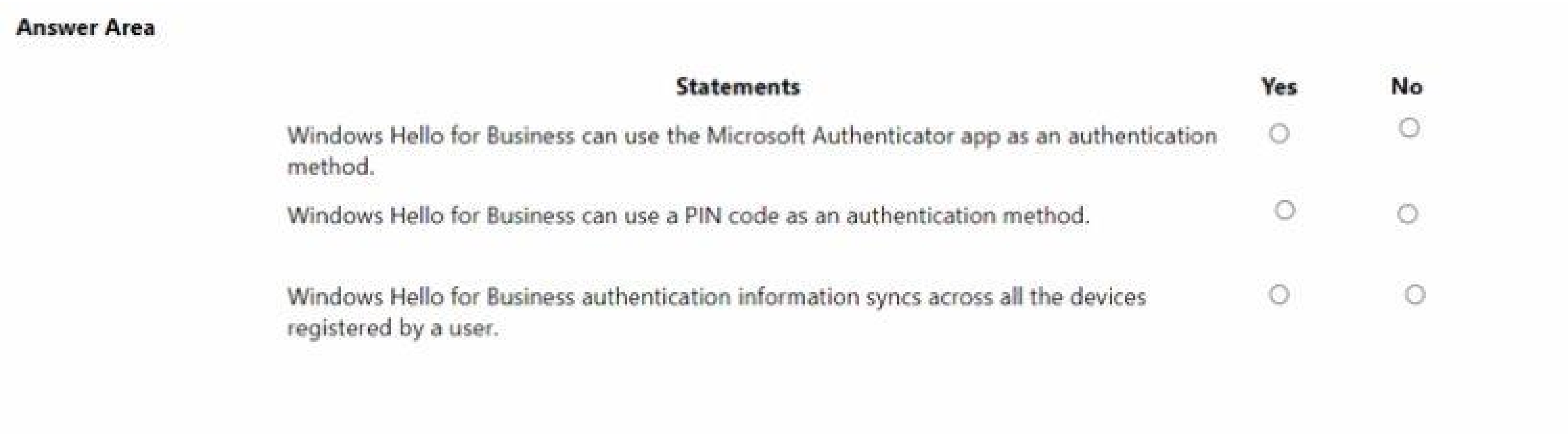
Templates ▾ track compliance with groupings of controls from a specific regulation or requirement.

Assessments
Improvement actions
Solutions
[✓ Templates]

Section:
Explanation:

QUESTION 87
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.

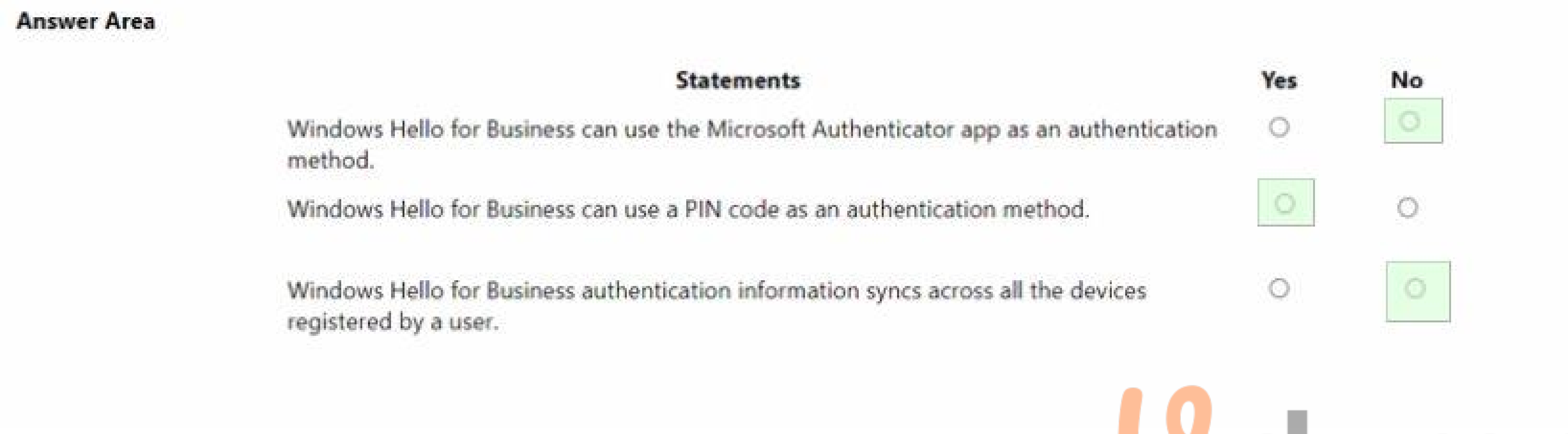
Hot Area:



Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	○
Windows Hello for Business can use a PIN code as an authentication method.	○	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	○

Answer Area:



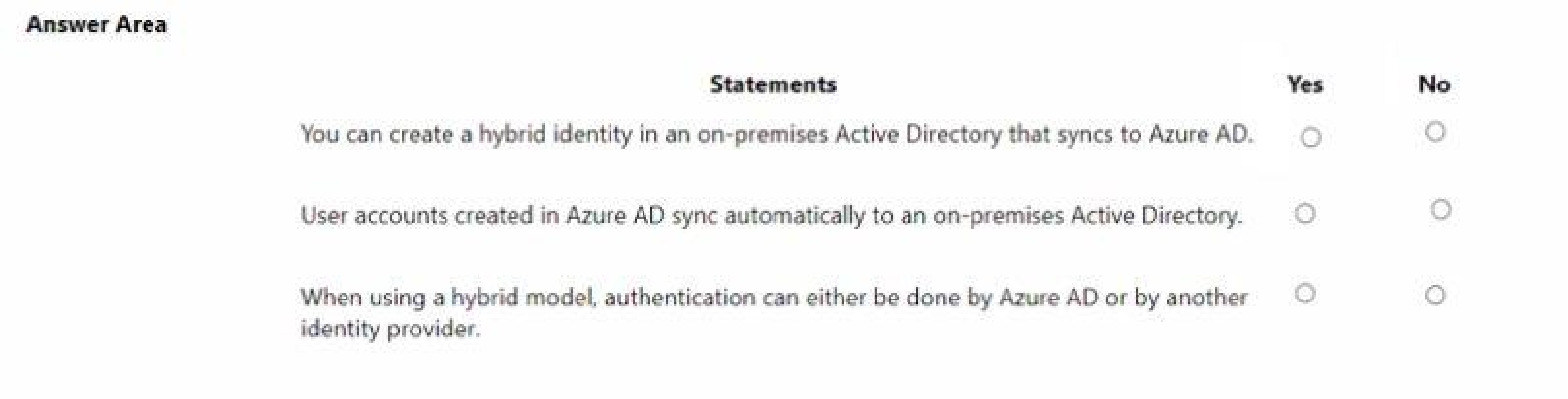
Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	[✓ ○]
Windows Hello for Business can use a PIN code as an authentication method.	[✓ ○]	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	[✓ ○]

Section:
Explanation:

QUESTION 88
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.

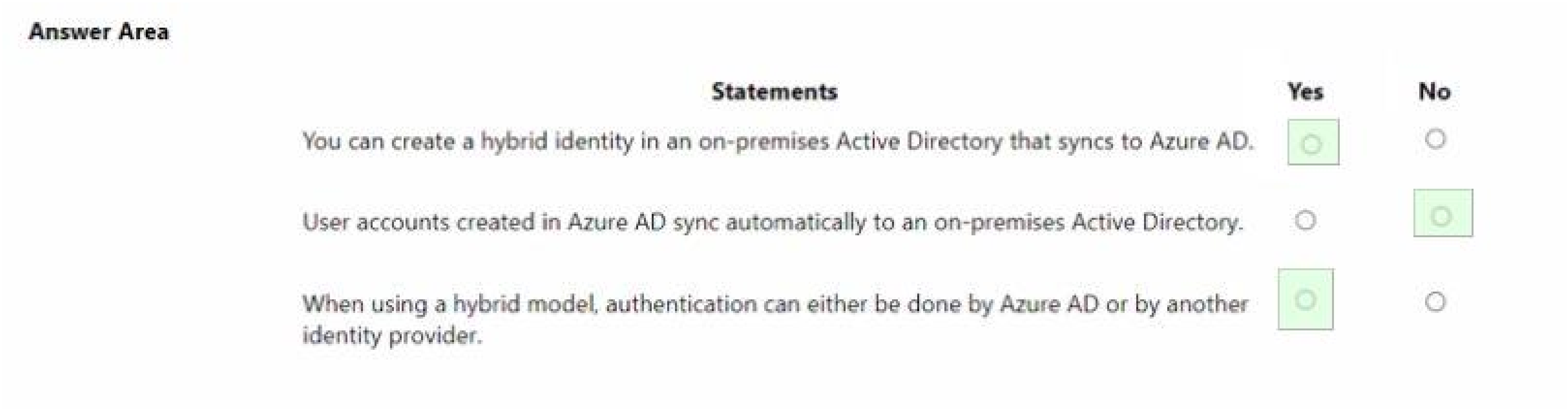
Hot Area:



