CertyIQ

CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.
https://www.CertyIQ.com

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

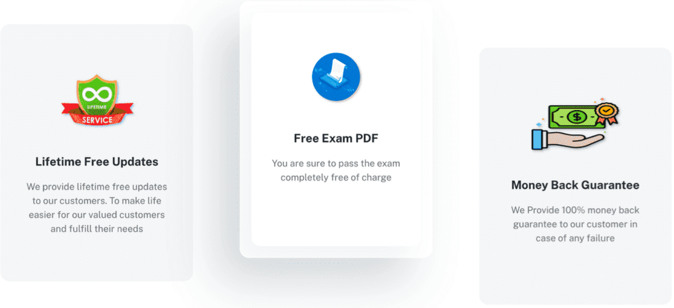
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

https://www.certyiq.com

Mail us on - certyiqofficial@gmail.com



Lifetime Free Updates

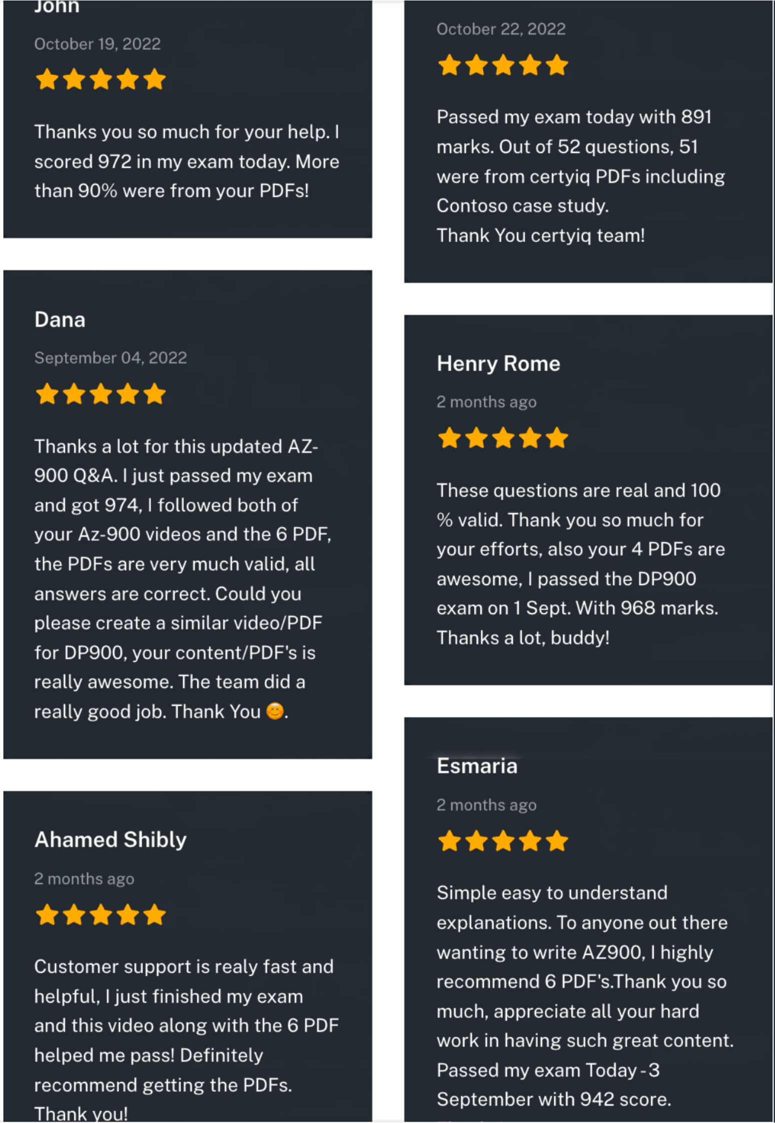
We provide lifetime free updates to our customers. To make life easier for our valued customers and fulfill their needs

Free Exam PDF

You are sure to pass the exam completely free of charge

Money Back Guarantee

We Provide 100% money back guarantee to our customer in case of any failure



John

October 19, 2022

★★★★★

Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

Dana

September 04, 2022

★★★★★

Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Ahamed Shibly

2 months ago

★★★★★

Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022

★★★★★

Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study.
Thank You certyiq team!

Henry Rome

2 months ago

★★★★★

These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago

★★★★★

Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's.Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today -3 September with 942 score.

Microsoft

(SC-900)

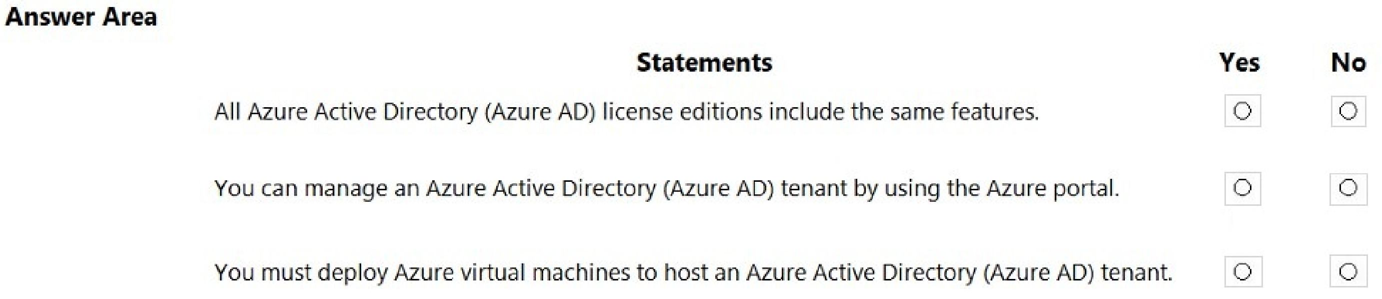
Microsoft Security, Compliance, and Identity Fundamentals

Total: **220 Questions**

Link: https://certyiq.com/papers/microsoft/sc-900

Question: 1

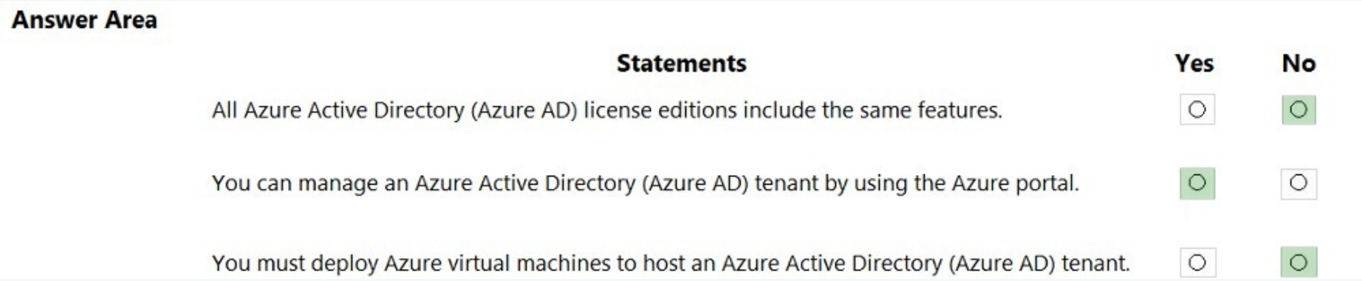
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	○
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	○	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	○

Answer:



Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	[✓ ○]
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	[✓ ○]	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	[✓ ○]

Explanation:

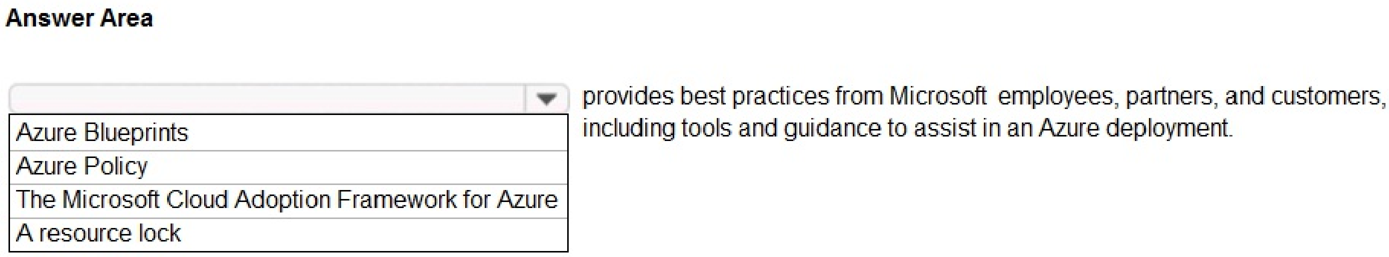
1) No - https://azure.microsoft.com/en-us/pricing/details/active-directory/: Azure Active Directory comes in four editions—Free, Office 365 apps, Premium P1, and Premium P2.

2) Yes - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant You can do all of your administrative tasks using the Azure Active Directory (Azure AD) portal, including creating a new tenant for your organization.

3) No - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service

Question: 2

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

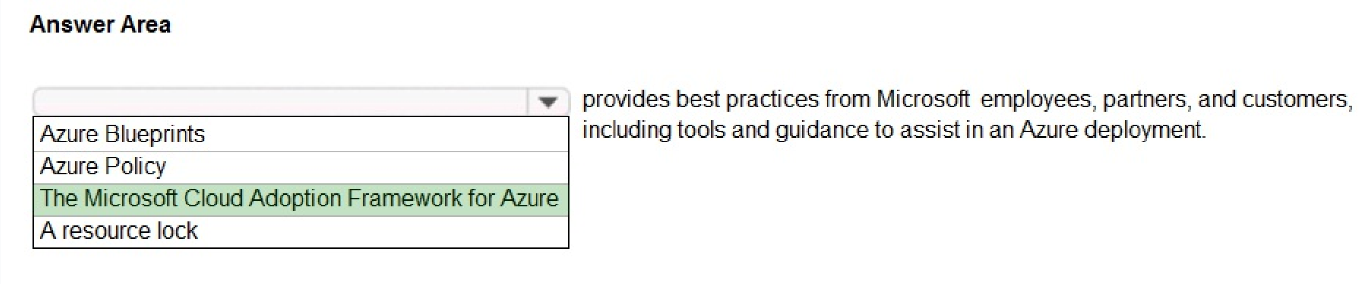


Answer Area

[▼] provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

- Azure Blueprints
- Azure Policy
- The Microsoft Cloud Adoption Framework for Azure
- A resource lock

Answer:



Answer Area

- Azure Blueprints
- Azure Policy
- [✓ The Microsoft Cloud Adoption Framework for Azure]
- A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Explanation:

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

"The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey."

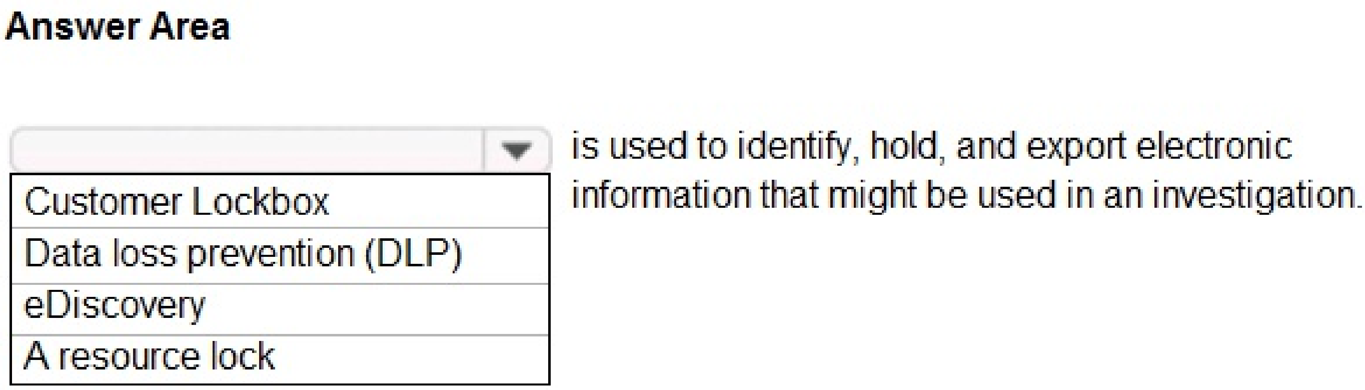
Reference:

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/

Question: 3

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

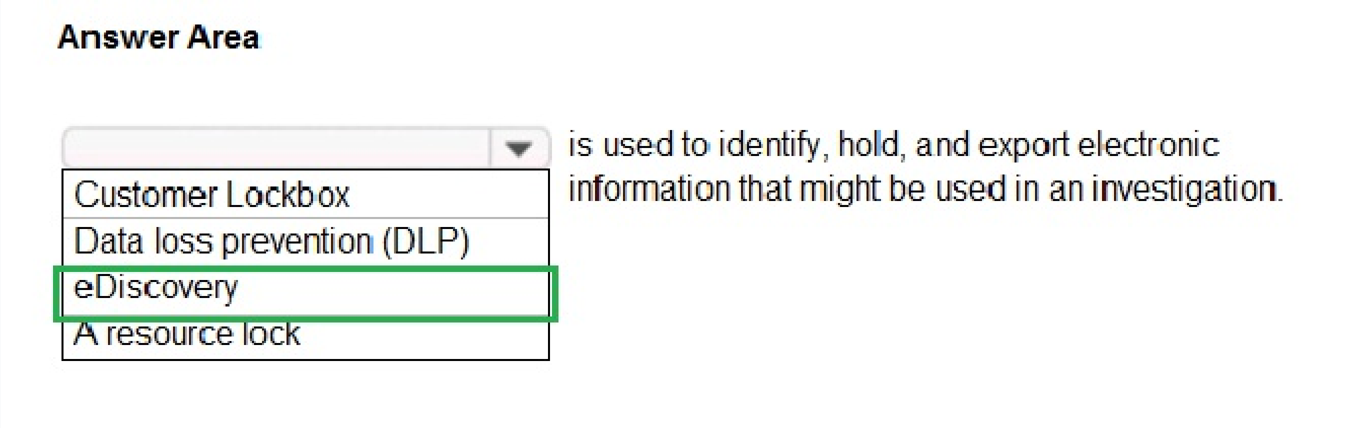


Answer Area

- Customer Lockbox
- Data loss prevention (DLP)
- eDiscovery
- A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Answer:



Answer Area

- Customer Lockbox
- Data loss prevention (DLP)
- [✓ eDiscovery]
- A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Explanation:

eDiscovery.

Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests.

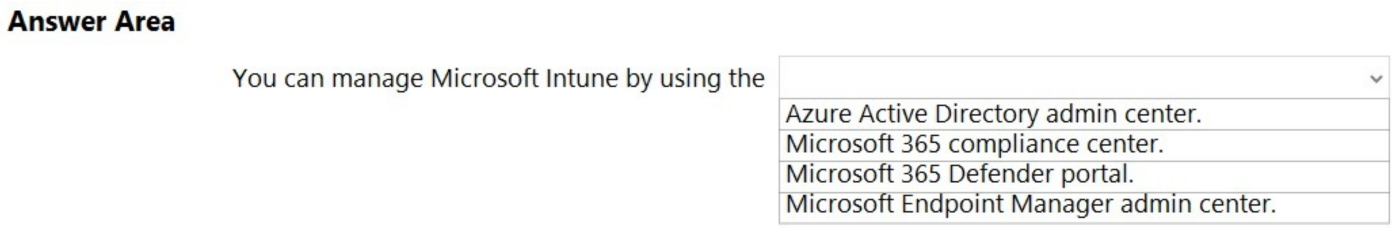
Customer Lockbox doesn't identify or hold export electronic data.

Reference:

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

Question: 4 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

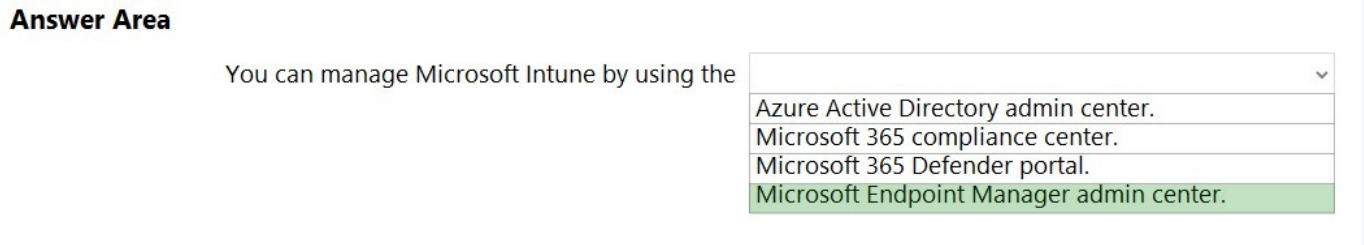


Answer Area

You can manage Microsoft Intune by using the

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

Answer:



Answer Area

You can manage Microsoft Intune by using the

- Azure Active Directory admin center.
- Microsoft 365 compliance center.
- Microsoft 365 Defender portal.
- [✓ Microsoft Endpoint Manager admin center.]

Explanation:

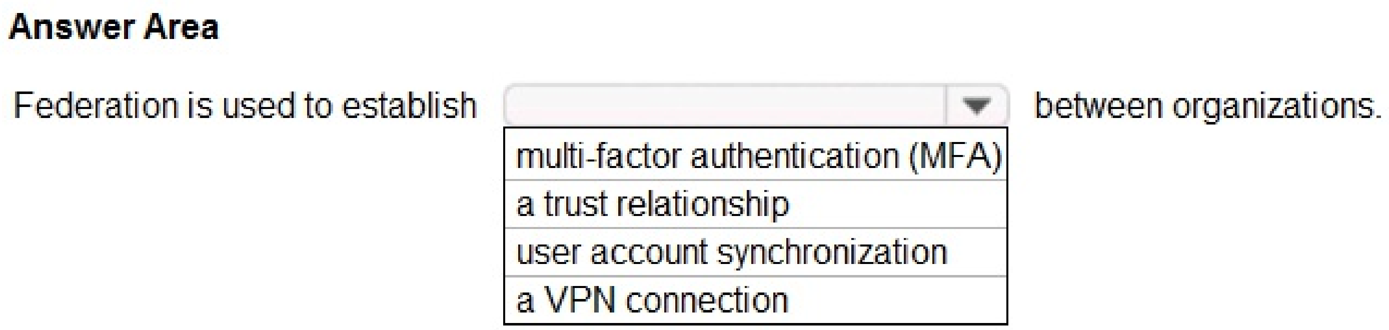
The answer is: Microsoft Endpoint Manager

"Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk."

Source - https://docs.microsoft.com/en-us/mem/endpoint-manager-overview

Question: 5 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

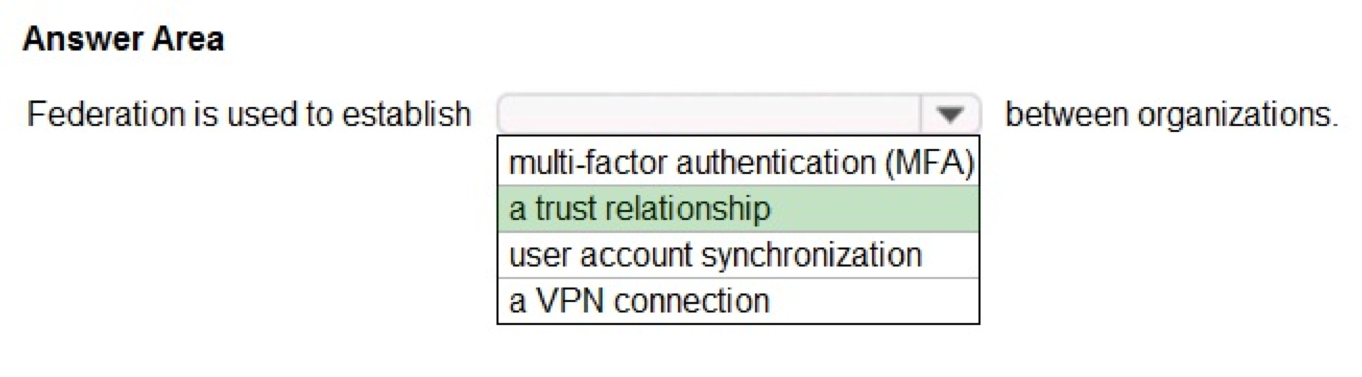


Answer Area

Federation is used to establish ▼ between organizations.

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

Answer:



Answer Area

Federation is used to establish ▼ between organizations.

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

Explanation:

"Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity provider. "

https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/6-describe-concept-federation

Federation is a collection of domains that have established trust.

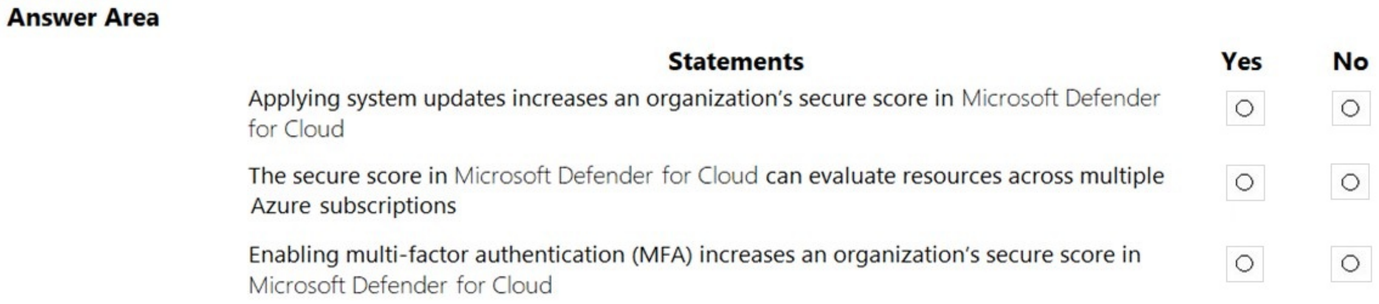
Reference:

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

Question: 6

CertyIQ

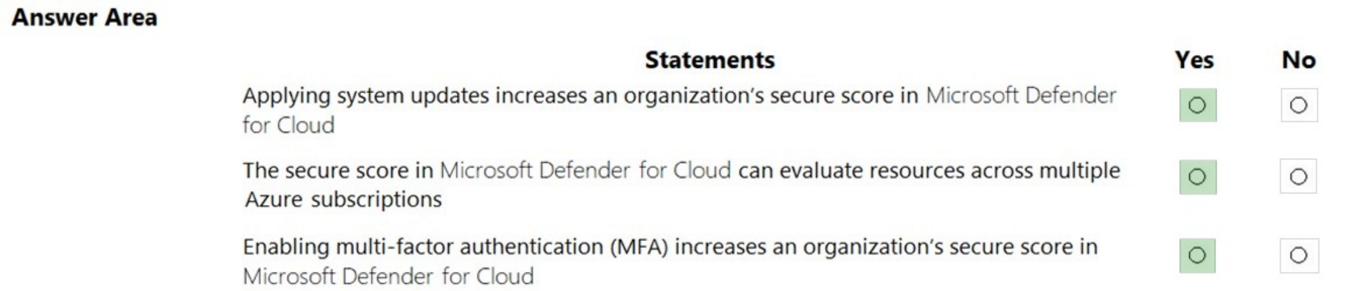
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

Explanation:

Box 1: Yes -

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

Box 2: Yes -

Box 3: Yes -

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

Reference:

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

Question: 7 CertyIQ

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

Answer: D

Explanation:

Answer is: Compliance score D

"Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps you manage your organization's compliance requirements with greater ease and convenience. Compliance Manager can help you throughout your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors."

Source - https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide&viewFallbackFrom=o365-worldwide%20https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fmicrosoft-365%2Fcompliance%2Fcompliance-score-calculation%3Fview%3Do365-worldwide

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: 8 CertyIQ

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 connector

Answer: D

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: 9 CertyIQ

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

Answer: C

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: 10 CertyIQ

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

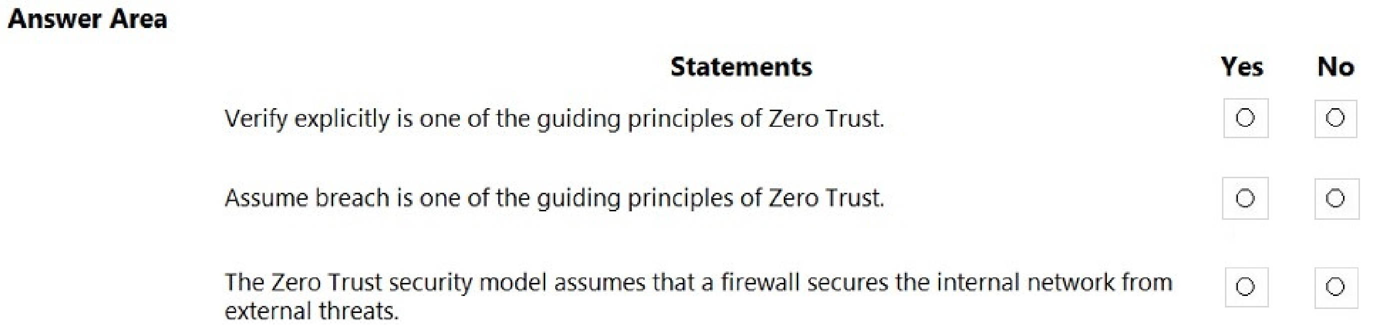
D. the management of the physical hardware

Answer: D

Question: 11

CertyIQ

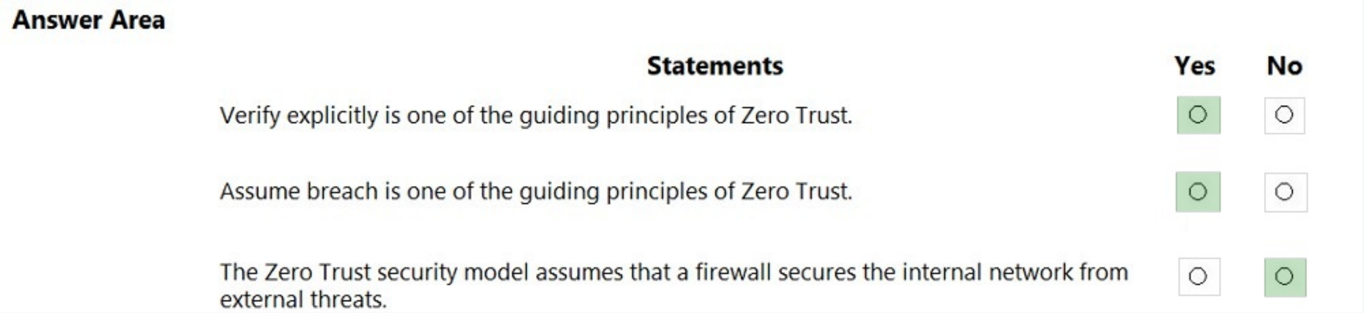
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

Explanation:

Box 1: Yes -

Box 2: Yes -

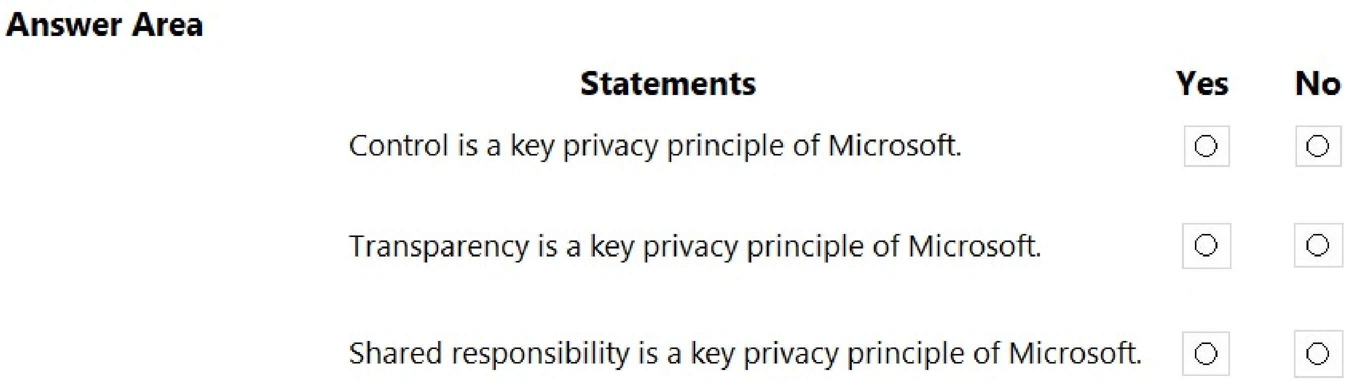
Box 3: No -
The Zero Trust model does not assume that everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.

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

Question: 12

CertyIQ

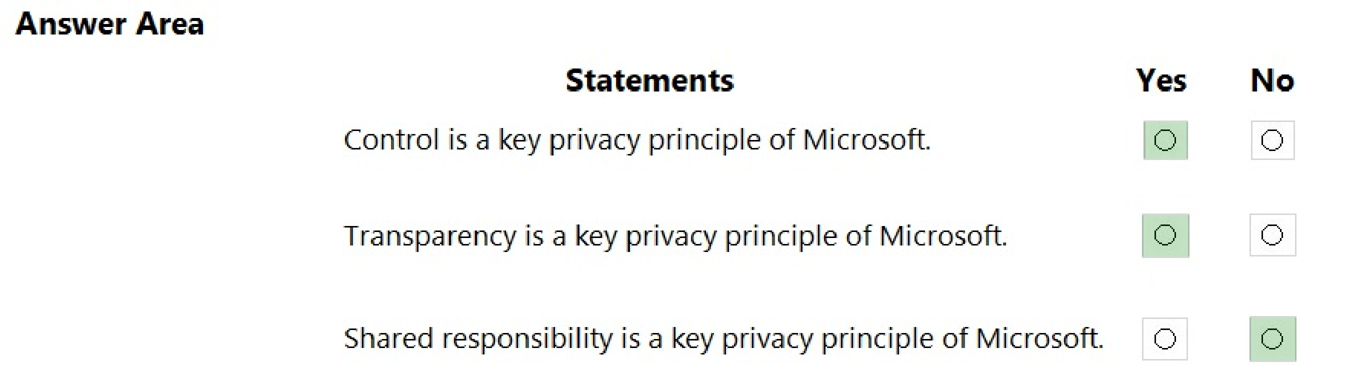
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	○	[✓ ○]

Explanation:

The Six privacy principles are:

Control: We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency: We will be transparent about data collection and use so you can make informed decisions.

Security: We will protect the data you entrust to us through strong security and encryption.

Strong legal protections: We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

No content-based targeting: We will not use your email, chat, files or other personal content to target ads to you.

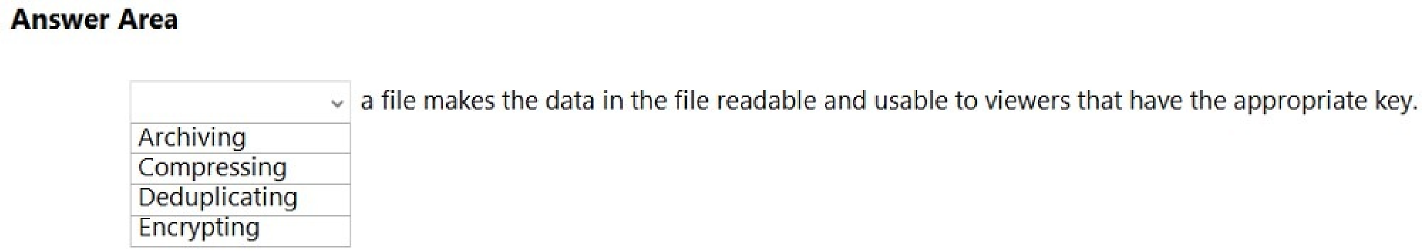
Benefits to you: When we do collect data, we will use it to benefit you and to make your experiences better.

Reference:

https://privacy.microsoft.com/en-US/

Question: 13 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

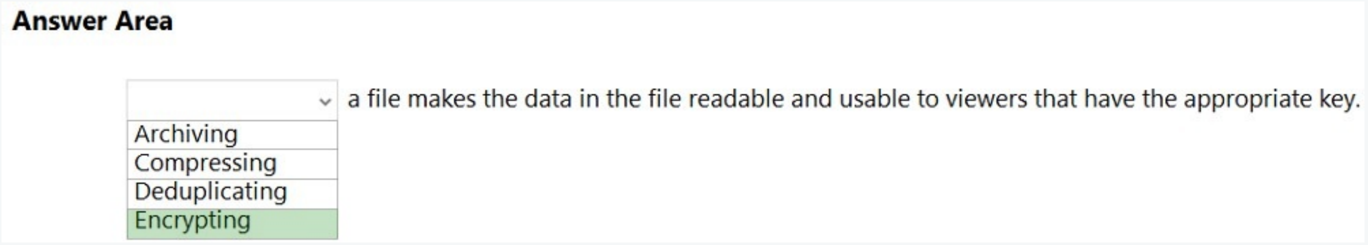


Answer Area

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

Archiving
Compressing
Deduplicating
Encrypting

Answer:



Answer Area

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

Archiving
Compressing
Deduplicating
[✓ Encrypting]

Explanation:

the question it says “to viewers that have the appropriate key”. So keyword is the word “KEY”.

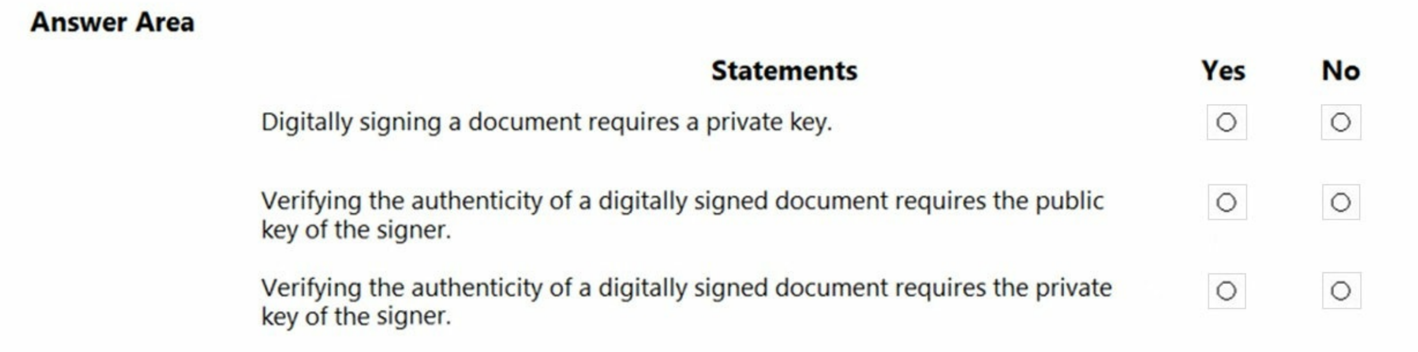
Encryption is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information.

Decryption is a process that transforms encrypted information into its original format. To do this, parties to a private conversation use an encryption scheme, called an algorithm, and the keys to encrypt and decrypt messages.

Question: 14

CertyIQ

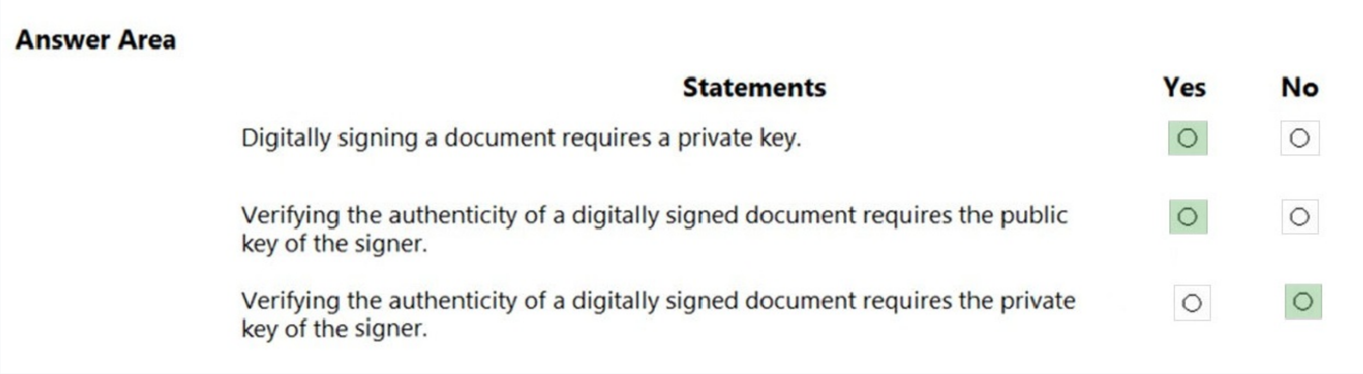
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

Explanation:

Box 1: Yes -

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

Box 2: Yes -

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

Box 3: No-

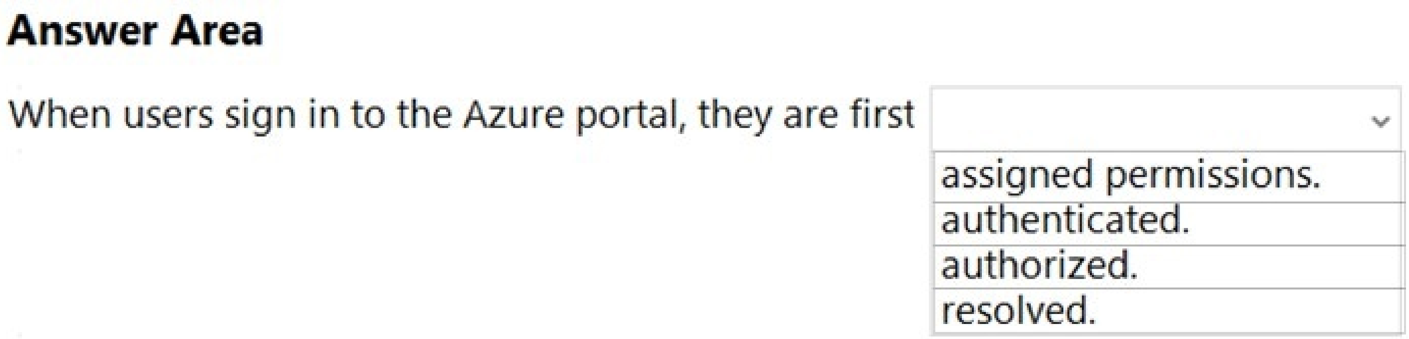
The private key is only used (and owned) by the signer to sign the document, and the associated public key is used to verify the authenticity.

Reference:

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

Question: 15 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

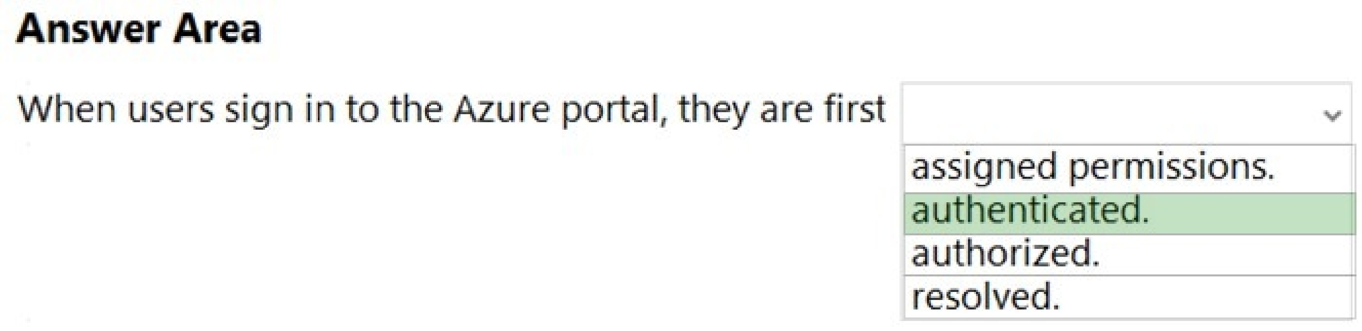


Answer Area

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

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

Answer:



Answer Area

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

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

Explanation:

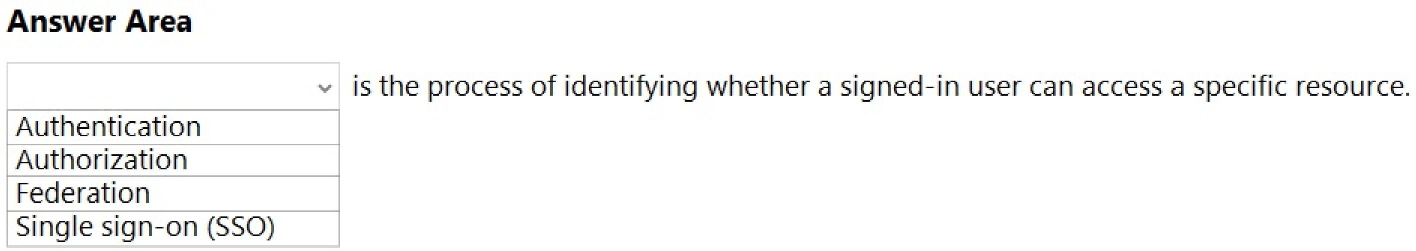
Authentication is who you say you are.

Authorization is what permission to do you have.

Question: 16

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

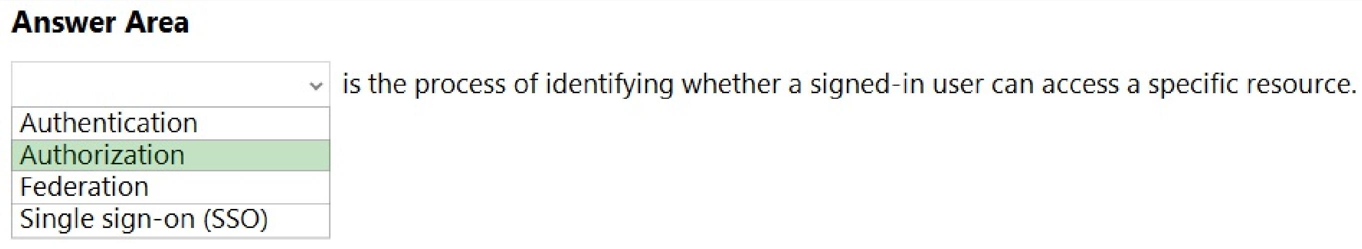


Answer Area

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

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

Answer:



Answer Area

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

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

Explanation:

Correct - from: https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization > "...authorization (providing access to secure data)..."