Answer Area

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	○	○
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	○	○
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	○	○

Answer Area:



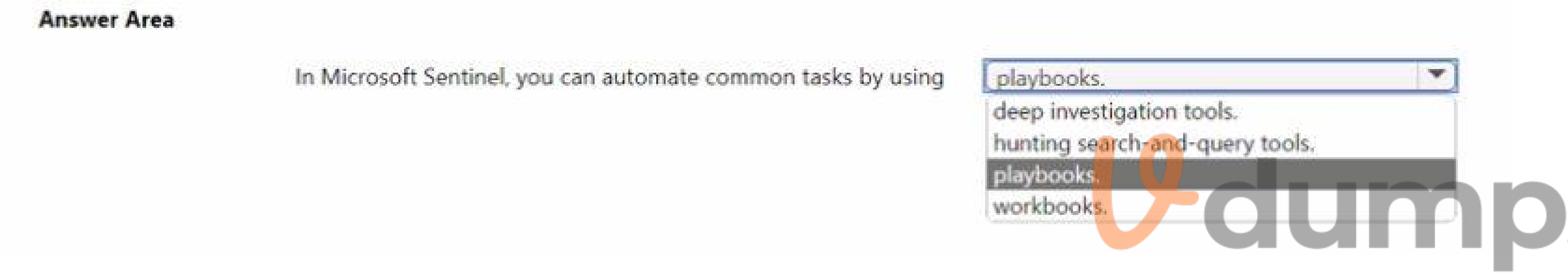
Answer Area

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	[✓ ○]	○
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	○	[✓ ○]
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	[✓ ○]	○

Section:
Explanation:

QUESTION 89
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

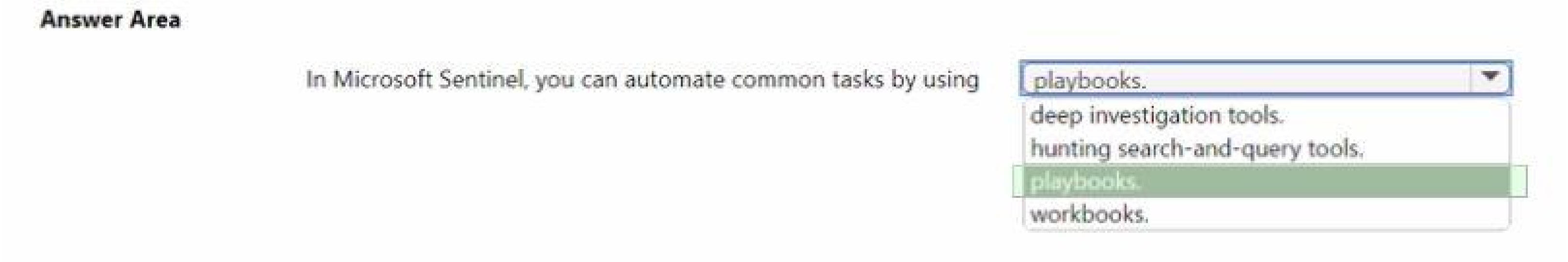


Answer Area

In Microsoft Sentinel, you can automate common tasks by using playbooks.

- deep investigation tools.
- hunting search-and-query tools.
- playbooks.
- workbooks.

Answer Area:



Answer Area

In Microsoft Sentinel, you can automate common tasks by using playbooks.

- deep investigation tools.
- hunting search-and-query tools.
- [✓ playbooks.]
- workbooks.

Section:
Explanation:

QUESTION 90
You have an Azure subscription that contains multiple resources.
You need to assess compliance and enforce standards for the existing resources.
What should you use?

A. the Anomaly Detector service
B. Microsoft Sentinel
C. Azure Blueprints
D. Azure Policy

Correct Answer: D

Section:

QUESTION 91
Which statement represents a Microsoft privacy principle?

A. Microsoft does not collect any customer data.
B. Microsoft uses hosted customer email and chat data for targeted advertising.
C. Microsoft manages privacy settings for its customers.
D. Microsoft respects the local privacy laws that are applicable to its customers.

Correct Answer: C
Section:

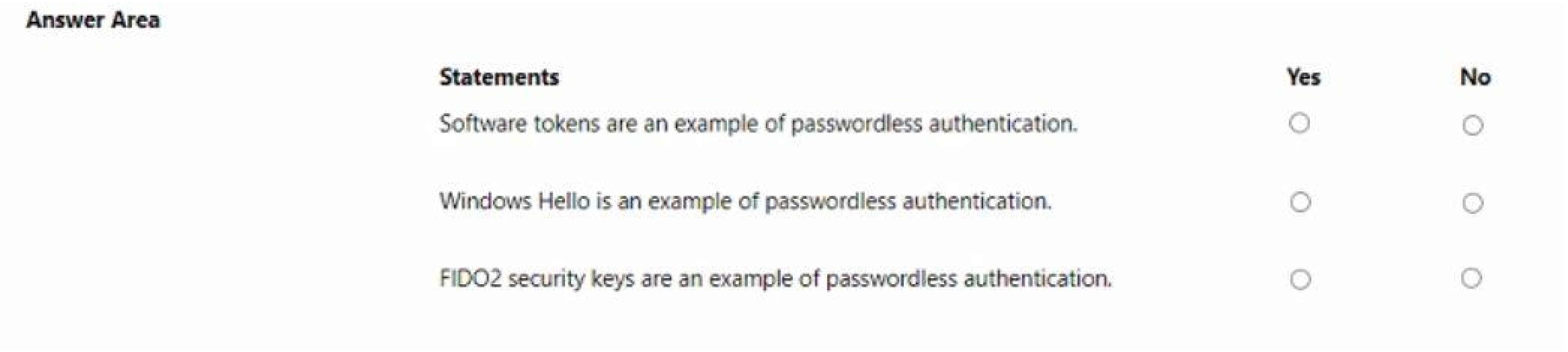
QUESTION 92
Which security feature is available in the free mode of Microsoft Defender for Cloud?

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: B
Section:

QUESTION 93
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.

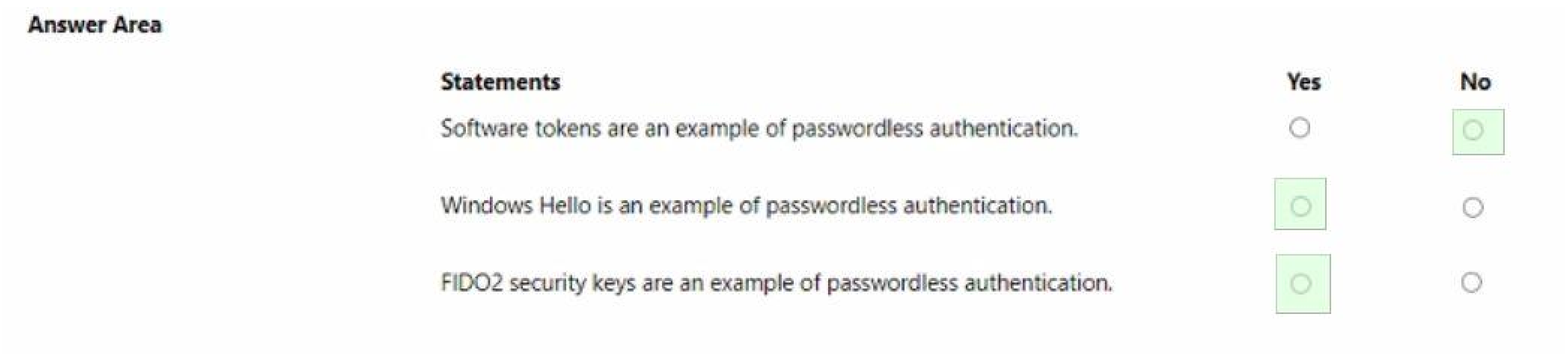
Hot Area:



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:



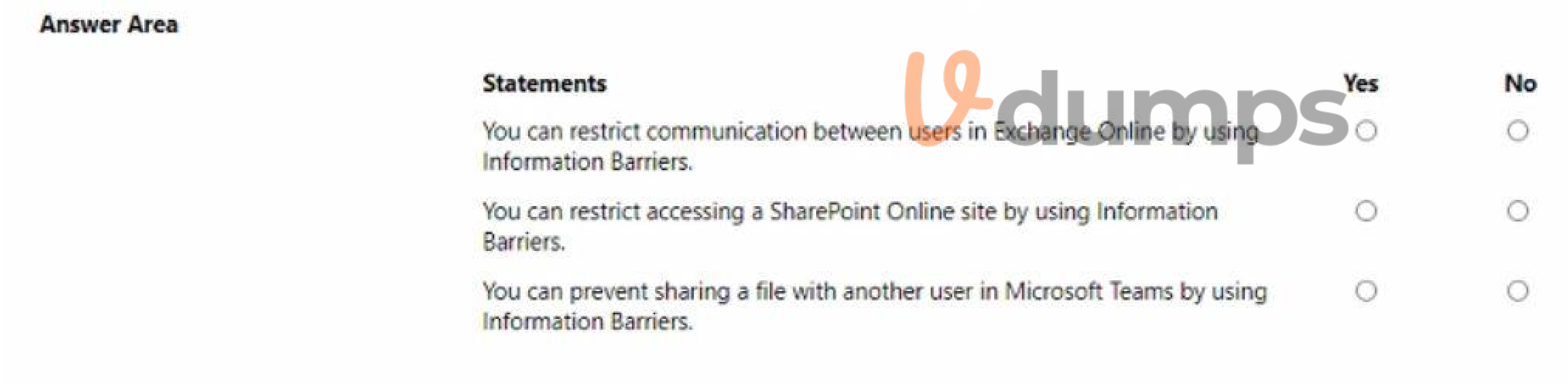
Answer Area

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 94
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.

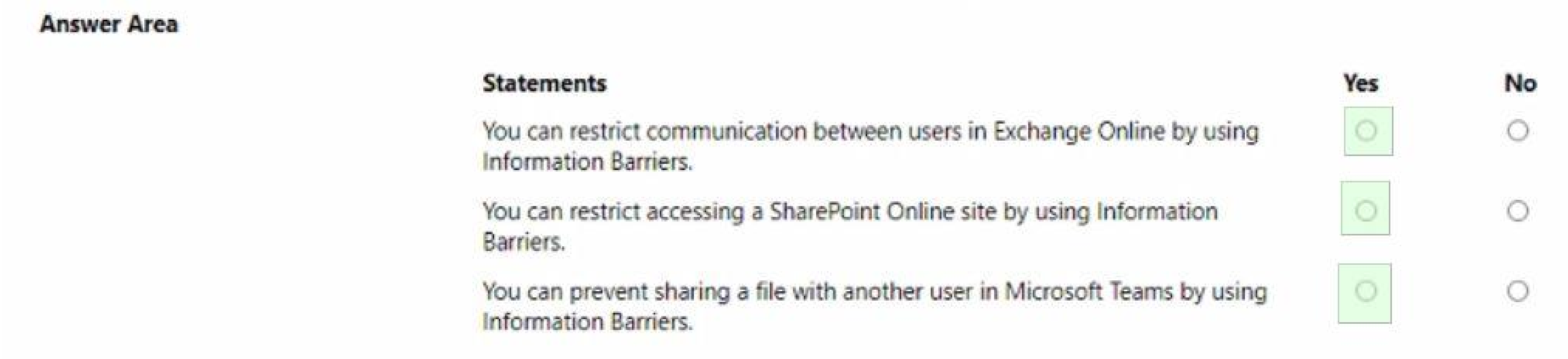
Hot Area:



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:

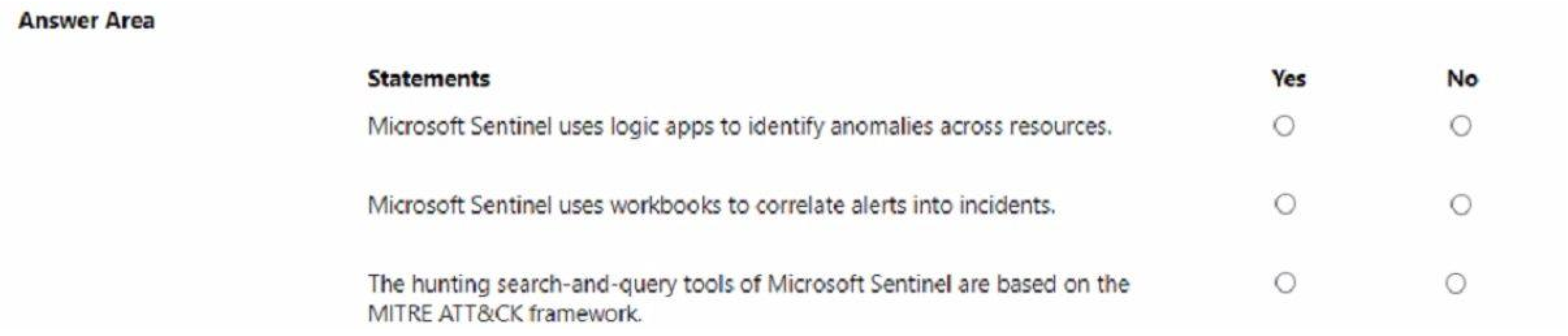
Explanation:

QUESTION 95

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.