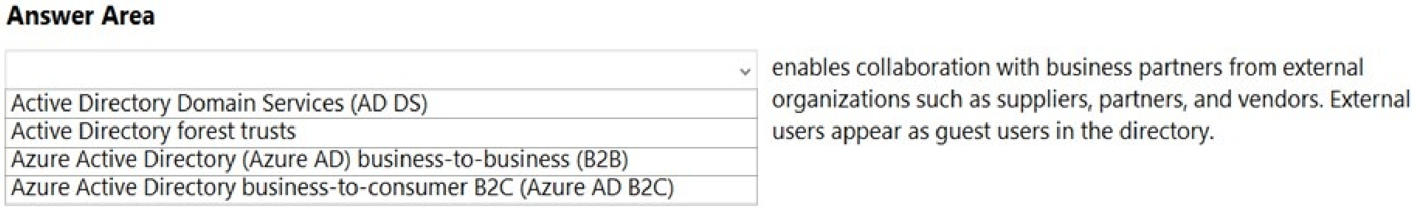
Reference:

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

Question: 17

CertyIQ

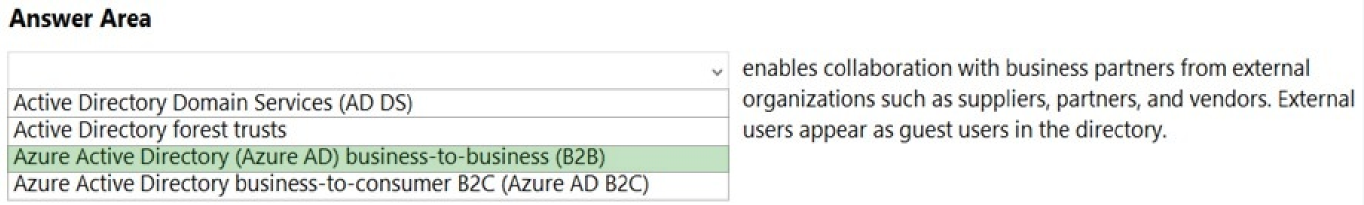
HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:



Answer Area

⌄	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.
Active Directory Domain Services (AD DS)	
Active Directory forest trusts	
Azure Active Directory (Azure AD) business-to-business (B2B)	
Azure Active Directory business-to-consumer B2C (Azure AD B2C)	

Answer:



Answer Area

⌄	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.
Active Directory Domain Services (AD DS)	
Active Directory forest trusts	
🟩 Azure Active Directory (Azure AD) business-to-business (B2B)	
Azure Active Directory business-to-consumer B2C (Azure AD B2C)	

Explanation:

"Azure Active Directory (Azure AD) business-to-business (B2B) collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization. With B2B collaboration, you can securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data."

Reference:

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

Question: 18 CertyIQ

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

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

Answer: AE

Explanation:

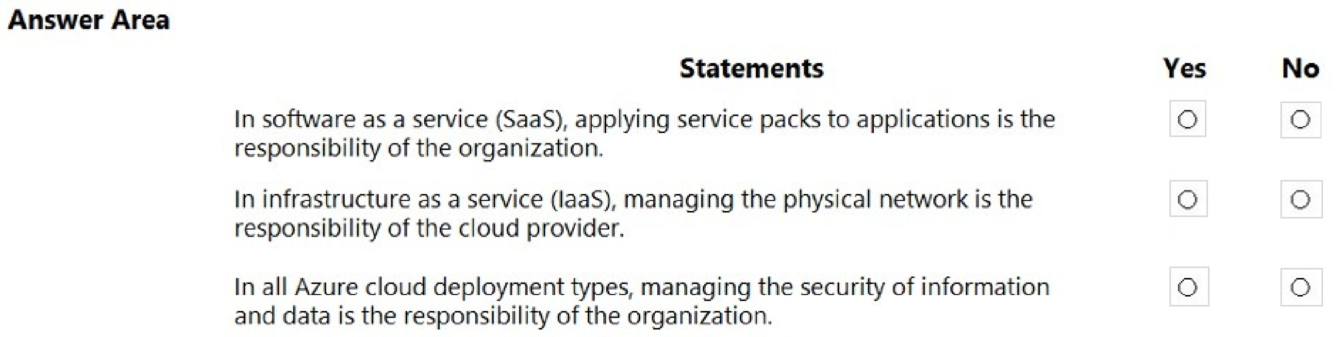
Plan and Define Strategy

Reference:

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview

Question: 19 CertyIQ

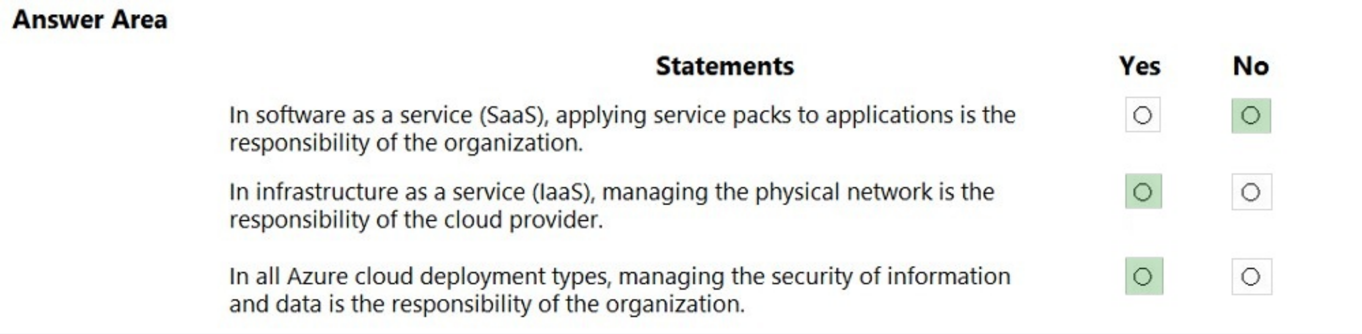
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

Explanation:

It’s NYY.

Question 2 say: Manaaging the physical network. That is the responsibility for Microsoft.

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

If it would have said “network controls” then it would have been NO as this is the responsibility for the customer

Assume we take this services SAAS , Iaas or

1 : In Saas - system updates - Cloud Provider

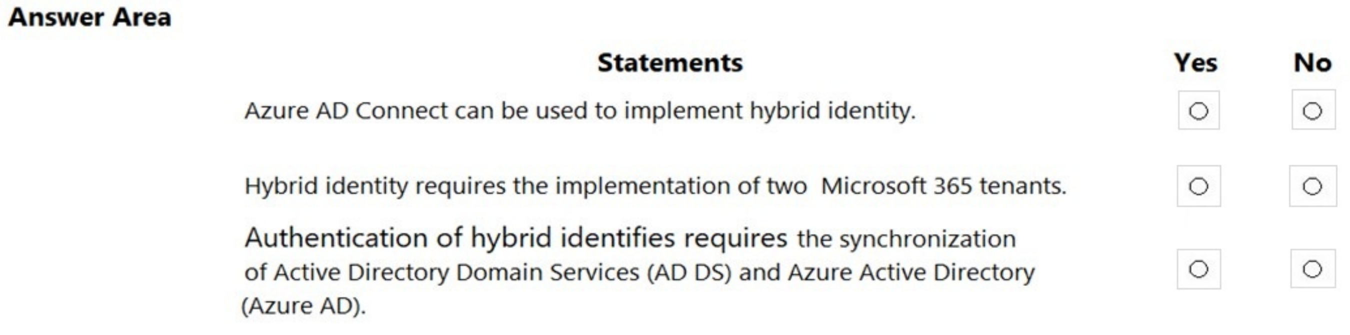
2 : We take Iaas : Physical Network - Cloud Provider

3. We take cloud services which provides IAAS, Saas Paas from provider , We give data and information - organization

Question: 20

CertyIQ

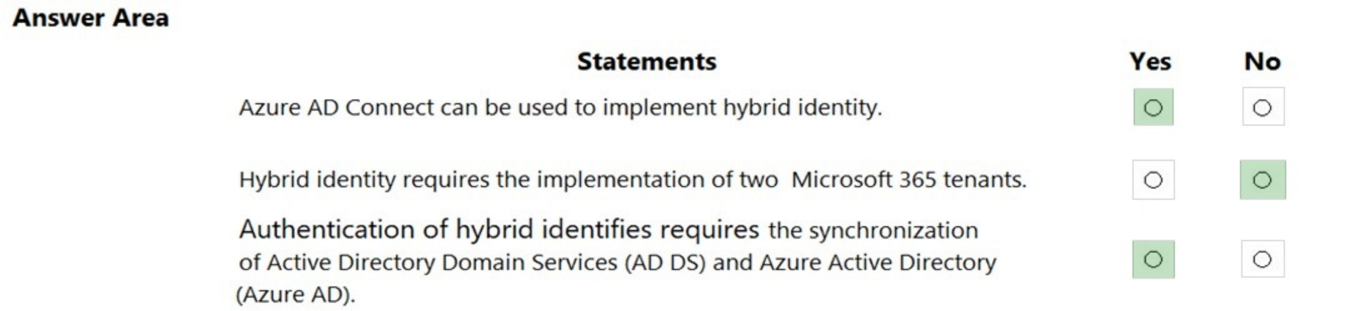
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



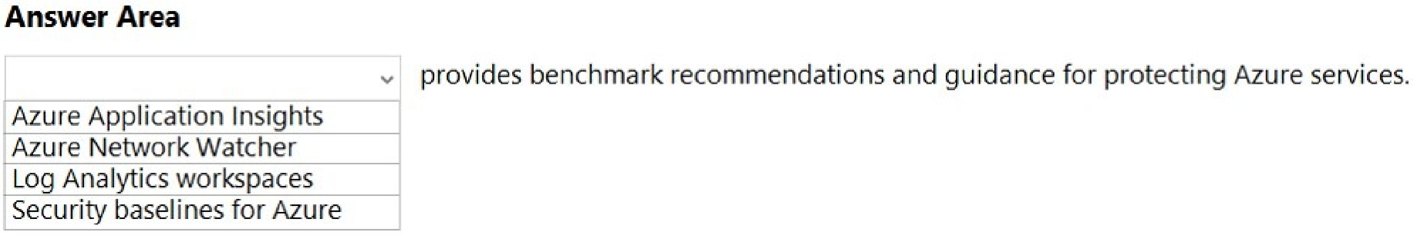
Answer Area

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

Question: 21

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

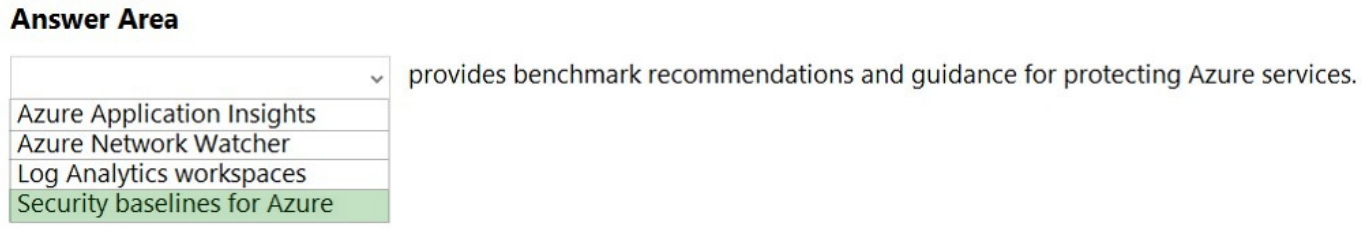


Answer Area

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

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

Answer:



Answer Area

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

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

Explanation:

"Security baselines for Azure help you strengthen security through improved tooling, tracking, and security features. They also provide you a consistent experience when securing your environment."

Reference:

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

Question: 22

CertyIQ

What is an example of encryption at rest?

A. encrypting communications by using a site-to-site VPN
B. encrypting a virtual machine disk
C. accessing a website by using an encrypted HTTPS connection
D. sending an encrypted email

Answer: B

Explanation:

Encryption at rest for PaaS customers

Platform as a Service (PaaS) customer's data typically resides in a storage service such as Blob Storage but may also be cached or stored in the application execution environment, such as a virtual machine. To see the encryption at rest options available to you, examine the Data encryption models: supporting services table for the storage and application platforms that you use.

Reference:

https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

Question: 23

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.

Answer: BCD

Explanation:

Zero Trust is a security a strategy. It is not a product or a service, but an approach in designing and implementing the following set of security principles:

Verify explicitly

Use least privilege access

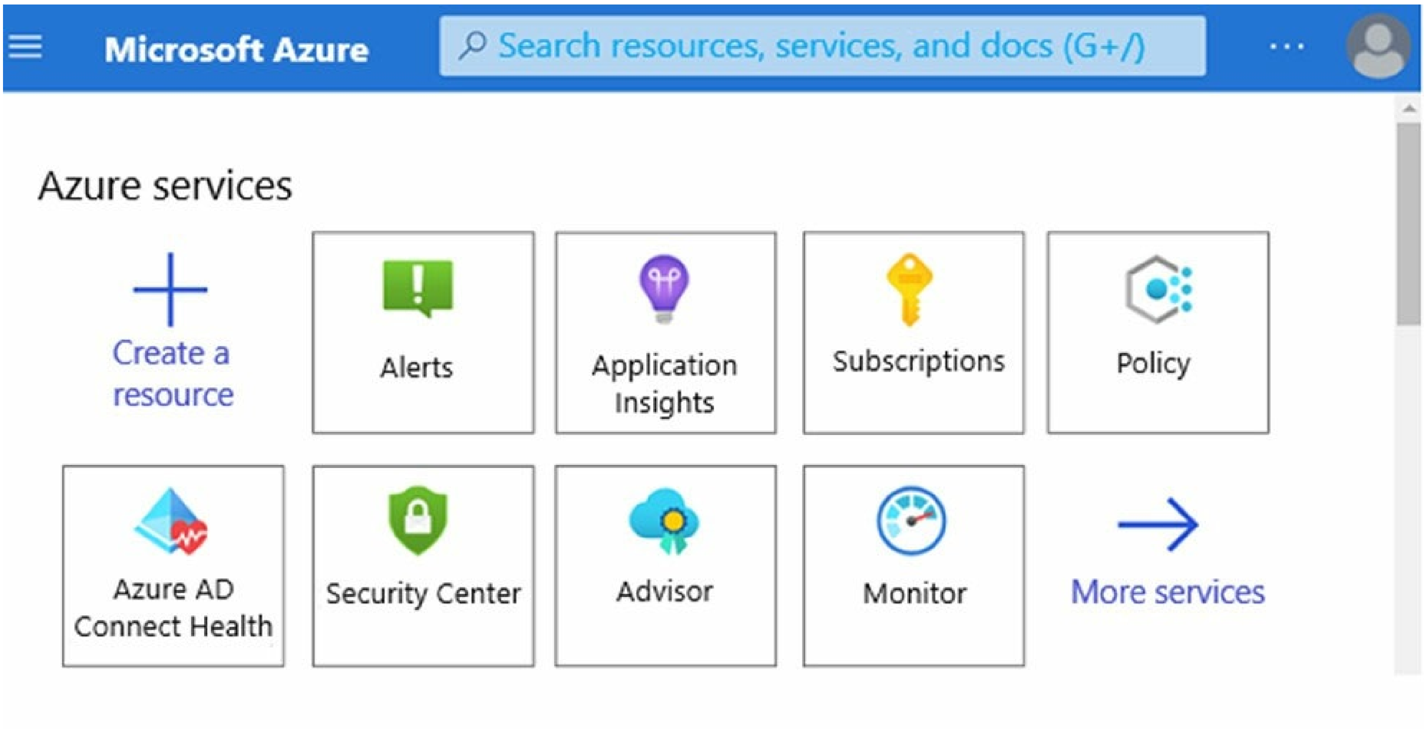
Assume breach

Reference:

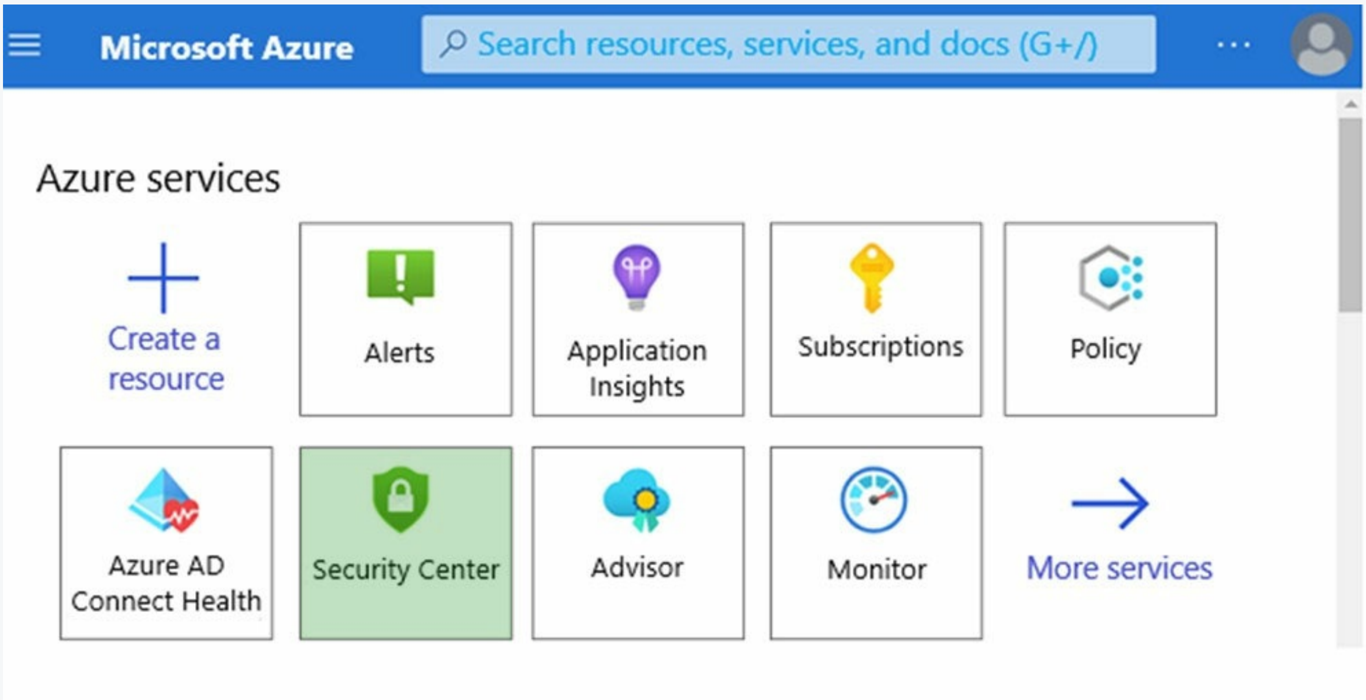
https://docs.microsoft.com/en-us/security/zero-trust/

Question: 24

HOTSPOT -
Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.
Hot Area:



Answer:



Explanation:

Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud

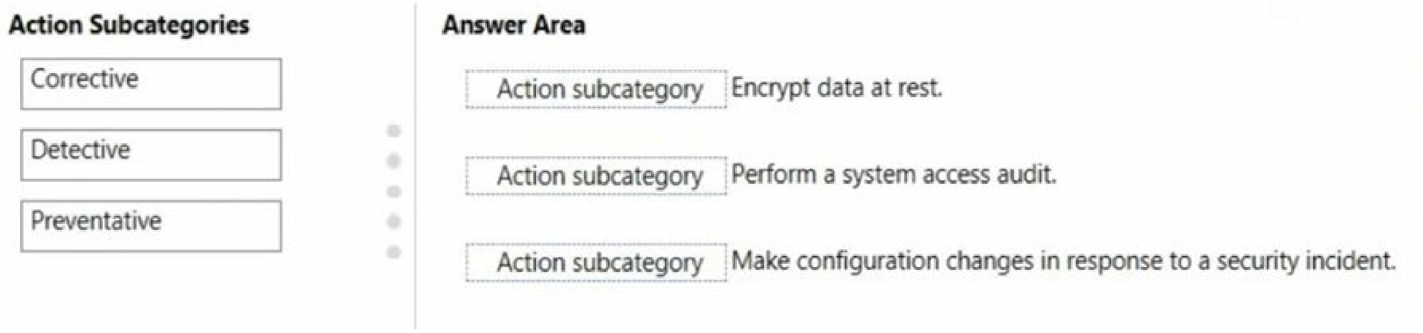
Reference:

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

Question: 25 CertyIQ

DRAG DROP -
You are evaluating the compliance score in 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

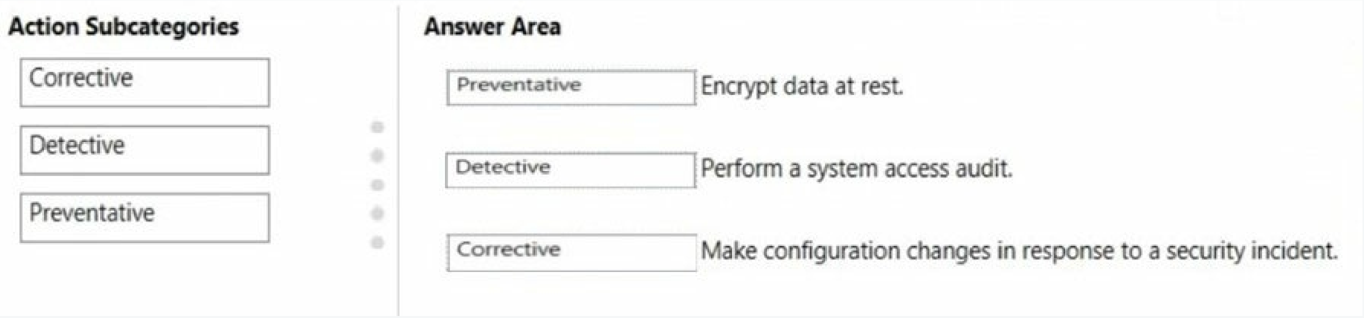
Detective

Preventative

Answer Area

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

Answer:



Action Subcategories

Corrective

Detective

Preventative

Answer Area

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

Explanation:

Box 1: Preventative -

Preventative actions address specific risks. For example, protecting information at rest using encryption is a preventative action against attacks and breaches.

Separation of duties is a preventative action to manage conflict of interest and guard against fraud.

Box 2: Detective -

Detective actions actively monitor systems to identify irregular conditions or behaviors that represent risk, or that can be used to detect intrusions or breaches.

Examples include system access auditing and privileged administrative actions. Regulatory compliance audits are a type of detective action used to find process issues.

Box 3: Corrective -

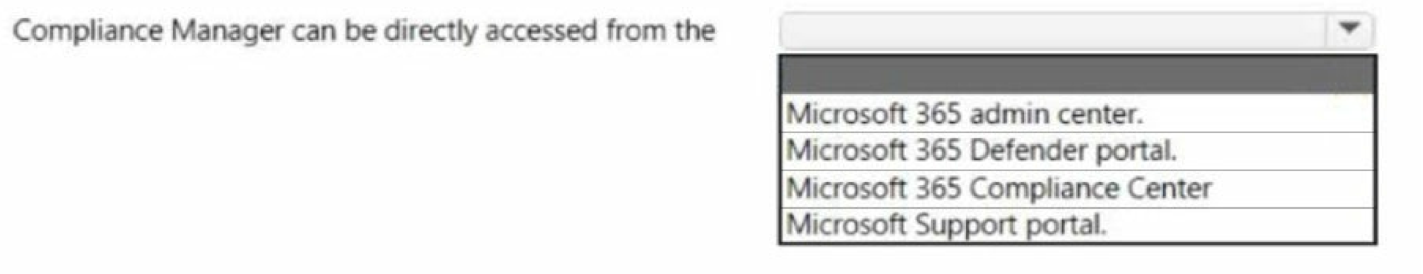
Corrective actions try to keep the adverse effects of a security incident to a minimum, take corrective action to reduce the immediate effect, and reverse the damage if possible. Privacy incident response is a corrective action to limit damage and restore systems to an operational state after a breach.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation

Question: 26 CertyIQ

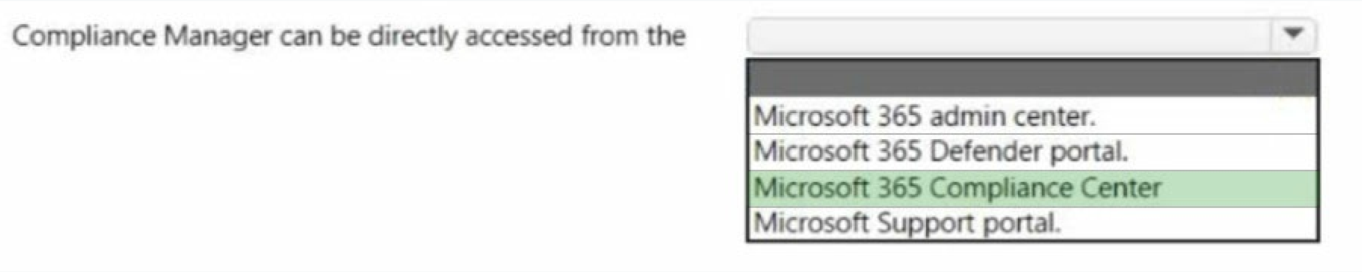
HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:



Compliance Manager can be directly accessed from the

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

Answer:



Compliance Manager can be directly accessed from the

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

Explanation:

Compliance Centre is now known as Microsoft Purview

Sign in to Compliance Manager -

1. Go to the Microsoft Purview compliance portal and sign in with your Microsoft 365 global administrator account.

2. Select Compliance Manager on the left navigation pane. You'll arrive at your Compliance Manager dashboard.

The direct link to access Compliance Manager is https://compliance.microsoft.com/compliancemanager

Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.

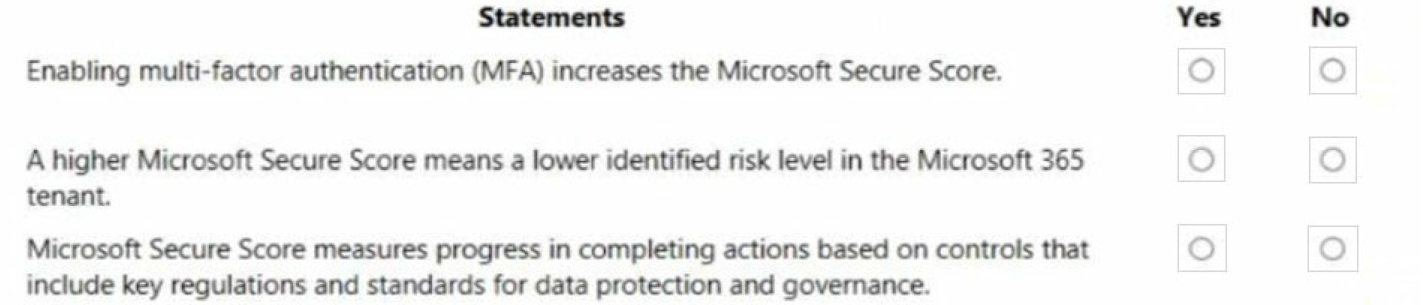
Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup

Question: 27

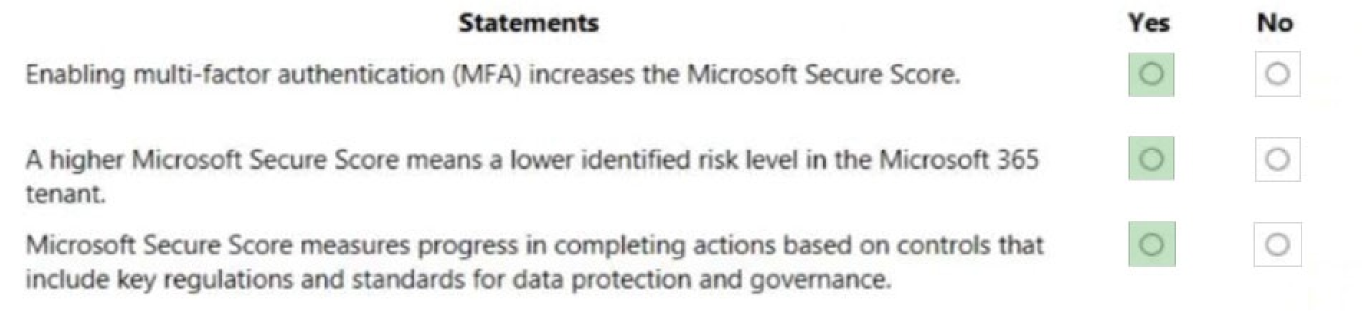
CertyIQ

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
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	○	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	○	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	○	○

Answer:



Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	[✓ ○]	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	[✓ ○]	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	[✓ ○]	○

Explanation:

Box 1: Yes -

Microsoft Secure Score has updated improvement actions to support security defaults in Azure Active Directory, which make it easier to help protect your organization with pre-configured security settings for common attacks.

If you turn on security defaults, you'll be awarded full points for the following improvement actions:

Ensure all users can complete multi-factor authentication for secure access (9 points)

Require MFA for administrative roles (10 points)

Enable policy to block legacy authentication (7 points)

Box 2: Yes -

Each improvement action is worth 10 points or less, and most are scored in a binary fashion. If you implement the improvement action, like create a new policy or turn on a specific setting, you get 100% of the points. For other improvement actions, points are given as a percentage of the total configuration.

Note: Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Box 3: Yes -

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score

Question: 28

CertyIQ

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

Answer: A

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Require approval to activate privileged roles

Enforce multi-factor authentication to activate any role

Use justification to understand why users activate

Get notifications when privileged roles are activated

Conduct access reviews to ensure users still need roles

Download audit history for internal or external audit

Prevents removal of the last active Global Administrator role assignment

Question: 29 CertyIQ

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. Microsoft Sentinel
C. Azure AD Connect
D. Azure AD Privileged Identity Management (PIM)

Answer: C

Explanation:

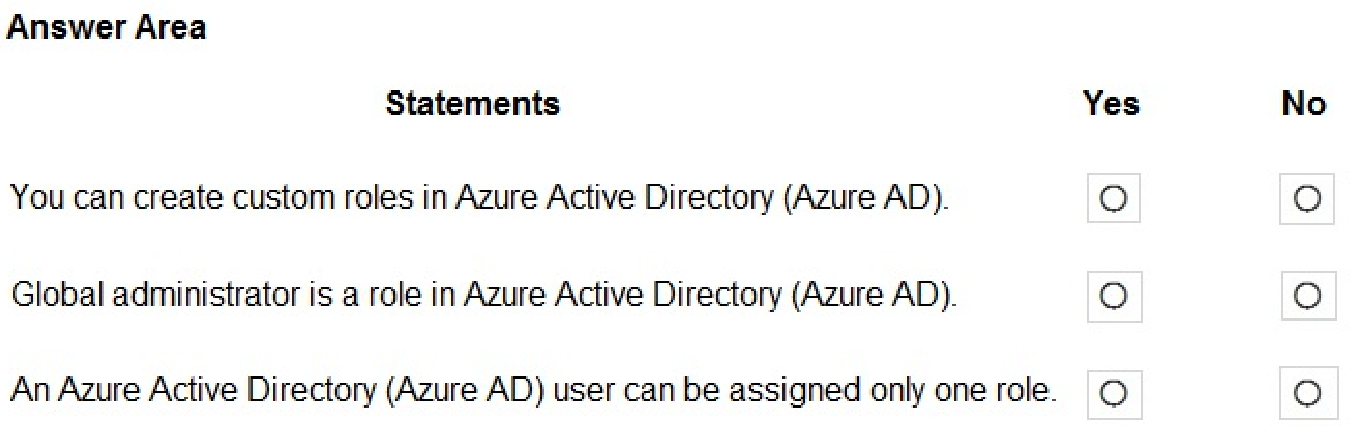
Azure AD Connect Sync Server,

Reference:

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

Question: 30 CertyIQ

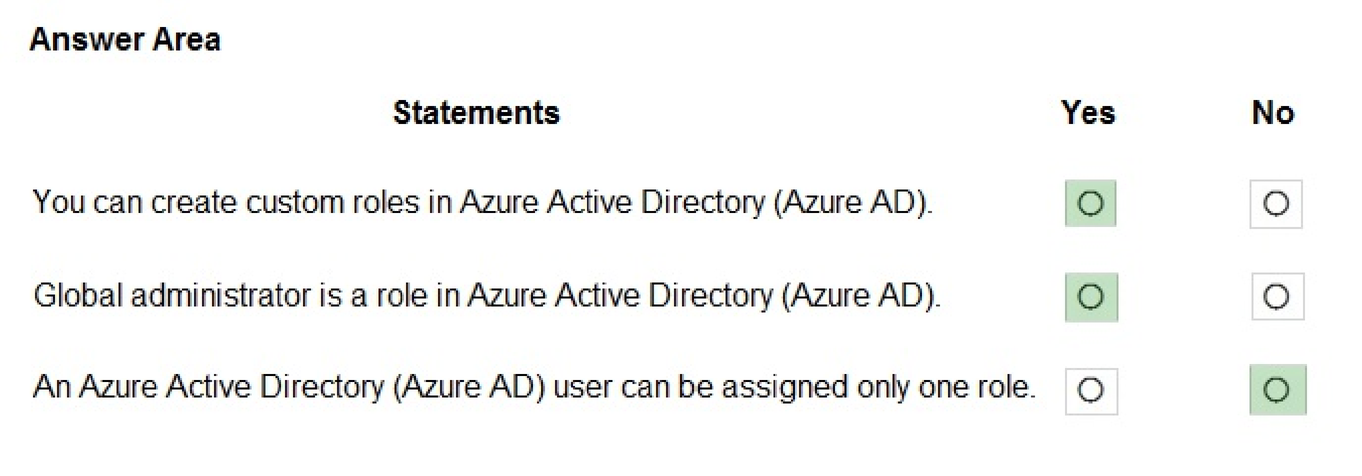
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	○	●

Explanation:
Box 1: Yes -
Azure AD supports custom roles.

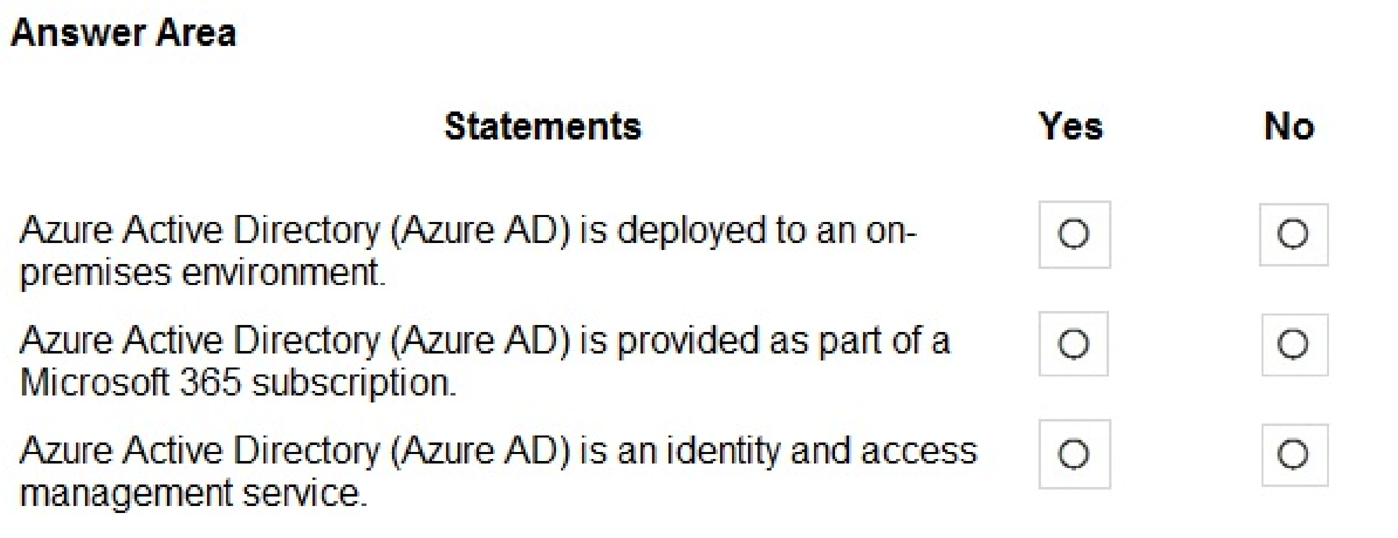
Box 2: Yes -
Global Administrator has access to all administrative features in Azure Active Directory.

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: 31 CertyIQ

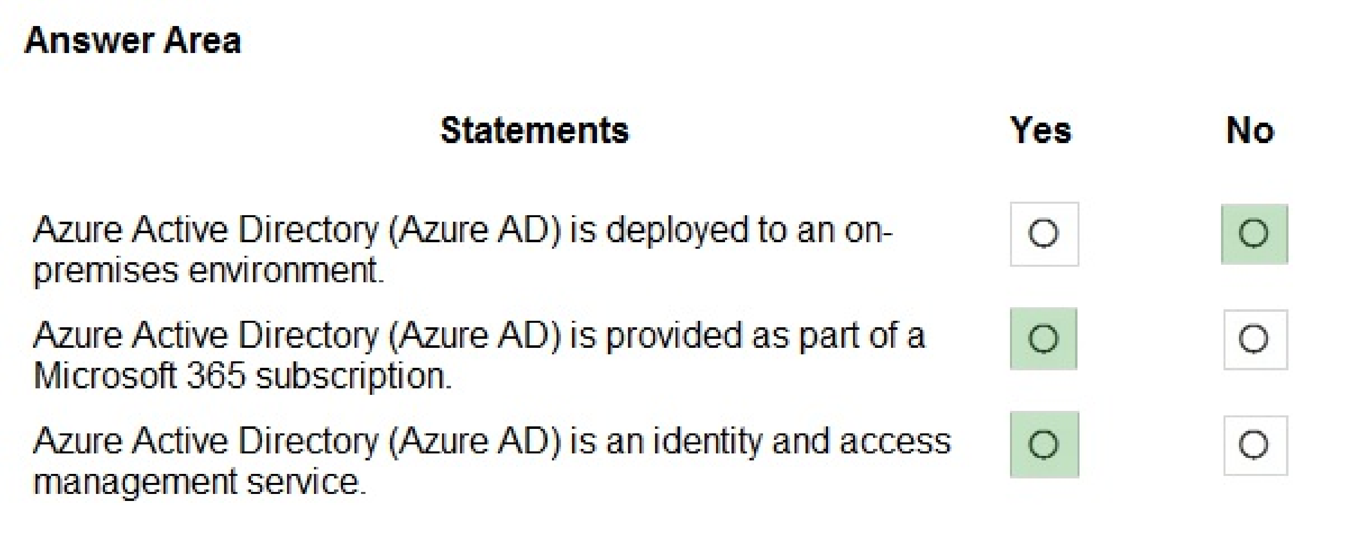
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	[✓ ○]	○

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

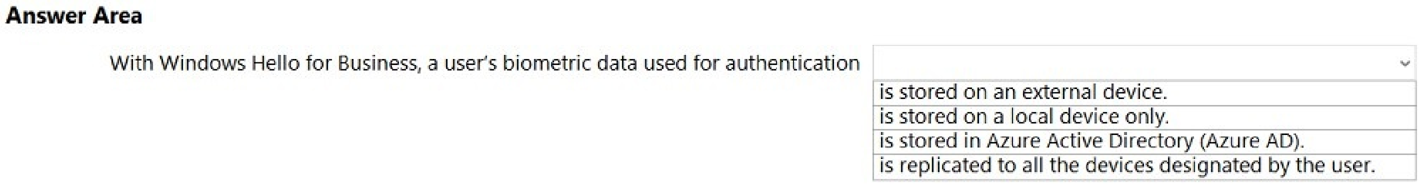
Question: 32

CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

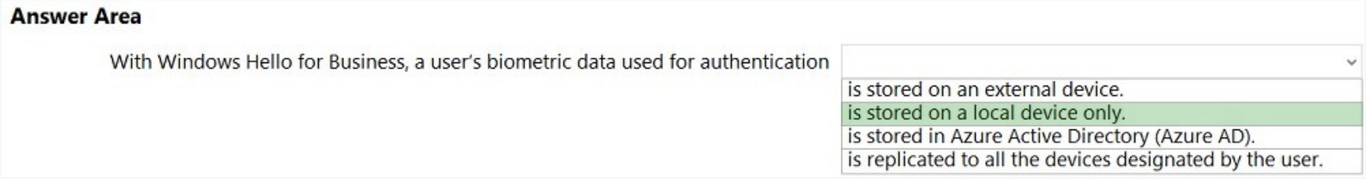


Answer Area

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:



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.

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: 33 CertyIQ

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

Answer: D

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: 34 CertyIQ

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

Answer: A

Explanation:

there is no capability to AUTOMATICALLY remove user access rights. The whole point of (manual user-driven) access reviews is that in some cases automation isn't possible. (See the link already provided here: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview)

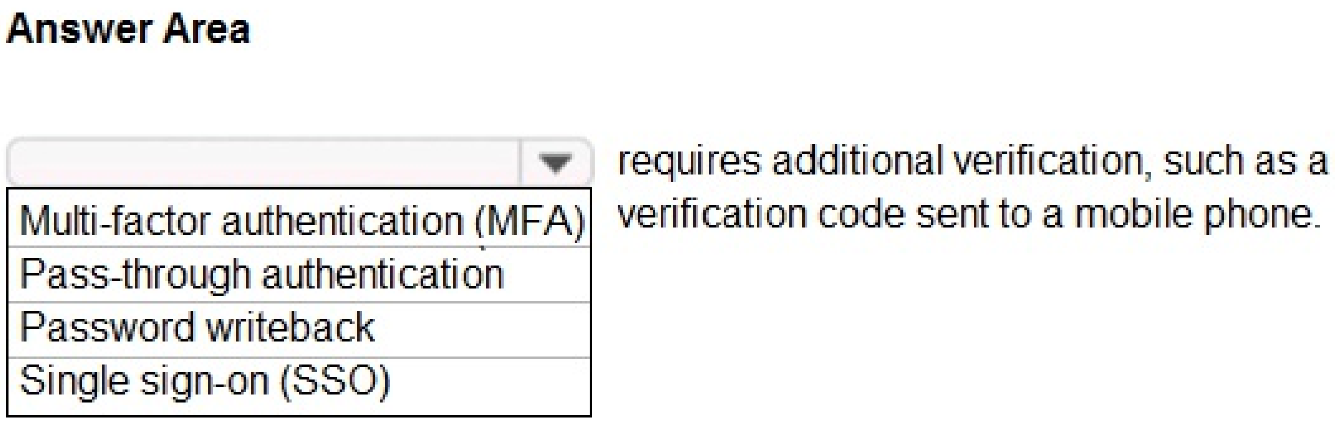
Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

Reference:

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

Question: 35 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

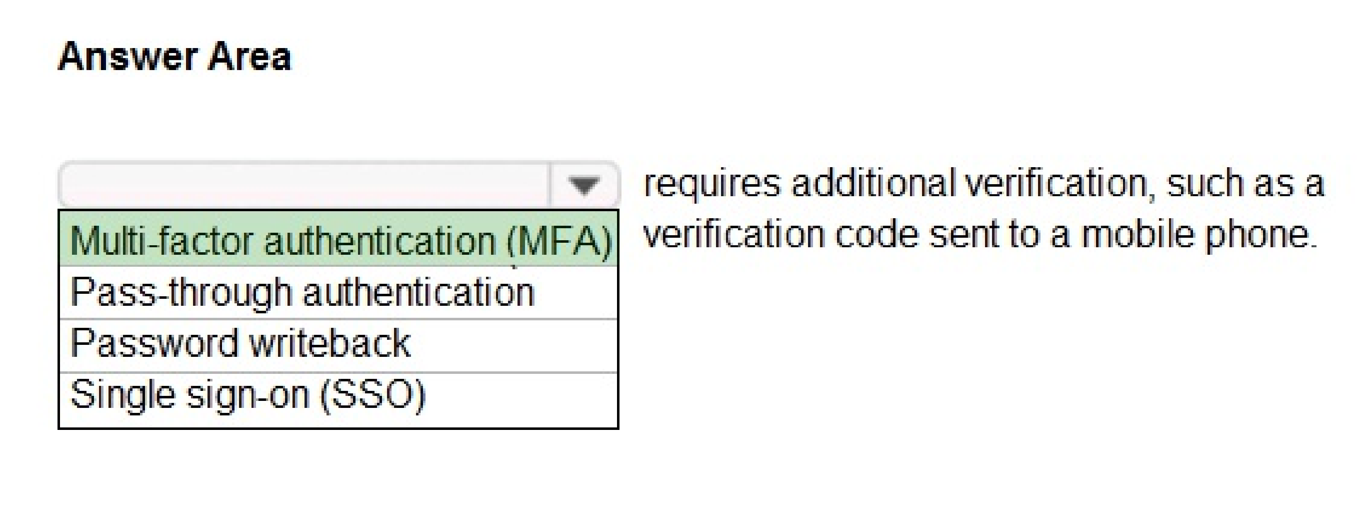


Answer Area

[▼] 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:



Answer Area

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

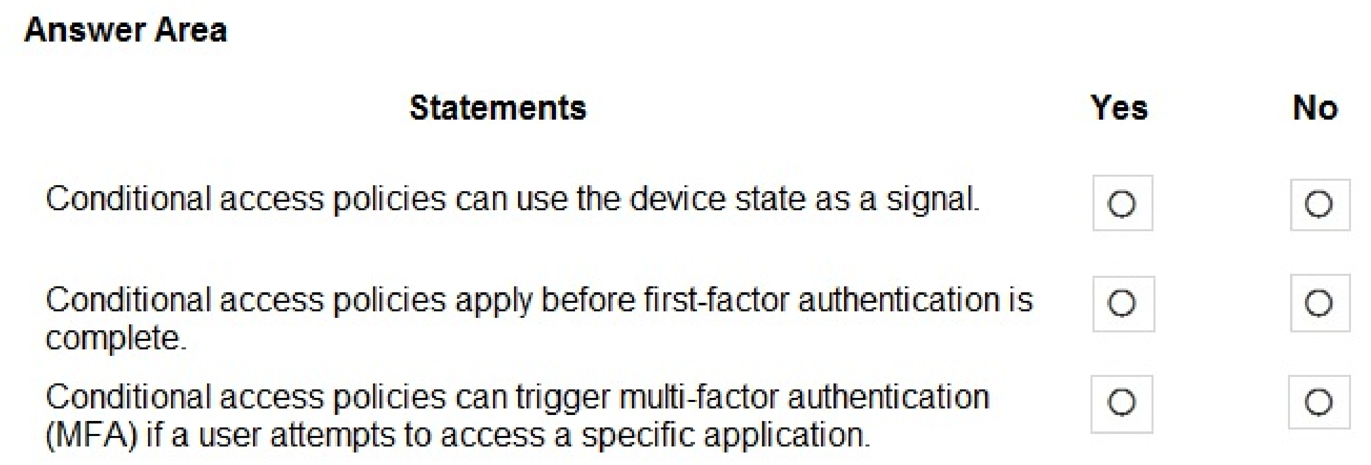
- [✓ Multi-factor authentication (MFA)]
- Pass-through authentication
- Password writeback
- Single sign-on (SSO)

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: 36

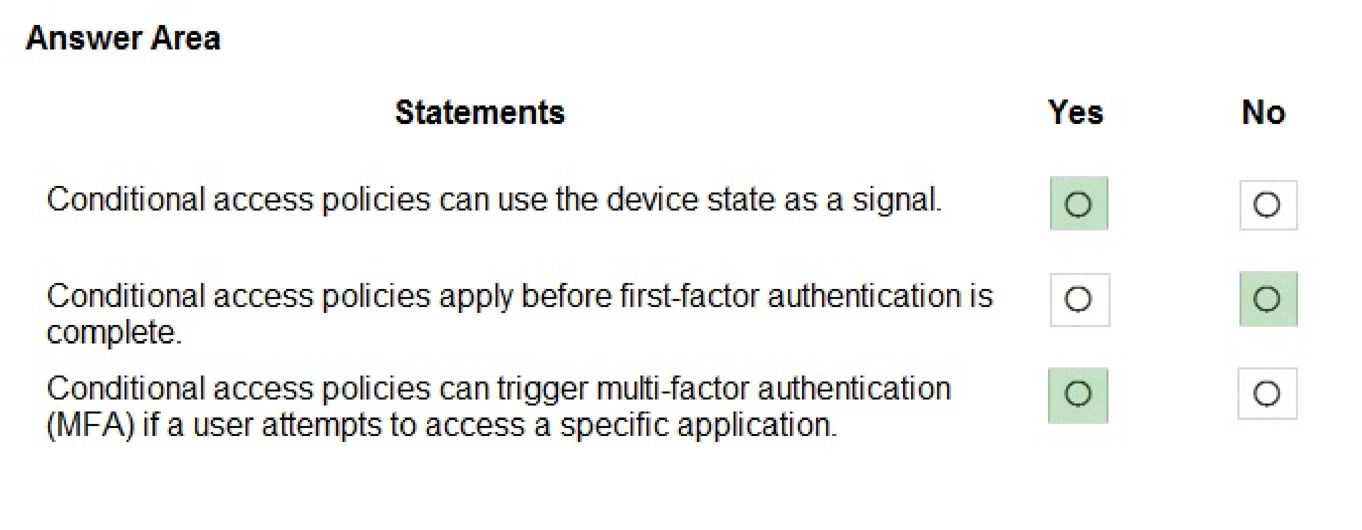
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
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:



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.	[✓ ○]	○

Explanation:
Box 1: Yes -

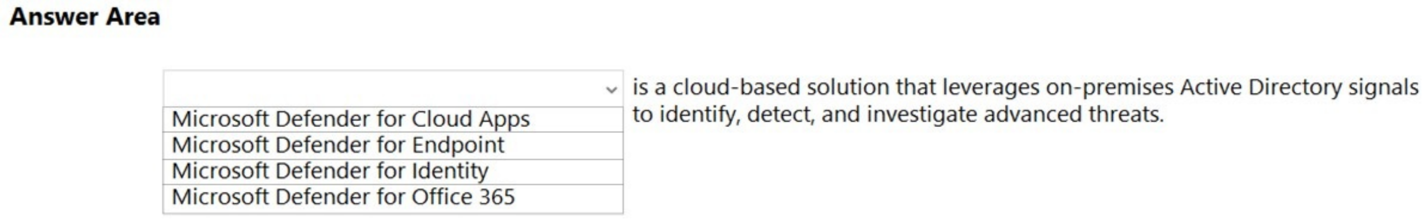
Box 2: No -
Conditional Access policies are enforced after first-factor authentication is completed.

Box 3: Yes -

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question: 37

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

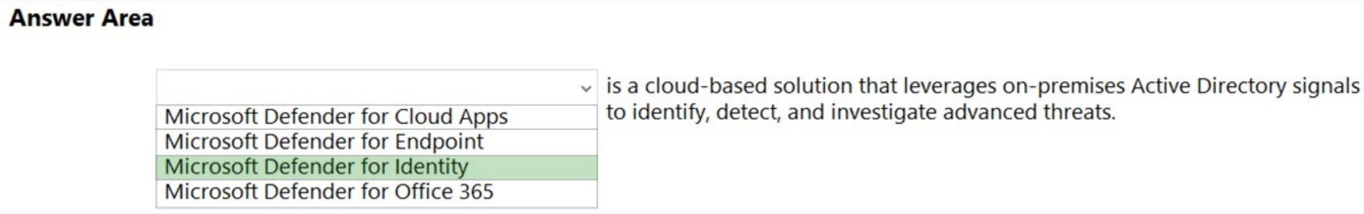


Answer Area

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

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

Answer:



Answer Area

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

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

Explanation:

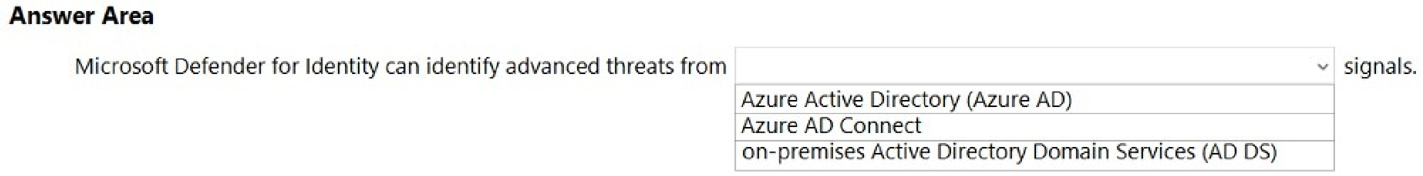
Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Reference:

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

Question: 38

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

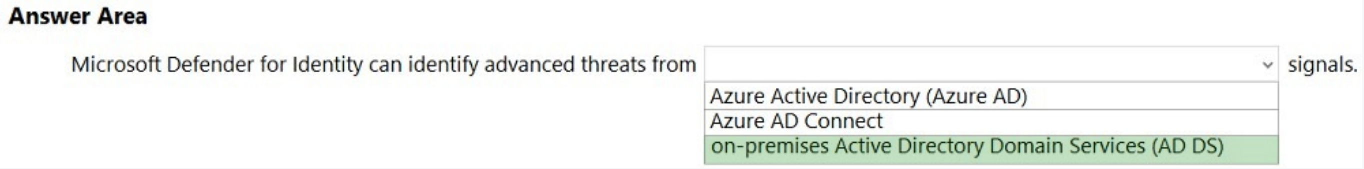


Answer Area

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:



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)]

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.

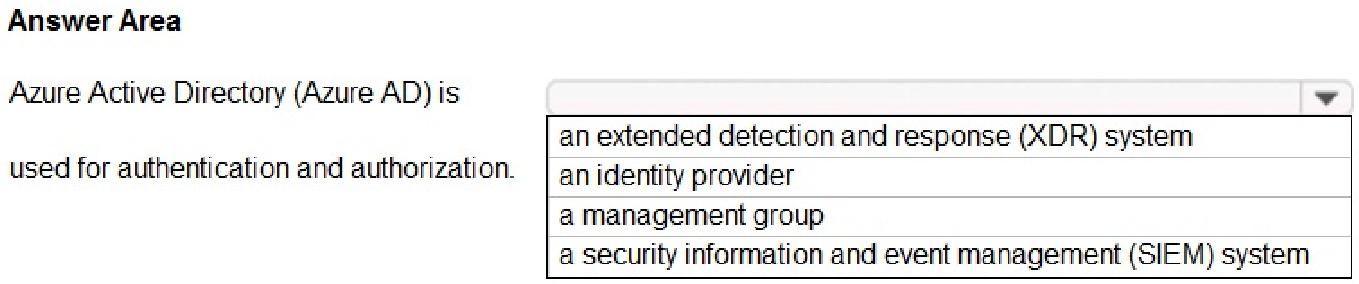
Reference:

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

Question: 39

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:



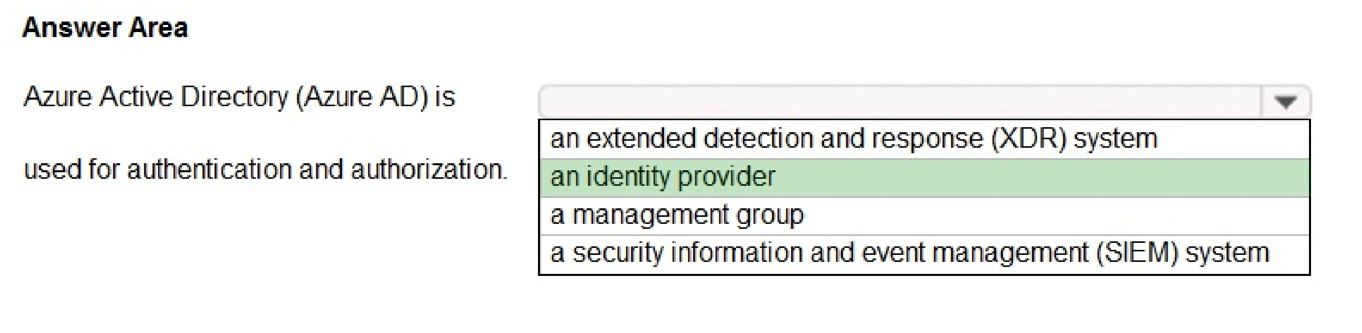
Answer Area

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:



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

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: 40

CertyIQ

Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

A. conditional access policies

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. authentication method policies

Answer: C

Explanation:

Azure AD Privileged Identity Management (PIM) provides just-in-time privileged access to Azure AD and Azure resources

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 41

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

Answer: ABD

Explanation:

Available verification methods

When users sign in to an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. Users can access My Profile to edit or add verification methods.

The following additional forms of verification can be used with Azure AD Multi-Factor Authentication:

Microsoft Authenticator app

Windows Hello for Business

FIDO2 security key

OATH hardware token (preview)

OATH software token

SMS

Voice call

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

Reference:

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

Question: 42

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

A. sensitivity label policies
B. Customer Lockbox
C. information barriers
D. Privileged Access Management (PAM)

Answer: C

Explanation:

INFORMATION BARRIERS are a Microsoft 365 feature which you can use to restrict communication and the sharing of information between members of two departments at your organization

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers

Question: 43

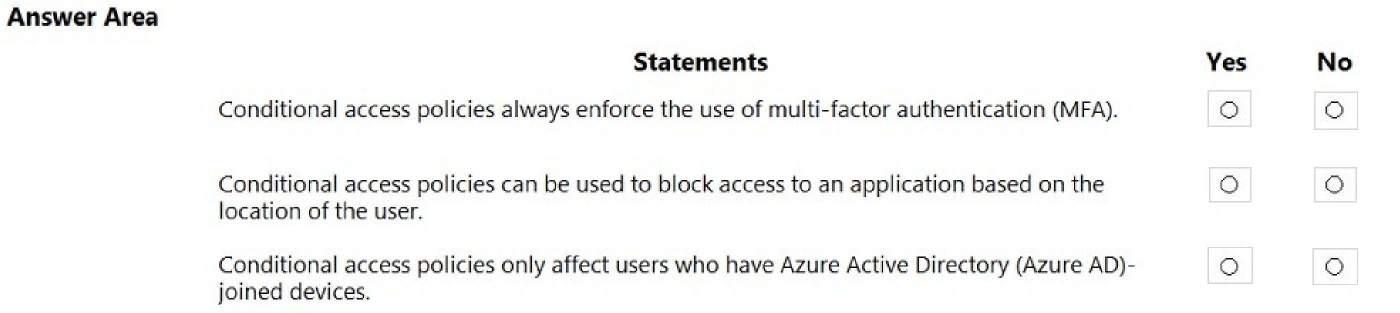
CertyIQ

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.

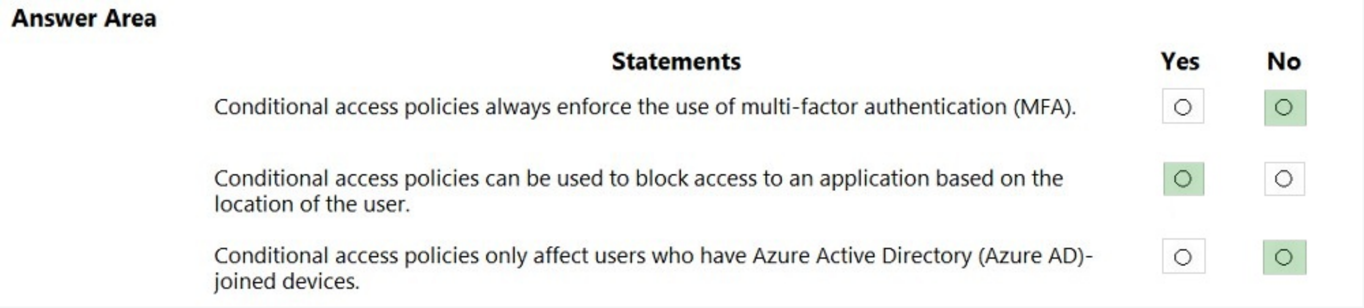
Hot Area:



Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	○	○
Conditional access policies can be used to block access to an application based on the location of the user.	○	○
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	○	○

Answer:



Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	○	●
Conditional access policies can be used to block access to an application based on the location of the user.	●	○
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	○	●

Explanation:

Reference:

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

Question: 44

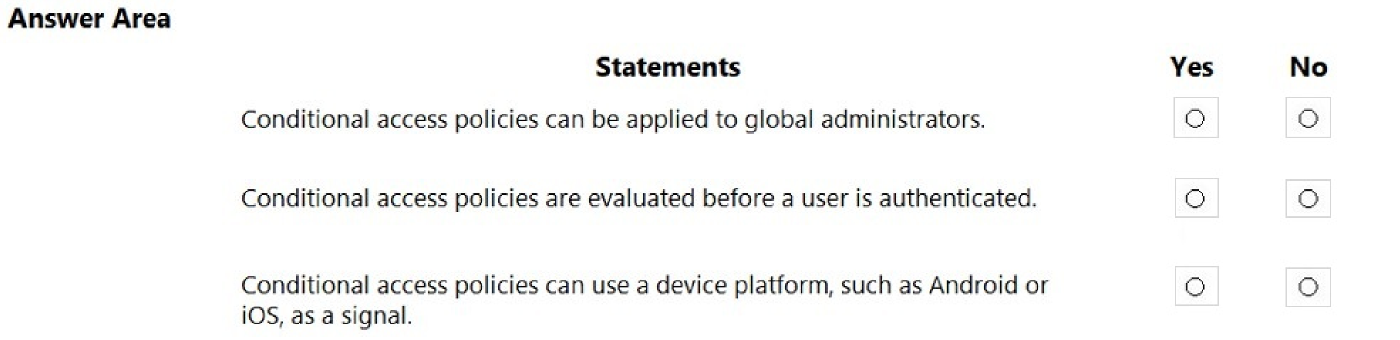
CertyIQ

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.

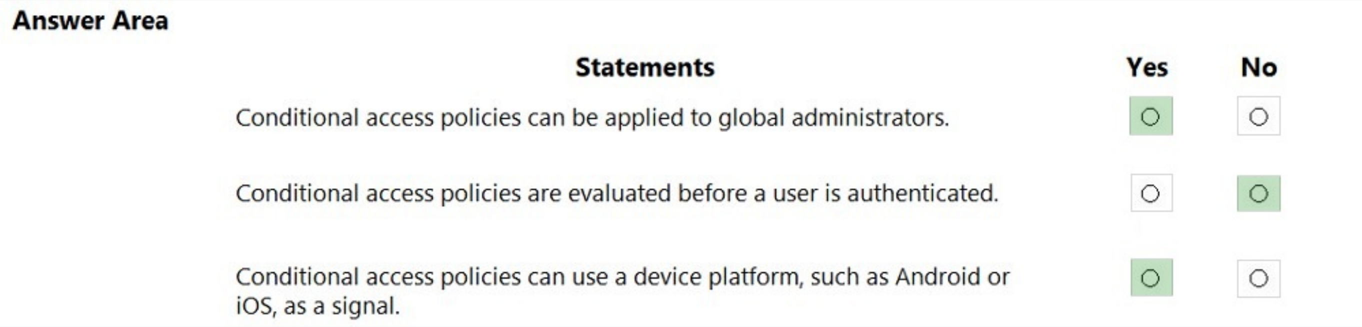
Hot Area:



Answer Area

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Answer:



Answer Area

Statements	Yes	No
Conditional access policies can be applied to global administrators.	[✓ ○]	○
Conditional access policies are evaluated before a user is authenticated.	○	[✓ ○]
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	[✓ ○]	○

Explanation:

Box 1: Yes -

Conditional access policies can be applied to all users

Box 2: No -

Conditional access policies are applied after first-factor authentication is completed.

Box 3: Yes -

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Reference:

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

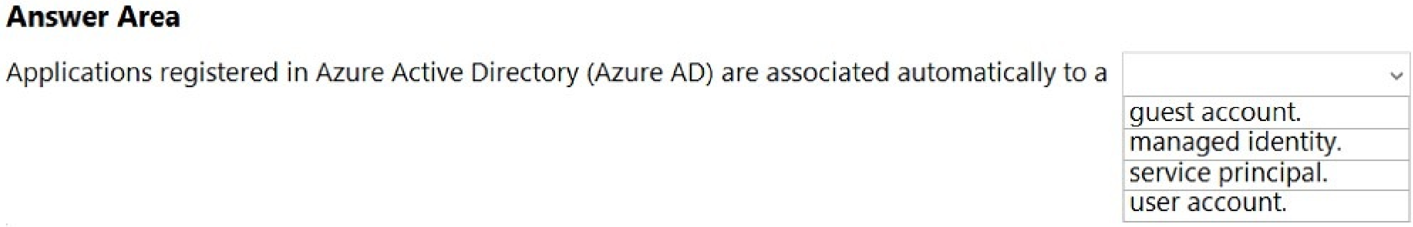
Question: 45

CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

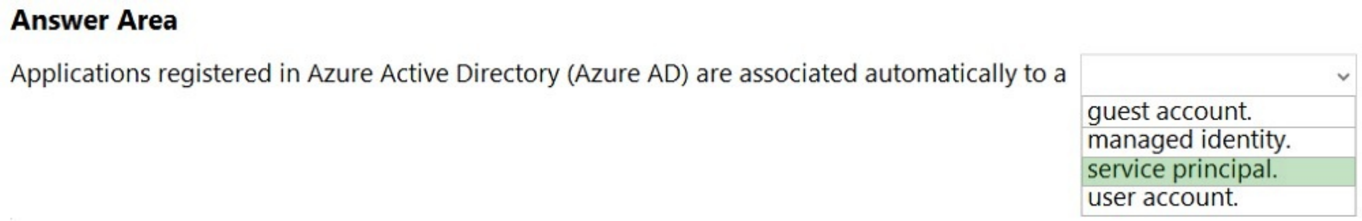


Answer Area

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

- guest account.
- managed identity.
- service principal.
- user account.

Answer:



Answer Area

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

- guest account.
- managed identity.
- [✓ service principal.]
- user account.

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.

A service principal is a security identity used to represent an application in Azure Active Directory (AAD). It is used to authenticate the application to access resources, and also to assign permissions to those resources.

A service principal is like a user identity (login and password or certificate) for an application.

An application object, on the other hand, is a representation of an application in Azure Active Directory. It contains information about the application, such as its name and URL, as well as its associated service principal.

In summary, a service principal is a security identity used to authenticate an application, while an application object is a representation of the application in Azure Active Directory that contains information about the application and its associated service principal.

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: 46

Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. fingerprint
B. facial recognition
C. PIN
D. email verification
E. security question

Answer: ABC

Explanation:

Windows Hello in Windows 10 enables users to sign in to their device using a PIN.
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password

Windows Hello lets your employees use fingerprint or facial recognition as an alternative method to unlocking a device. With Windows Hello, authentication happens when the employee provides his or her unique biometric identifier while accessing the device-specific Windows Hello credentials.

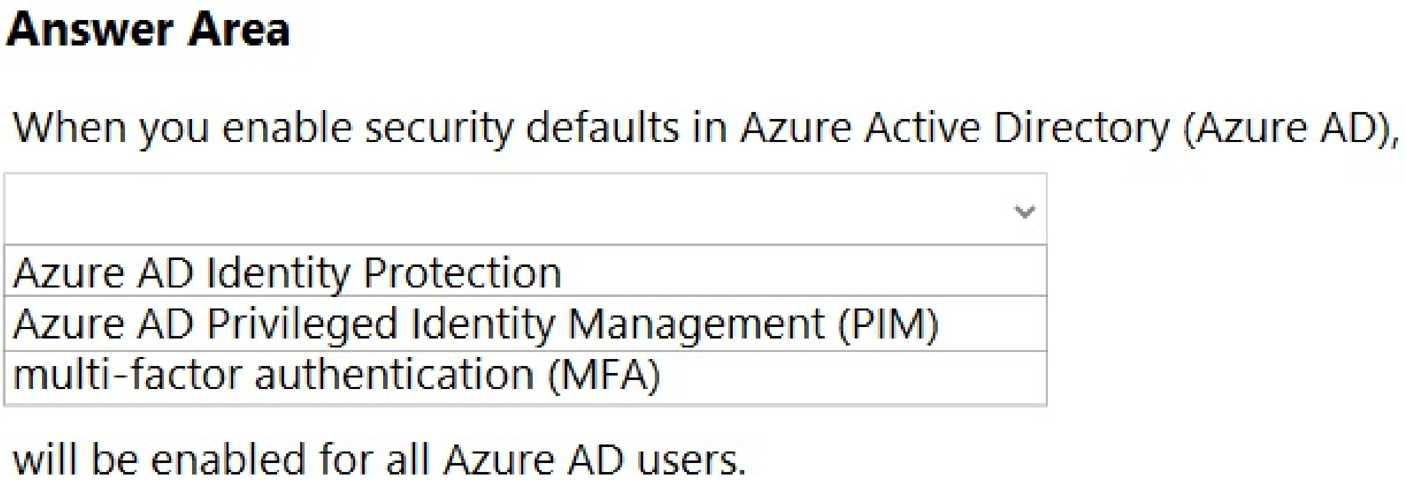
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication

Question: 47

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:



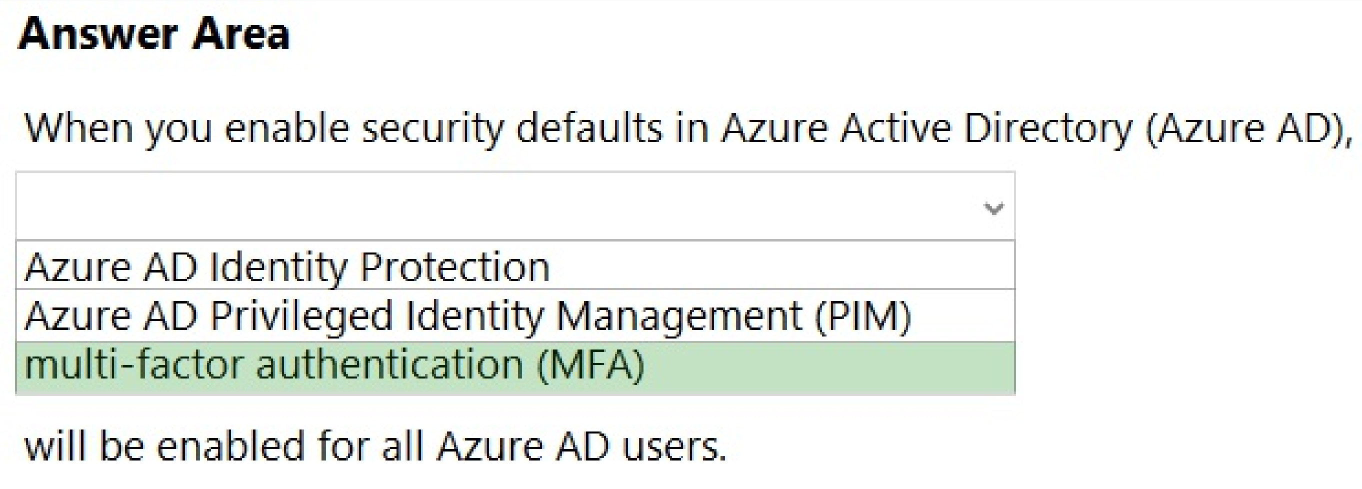
Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

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

will be enabled for all Azure AD users.

Answer:



Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

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

will be enabled for all Azure AD users.

Explanation:

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

Security defaults make it easier to help protect your organization from these attacks with 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: 48 CertyIQ

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)

Answer: D

Explanation:

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

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is designed specifically for implementing approval-based, time-bound role activation in an Azure subscription. PIM allows you to manage and control access to privileged roles in Azure AD, Azure resources, and Azure AD-integrated SaaS apps. It enables you to elevate access on a just-in-time basis and provides an approval workflow for role activation, which can be restricted to specific time periods. This makes it an ideal choice for implementing the requirements specified in the question.

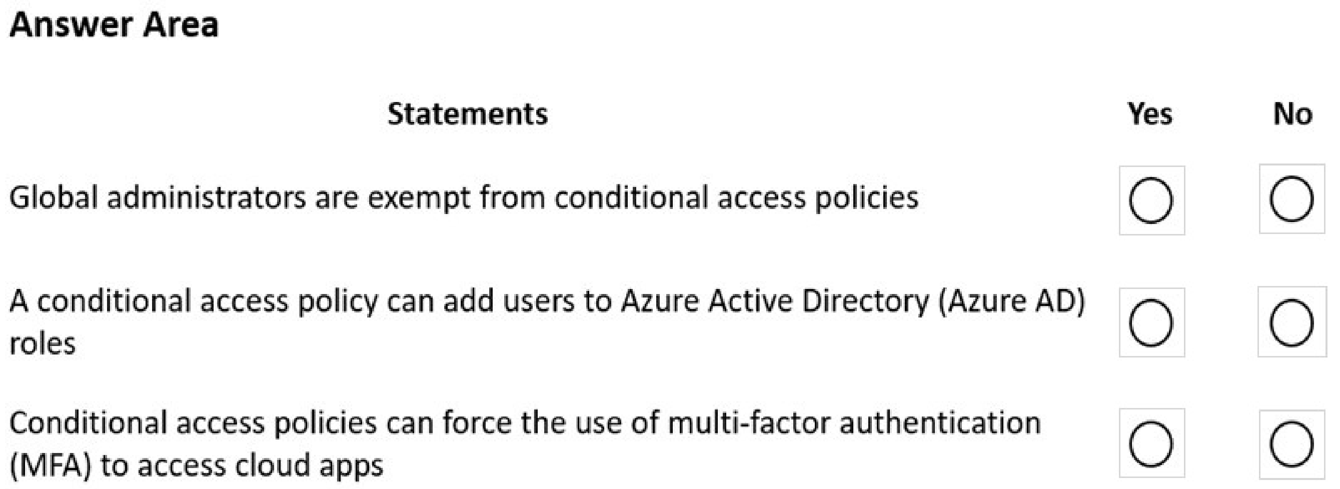
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 49

CertyIQ

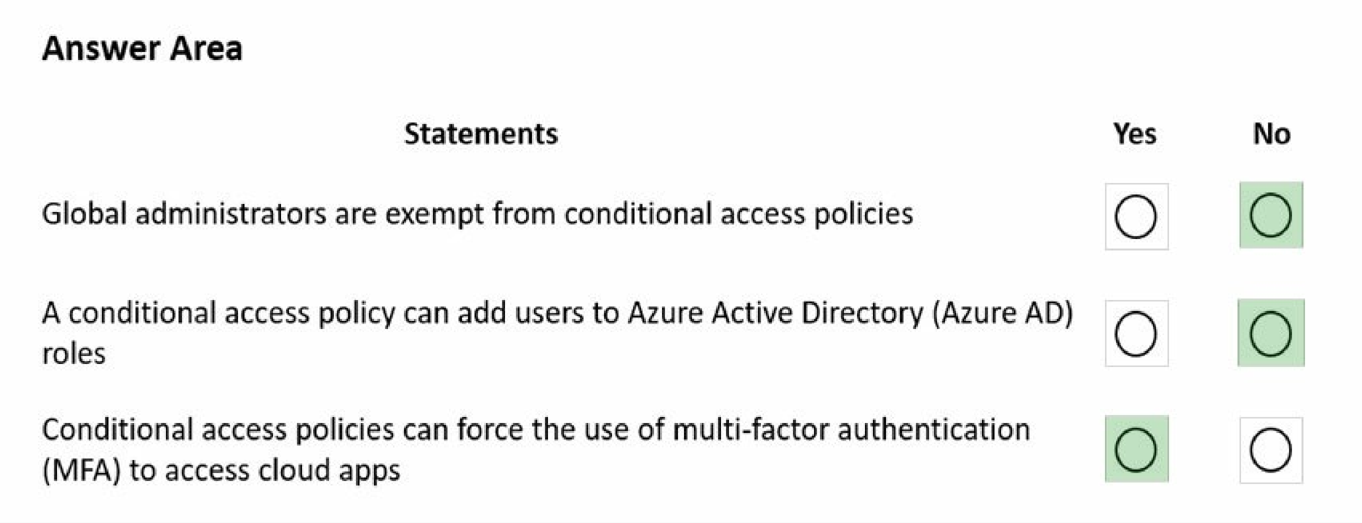
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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	[✓ ○]	○

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: 50 CertyIQ

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.

Answer: BC

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: 51 CertyIQ

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

Answer: D

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: 52 CertyIQ

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.

Answer: BCD

Explanation:

BCD

Directly from the SC-900 Fundamentals training slides:

Azure Identity Protection

Enables organizations to accomplish three key tasks:

• Automate the detection and remediation of identity based risks.

• Investigate risks using data in the portal.

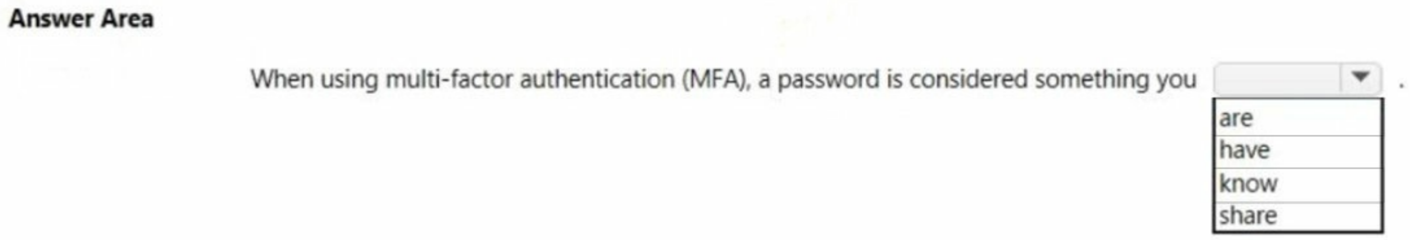
• Export risk detection data to third party utilities for further analysis.

Question: 53 CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.

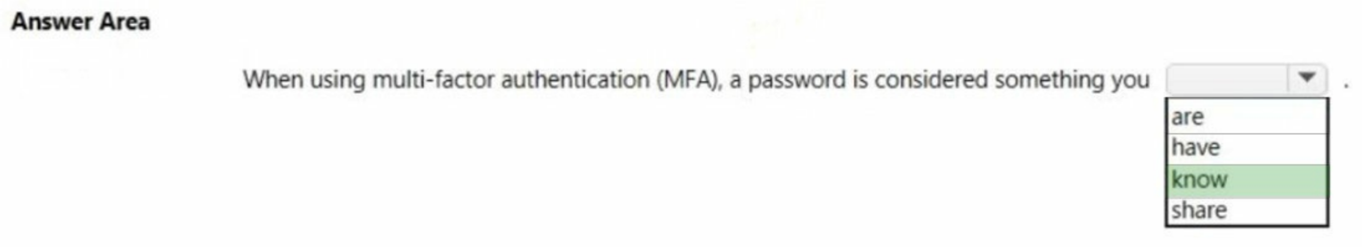
Hot Area:



Answer Area

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

Answer:



Answer Area

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

- are
- have
- [✓ know]
- share

Explanation:

Box 1: know -

Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

Reference:

https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Question: 54

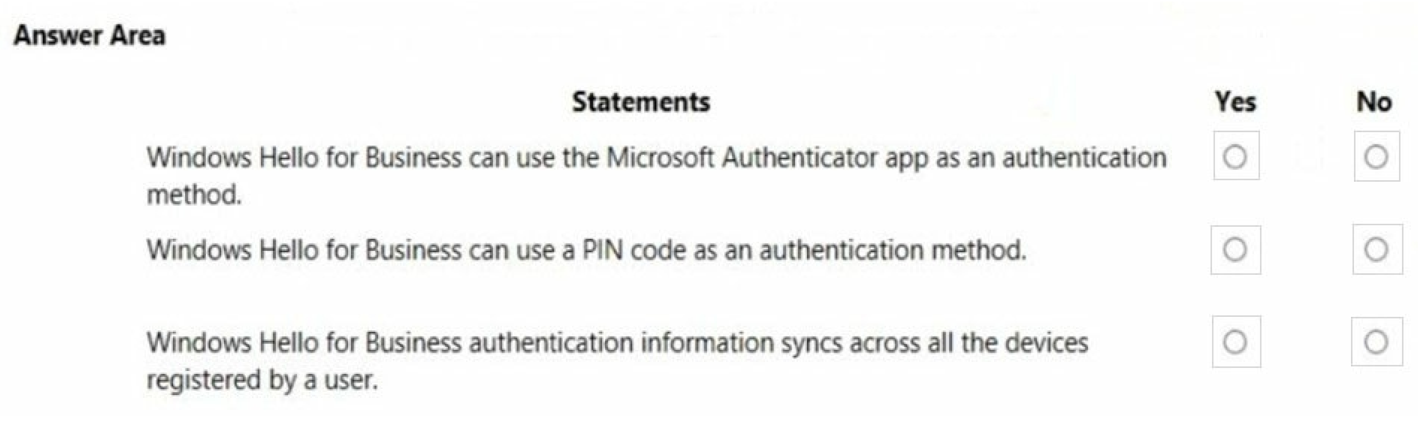
CertyIQ

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.

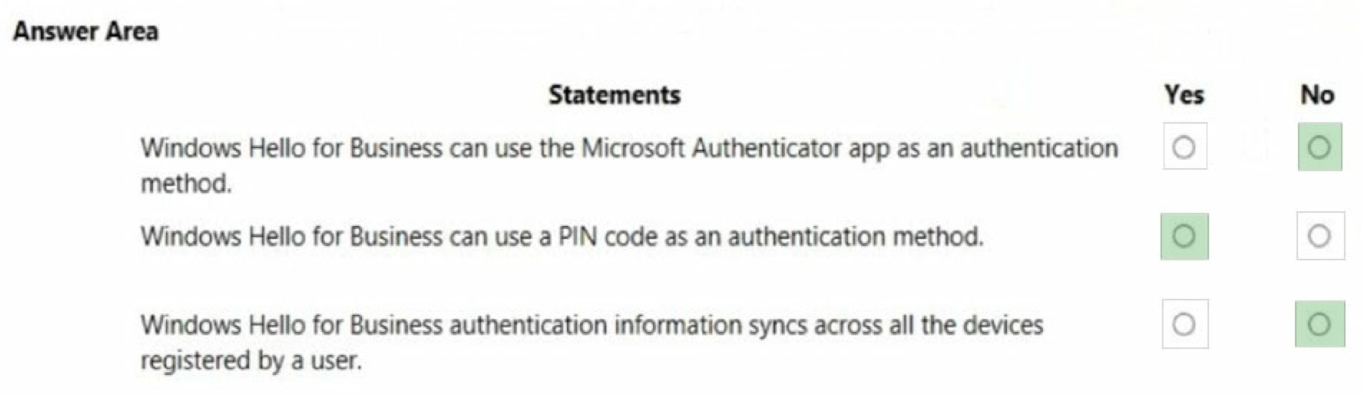
Hot Area:



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:



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.	○	[✓ ○]

Explanation:

Box 1: No -

The Microsoft Authenticator app helps you sign in to your accounts when you're using two-factor verification. Two-factor verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised. Two-factor verification uses a second factor like your phone to make it harder for other people to break in to your account.

Box 2: Yes -

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Box 3: No -

Windows Hello credentials are based on certificate or asymmetrical key pair. Windows Hello credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device.

Reference:

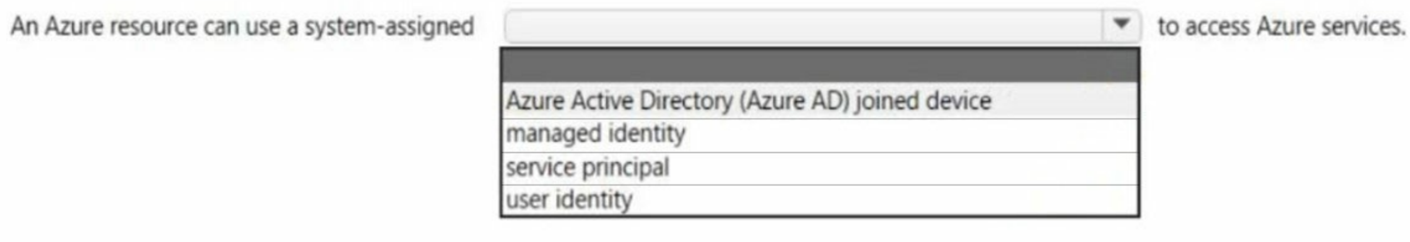
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Question: 55 CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.

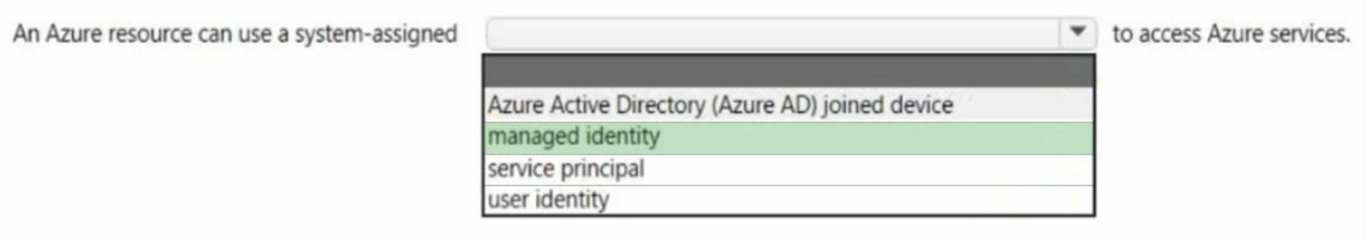
Hot Area:



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:



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

Explanation:

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

Here are some of the benefits of using managed identities:

You don't need to manage credentials. Credentials aren't even accessible to you.

You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.

Reference:

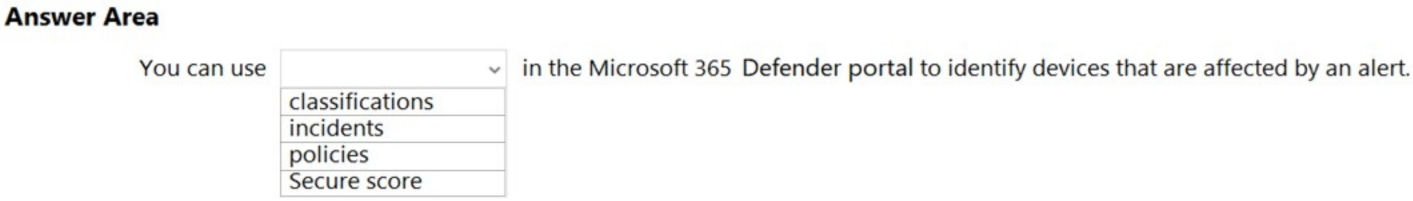
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question: 56 CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

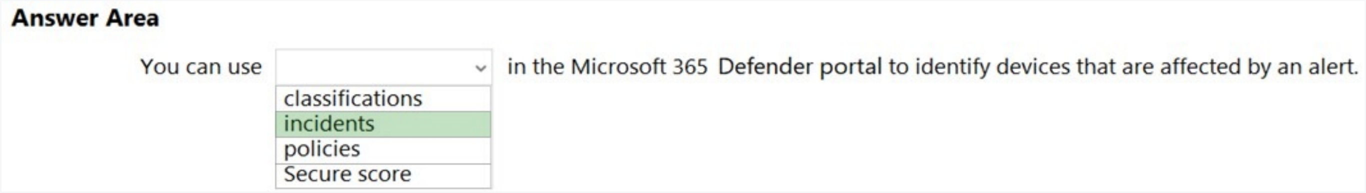


Answer Area

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

- classifications
- incidents
- policies
- Secure score

Answer:



Answer Area

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

- classifications
- incidents
- policies
- Secure score

Explanation:

Reference:

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

Question: 57

CertyIQ

What are two capabilities of Microsoft Defender for Endpoint? Each correct selection presents a complete solution.
NOTE: Each correct selection is worth one point.

A. automated investigation and remediation

B. transport encryption

C. shadow IT detection

D. attack surface reduction

Answer: AD

Explanation:

Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale. While The attack surface reduction set of capabilities provides the first line of defence in the stack.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide#microsoft-defender-for-endpoint

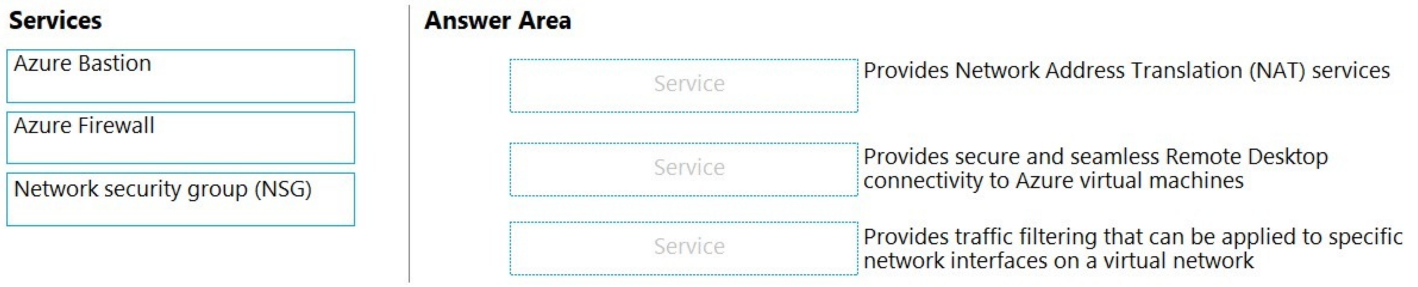
Reference:

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

Question: 58

CertyIQ

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



Services

Azure Bastion

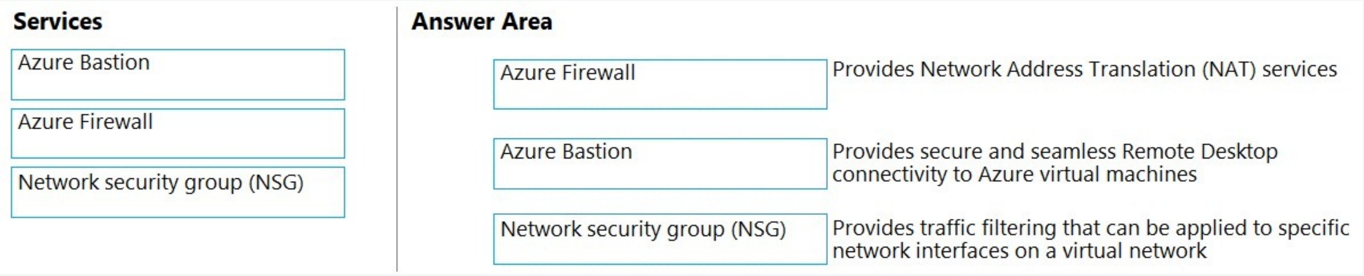
Azure Firewall

Network security group (NSG)

Answer Area

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

Answer:



Services

Azure Bastion

Azure Firewall

Network security group (NSG)

Answer Area

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

Explanation:

Box 1: Azure Firewall -

Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion -

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Box 3: Network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.

Reference:

https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview https://docs.microsoft.com/en-us/azure/bastion/bastion-overview https://docs.microsoft.com/en-us/azure/firewall/features https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

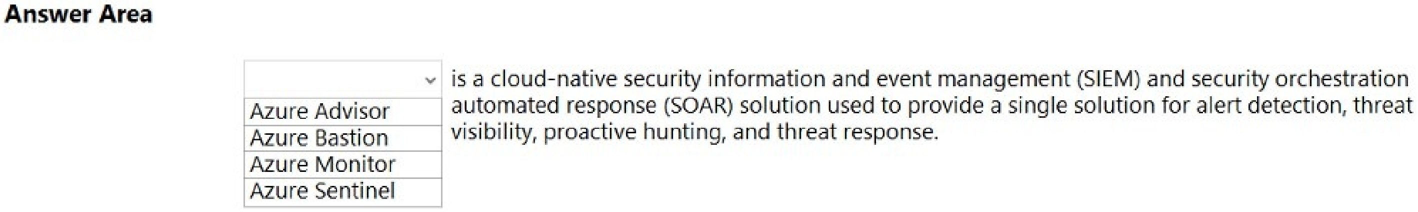
Question: 59

CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

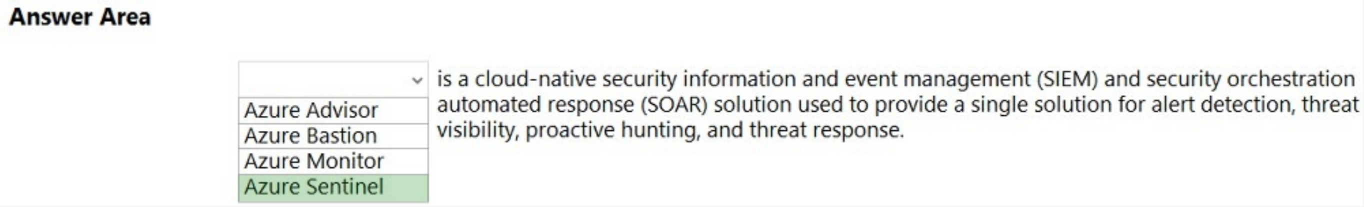


Answer Area

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

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

Answer:



Answer Area

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

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

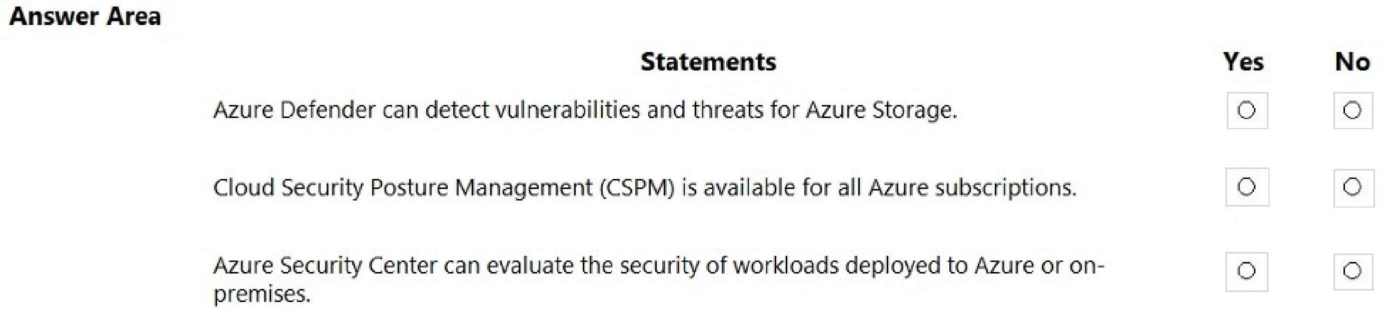
Explanation:

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: 60 CertyIQ

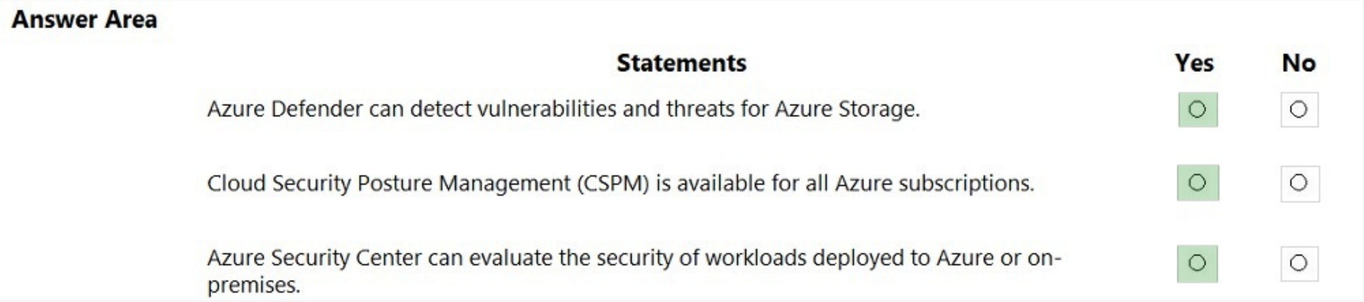
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	[✓ ○]	○

Explanation:

Box 1: Yes -
Microsoft Defender for Cloud 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.

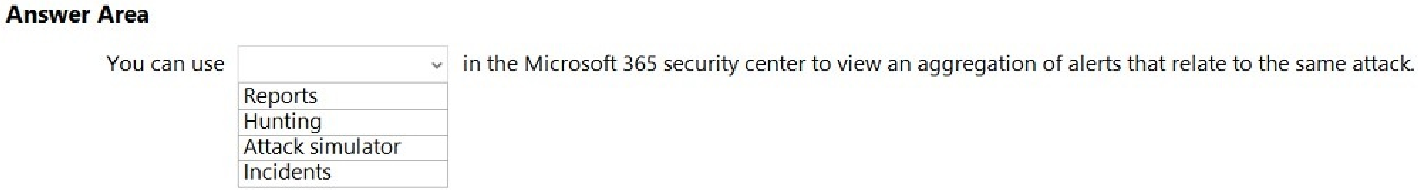
Box 3: Yes -
Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

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: 61 CertyIQ

HOTSPOT -

Select the answer that correctly completes the sentence.
Hot Area:

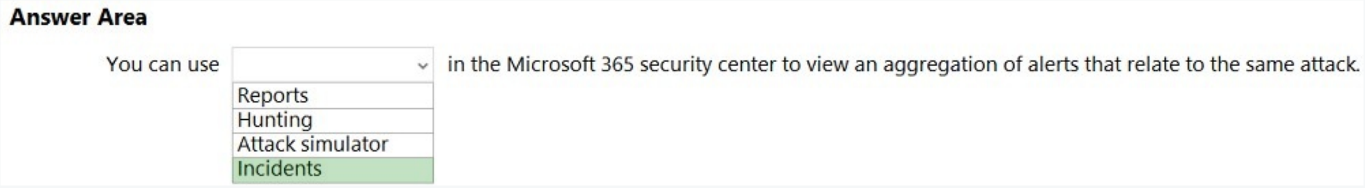


Answer Area

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

- Reports
- Hunting
- Attack simulator
- Incidents

Answer:



Answer Area

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

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

Explanation:

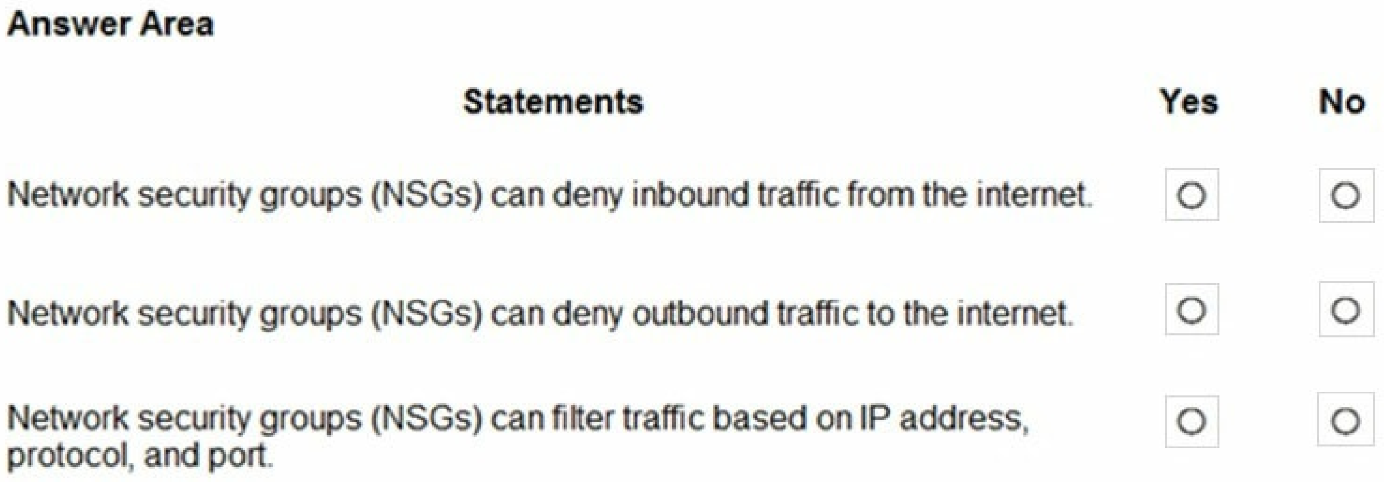
" A view of threat-related incidents which aggregate alerts into end-to-end attack stories across Microsoft Defender for Endpoint and Microsoft Defender for Office 365 to reduce the work queue, as well as simplify and speed up your investigation."

Reference:

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

Question: 62 CertyIQ

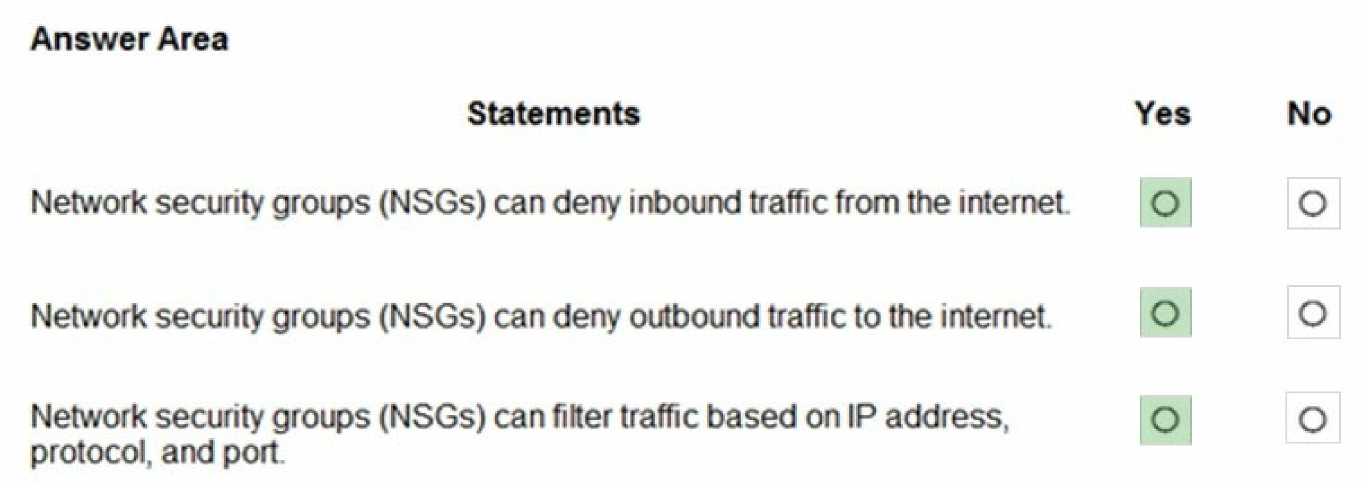
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	[✓ ○]	○

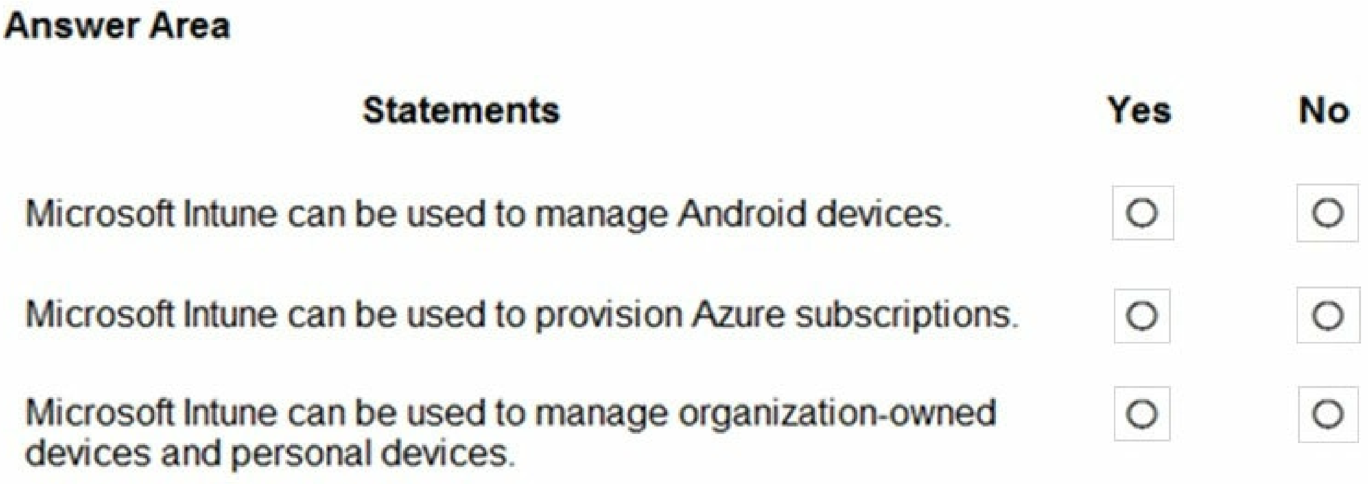
Explanation:

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: 63 CertyIQ

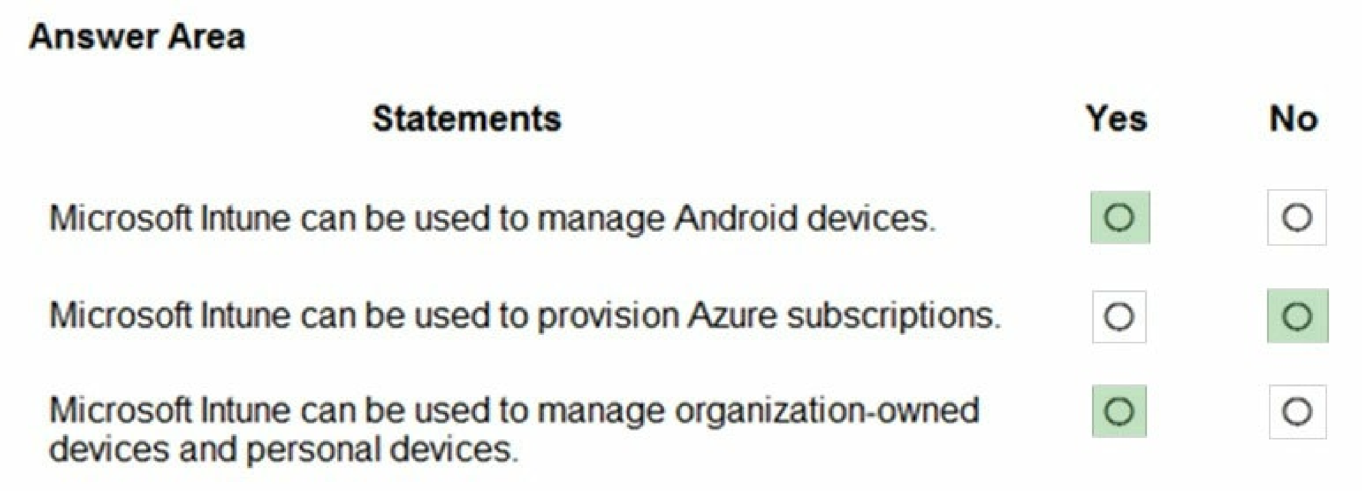
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



Answer Area

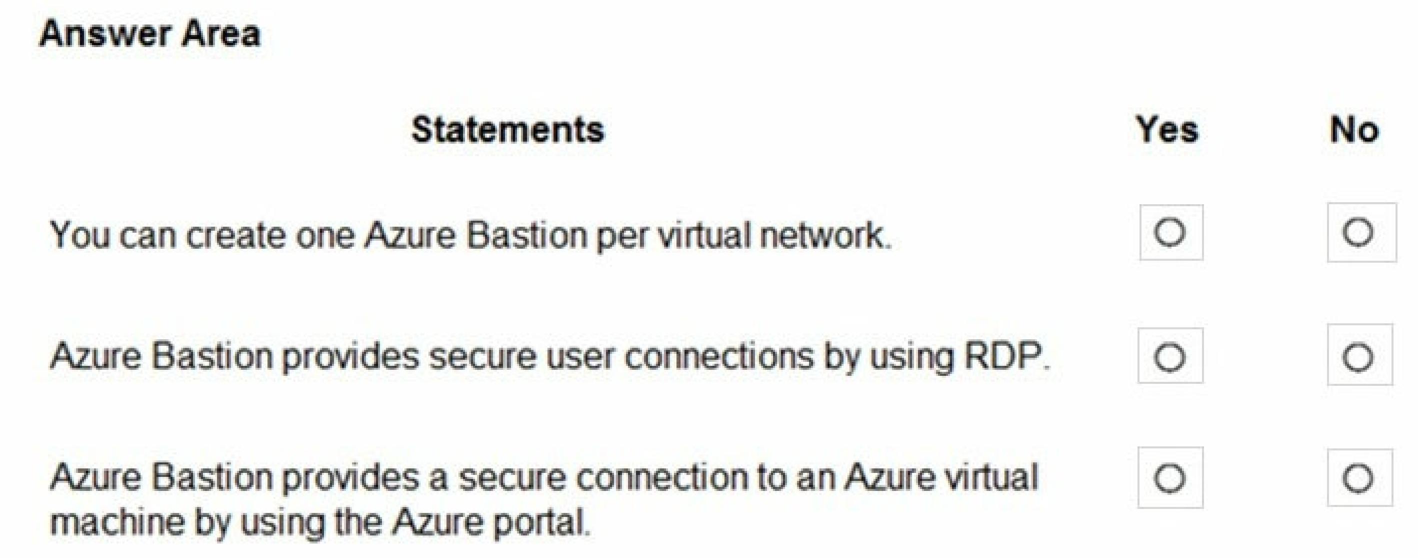
Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	[✓ ○]	○
Microsoft Intune can be used to provision Azure subscriptions.	○	[✓ ○]
Microsoft Intune can be used to manage organization-owned devices and personal devices.	[✓ ○]	○

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: 64 CertyIQ

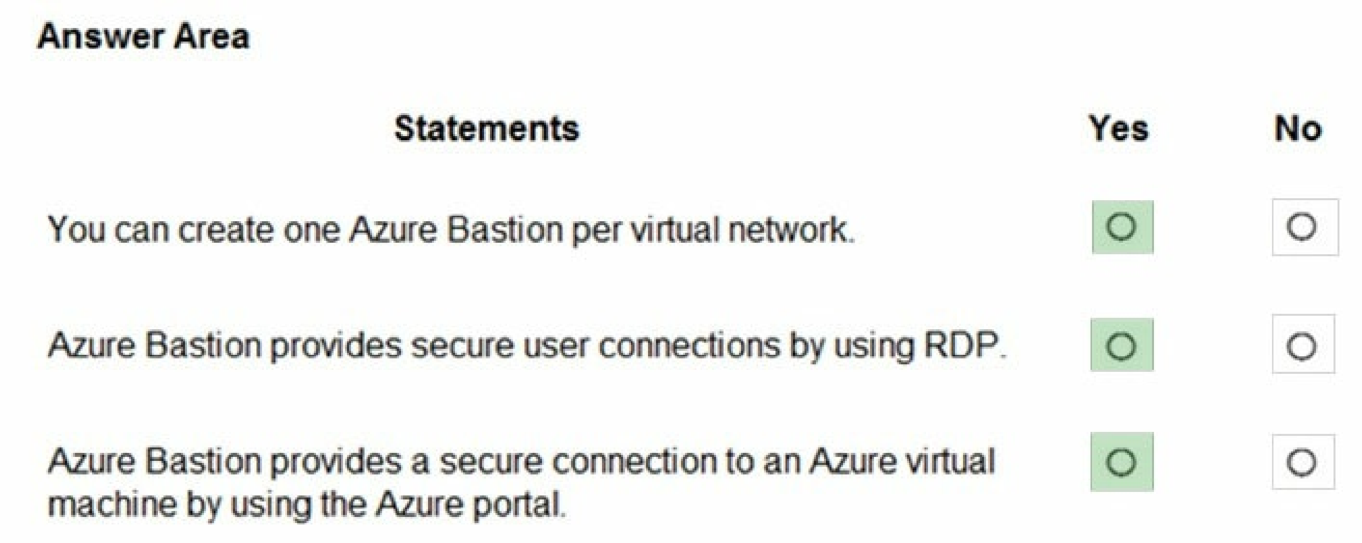
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	[✓ ○]	○

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: 65

What feature in Microsoft Defender for Endpoint provides the first line of defense against cyberthreats by reducing the attack surface?

A. automated remediation
B. automated investigation
C. advanced hunting
D. network protection

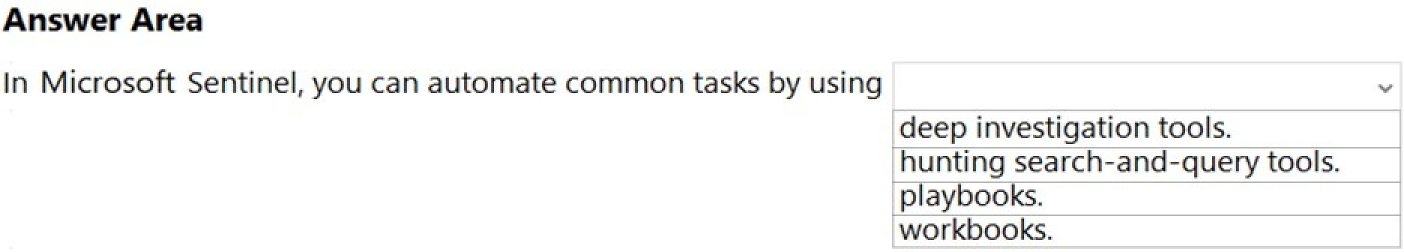
Answer: D

Explanation:
Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide

Question: 66

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

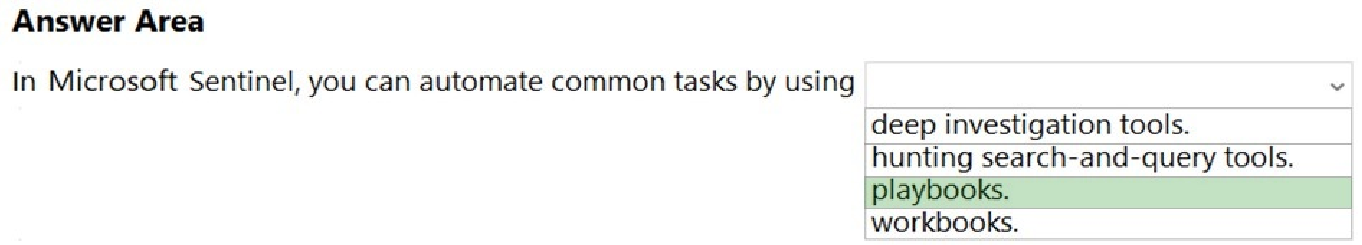


Answer Area

In Microsoft Sentinel, you can automate common tasks by using

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

Answer:



Answer Area

In Microsoft Sentinel, you can automate common tasks by using

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

Explanation:

Workbooks in Azure Sentinel are interactive dashboards that allow users to explore and analyze security data. They provide a visual representation of security data, allowing users to quickly identify patterns and trends. Workbooks can be customized to display specific data and can be shared with other users.

Playbooks in Azure Sentinel are automated response capabilities that allow users to take action on security incidents. They provide a set of predefined playbooks and actions to help users respond to security incidents quickly and effectively. Playbooks can be triggered by specific events or conditions, and can be customized to fit the needs of the organization. They also have the capability to integrate with other Azure services and third-party tools, and can be used to automate incident triage, investigations, and remediation tasks.

In summary, Workbooks are for analysis and visualization of security data, whereas Playbooks are for automated incident response.

Reference:

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

Question: 67 CertyIQ

Which two types of resources can be protected by using Azure Firewall? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure virtual machines

B. Azure Active Directory (Azure AD) users

C. Microsoft Exchange Online inboxes

D. Azure virtual networks

E. Microsoft SharePoint Online sites

Answer: AD

Explanation:

A and D

Question: 68 CertyIQ

You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure.
Which security methodology does this represent?

A. threat modeling

B. identity as the security perimeter
C. defense in depth
D. the shared responsibility model

Answer: C

Explanation:

right answers Defence in depth spanning

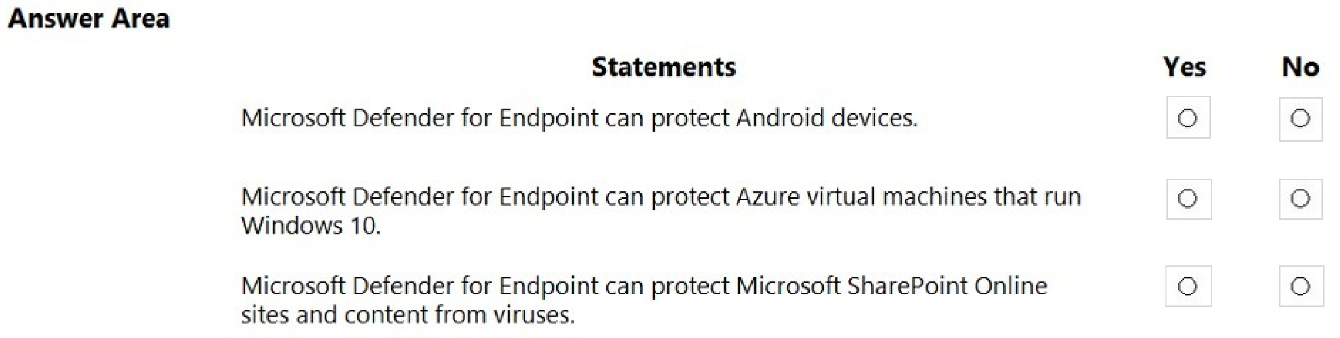
Data, Application, Compute, Network , Perimeter , Identity and Access and Physical. Of this physical is more of cloud provider responsibility

Reference:

https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth

Question: 69 CertyIQ

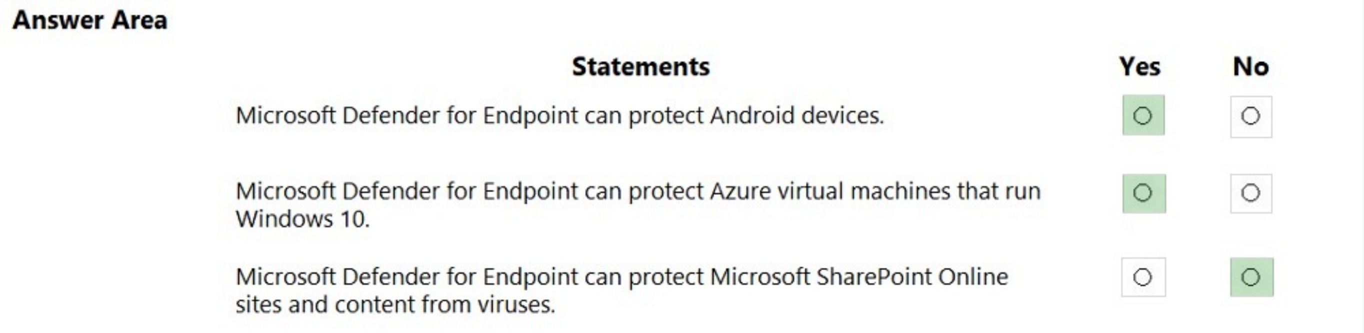
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	○	○
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	○	○
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	○	○

Answer:



Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	[✓ ○]	○
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	[✓ ○]	○
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	○	[✓ ○]

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/android-intune?view=o365-worldwide#:~:text=Defender%20for%20Endpoint%20supports%20Device,up%20VPN%20service%20while%20on

Question: 70 CertyIQ

What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?

A. Microsoft Defender for Office 365

B. Microsoft Defender Antivirus

C. Microsoft Defender for Identity

D. Microsoft Defender for Endpoint

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

Question: 71 CertyIQ

Which feature provides the extended detection and response (XDR) capability of Azure Sentinel?

A. integration with the Microsoft 365 compliance center

B. support for threat hunting

C. integration with Microsoft 365 Defender

D. support for Azure Monitor Workbooks

Answer: C

Explanation:

The Microsoft 365 Defender connector for Azure Sentinel (preview) sends all Microsoft 365 Defender incidents and alerts information to Azure Sentinel and keeps the incidents synchronized.

Once you add the connector, Microsoft 365 Defender incidents — which include all associated alerts, entities, and relevant information received from Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Cloud App Security — are streamed to Azure Sentinel as security information and event management (SIEM) data, providing you with context to perform triage and incident response with Azure Sentinel.

Once in Azure Sentinel, incidents remain bi-directionally synchronized with Microsoft 365 Defender, allowing you to take advantage of the benefits of both the Microsoft 365 Defender portal and Azure Sentinel in the Azure portal for incident investigation and response.

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-integration-with-azure-sentinel?view=o365-worldwide

Reference:

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

Question: 72 CertyIQ

What can you use to provide threat detection for Azure SQL Managed Instance?

A. Microsoft Secure Score

B. application security groups

C. Microsoft Defender for Cloud

D. Azure Bastion

Answer: C

Explanation:

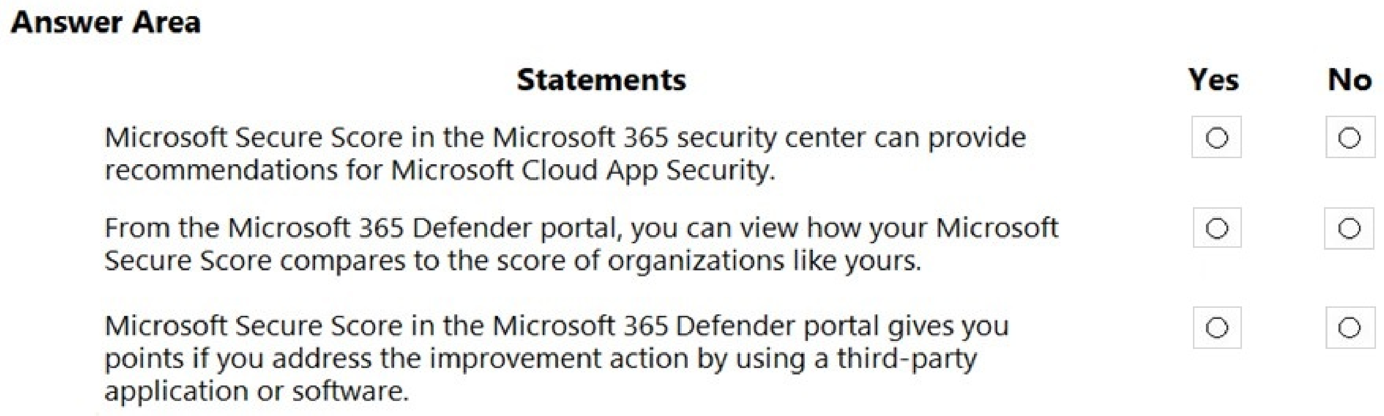
Microsoft Defender for SQL is a Defender plan in Microsoft Defender for Cloud. Microsoft Defender for SQL includes functionality for surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities.

Microsoft Defender for SQL

https://learn.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql

Question: 73 CertyIQ

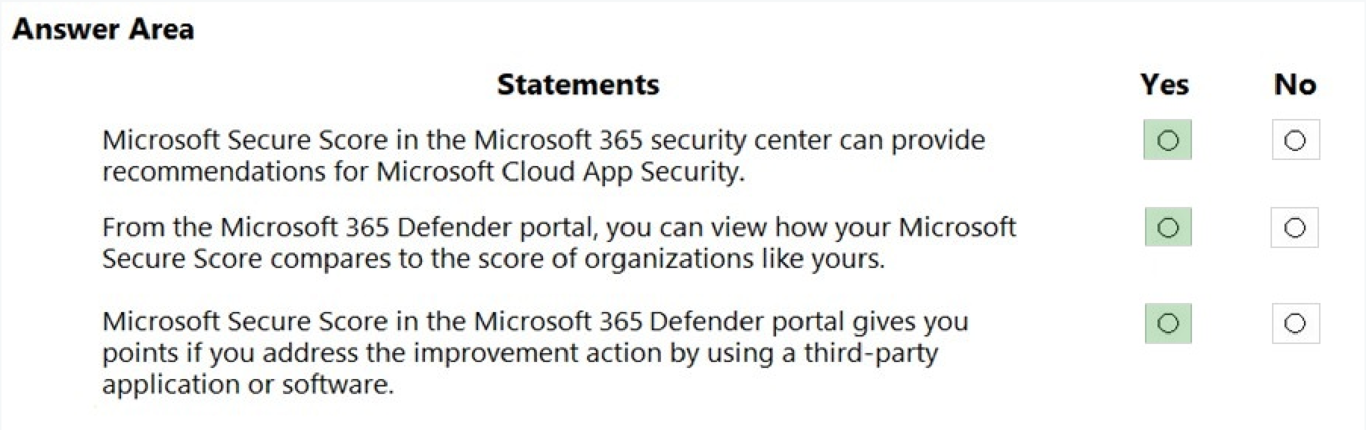
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.	○	○

Answer:



Answer Area

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	[✓ ○]	○
From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	[✓ ○]	○
Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.	[✓ ○]	○

Explanation:

Organizations gain access to robust visualizations of metrics and trends, integration with other Microsoft products, score comparison with similar organizations, and much more. The score can also reflect when third-party solutions have addressed recommended actions.

Question: 74 CertyIQ

Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune-managed devices from accessing corporate resources?

A. network security groups (NSGs)
B. Azure AD Privileged Identity Management (PIM)
C. conditional access policies
D. resource locks

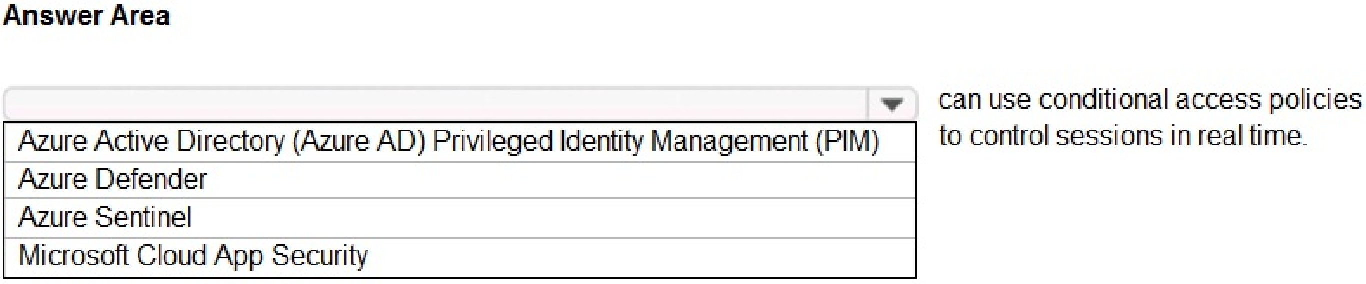
Answer: C

Explanation:

When you use Conditional Access, you can configure your Conditional Access policies to use the results of your device compliance policies to determine which devices can access your organizational resources. This access control is in addition to and separate from the actions for noncompliance that you include in your device compliance policies

Question: 75 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

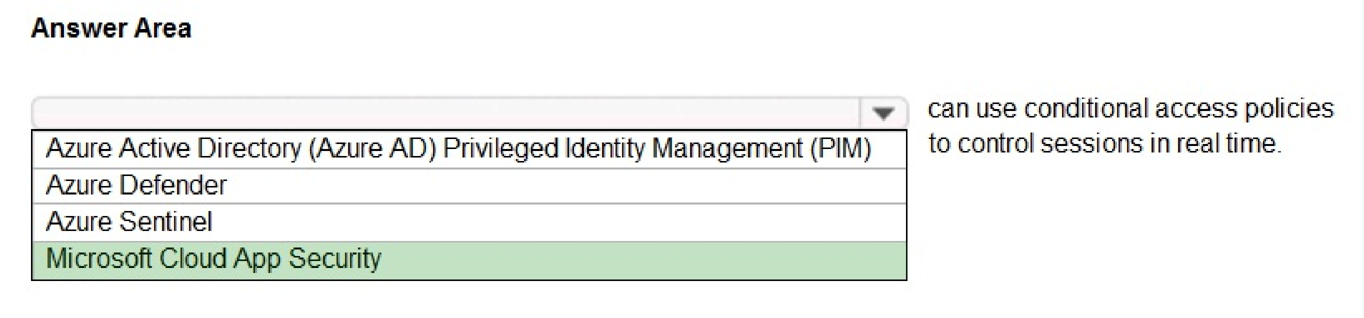


Answer Area

[▼] 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:



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

Explanation:

Microsoft Cloud App Security has been renamed to Microsoft Defender for Cloud Apps:

https://techcommunity.microsoft.com/t5/itops-talk-blog/azure-security-product-name-changes-microsoftignite-november/ba-p/3004418?WT.mc_id=modinfra-48365-socuff

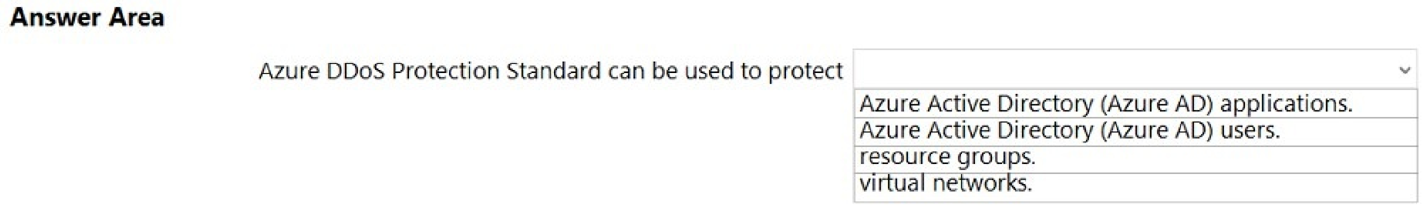
Reference:

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

Question: 76

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:



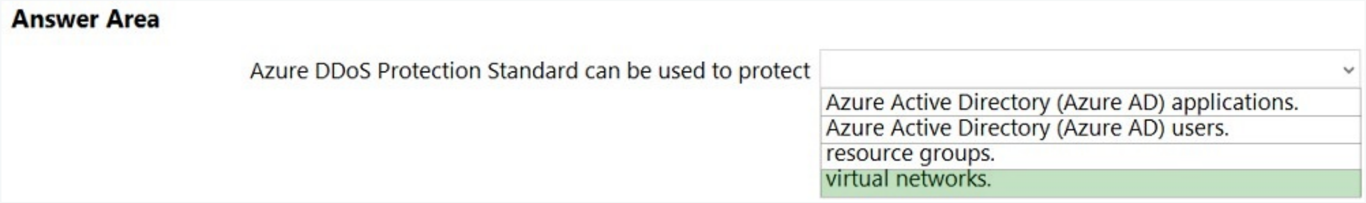
Answer Area

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: D

Explanation:



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.

Reference:

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

Question: 77

CertyIQ

What should you use in the Microsoft 365 Defender portal to view security trends and track the protection status of identities?

A. Attack simulator

B. Reports

C. Hunting

D. Incidents

Answer: B

Explanation:

Keyword is trends = reports

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-and-insights-in-security-and-compliance?view=o365-worldwide

Question: 78

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

Answer: C

Explanation:

Microsoft 365 unified auditing helps to track activities performed in the different Microsoft 365 services by both users and admins. Basic auditing is enabled by default for most Microsoft 365 organizations. In the Basic audit, audit records are retained and searchable for the last 90 days.

https://o365reports.com/2021/07/07/microsoft-365-retrieve-audit-log-for-1-year-for-all-subscriptions/

Question: 79

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

Answer: C

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: 80

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

Answer: ACE

Explanation:

The correct answers can be found via https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps. Look for the following title in the article "The Defender for Cloud Apps framework"

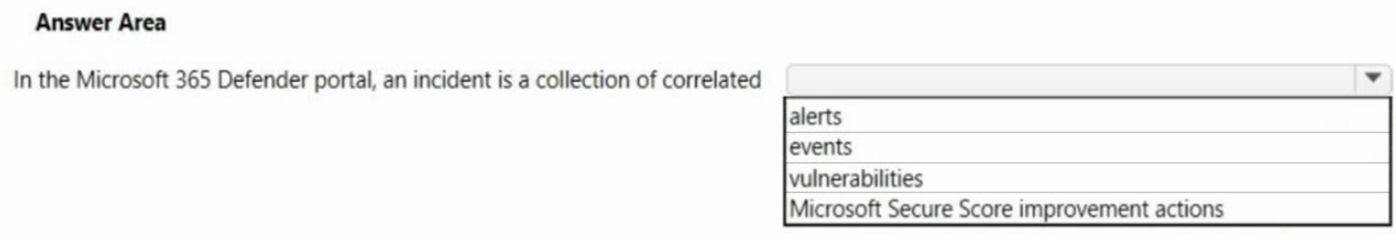
Reference:

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

Question: 81

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

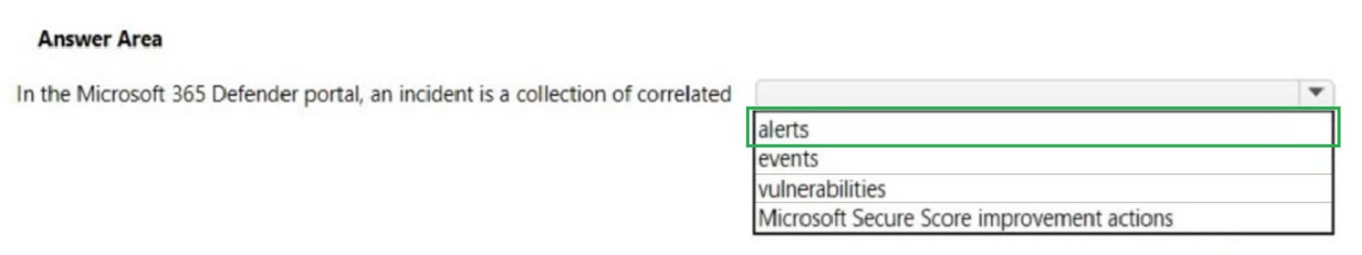


Answer Area

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

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

Answer:



Answer Area

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

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

Explanation:

Alerts

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

https://learn.microsoft.com/es-es/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

Question: 82

CertyIQ

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

A. PowerShell remoting

B. the Azure portal

C. the Remote Desktop Connection client

D. an SSH client

Answer: B

Explanation:

Azure portal, B. whole idea of bastion is to keep rdp port 3389 closed.

Azure Portal is the only option given, that does not require the native SSH or RDP client already installed on your local computer. So, I should use Azure Portal.

Question: 83

Which service includes the Attack simulation training feature?

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

Answer: D

Explanation:
Attack simulation training in Microsoft Defender for Office 365 Plan 2 or Microsoft 365 E5 lets you run benign cyberattack simulations in your organization. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training

Question: 84

Which type of alert can you manage from the Microsoft 365 Defender portal?

A. Microsoft Defender for Storage
B. Microsoft Defender for SQL
C. Microsoft Defender for Endpoint
D. Microsoft Defender for IoT

Answer: C

Explanation:
The Alerts queue shows the current set of alerts. You get to the alerts queue from Incidents & alerts > Alerts on the quick launch of the Microsoft 365 Defender portal.
Alerts from different Microsoft security solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft 365 Defender appear here.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts

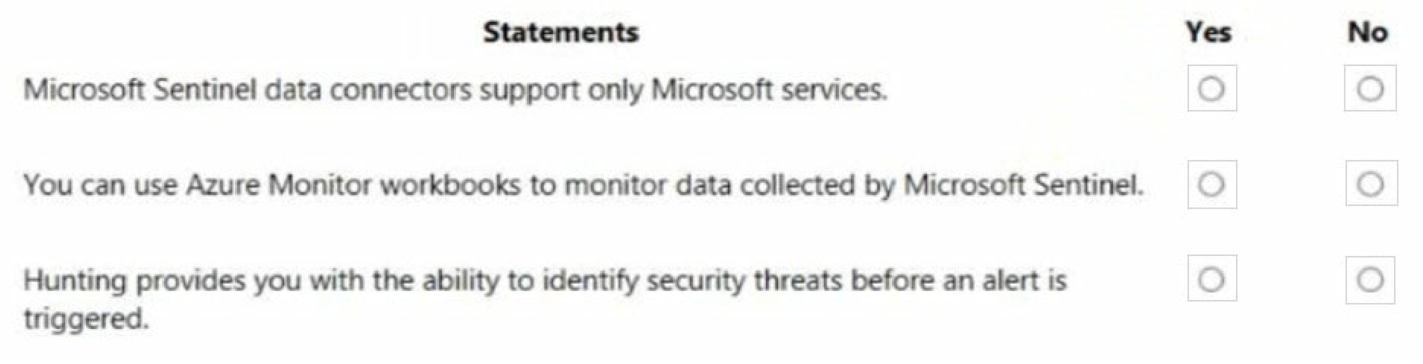
Question: 85 CertyIQ

HOTSPOT -

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

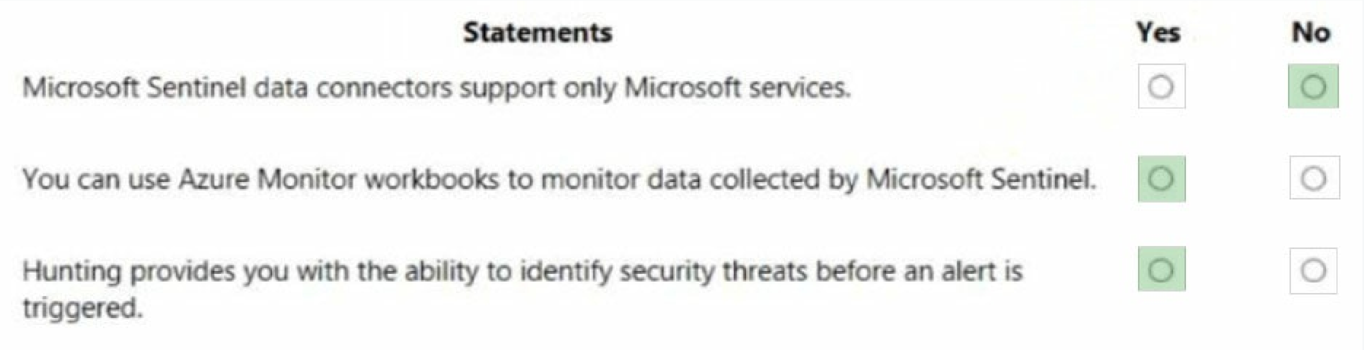
NOTE: Each correct selection is worth one point.

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:



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.	●	○

Explanation:

Box 1: No -

Microsoft Sentinel data connectors are available for non-Microsoft services like Amazon Web Services.

Box 2: Yes -

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor

Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Box 3: Yes -

To help security analysts look proactively for new anomalies that weren't detected by your security apps or even by your scheduled analytics rules, Microsoft

Sentinel's built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data https://docs.microsoft.com/en-us/azure/sentinel/hunting

Question: 86 CertyIQ

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

Answer: AB

Explanation:
Association of network security groups
You can associate a network security group with virtual machines, NICs, and subnets, depending on the deployment model you use.

Reference:
https://aviatrix.com/learn-center/cloud-security/create-network-security-groups-in-azure/

Question: 87 CertyIQ

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

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

Answer: B

Explanation:

correct answer is B:Information barriers are supported in Microsoft Teams, SharePoint Online, and OneDrive for Business. A compliance administrator or information barriers administrator can define policies to allow or prevent communications between groups of users in Microsoft Teams. Information barrier policies can be used for situations like these:

Question: 88 CertyIQ

What can you use to deploy Azure resources across multiple subscriptions in a consistent manner?

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

Answer: B

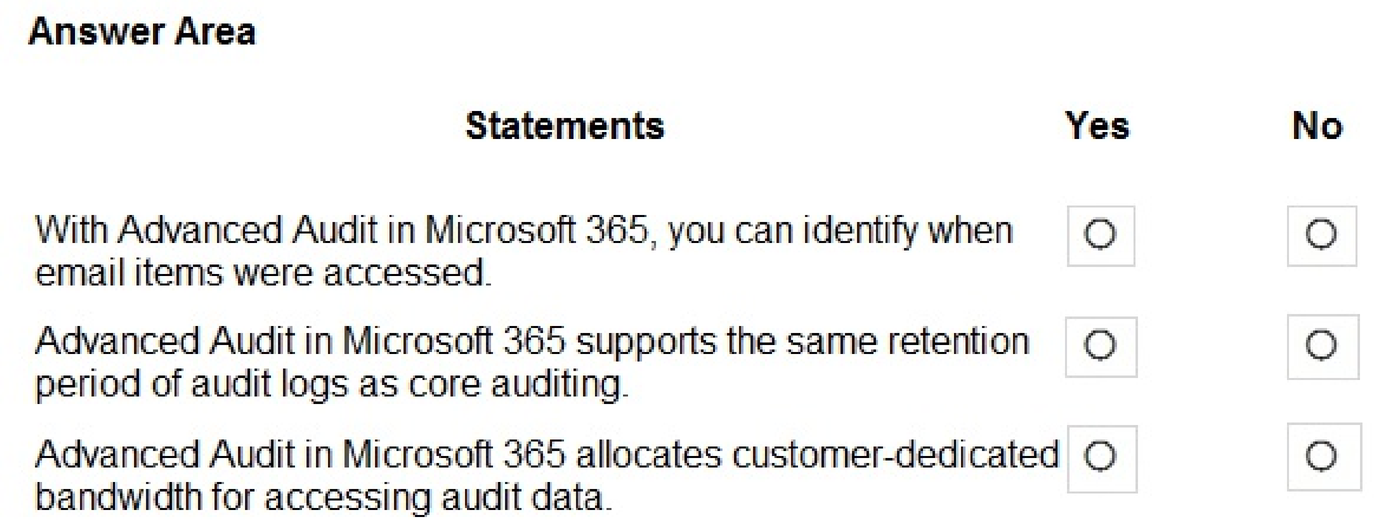
Explanation:

Reference:

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

Question: 89 CertyIQ

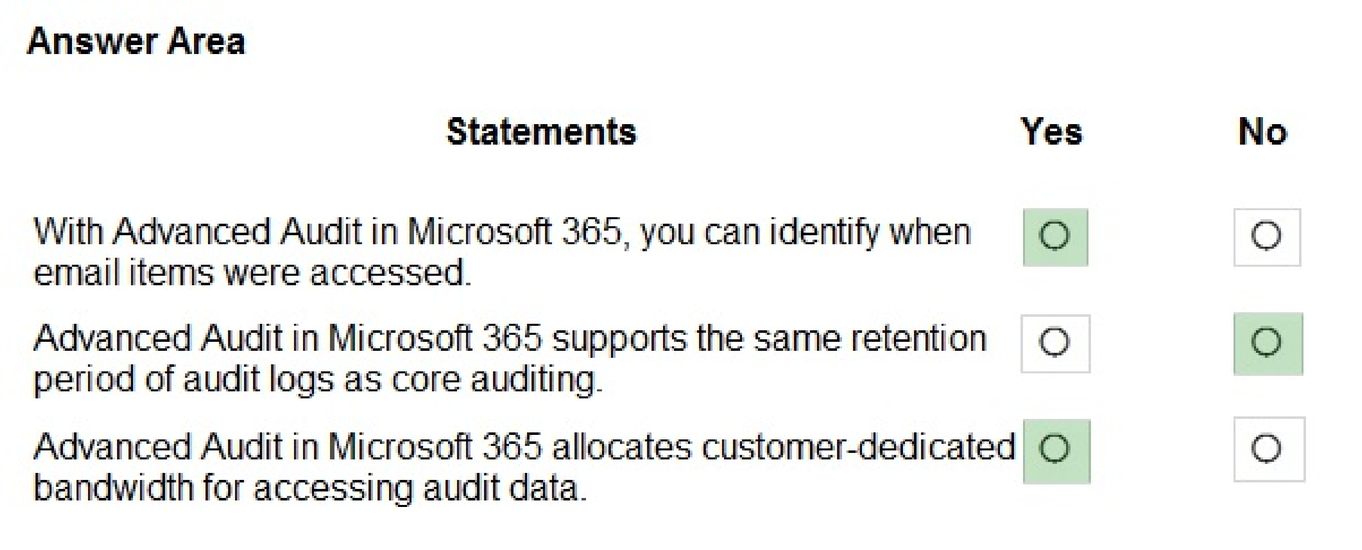
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	[✓ ○]	○

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 -

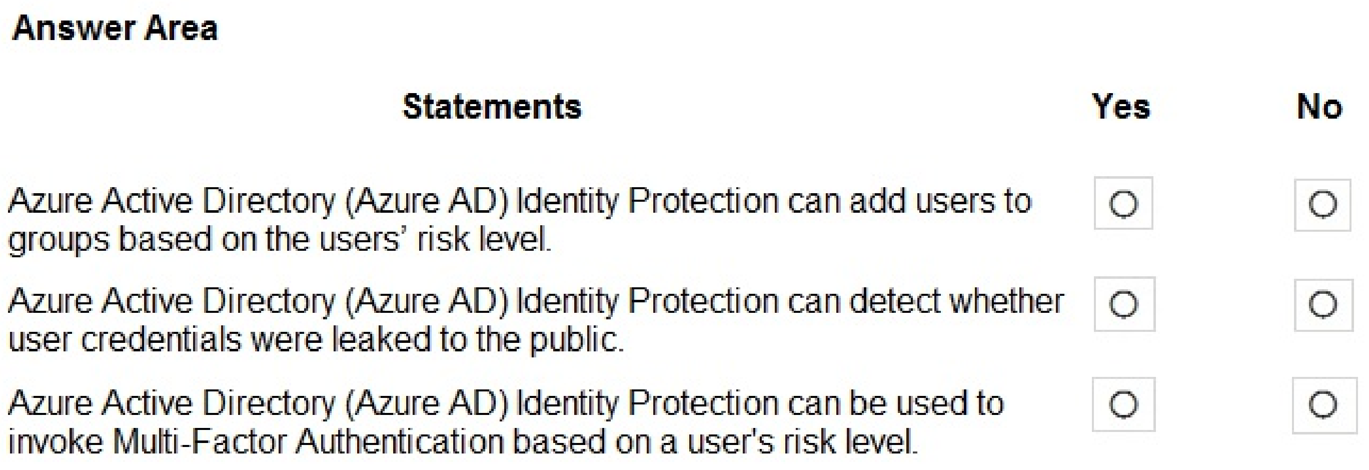
Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.

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: 90

CertyIQ

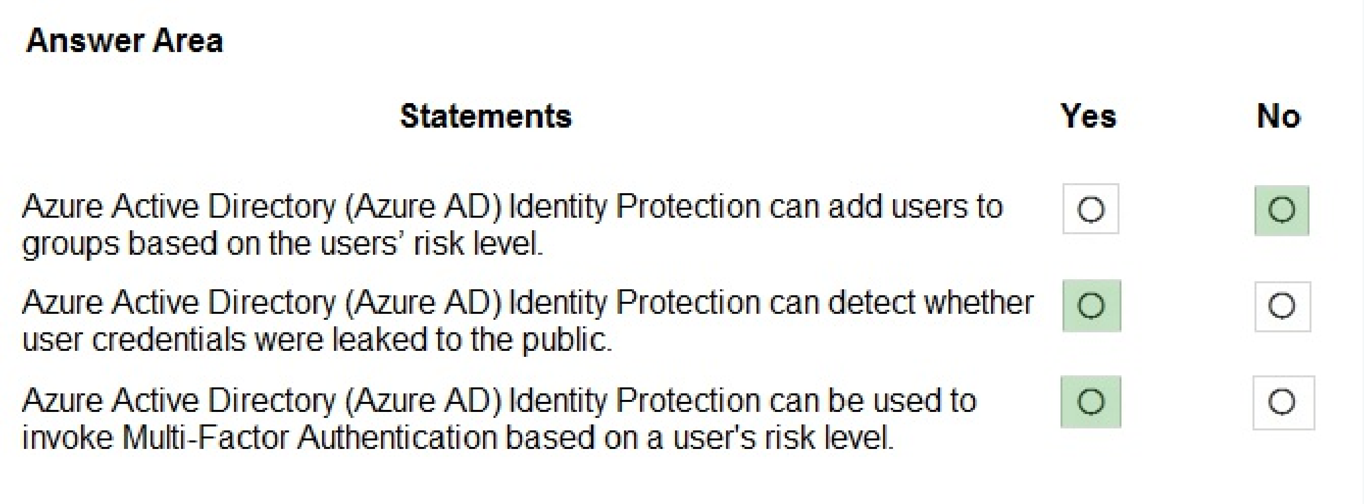
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	[✓ ○]	○

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: 91 CertyIQ

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

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

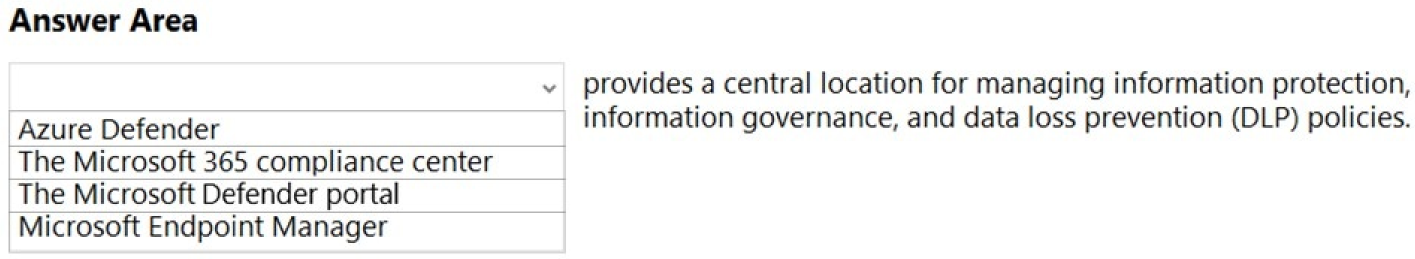
Answer: C

Explanation:
The Content Search tool in the Security & Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and
OneDrive locations, and instant messaging conversations in Skype for Business.
The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide

Question: 92 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

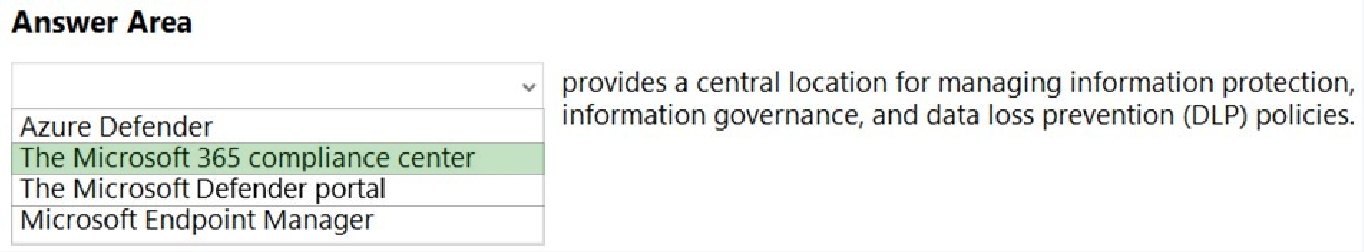


Answer Area

[▾] provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

- Azure Defender
- The Microsoft 365 compliance center
- The Microsoft Defender portal
- Microsoft Endpoint Manager

Answer:



Answer Area

[▾] provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

- Azure Defender
- [✓ The Microsoft 365 compliance center]
- The Microsoft Defender portal
- Microsoft Endpoint Manager

Explanation:

They have change the name to Microsoft Purview compliance portal

Reference:

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

Question: 93 CertyIQ

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

A. retention policies

B. data loss prevention (DLP) policies

C. conditional access policies

D. information barriers

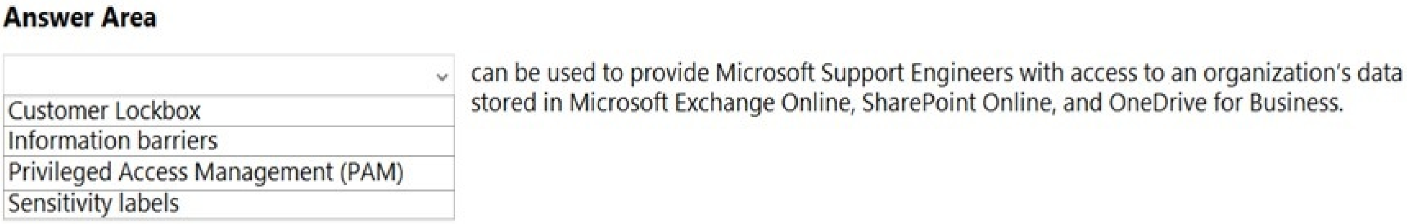
Answer: B

Explanation:

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

Question: 94 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

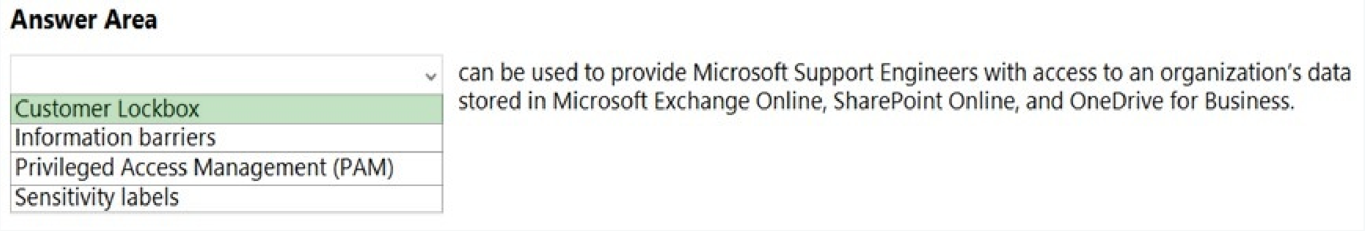


Answer Area

Customer Lockbox
Information barriers
Privileged Access Management (PAM)
Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Answer:



Answer Area

[✓ Customer Lockbox]
Information barriers
Privileged Access Management (PAM)
Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Explanation:

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

Question: 95 CertyIQ

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

A. Create an eDiscovery hold.
B. Run Express Analysis.
C. Configure attorney-client privilege detection.
D. Export and download results.

Answer: A

Explanation:

From https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide:

Create an eDiscovery hold. The first step after creating a case is placing a hold (also called an eDiscovery hold) on the content locations of the people of interest in your investigation. ... While this step is optional,...

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide

Question: 96 CertyIQ

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

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

Answer: A

Explanation:

The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

Question: 97 CertyIQ

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

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

Answer: D

Explanation:

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

Question: 98

What can you specify in Microsoft 365 sensitivity labels?

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

Answer: C

Explanation:

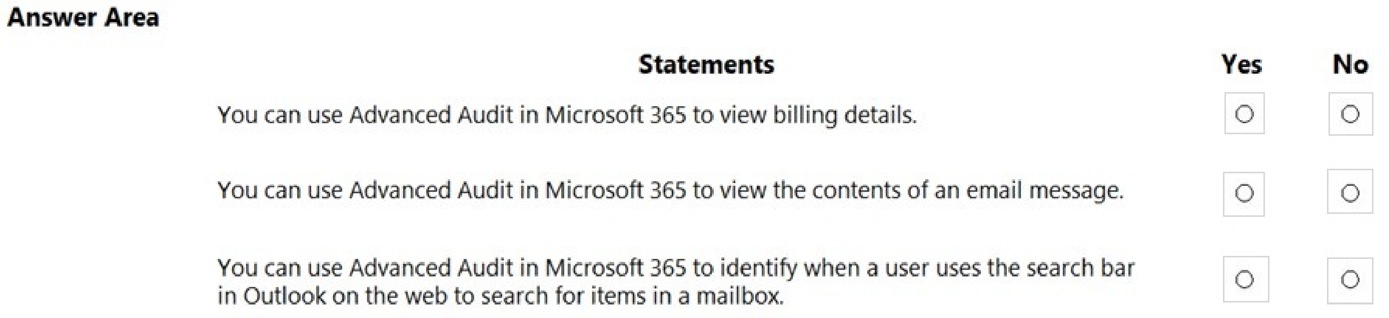
Creating classification for sensitive information/data

Reference:

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

Question: 99

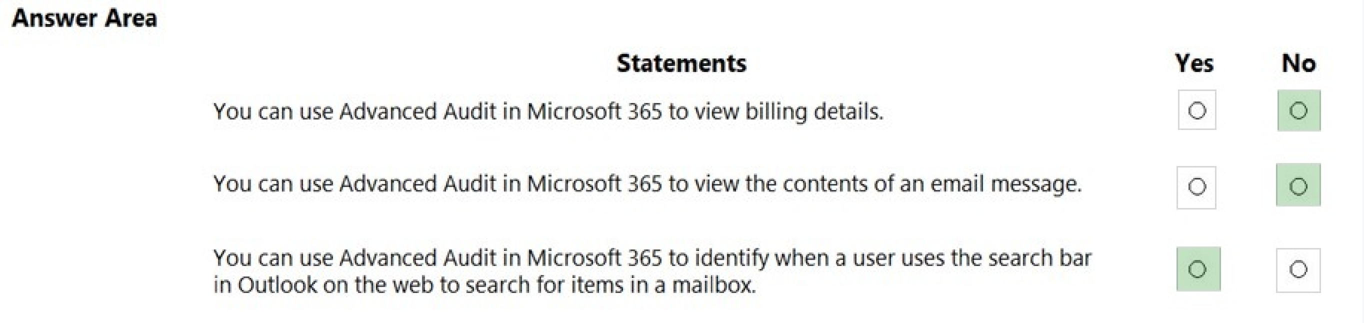
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

Explanation:

Box 1: No -

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

Box 2: No -

Box 3: Yes -

Send

The Send event is also a mailbox auditing action and is triggered when a user performs one of the following actions:

Sends an email message

Replies to an email message

Forwards an email message

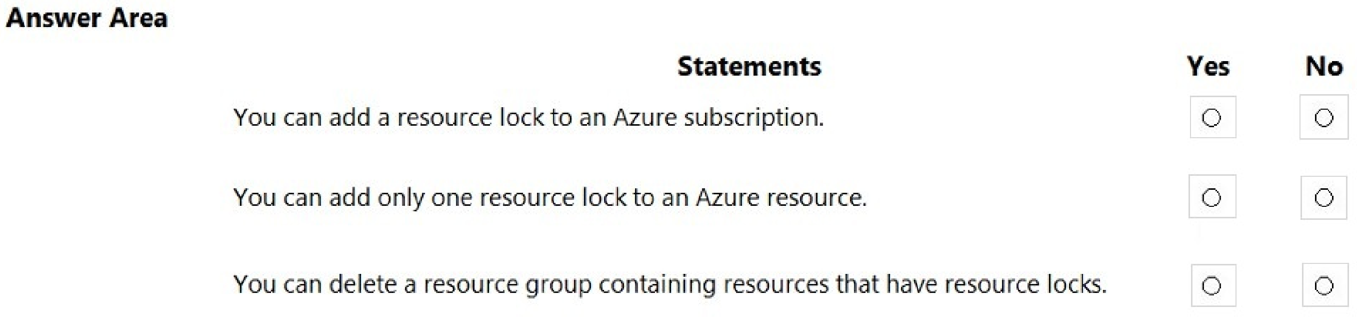
Investigators can use the Send event to identify email sent from a compromised account. The audit record for a Send event contains information about the message, such as when the message was sent, the InternetMessage ID, the subject line, and if the message contained attachments. This auditing information can help investigators identify information about email messages sent from a compromised account or sent by an attacker. Additionally, investigators can use a Microsoft 365 eDiscovery tool to search for the message (by using the subject line or message ID) to identify the recipients the message was sent to and the actual contents of the sent message.

Reference:

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

Question: 100

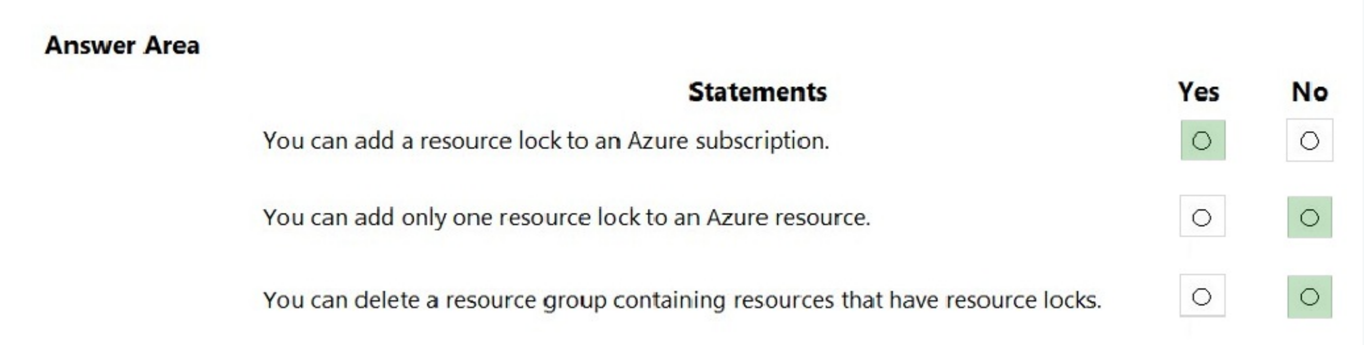
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

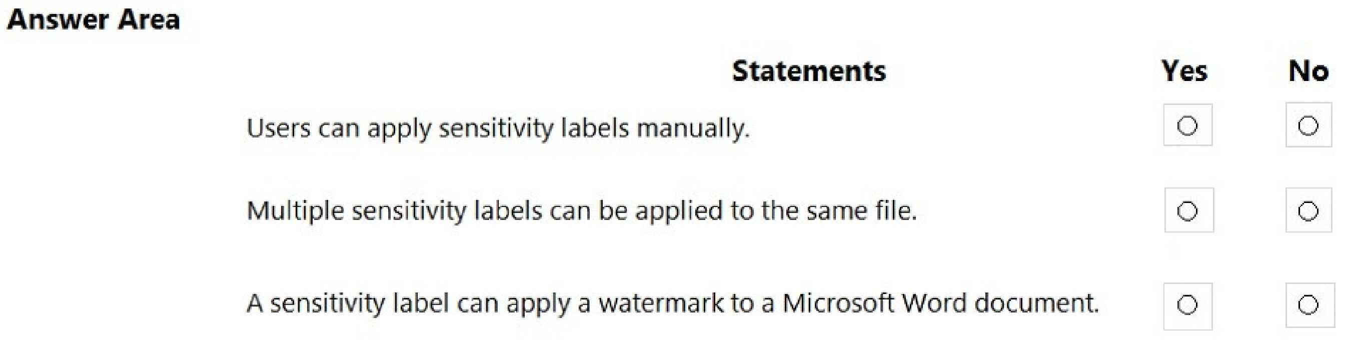
Explanation:

If you have a Delete lock on a resource and attempt to delete its resource group, the whole delete operation is blocked. Even if the resource group or other resources in the resource group aren't locked, the deletion doesn't happen. You never have a partial deletion.

source : https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

Question: 101 CertyIQ

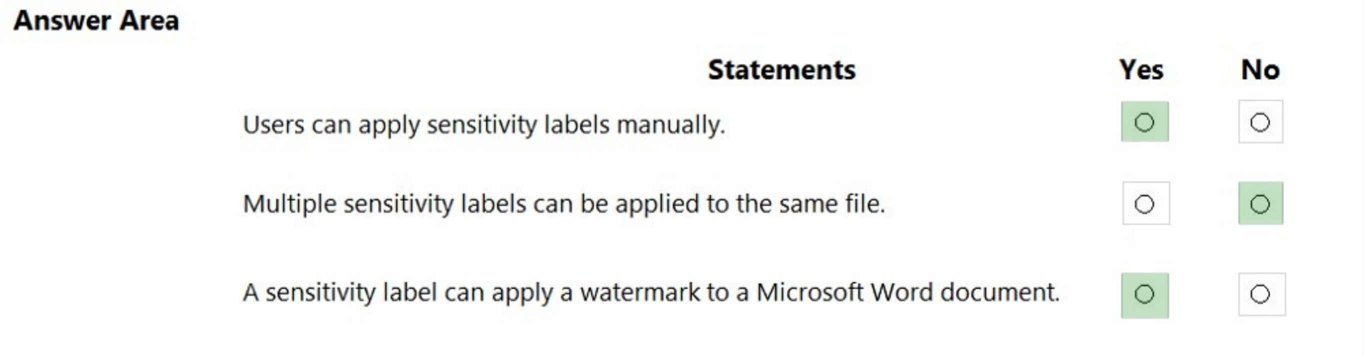
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

Answer:



Answer Area

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

Explanation:

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

Question: 102

CertyIQ

Which two tasks can you implement by using data loss prevention (DLP) policies in Microsoft 365? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Display policy tips to users who are about to violate your organization's policies.

B. Enable disk encryption on endpoints.

C. Protect documents in Microsoft OneDrive that contain sensitive information.

D. Apply security baselines to devices.

Answer: AC

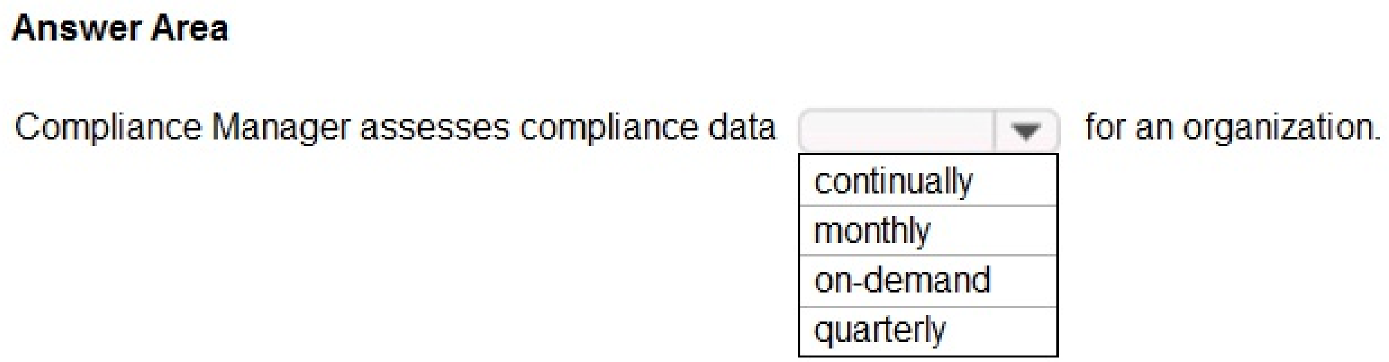
Explanation:

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

Question: 103

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

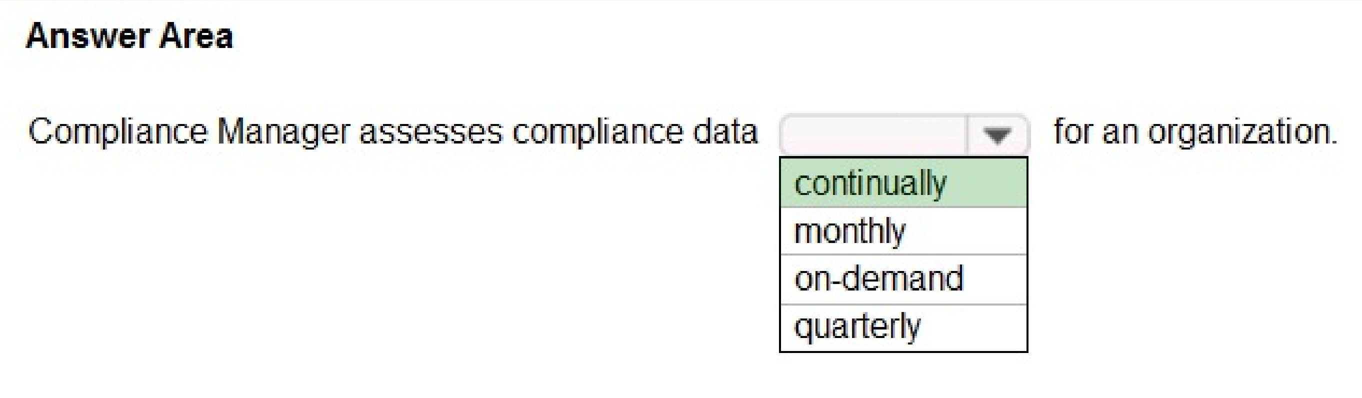


Answer Area

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

- continually
- monthly
- on-demand
- quarterly

Answer:



Answer Area

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

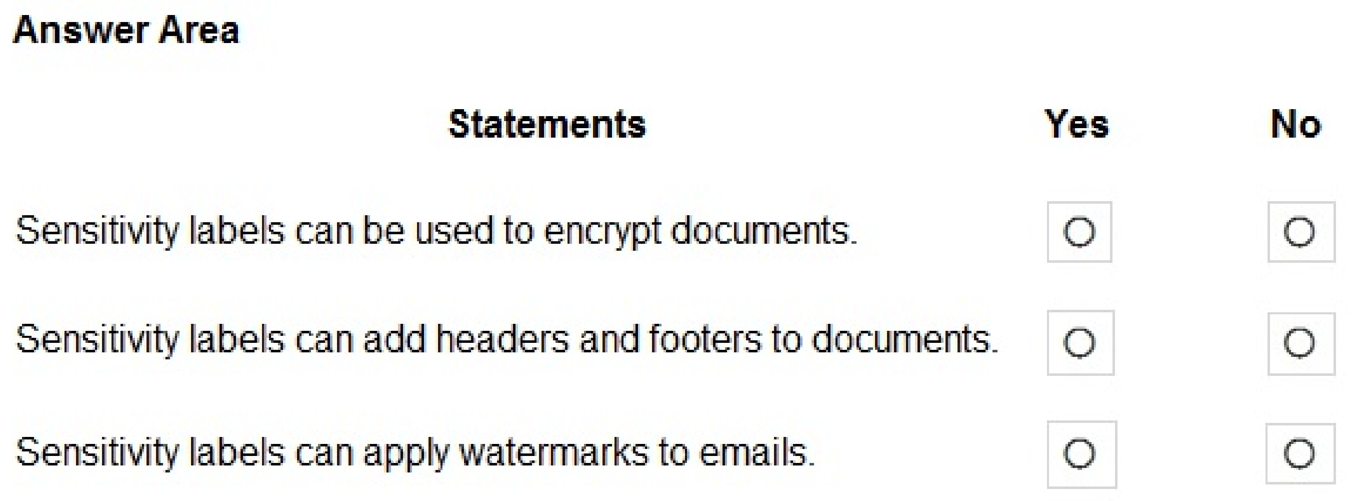
- continually ✓
- monthly
- on-demand
- quarterly

Explanation:

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

Question: 104 CertyIQ

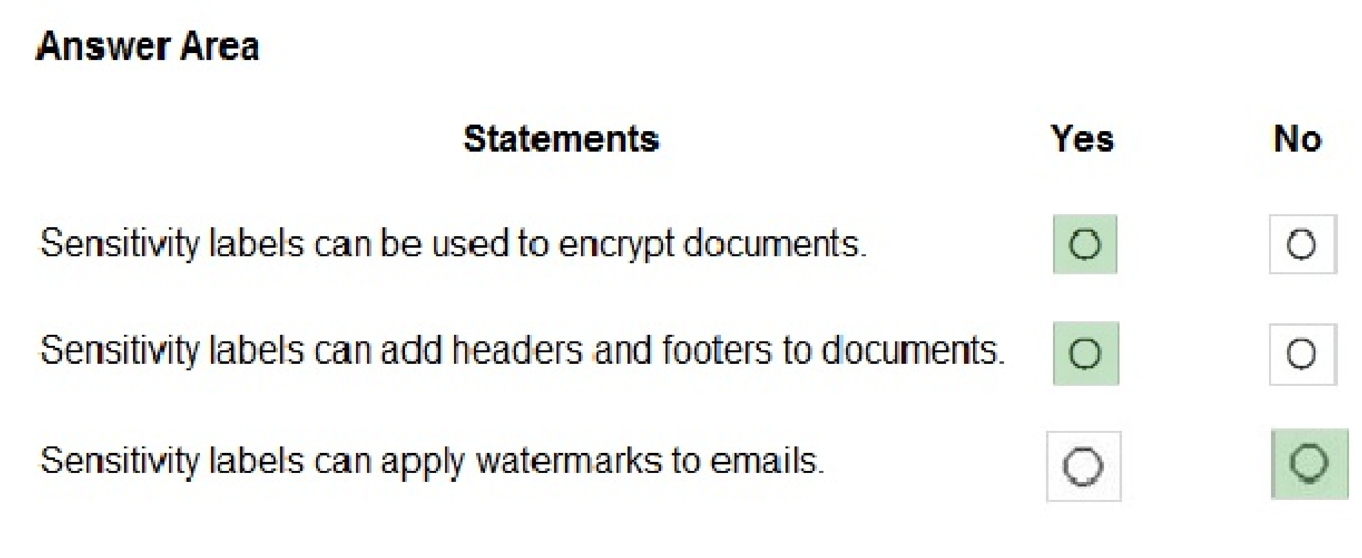
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	○	●

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: No-

Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied. Watermarks can be applied to documents but not email."

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

Reference:

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

Question: 105 CertyIQ

Which Microsoft 365 compliance feature can you use to encrypt content automatically based on specific conditions?

A. Content Search
B. sensitivity labels
C. retention policies
D. eDiscovery

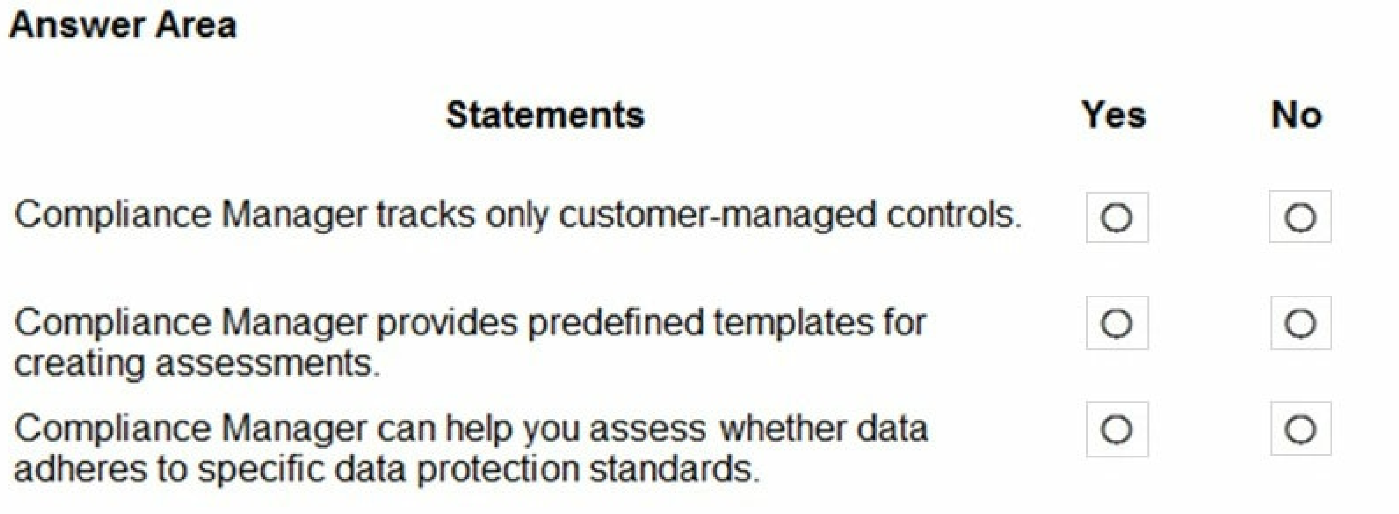
Answer: B

Explanation:

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

Question: 106 CertyIQ

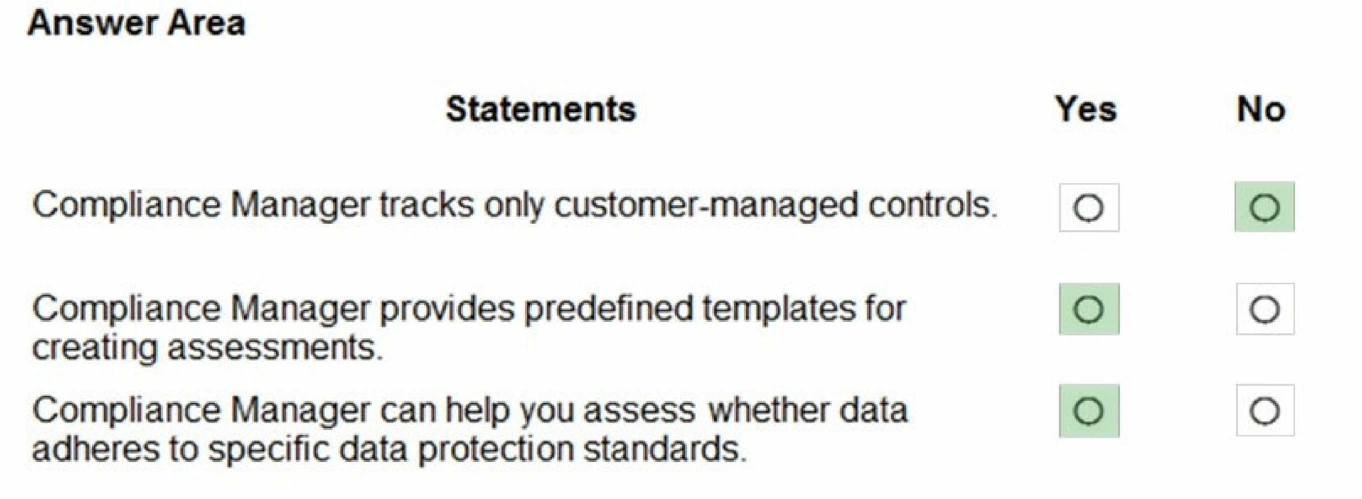
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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 assess whether data adheres to specific data protection standards.	○	○

Answer:



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 assess whether data adheres to specific data protection standards.	[✓ ○]	○

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: 107

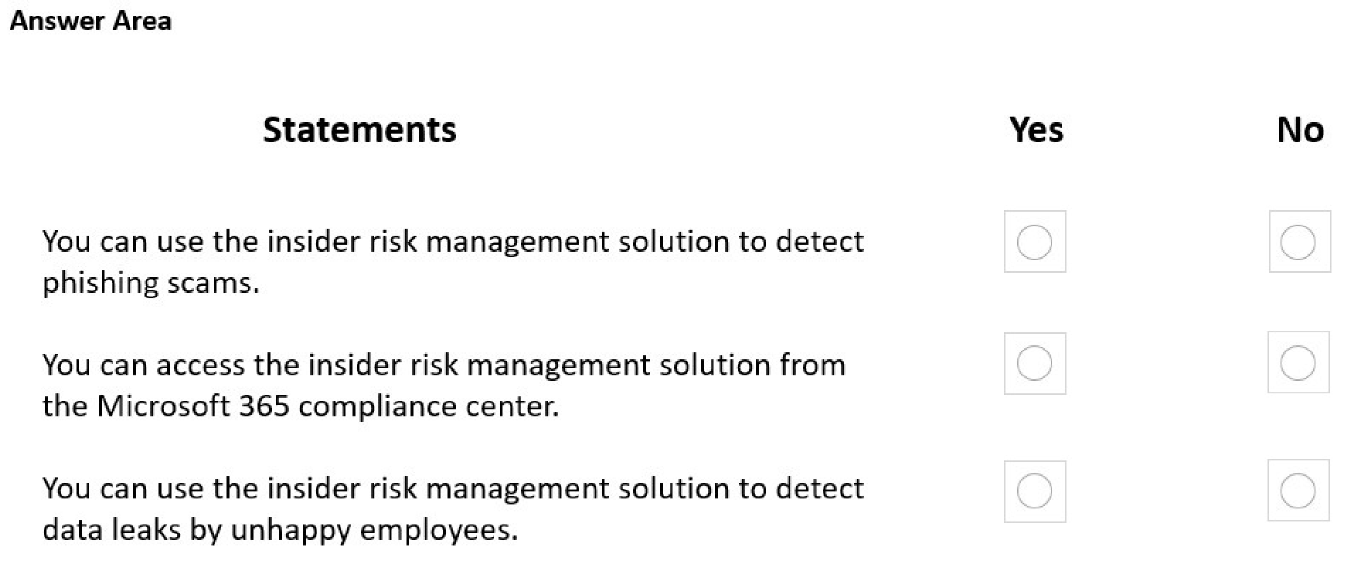
CertyIQ

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.

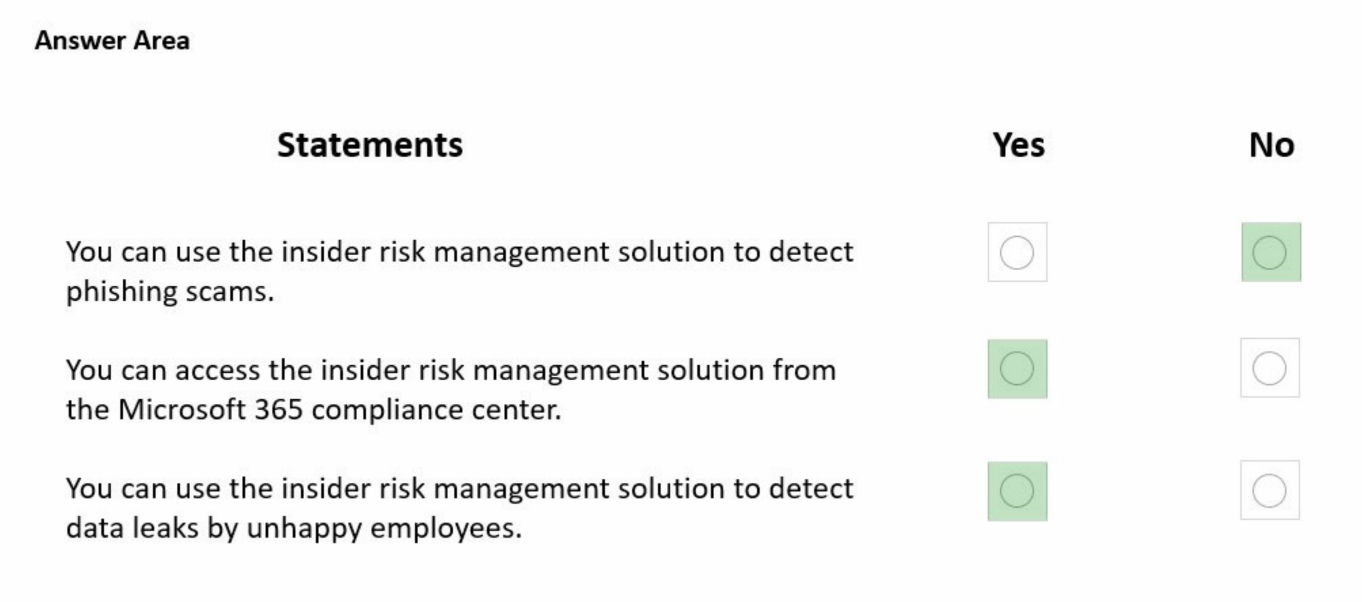
Hot Area:



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:


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.	[✓ ○]	○

Explanation:
Box 1: No -
Phishing scams are external threats.

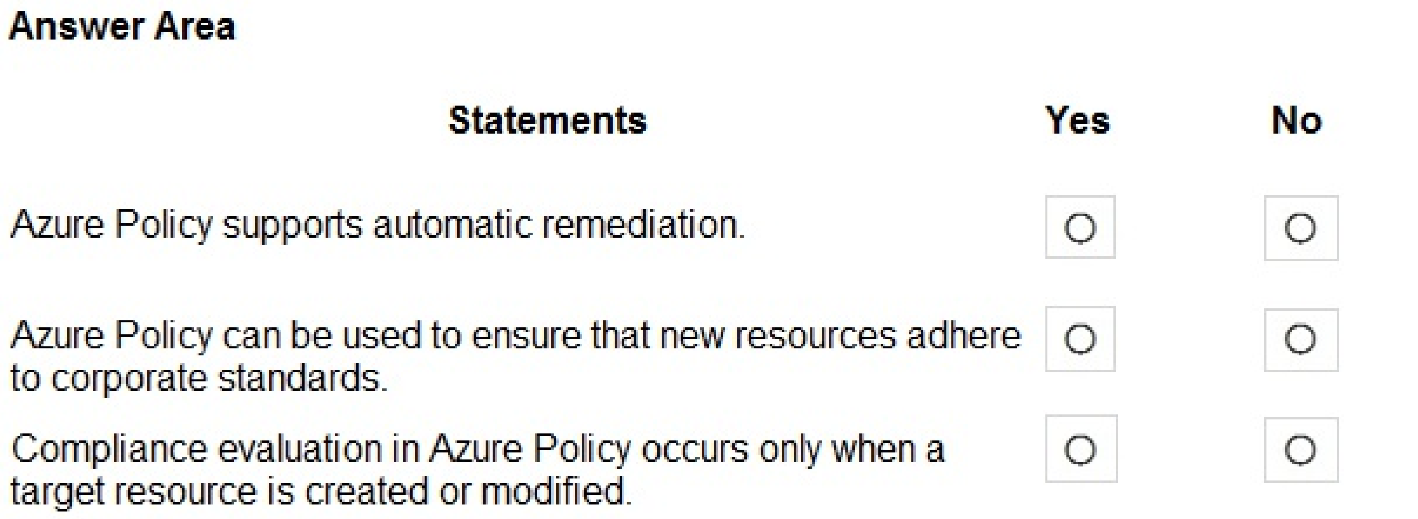
Box 2: Yes -
Insider risk management is a compliance solution in Microsoft 365.

Box 3: Yes -
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 violations

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

Question: 108 CertyIQ

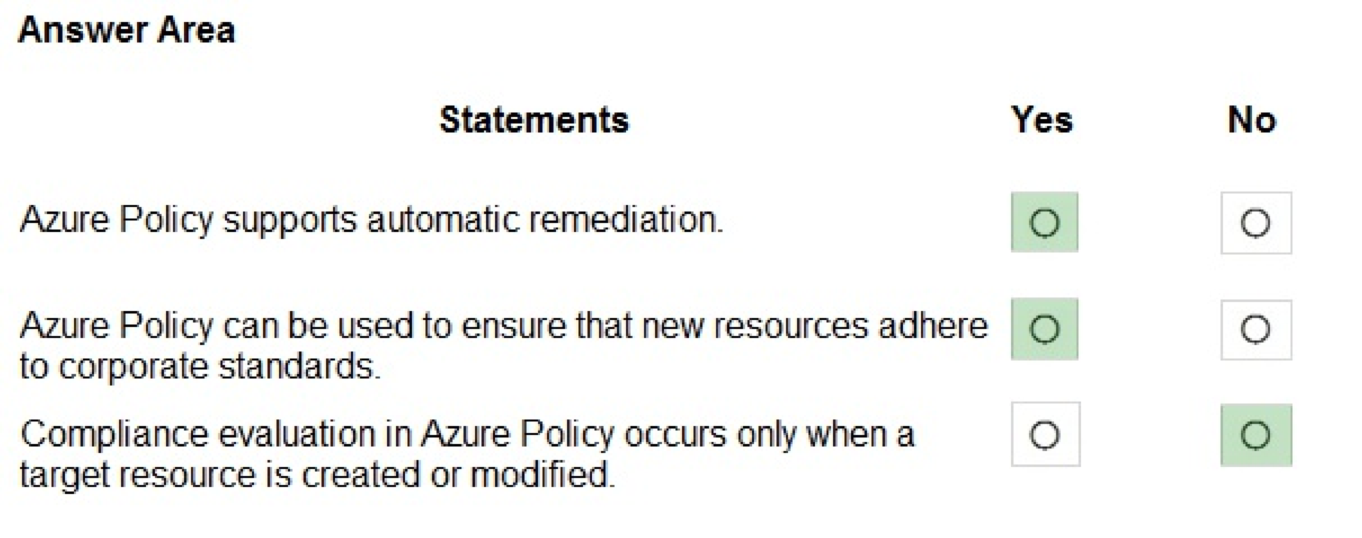
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



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:



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.	○	[✓ ○]

Explanation:

1.- Azure Policy supports automatic remediation (Y) R/=

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity. If the managed identity is missing roles, an error is displayed during the assignment of the policy or an initiative. When using the portal, Azure Policy automatically grants the managed identity the listed roles once assignment starts. When using SDK, the roles must manually be granted to the managed identity. The location of the managed identity doesn't impact its operation with Azure Policy.

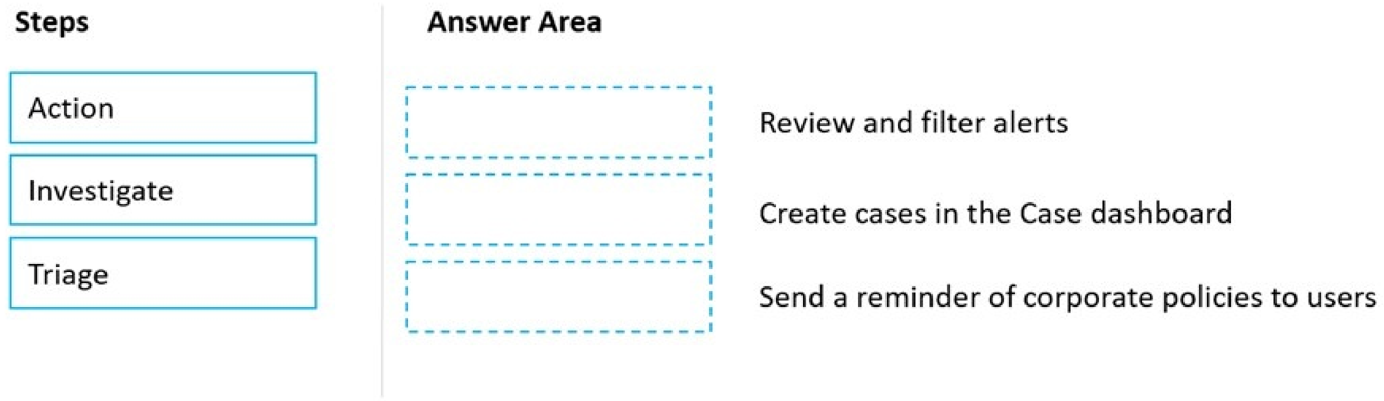
Reference:

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

Question: 109 CertyIQ

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

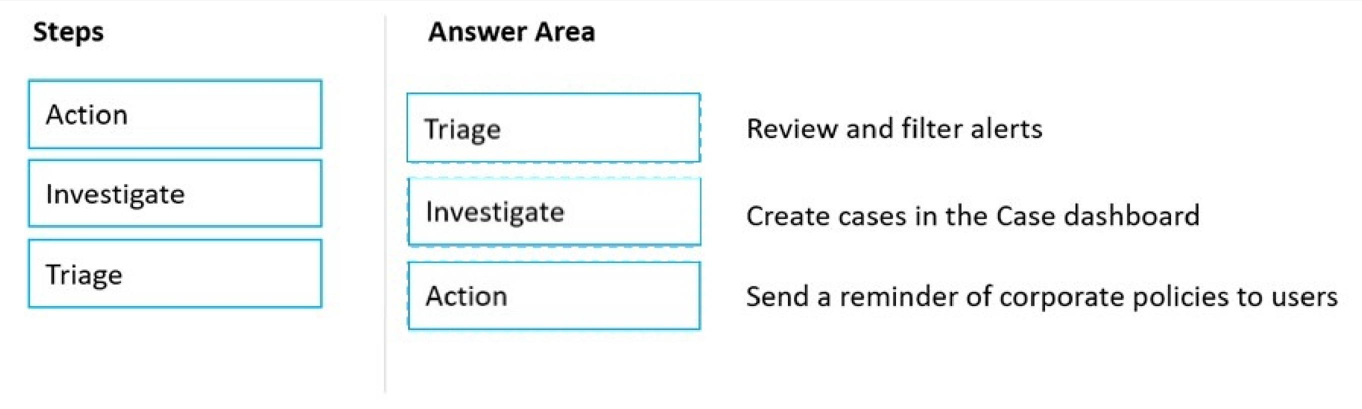
Answer Area

Review and filter alerts

Create cases in the Case dashboard

Send a reminder of corporate policies to users

Answer:



Steps

Action

Investigate

Triage

Answer Area

Triage — Review and filter alerts

Investigate — Create cases in the Case dashboard

Action — Send a reminder of corporate policies to users

Explanation:

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

Question: 110

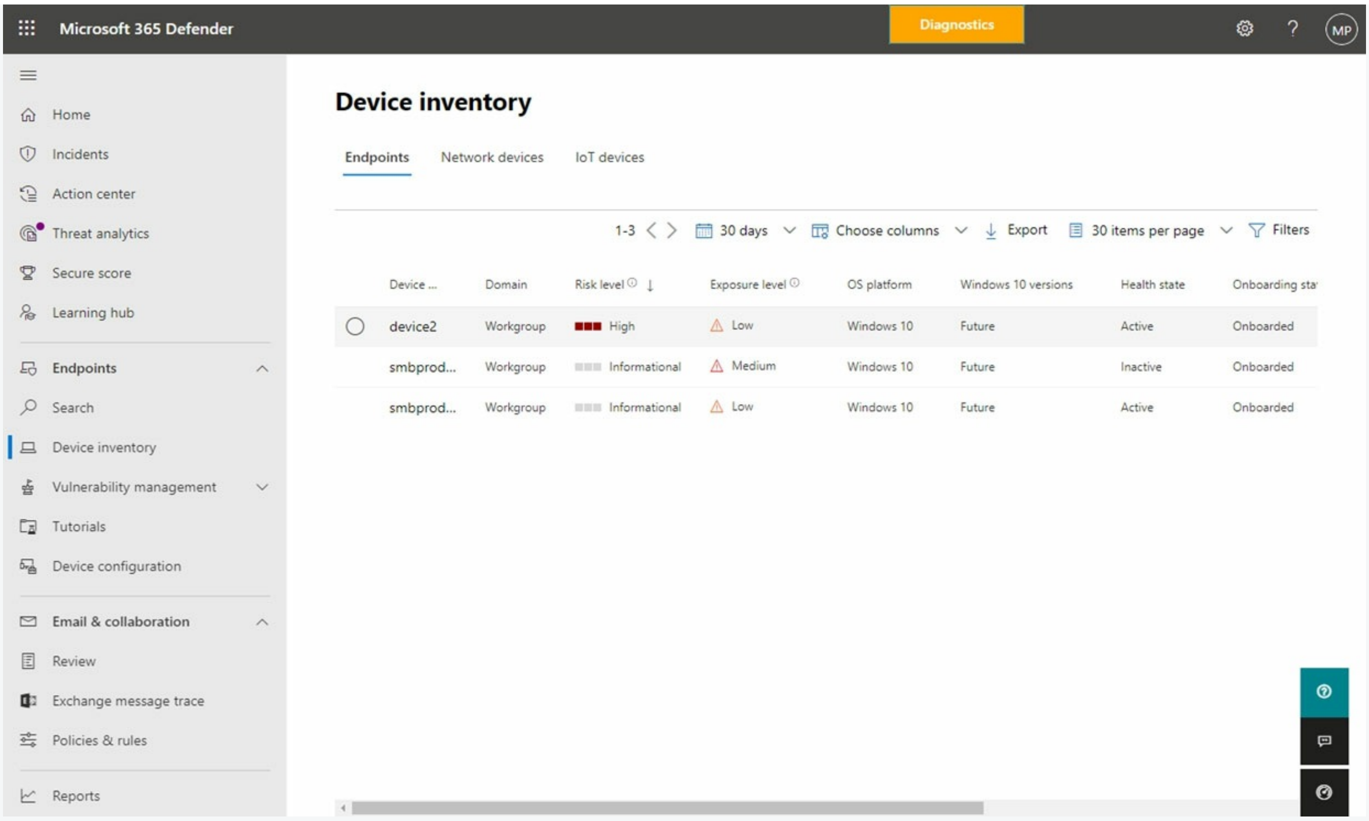
CertyIQ

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

Answer: AE

Explanation:
A: The Devices at risk card includes a View details button. Selecting that button takes us to the Device inventory page, as shown in the following image



Device inventory

Device ...	Domain	Risk level	Exposure level	OS platform	Windows 10 versions	Health state	Onboarding sta
○ device2	Workgroup	High	Low	Windows 10	Future	Active	Onboarded
smbprod...	Workgroup	Informational	Medium	Windows 10	Future	Inactive	Onboarded
smbprod...	Workgroup	Informational	Low	Windows 10	Future	Active	Onboarded

E: The Microsoft 365 Defender portal cards fall into these categories:
Identities- Monitor the identities in your organization and keep track of suspicious or risky behaviors. Here you can find the Users at risk card.
Data - Help track user activity that could lead to unauthorized data disclosure.
Devices - Get up-to-date information on alerts, breach activity, and other threats on your devices.
Apps - Gain insight into how cloud apps are being used in your organization.
Incorrect:
Not C: The Service Health card can be reached from the Microsoft 365 admin center.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-respond-mitigate-threats

Question: 111 CertyIQ

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

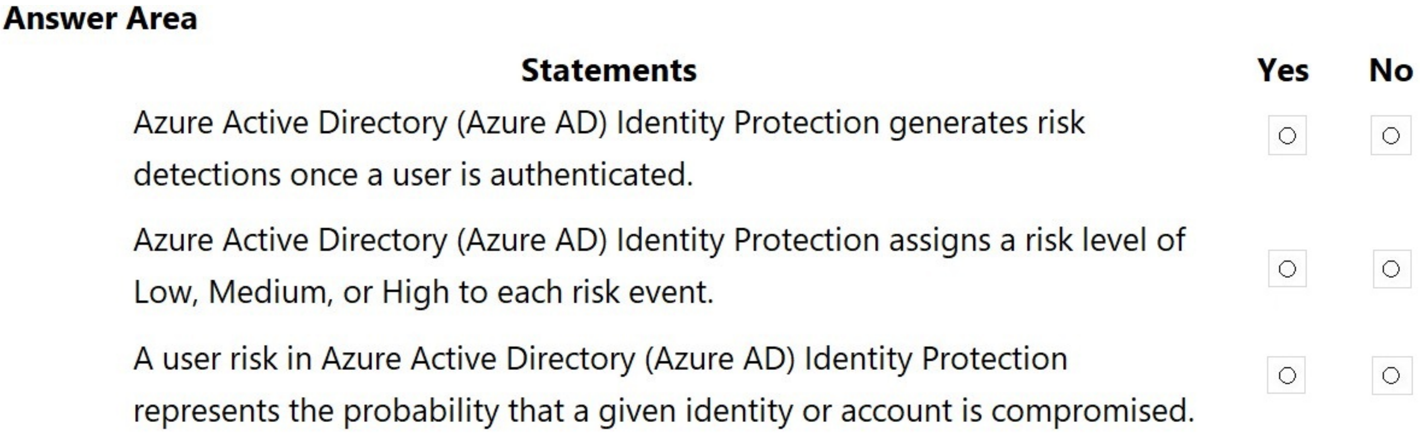
Answer: D

Explanation:

Conditional Access is a feature in Azure AD that allows you to create policies that are used to control access to Azure AD-connected resources. These policies can be based on a variety of factors, such as the user's location, device state, and sign-in risk.

Question: 112

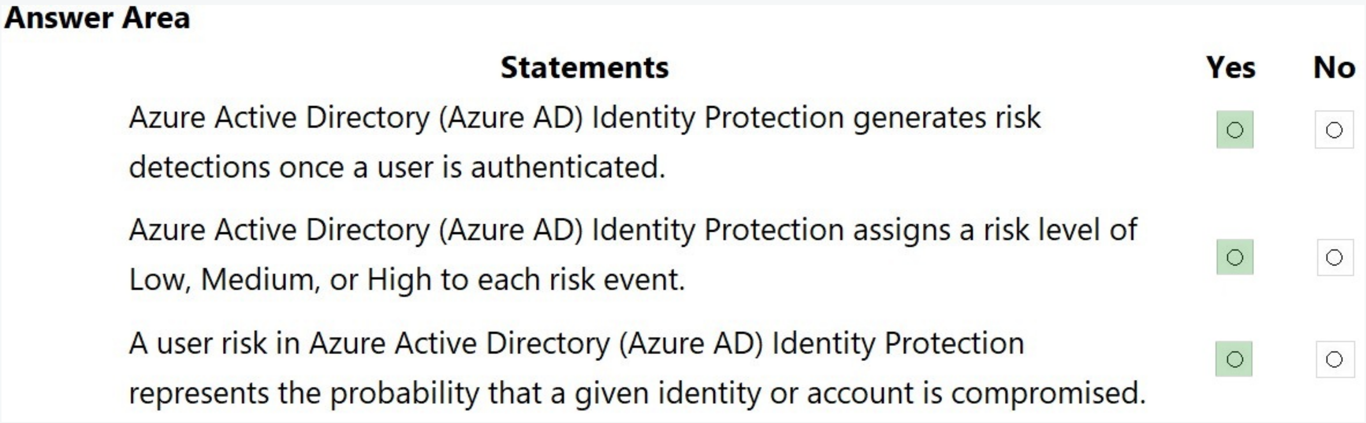
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection generates risk detections once a user is authenticated.	○	○
Azure Active Directory (Azure AD) Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	○	○
A user risk in Azure Active Directory (Azure AD) Identity Protection represents the probability that a given identity or account is compromised.	○	○

Answer:



Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection generates risk detections once a user is authenticated.	[✓ ○]	○
Azure Active Directory (Azure AD) Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	[✓ ○]	○
A user risk in Azure Active Directory (Azure AD) Identity Protection represents the probability that a given identity or account is compromised.	[✓ ○]	○

Explanation:

Box 1: Yes

Identity Protection generates risk detections only when the correct credentials are used. If incorrect credentials are used on a sign-in, it does not represent risk of credential compromise.

Box 2: Yes

Identity Protection categorizes risk into three tiers: low, medium, and high. When configuring Identity protection policies, you can also configure it to trigger upon No risk level. No Risk means there's no active indication that the user's identity has been compromised.

Box 3: Yes

Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user.

Reference

What is risk?

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Question: 113 CertyIQ

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 retention policy

B. an insider risk policy

C. a data loss prevention (DLP) policy

D. a sensitivity label policy

Answer: A

Explanation:

In order to keep a copy of all files in a Microsoft SharePoint site for one year, even if users delete the files from the site, you should enable the Recycle Bin feature in SharePoint and set the retention period to one year.

Question: 114 CertyIQ

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

A. the Microsoft 365 Compliance center

B. the Microsoft Endpoint Manager admin center

C. the Microsoft 365 admin center

D. the Microsoft 365 Defender portal

Answer: A

Explanation:

"you can configure DLP policies for all workloads through the Microsoft Purview compliance portal,"

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy

Question: 115 CertyIQ

What is an assessment in Compliance Manager?

A. A policy initiative that includes multiple policies.

B. A dictionary of words that are not allowed in company documents.

C. A grouping of controls from a specific regulation, standard or policy.

D. Recommended guidance to help organizations align with their corporate standards.

Answer: C

Explanation:

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

worldwide#assessments

An assessment is grouping of controls from a specific regulation, standard, or policy.

Question: 116 CertyIQ

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

Answer: B

Explanation:

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal.

Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture.

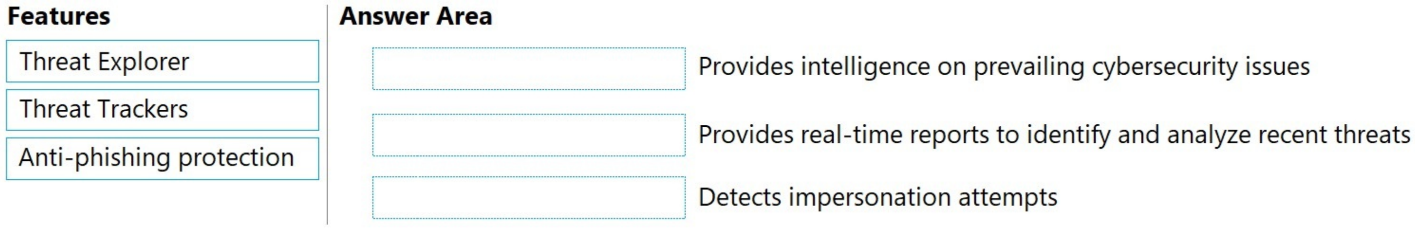
So:

MS Defender for Endpoint, and MS 365 defender (if forwarded).

But NOT Defender for O365

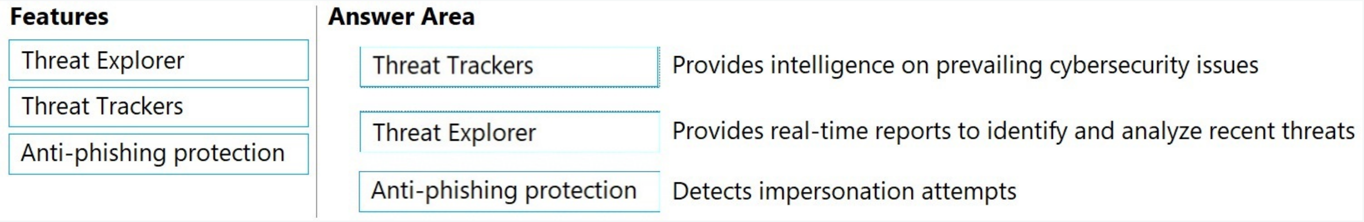
Question: 117 CertyIQ

DRAG DROP -
Match the Microsoft Defender for Office 365 feature to the correct description.
To answer, drag the appropriate feature from the column on the left to its description on the right. Each feature may be used once, more than once, or not at all.
NOTE: Each correct match is worth one point.
Select and Place:



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

Answer:



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

Explanation:

Keywords:

Prevailing = Trackers

Real-time = Explorer

Impersonation = Anti-phishing

Threat tracker

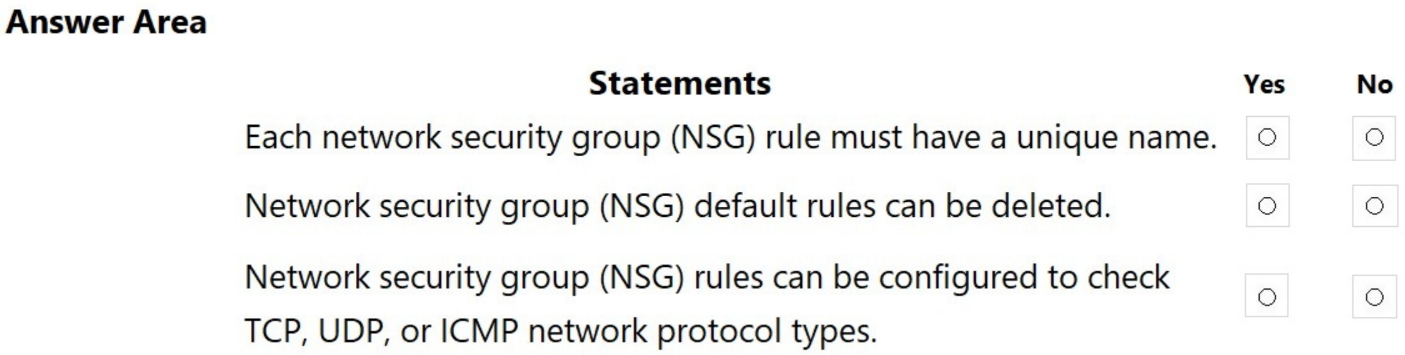
https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-defender-for-office-365-features#threat-trackers

Threat Explorer

https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-defender-for-office-365-features#threat-explorer

Question: 118

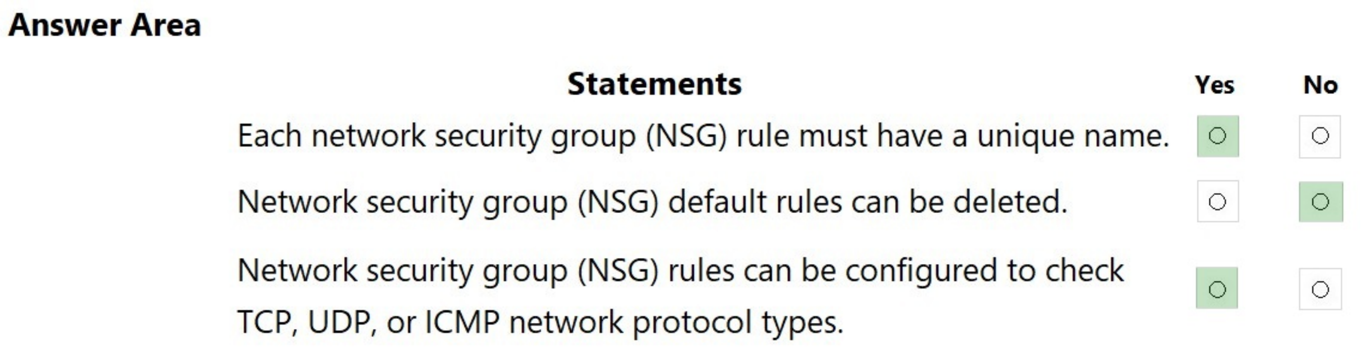
HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	○	○
Network security group (NSG) default rules can be deleted.	○	○
Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types.	○	○

Answer:



Answer Area

Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	[✓ ○]	○
Network security group (NSG) default rules can be deleted.	○	[✓ ○]
Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types.	[✓ ○]	○

Explanation:

Box 1: Yes

Security rules must have a unique name within the network security group (NSG)

Box 2: No

You can't remove the default rules, but you can override them by creating rules with higher priorities.

Box 3: Yes

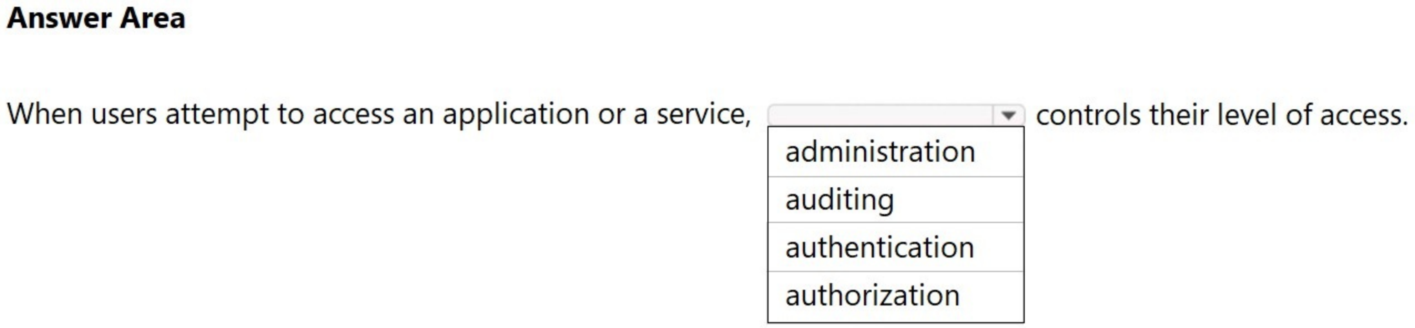
Reference

Network security groups

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

Question: 119 CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

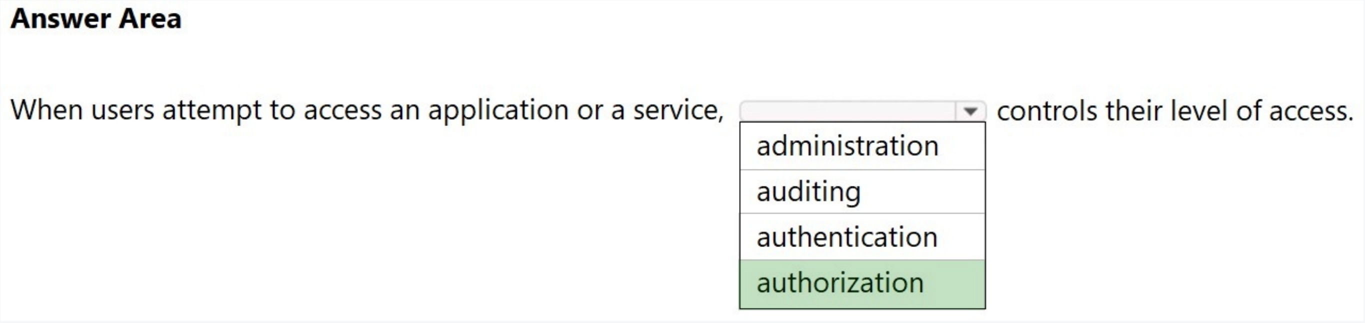


Answer Area

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

- administration
- auditing
- authentication
- authorization

Answer:



Answer Area

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

- administration
- auditing
- authentication
- [✓ authorization]

Explanation:

you can simply memorize:

authENTication = ENTER = can i go in?

authoRIzation = RIGHTS = where i can then go?

Question: 120 CertyIQ

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

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

Answer: D

Explanation:

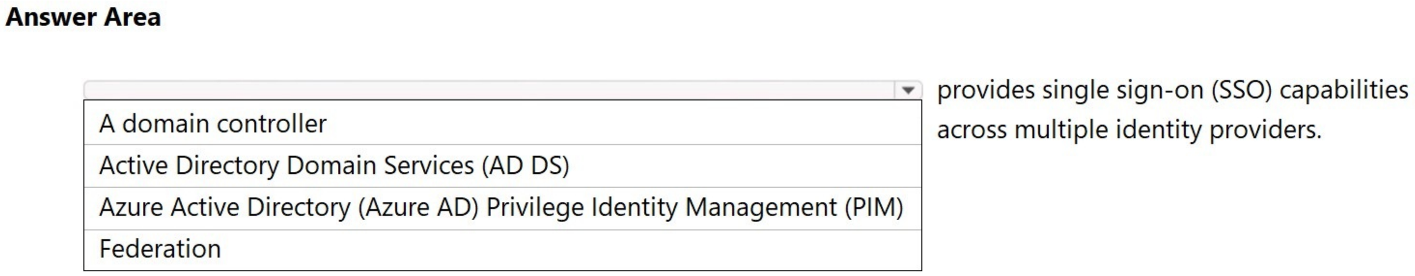
" Accounts and Identities"; Since it's a SaaS

It's (SaaS) cloud services model so the company is only responsible for the accounts and ID

Question: 121

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

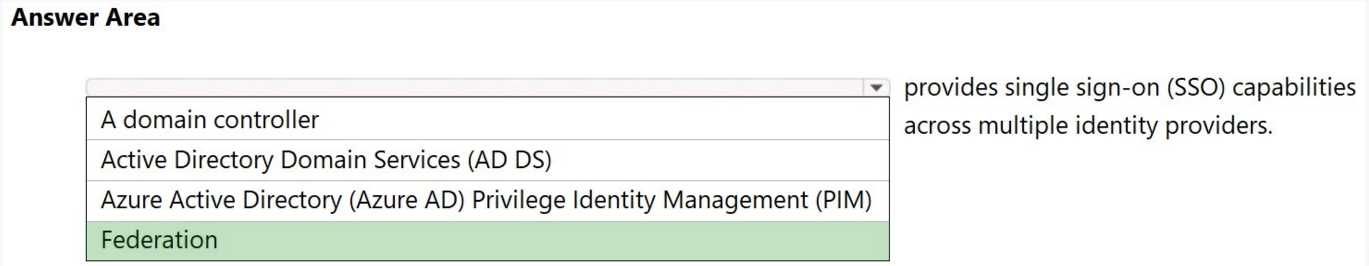


Answer Area

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.

Answer:



Answer Area

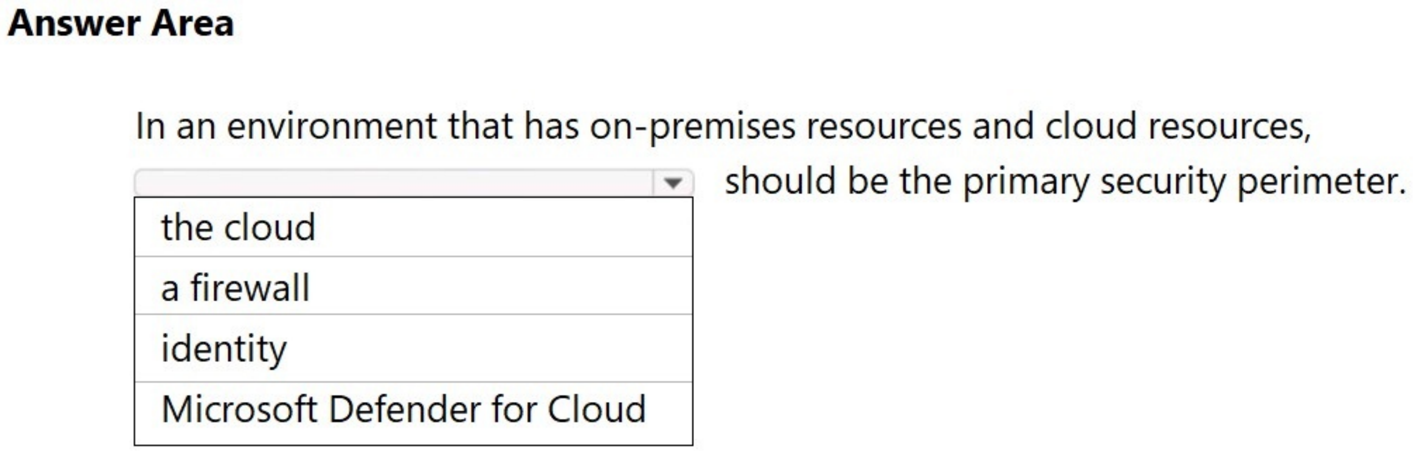
A domain controller
Active Directory Domain Services (AD DS)
Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
[✓ Federation]

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

Question: 122

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:



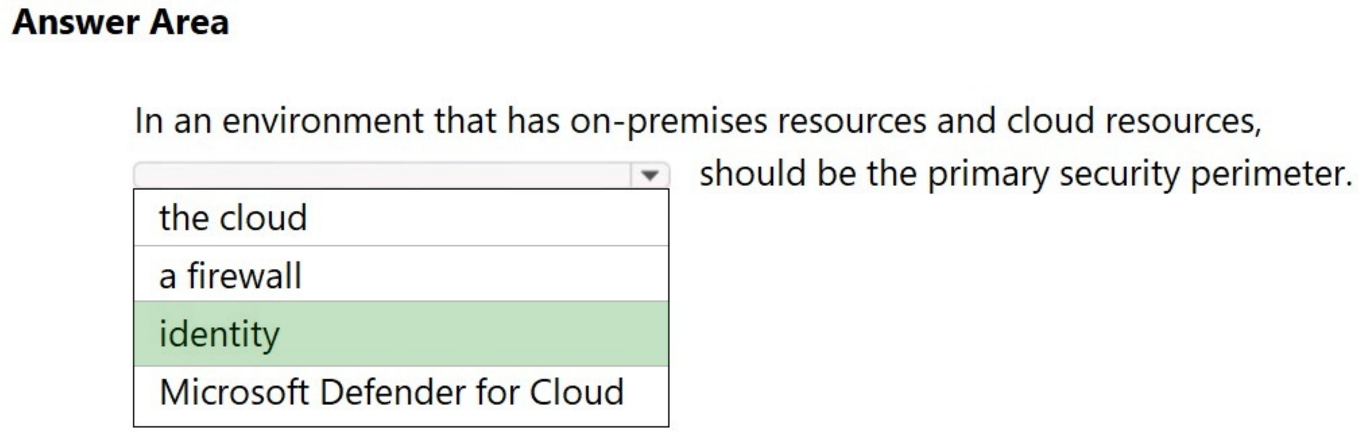
Answer Area

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:



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

Explanation:

Answer: Identity

Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security.

Best practice: Center security controls and detections around user and service identities.

Detail: Use Azure AD to collocate controls and identities.

Reference

Azure Identity Management and access control security best practices

https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Question: 123

What does Conditional Access evaluate by using Azure Active Directory (Azure AD) Identity Protection?

A. user actions
B. group membership
C. device compliance
D. user risk

Answer: D

Explanation:

D

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection Its about Identity Protection

Its's user risk including the below:

Anonymous IP address use

Atypical travel

Malware linked IP address

Unfamiliar sign-in properties

Leaked credentials

Password spray

Question: 124

CertyIQ

Which statement represents a Microsoft privacy principle?

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

Answer: B

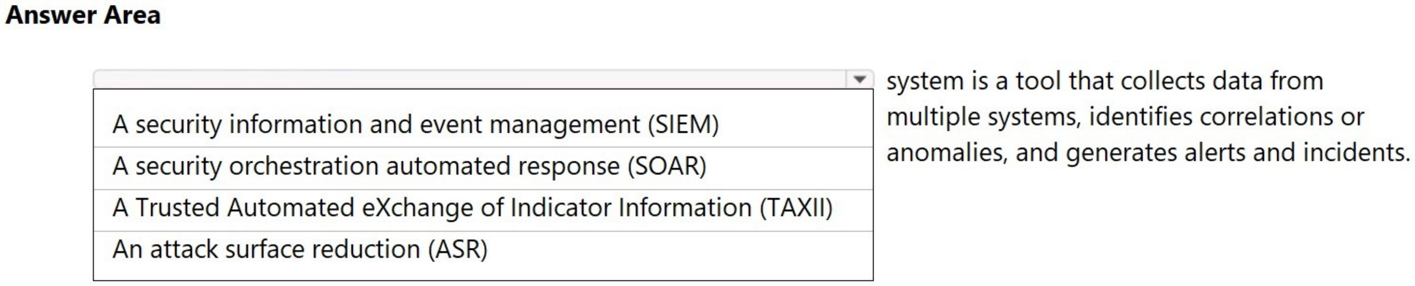
Explanation:

Then, Strong legal protections. Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

Question: 125

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

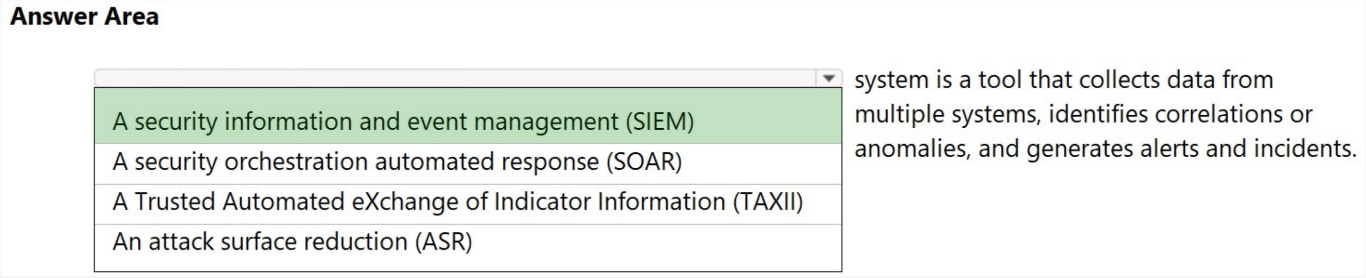


Answer Area

▾ system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.

- A security information and event management (SIEM)
- A security orchestration automated response (SOAR)
- A Trusted Automated eXchange of Indicator Information (TAXII)
- An attack surface reduction (ASR)

Answer:



Answer Area

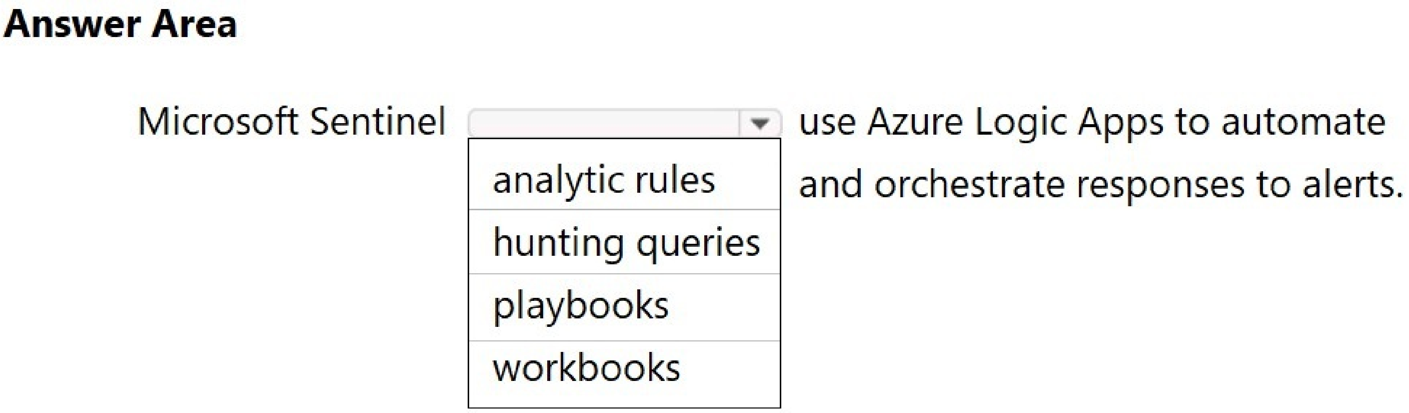
▾ system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.

- [✓ A security information and event management (SIEM)]
- A security orchestration automated response (SOAR)
- A Trusted Automated eXchange of Indicator Information (TAXII)
- An attack surface reduction (ASR)

Question: 126

CertyIQ

HOTSPOT -
Select the answer that correctly completes the sentence.
Hot Area:

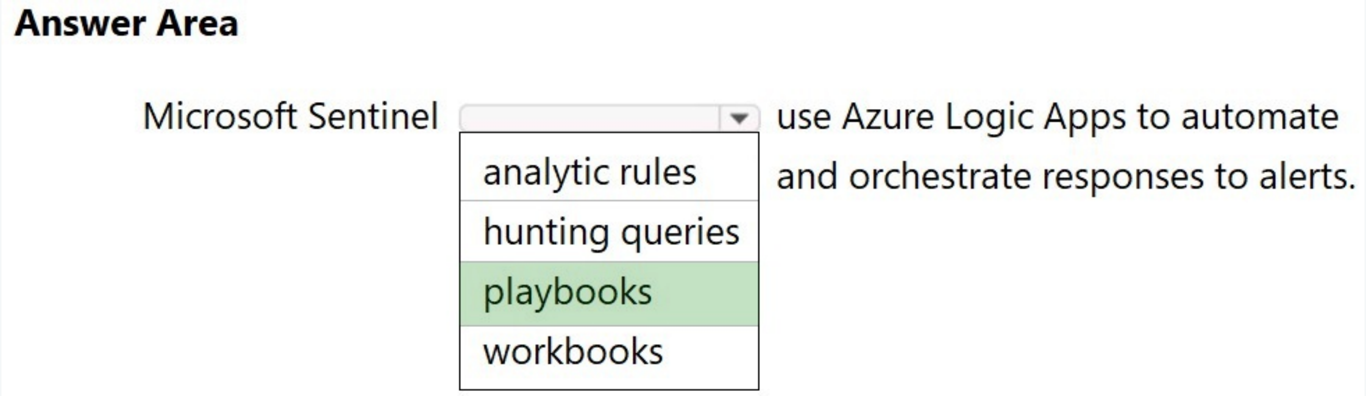


Answer Area

Microsoft Sentinel ▾ use Azure Logic Apps to automate and orchestrate responses to alerts.

- analytic rules
- hunting queries
- playbooks
- workbooks

Answer:



Answer Area

Microsoft Sentinel ▾ use Azure Logic Apps to automate and orchestrate responses to alerts.

- analytic rules
- hunting queries
- [✓ playbooks]
- workbooks

Explanation:

Answer: playbooks

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Reference

Tutorial: Use playbooks with automation rules in Microsoft Sentinel

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Question: 127

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

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

Answer: A

Explanation:

Correct: https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-tc-definitions?view=o365-

worldwide#resume

Question: 128 CertyIQ

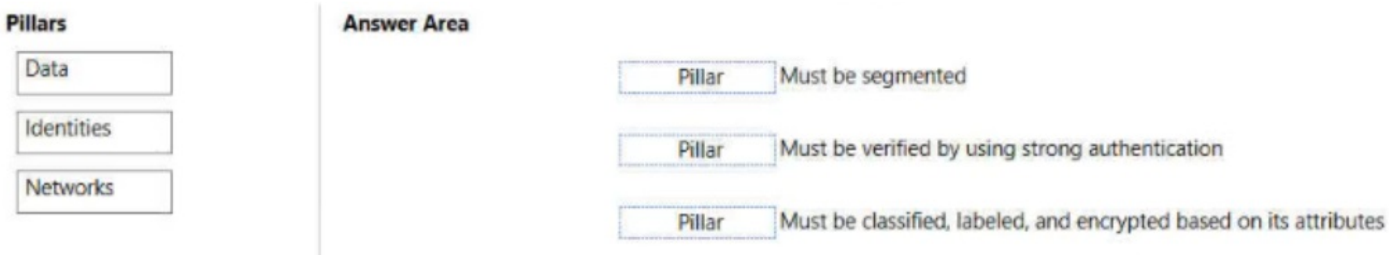
DRAG DROP

-

Match the pillars of Zero Trust to the appropriate requirements.

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

NOTE: Each correct match is worth one point.



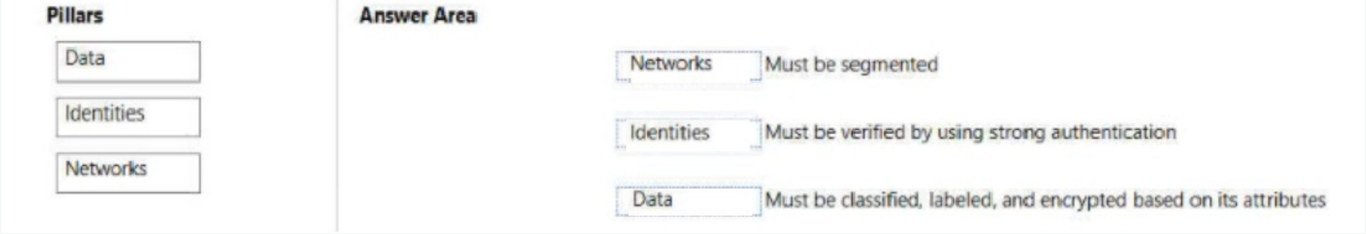
Pillars

- Data
- Identities
- Networks

Answer Area

Pillar	Must be segmented
Pillar	Must be verified by using strong authentication
Pillar	Must be classified, labeled, and encrypted based on its attributes

Answer:



Pillars

- Data
- Identities
- Networks

Answer Area

Networks	Must be segmented
Identities	Must be verified by using strong authentication
Data	Must be classified, labeled, and encrypted based on its attributes

Explanation:

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/4-describe-zero-trust-model

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- Identities may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.

- Data should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.

- Networks should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

Question: 129 CertyIQ

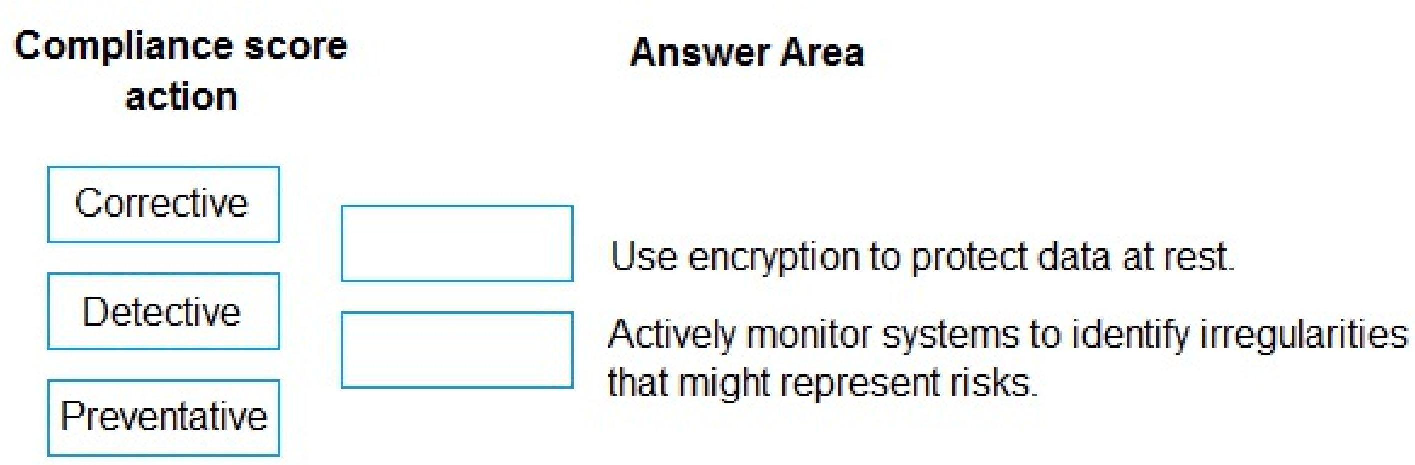
DRAG DROP

-

Match the types of compliance score actions to the appropriate tasks.

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

NOTE: Each correct match is worth one point.



Compliance score action

Answer Area

Corrective

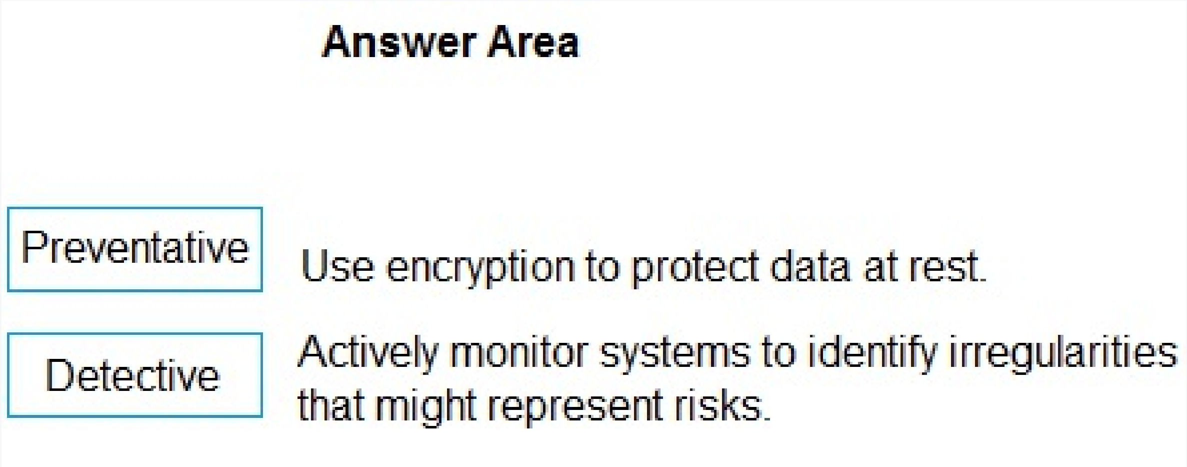
Detective

Preventative

Use encryption to protect data at rest.

Actively monitor systems to identify irregularities that might represent risks.

Answer:



Answer Area

Preventative — Use encryption to protect data at rest.

Detective — Actively monitor systems to identify irregularities that might represent risks.

Explanation:

Protect = prevent

Monitor = detect

Question: 130 CertyIQ

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

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

Answer: B

Explanation:

Auditing is correct - the key word here is tracking, otherwise it would have been authorization.

See below article.

https://social.technet.microsoft.com/wiki/contents/articles/15530.the-four-pillars-of-identity-identity-management-in-the-age-of-hybrid-it.aspx

Question: 131 CertyIQ

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

A. line-of-business (LOB) applications that require modern authentication
B. computer accounts
C. software as a service (SaaS) applications that require modern authentication
D. mobile devices

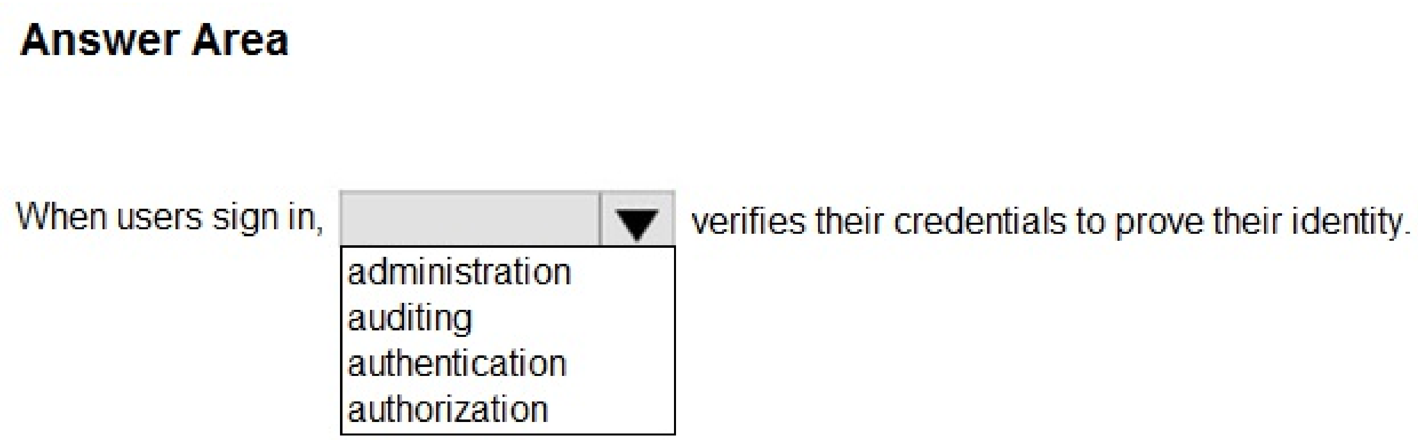
Answer: B

Question: 132 CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

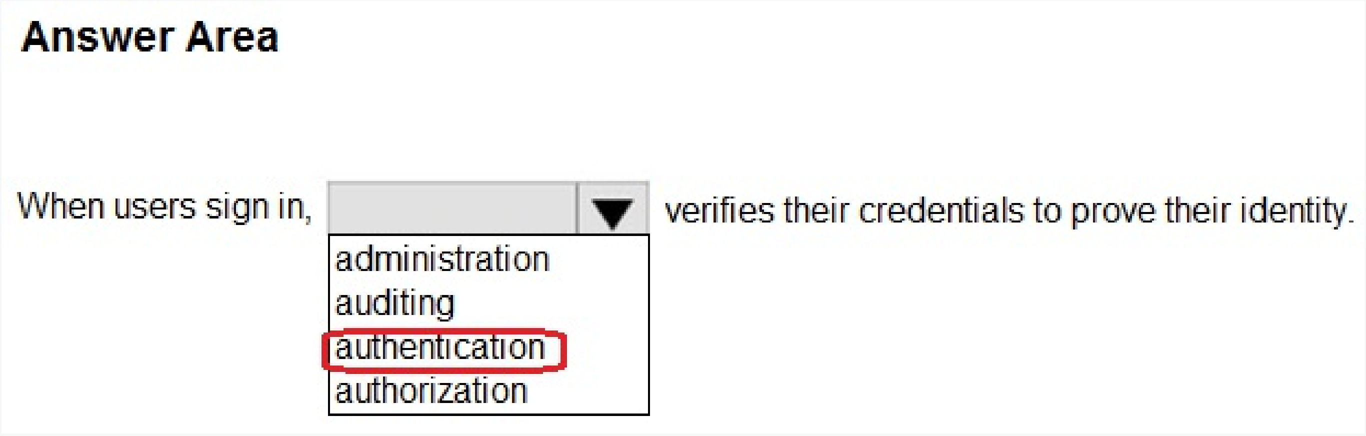


Answer Area

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

- administration
- auditing
- authentication
- authorization

Answer:



Answer Area

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

- administration
- auditing
- [✓ authentication]
- authorization

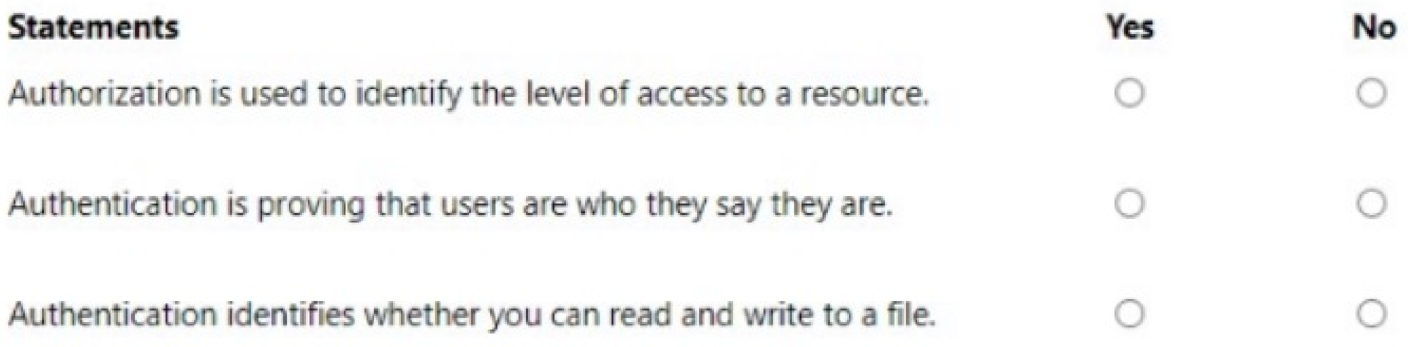
Question: 133 CertyIQ

HOTSPOT

-

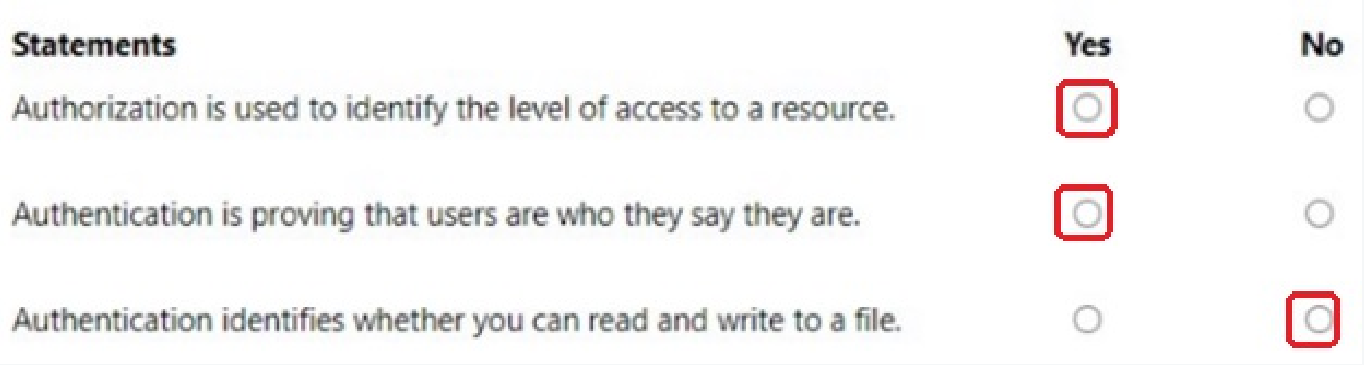
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Statements	Yes	No
Authorization is used to identify the level of access to a resource.	○	○
Authentication is proving that users are who they say they are.	○	○
Authentication identifies whether you can read and write to a file.	○	○

Answer:



Statements	Yes	No
Authorization is used to identify the level of access to a resource.	[✓ ○]	○
Authentication is proving that users are who they say they are.	[✓ ○]	○
Authentication identifies whether you can read and write to a file.	○	[✓ ○]

Question: 134 CertyIQ

What is a function of Conditional Access session controls?

A. enforcing device compliance

B. enforcing client app compliance

C. enable limited experiences, such as blocking download of sensitive information

D. prompting multi-factor authentication (MFA)

Answer: C

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

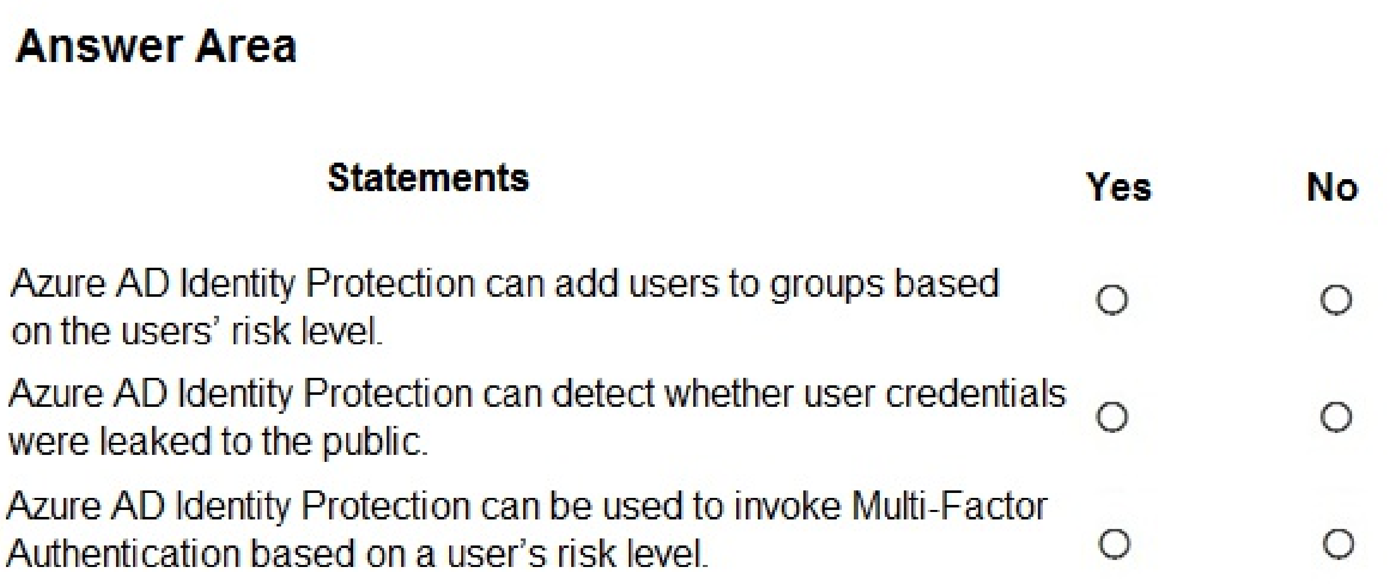
Question: 135 CertyIQ

HOTSPOT

-

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

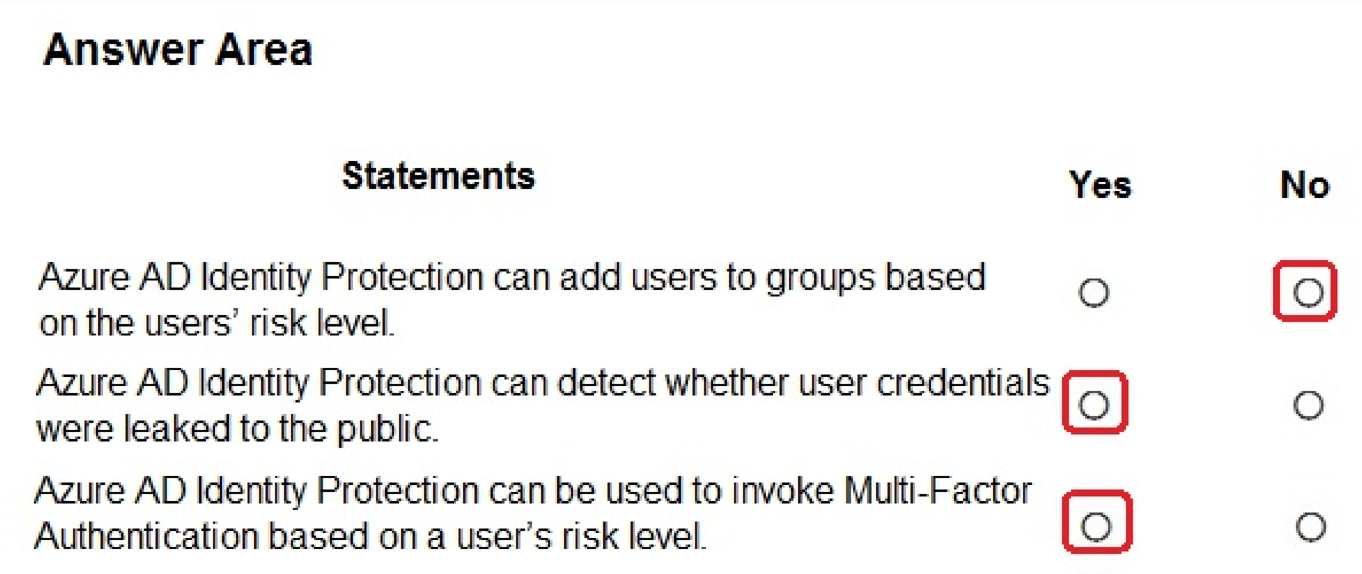
NOTE: Each correct selection is worth one point.



Answer Area

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

Answer:



Answer Area

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

Question: 136 CertyIQ

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

A. Azure Policy

B. a communication compliance policy

C. a Conditional Access policy

D. a user risk policy

Answer: C

Explanation:

ref: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question: 137

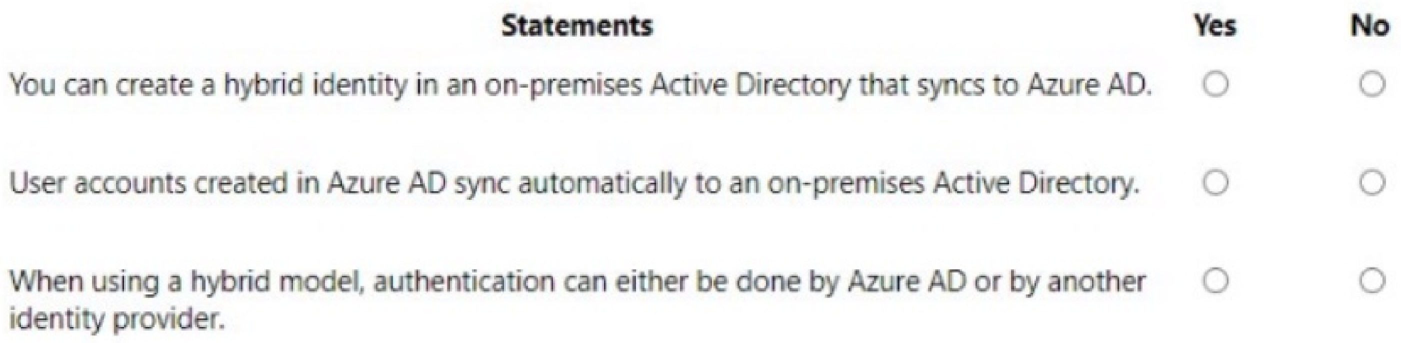
CertyIQ

HOTSPOT

-

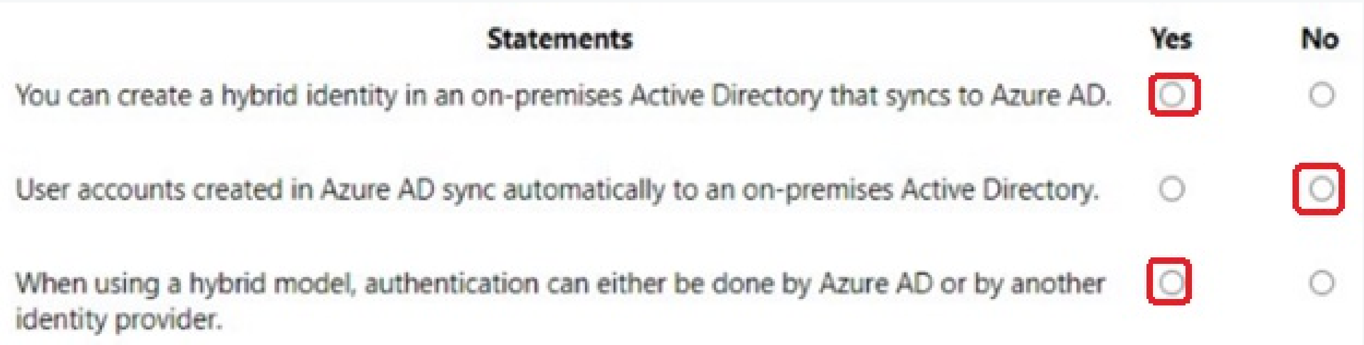
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



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:



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.	[✓ ○]	○

Question: 138

CertyIQ

Which three authentication methods can Azure AD users use to reset their password? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. mobile app notification

B. text message to a phone

C. security questions

D. certificate

E. picture password

Answer: ABC

Explanation:

Correct: https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#select-authentication-methods-and-registration-options

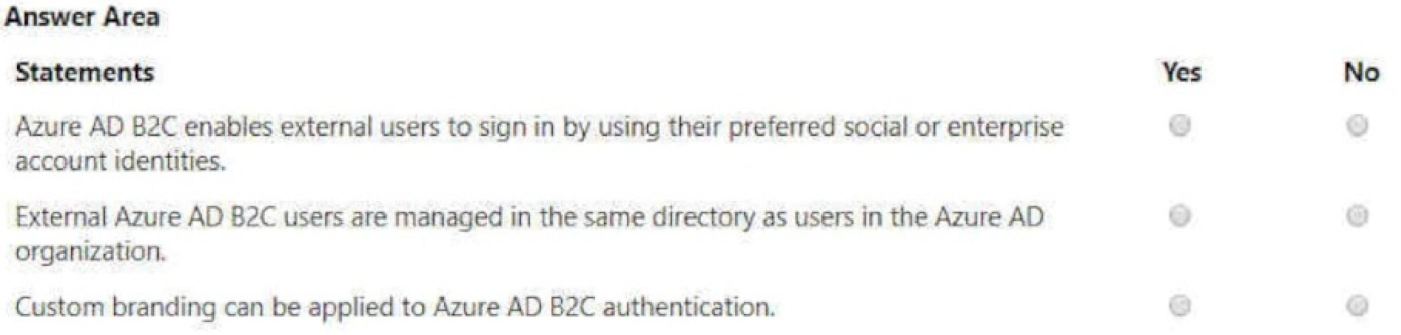
Question: 139 CertyIQ

HOTSPOT

-

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

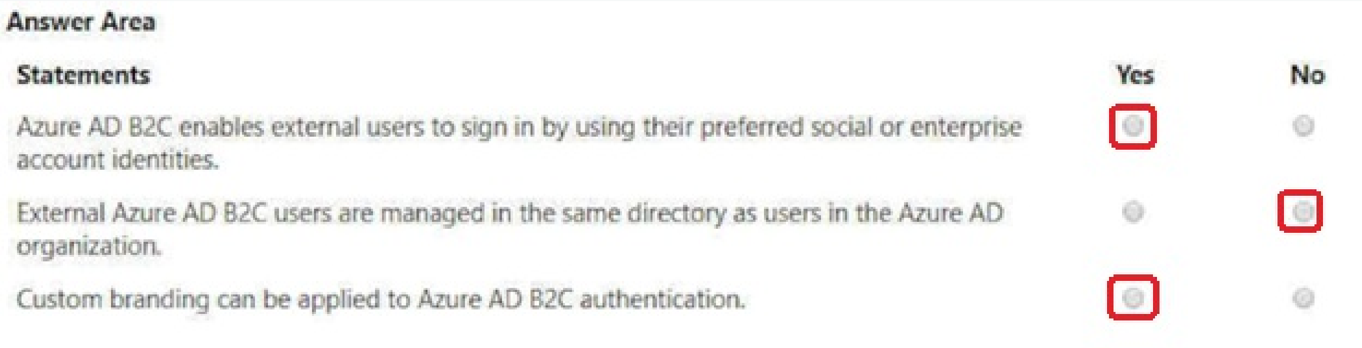
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Azure AD B2C enables external users to sign in by using their preferred social or enterprise account identities.	○	○
External Azure AD B2C users are managed in the same directory as users in the Azure AD organization.	○	○
Custom branding can be applied to Azure AD B2C authentication.	○	○

Answer:



Answer Area

Statements	Yes	No
Azure AD B2C enables external users to sign in by using their preferred social or enterprise account identities.	[✓ ○]	○
External Azure AD B2C users are managed in the same directory as users in the Azure AD organization.	○	[✓ ○]
Custom branding can be applied to Azure AD B2C authentication.	[✓ ○]	○

Explanation:

https://azure.microsoft.com/nl-nl/blog/easily-enable-identity-and-access-management-with-social-logins-for-b2c-apps/

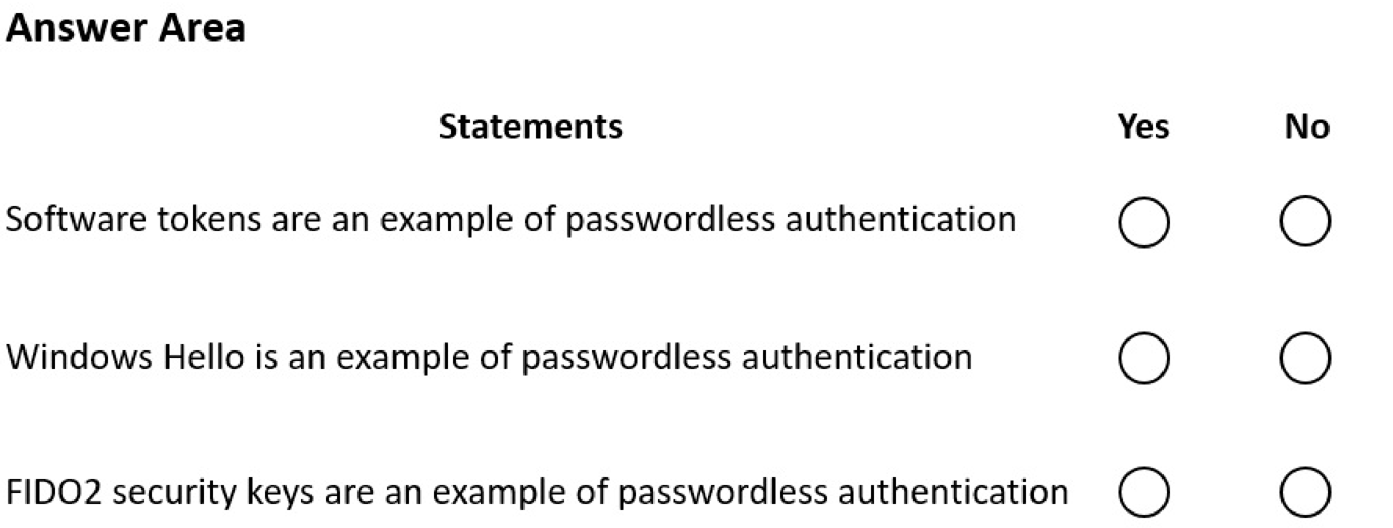
Question: 140 CertyIQ

HOTSPOT

-

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

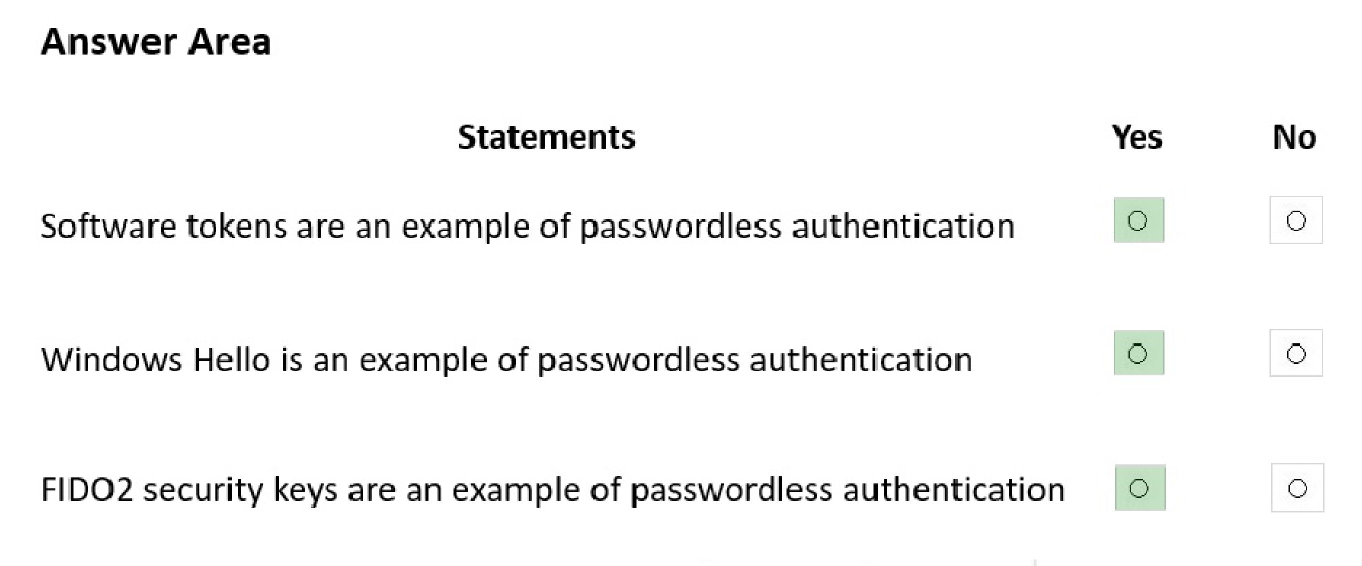
NOTE: Each correct selection is worth one point.



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:



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	[✓ ○]	○

Explanation:

1. **Software tokens are an example of passwordless authentication - Yes**
   In the Microsoft context, software tokens like the Microsoft Authenticator app can be used for passwordless authentication, as supported by Entra ID.
2. **Windows Hello is an example of passwordless authentication - Yes**
   Windows Hello provides a passwordless authentication method by using biometrics or a PIN tied to the device.
3. **FIDO2 security keys are an example of passwordless authentication - Yes**
   FIDO2 security keys offer passwordless authentication based on public key cryptography.

Question: 141

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

A. threat protection alerts

B. just-in-time (JIT) VM access to Azure virtual machines

C. vulnerability scanning of virtual machines

D. secure score

Answer: D

Question: 142 CertyIQ

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

A. Windows 10 and newer only

B. Windows 10 and newer and Android only

C. Windows 10 and newer and iOS only

D. Windows 10 and newer, Android, and iOS

Answer: C

Explanation:

Windows 10 and newer and iOS only.

Reference:

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

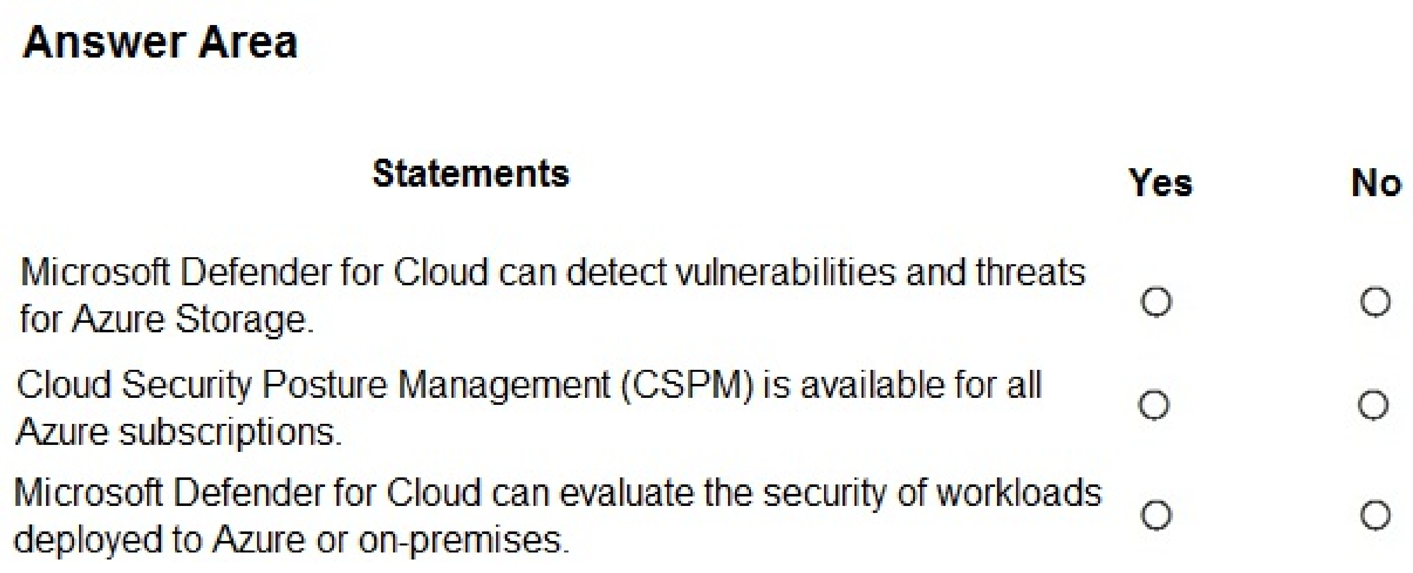
Question: 143 CertyIQ

HOTSPOT

-

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

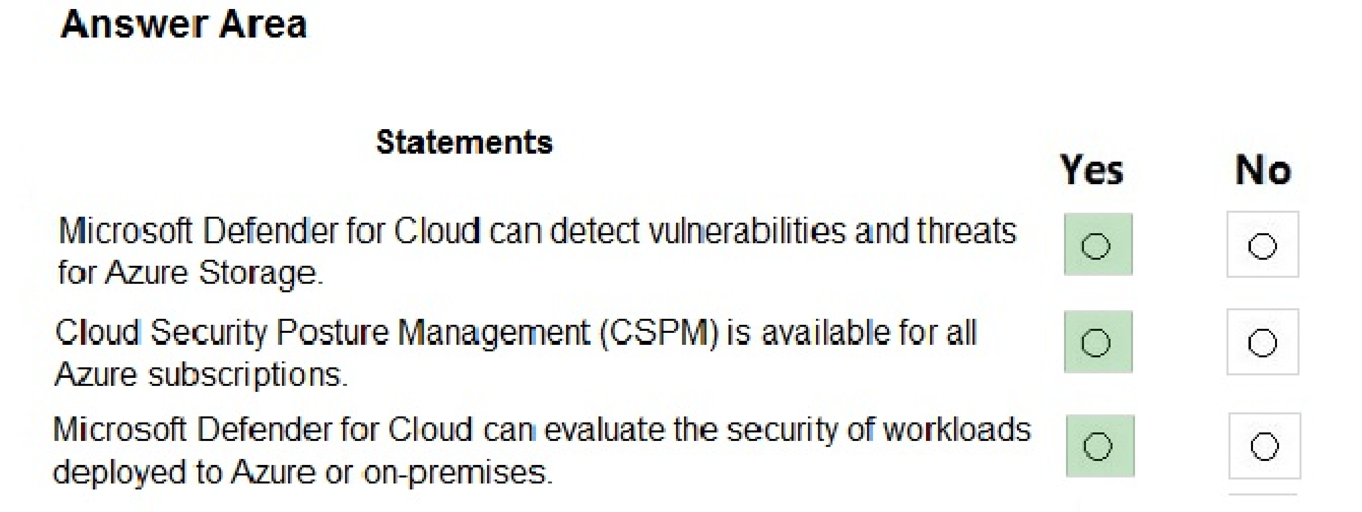
NOTE: Each correct selection is worth one point.



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.	○	○

Answer:



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.	[✓ ○]	○

Explanation:

Box 1: Yes- Microsoft Defender for Cloud 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.

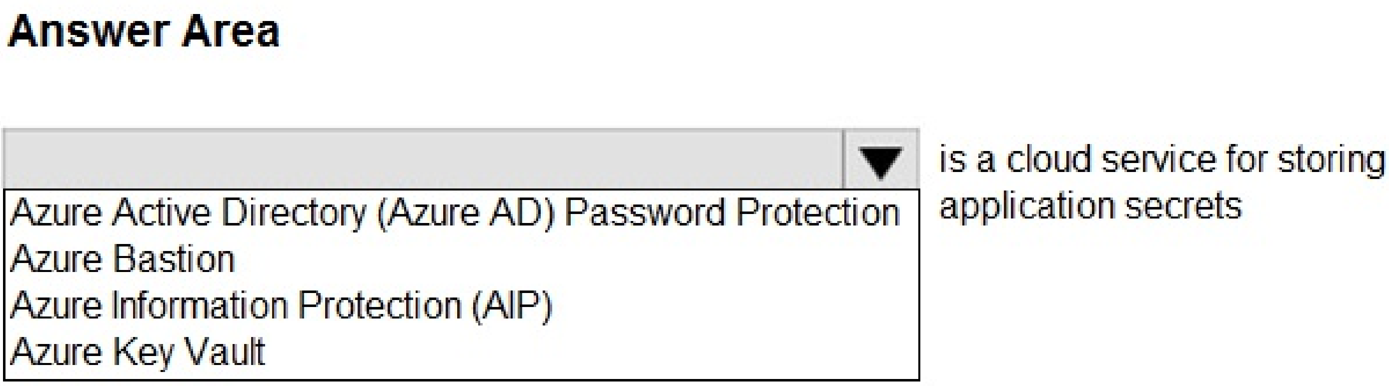
Question: 144

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

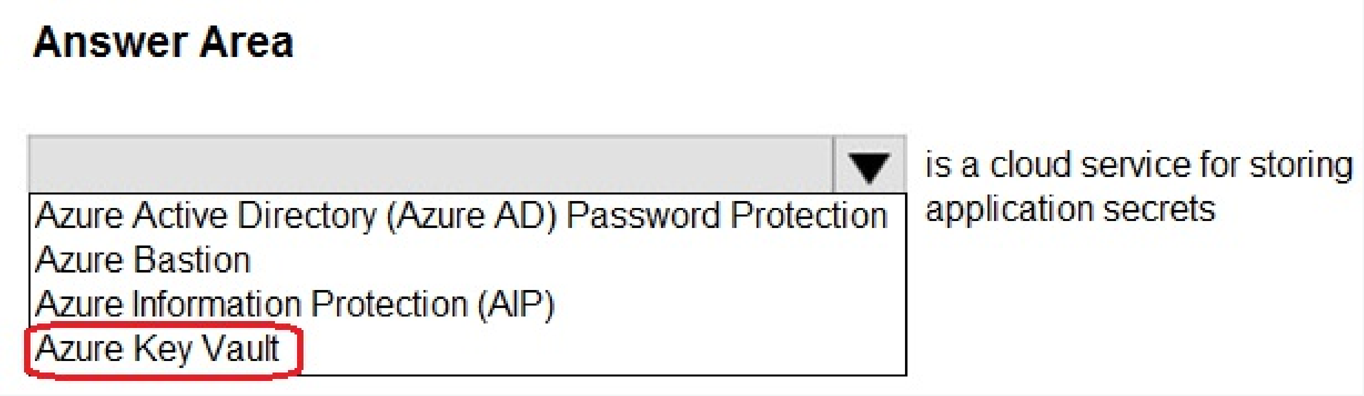


Answer Area

▼ is a cloud service for storing application secrets

Azure Active Directory (Azure AD) Password Protection
Azure Bastion
Azure Information Protection (AIP)
Azure Key Vault

Answer:



Answer Area

▼ is a cloud service for storing application secrets

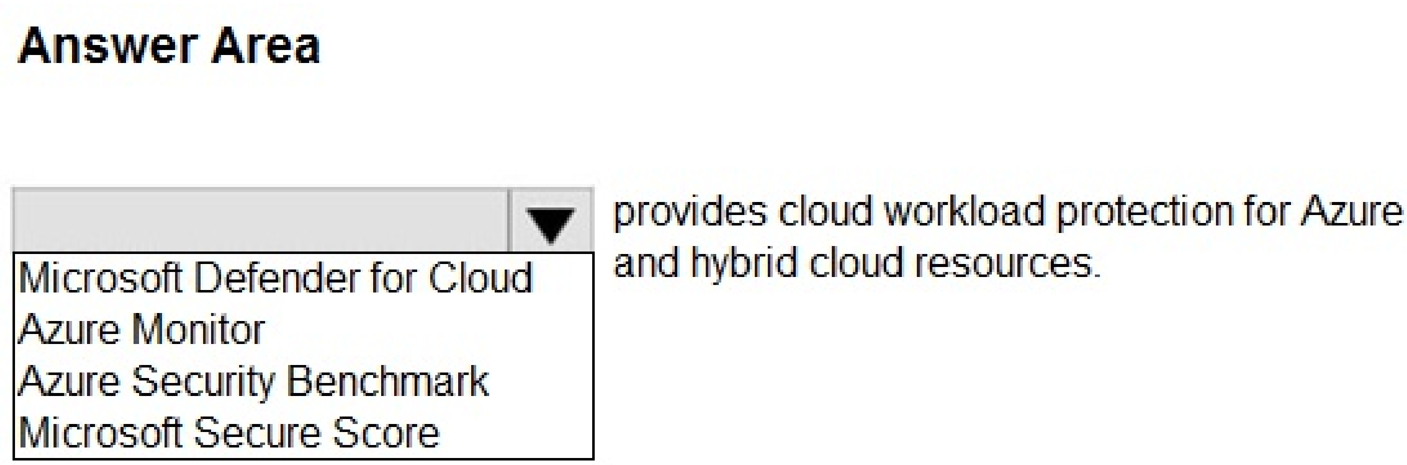
Azure Active Directory (Azure AD) Password Protection
Azure Bastion
Azure Information Protection (AIP)
[✓ Azure Key Vault]

Question: 145 **CertyIQ**

HOTSPOT

-

Select the answer that correctly completes the sentence.

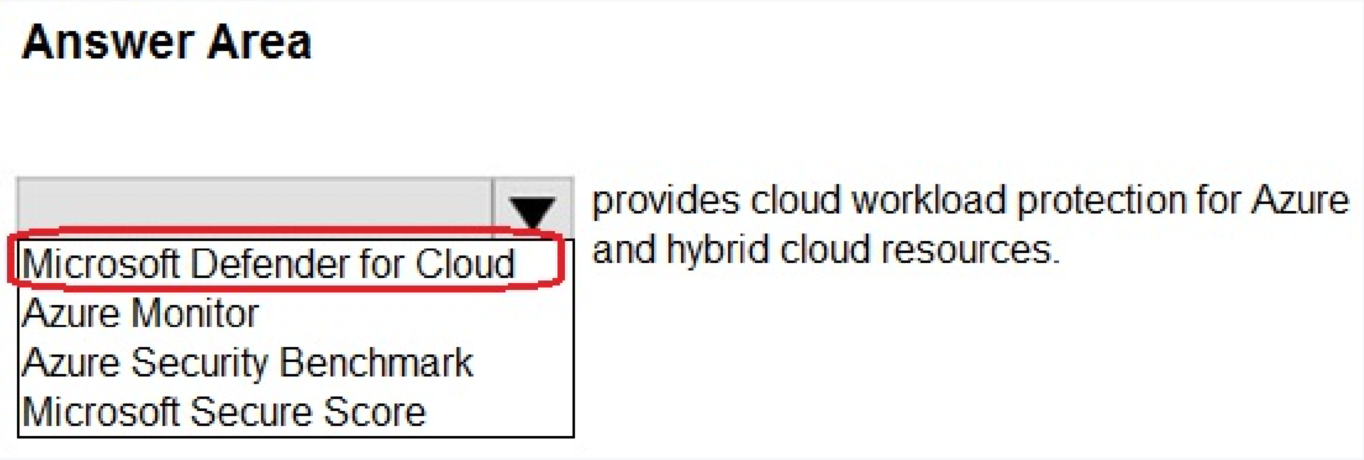


Answer Area

▼ provides cloud workload protection for Azure and hybrid cloud resources.

Microsoft Defender for Cloud
Azure Monitor
Azure Security Benchmark
Microsoft Secure Score

Answer:



Answer Area

▼ provides cloud workload protection for Azure and hybrid cloud resources.

[✓ Microsoft Defender for Cloud]
Azure Monitor
Azure Security Benchmark
Microsoft Secure Score

Explanation:

ref: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Question: 146 **CertyIQ**

What is the maximum number of resources that Azure DDoS Protection Standard can protect without additional costs?

A. 50
B. 100
C. 500
D. 1000

Answer: B

Explanation:

DDoS protection plans have a fixed monthly charge that covers up to 100 public IP addresses. Protection for additional resources is available.

https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-faq#how-does-pricing-work

Question: 147

What are two reasons to deploy multiple virtual networks instead of using just one virtual network? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: AD

Explanation:

The main reasons for segmentation are:

The ability to group related assets that are a part of (or support) workload operations.

Isolation of resources.

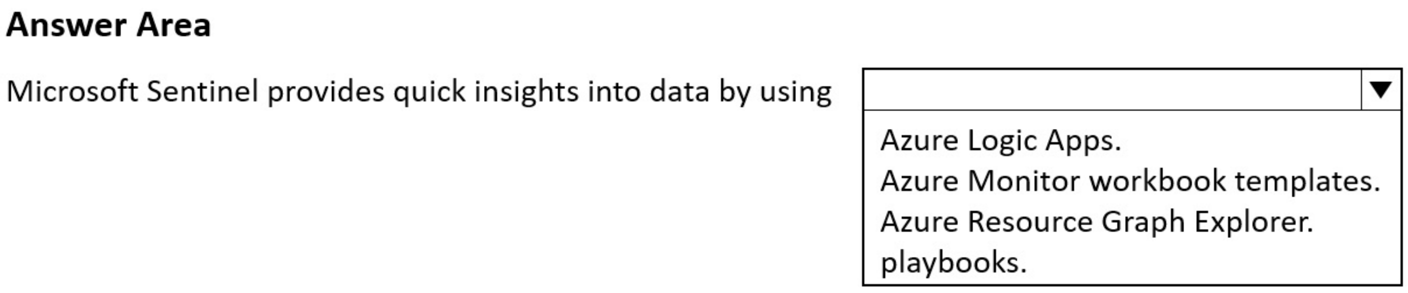
Governance policies set by the organization.

See: https://learn.microsoft.com/en-us/azure/architecture/framework/security/design-network-segmentation

Question: 148

HOTSPOT
-

Select the answer that correctly completes the sentence.

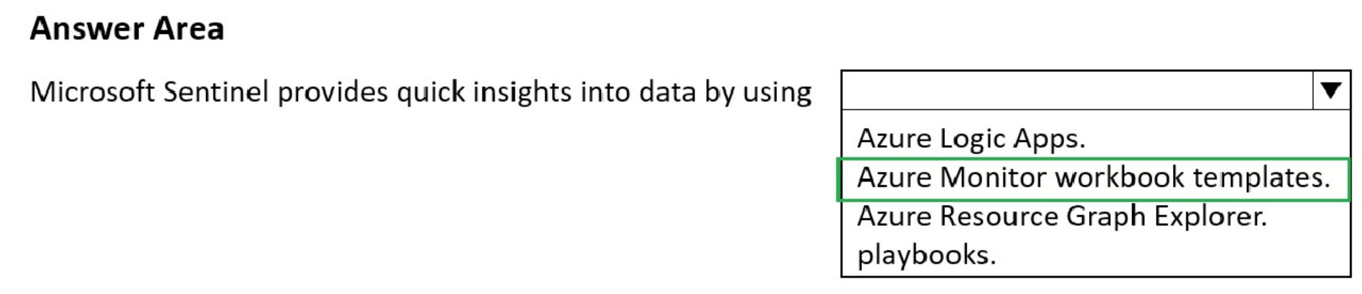


Answer Area

Microsoft Sentinel provides quick insights into data by using ▼

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

Answer:



Answer Area

Microsoft Sentinel provides quick insights into data by using ▼

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

Explanation:

"Azure Monitor workbook templates" is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/overview#create-interactive-reports-by-using-workbooks

After you onboard to Microsoft Sentinel, monitor your data by using the integration with Azure Monitor workbooks.

Workbooks display differently in Microsoft Sentinel than in Azure Monitor. But it may be useful for you to see how to create a workbook in Azure Monitor. Microsoft Sentinel allows you to create custom workbooks across your data. Microsoft Sentinel also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Question: 149 CertyIQ

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

Answer: D

Question: 150 CertyIQ

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

A. secure score

B. resource health

C. completed controls

D. the status of recommendations

Answer: A

Explanation:

if it was resources issues/health then it would have been resources health BUT the question is Security health hence its Secure Score.

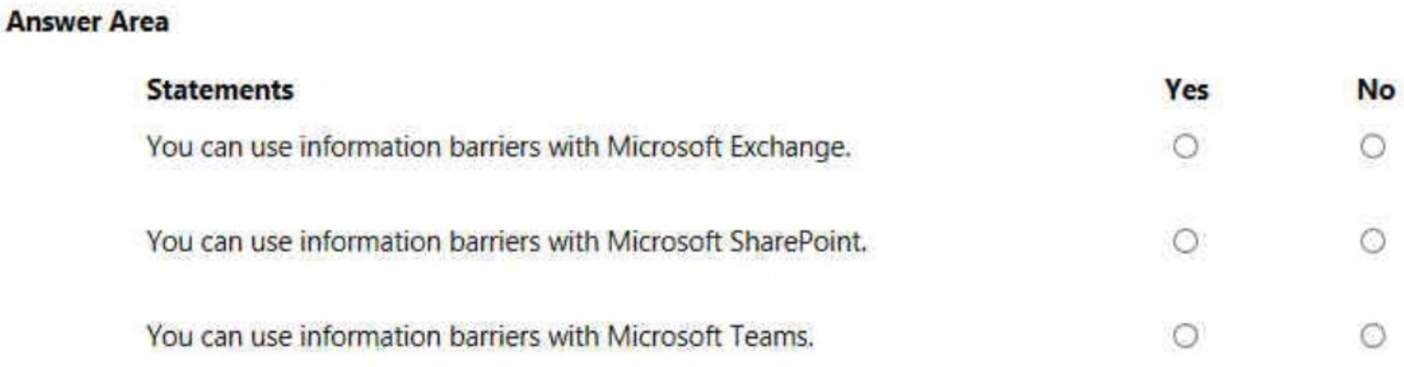
Question: 151 CertyIQ

HOTSPOT

-

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

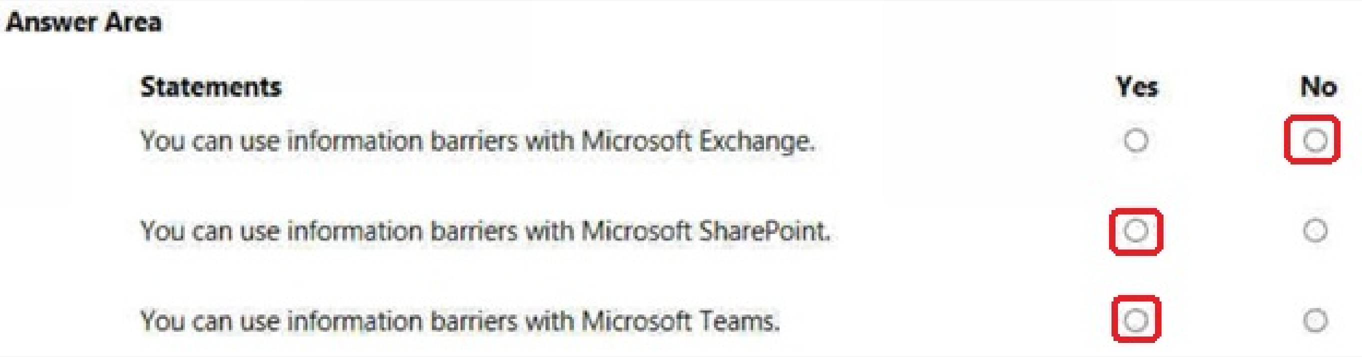
NOTE: Each correct selection is worth one point.



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.	○	○

Answer:



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.	[✓ ○]	○

Explanation:

NO - https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide#information-barriers-and-exchange-online

Only Exchange Online deployments are currently supported for IB policies. If your organization needs to define and control email communications, consider using Exchange mail flow rules.

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.

YES - https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide

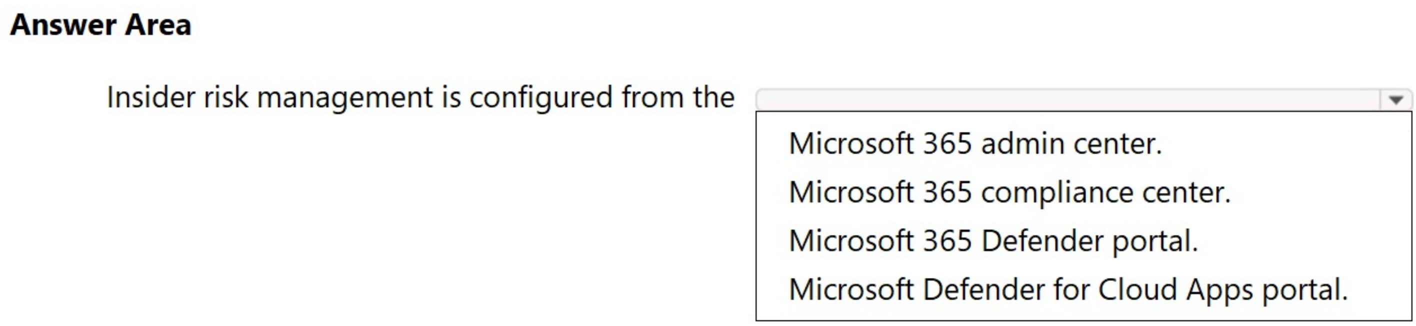
YES - https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide

Question: 152 CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

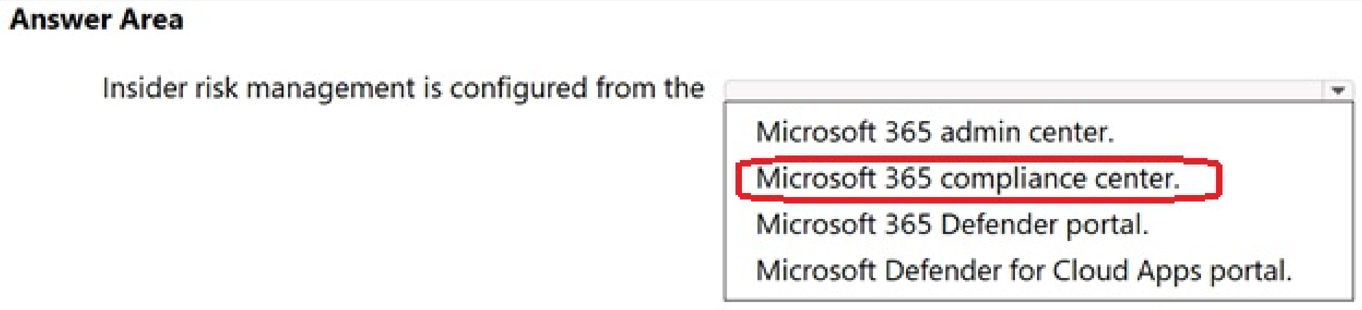


Answer Area

Insider risk management is configured from the

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

Answer:



Answer Area

Insider risk management is configured from the

- Microsoft 365 admin center.
- [✓ Microsoft 365 compliance center.]
- Microsoft 365 Defender portal.
- Microsoft Defender for Cloud Apps portal.

Explanation:

its renamed so I assume the exam is still labelling it as M365 Compliance Center. Just remember its now Microsoft Purview.

Question: 153 CertyIQ

You need to ensure repeatability when creating new resources in an Azure subscription.

What should you use?

A. Microsoft Sentinel
B. Azure Policy
C. Azure Batch
D. Azure Blueprints

Answer: D

Question: 154

CertyIQ

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

A. encrypted

B. restricted to predefined categories

C. persistent

Answer: C

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-a-sensitivity-label-is

Question: 155

CertyIQ

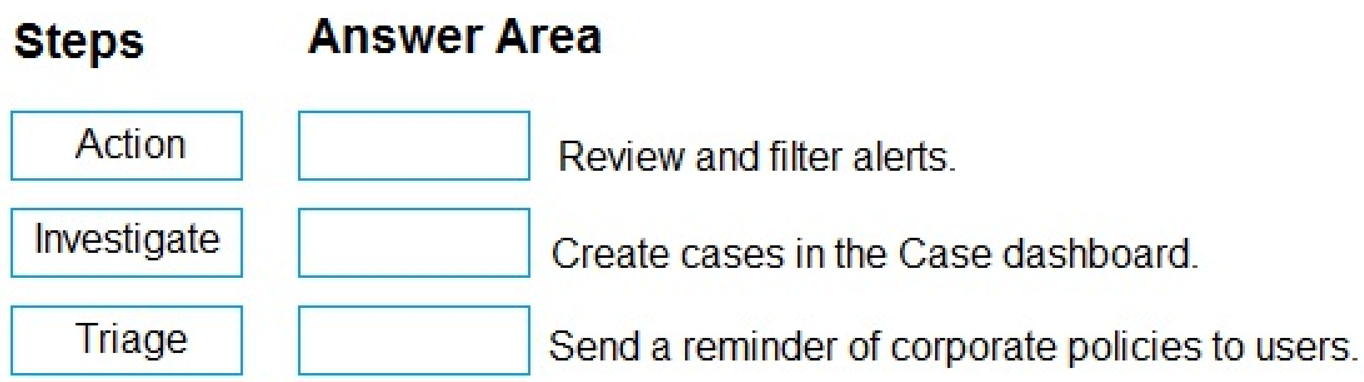
DRAG DROP

-

Match the Microsoft Purview 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.



Steps

Action

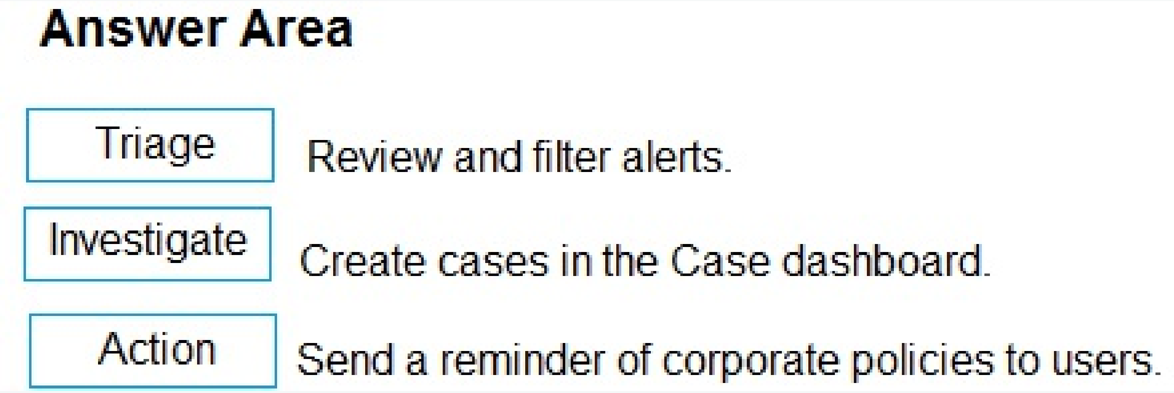
Investigate

Triage

Answer Area

	Review and filter alerts.
	Create cases in the Case dashboard.
	Send a reminder of corporate policies to users.

Answer:



Answer Area

Triage	Review and filter alerts.
Investigate	Create cases in the Case dashboard.
Action	Send a reminder of corporate policies to users.

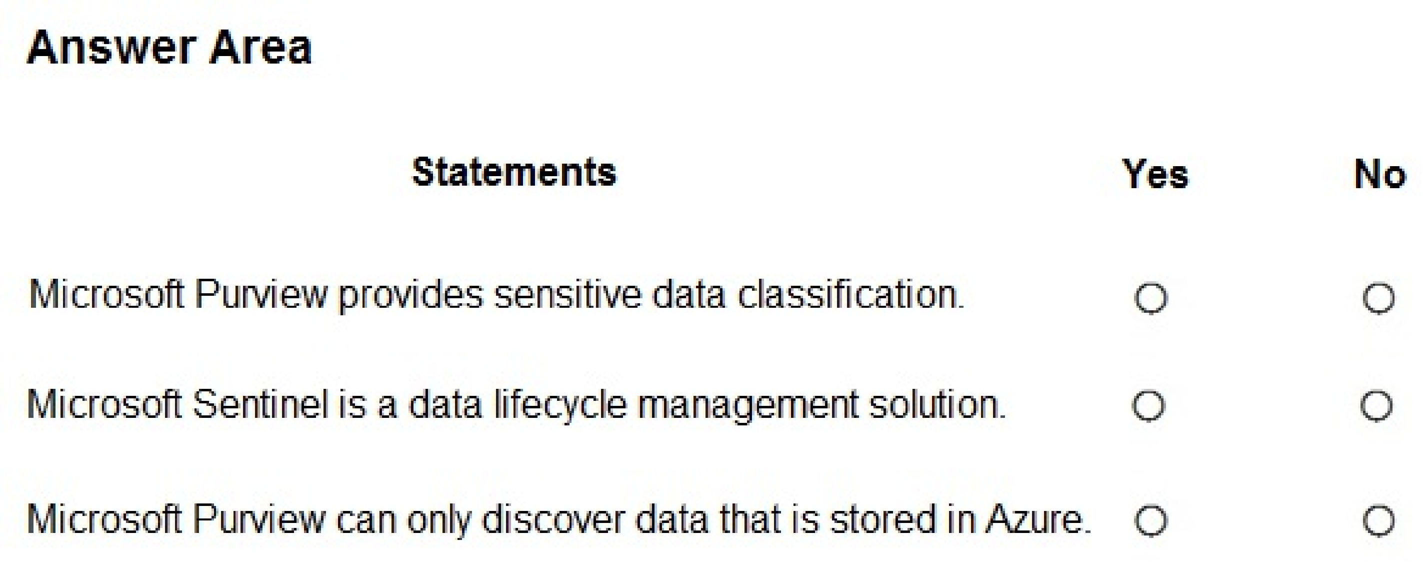
Question: 156

HOTSPOT

-

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

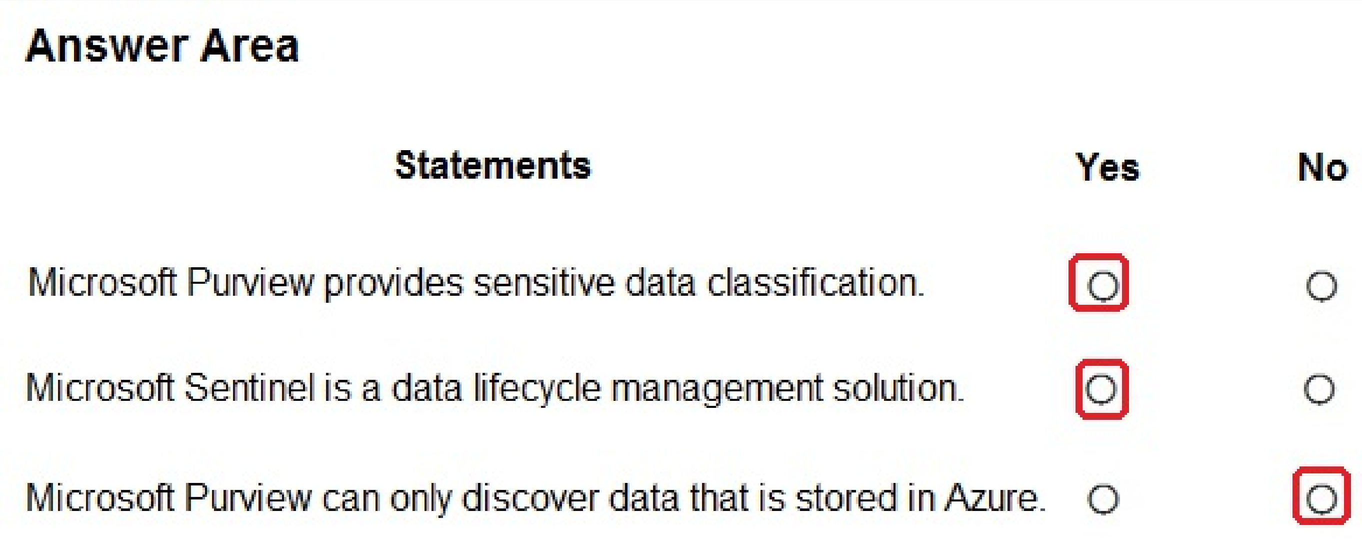
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Microsoft Purview provides sensitive data classification.	○	○
Microsoft Sentinel is a data lifecycle management solution.	○	○
Microsoft Purview can only discover data that is stored in Azure.	○	○

Answer:



Answer Area

Statements	Yes	No
Microsoft Purview provides sensitive data classification.	[✓ ○]	○
Microsoft Sentinel is a data lifecycle management solution.	[✓ ○]	○
Microsoft Purview can only discover data that is stored in Azure.	○	[✓ ○]

Explanation:

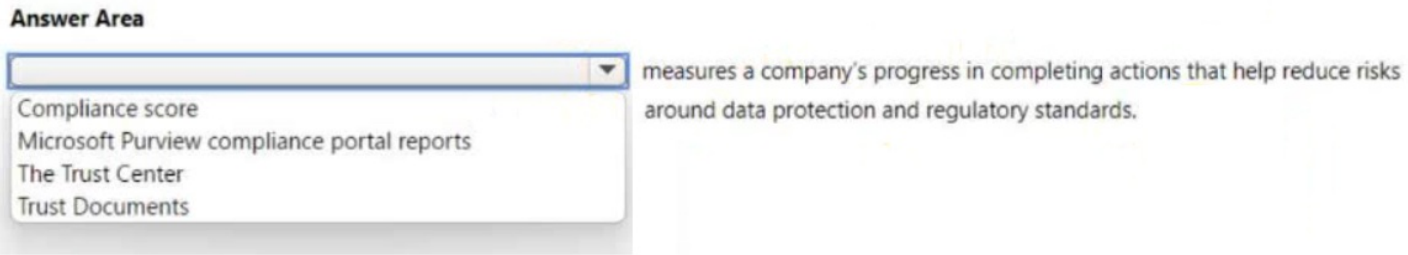
Microsoft Purview Data Lifecycle Management was formerly named Microsoft Information Governance. It helps organizations manage their risk through discovering, classifying, labeling, and governing their data. NOT Sentinel

Question: 157

HOTSPOT

-

Select the answer that correctly completes the sentence.

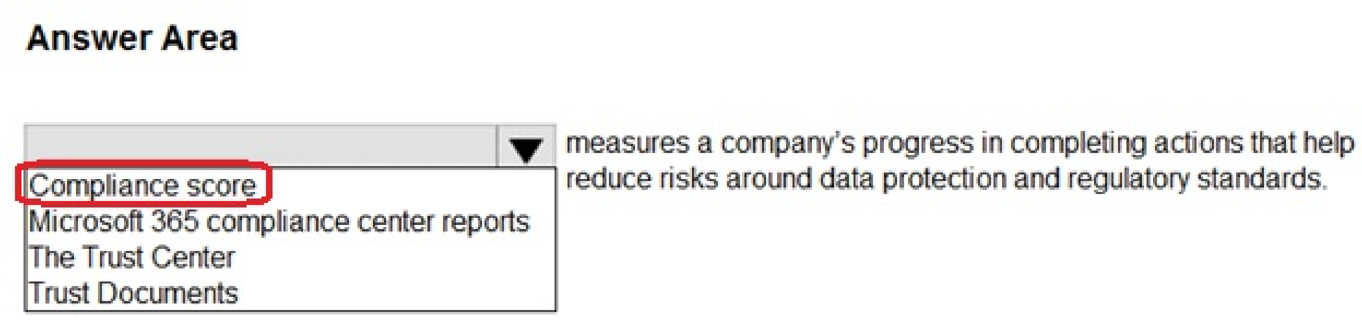


Answer Area

[▼] measures a company's progress in completing actions that help reduce risks around data protection and regulatory standards.

- Compliance score
- Microsoft Purview compliance portal reports
- The Trust Center
- Trust Documents

Answer:



Answer Area

[▼] measures a company's progress in completing actions that help reduce risks around data protection and regulatory standards.

- [✓ Compliance score]
- Microsoft 365 compliance center reports
- The Trust Center
- Trust Documents

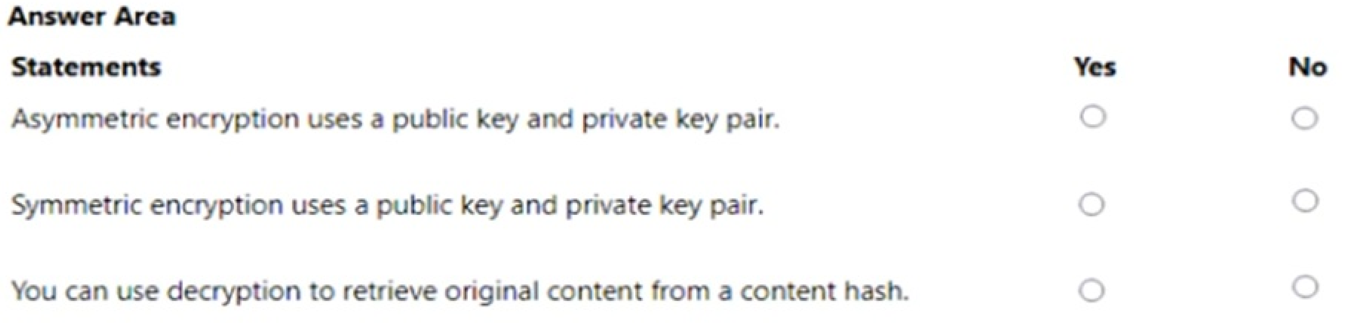
Question: 158 CertyIQ

HOTSPOT

-

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

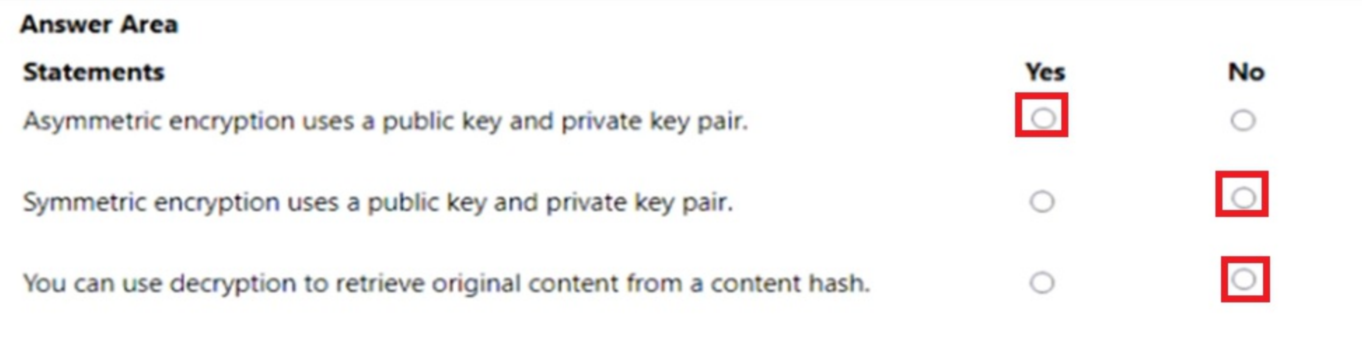
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Asymmetric encryption uses a public key and private key pair.	○	○
Symmetric encryption uses a public key and private key pair.	○	○
You can use decryption to retrieve original content from a content hash.	○	○

Answer:



Answer Area

Statements	Yes	No
Asymmetric encryption uses a public key and private key pair.	[✓ ○]	○
Symmetric encryption uses a public key and private key pair.	○	[✓ ○]
You can use decryption to retrieve original content from a content hash.	○	[✓ ○]

Explanation:

YNN is the answer.

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/5-describe-encryption-hashingHashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.

Question: 159

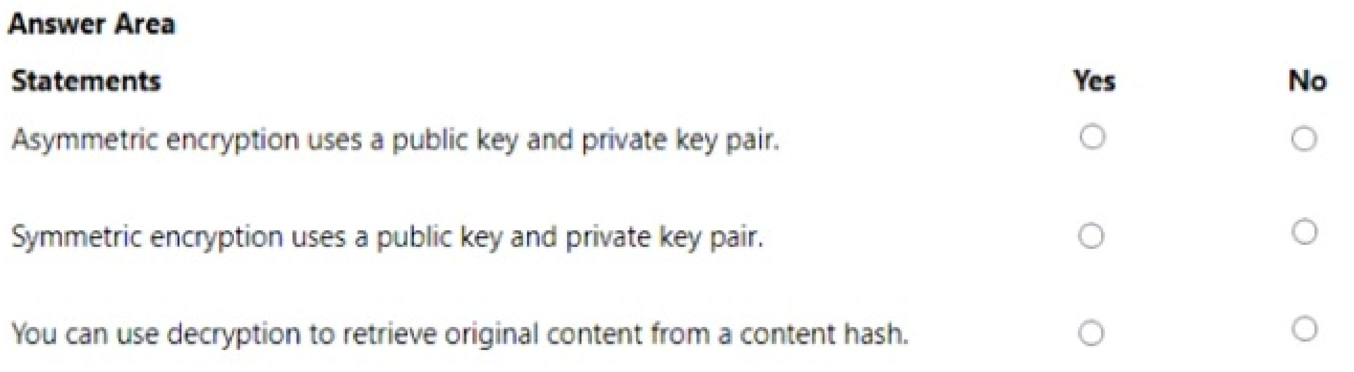
CertyIQ

HOTSPOT

-

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