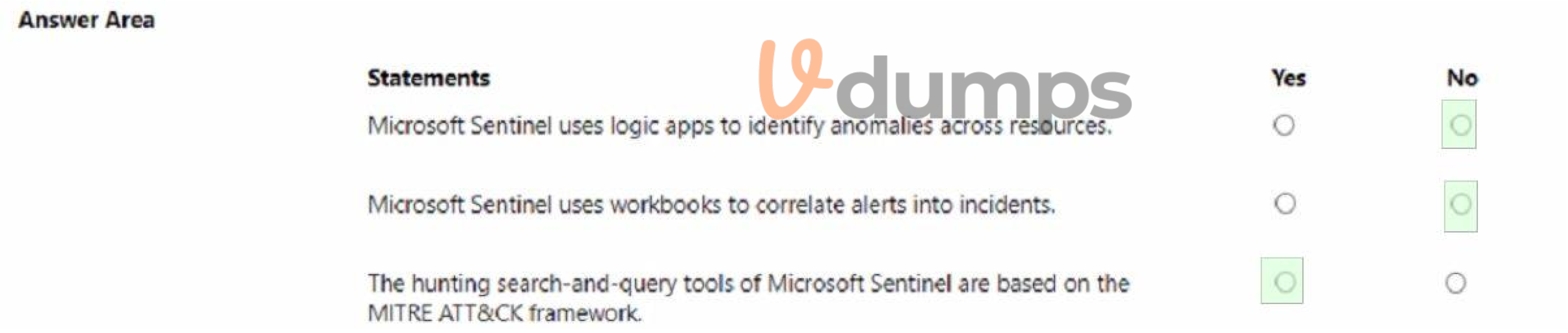
Hot Area:



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:

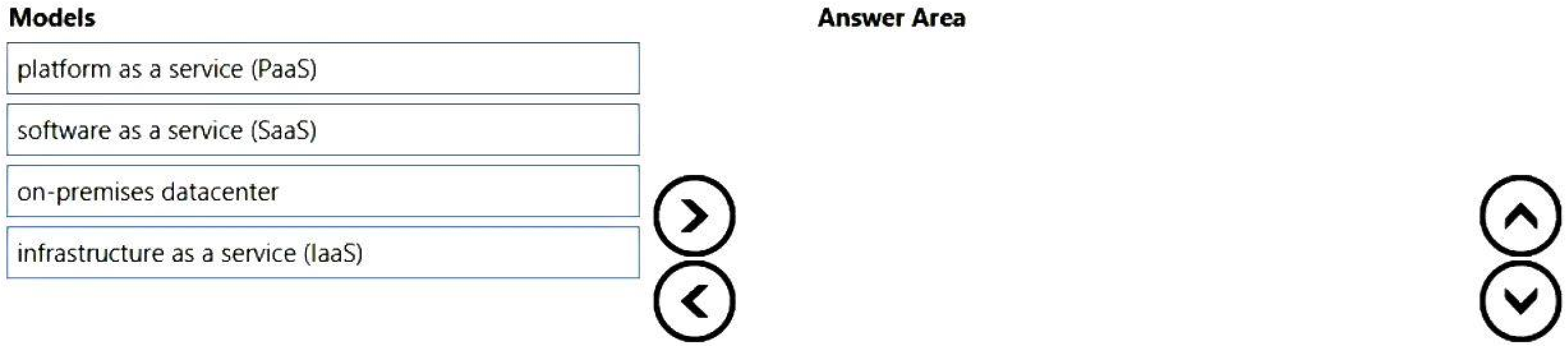
QUESTION 96

DRAG DROP

You need to identify which cloud service models place the most responsibility on the customer in a shared responsibility model.

in which order should you list the service models from the most customer responsibility (on the top) to the least customer responsibility (on the bottom)? To answer, move all models from the list of models to the answer area and arrange them in the correct order.

Select and Place:



Models

platform as a service (PaaS)

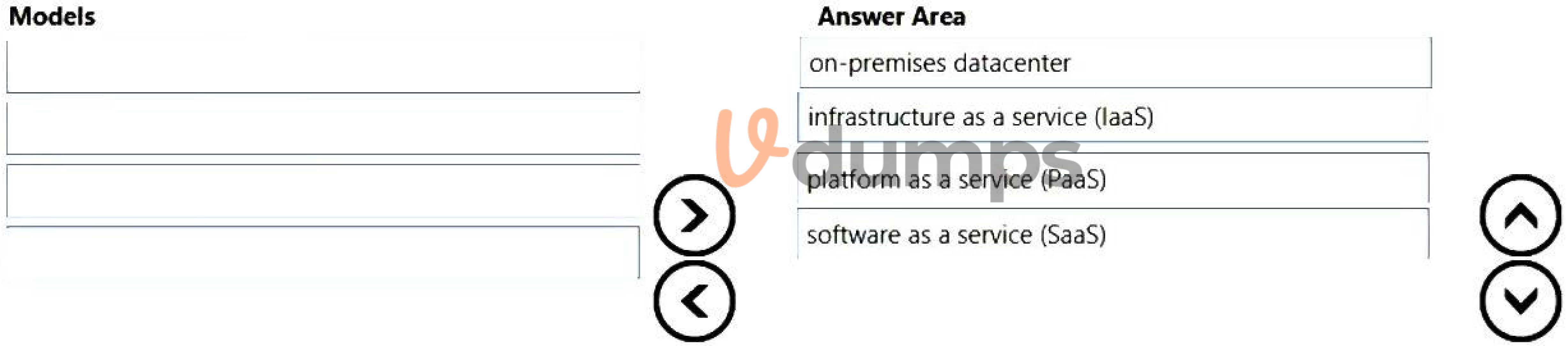
software as a service (SaaS)

on-premises datacenter

infrastructure as a service (IaaS)

Answer Area

Correct Answer:



Models

Answer Area

on-premises datacenter

infrastructure as a service (IaaS)

platform as a service (PaaS)

software as a service (SaaS)

Section:
Explanation:
on-premises datacenter
infrastructure as a service (IaaS)
platform as a service (PaaS)
software as a service (SaaS)

QUESTION 97

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

A. Microsoft Entra ID Protection

B. Microsoft Entra Conditional access

C. Microsoft Entra Privileged Management

D. Microsoft Entra Access Reviews

Correct Answer: A
Section:

QUESTION 98
What Microsoft Purview feature can use machine learning algorithms to detect and automatically protect sensitive items?

A. eDiscovery

B. Data loss prevention

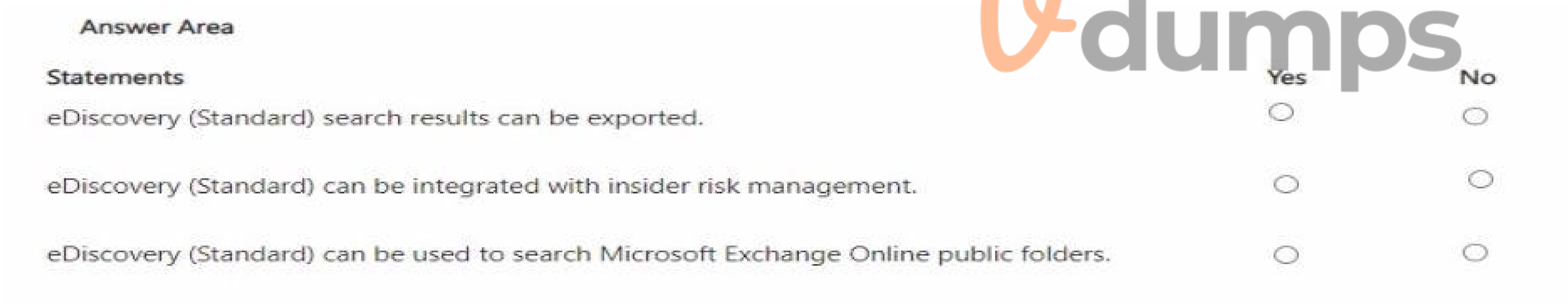
C. Information risks

D. Communication compliance

Correct Answer: B
Section:

QUESTION 99
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.

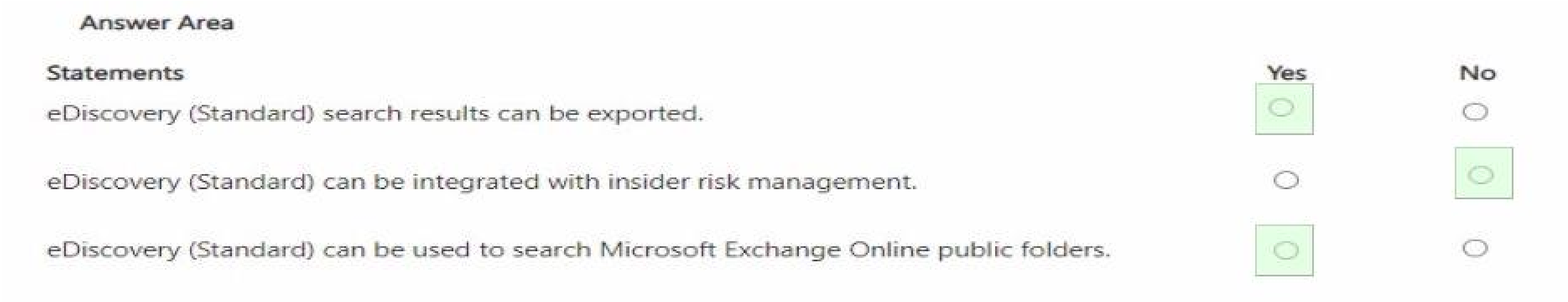
Hot Area:



Answer Area

Statements	Yes	No
eDiscovery (Standard) search results can be exported.	○	○
eDiscovery (Standard) can be integrated with insider risk management.	○	○
eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders.	○	○

Answer Area:



Answer Area

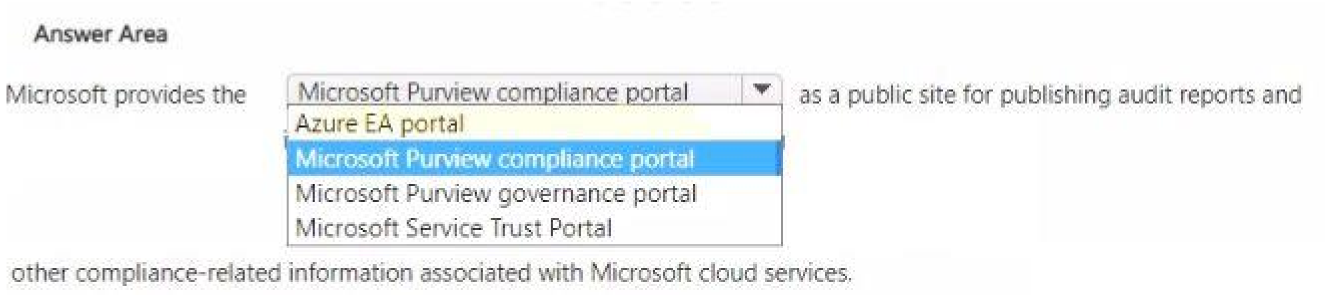
Statements	Yes	No
eDiscovery (Standard) search results can be exported.	[✓ ○]	○
eDiscovery (Standard) can be integrated with insider risk management.	○	[✓ ○]
eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders.	[✓ ○]	○

Section:
Explanation:

QUESTION 100
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

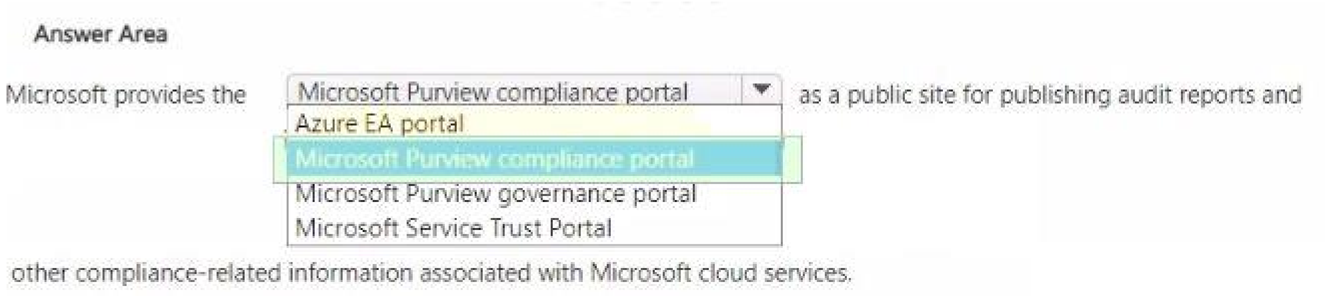


Answer Area

Microsoft provides the [Microsoft Purview compliance portal ▼] as a public site for publishing audit reports and other compliance-related information associated with Microsoft cloud services.

- Azure EA portal
- Microsoft Purview compliance portal
- Microsoft Purview governance portal
- Microsoft Service Trust Portal

Answer Area:



Answer Area

Microsoft provides the [Microsoft Purview compliance portal ▼] as a public site for publishing audit reports and other compliance-related information associated with Microsoft cloud services.

- Azure EA portal
- Microsoft Purview compliance portal
- Microsoft Purview governance portal
- Microsoft Service Trust Portal

Section:
Explanation: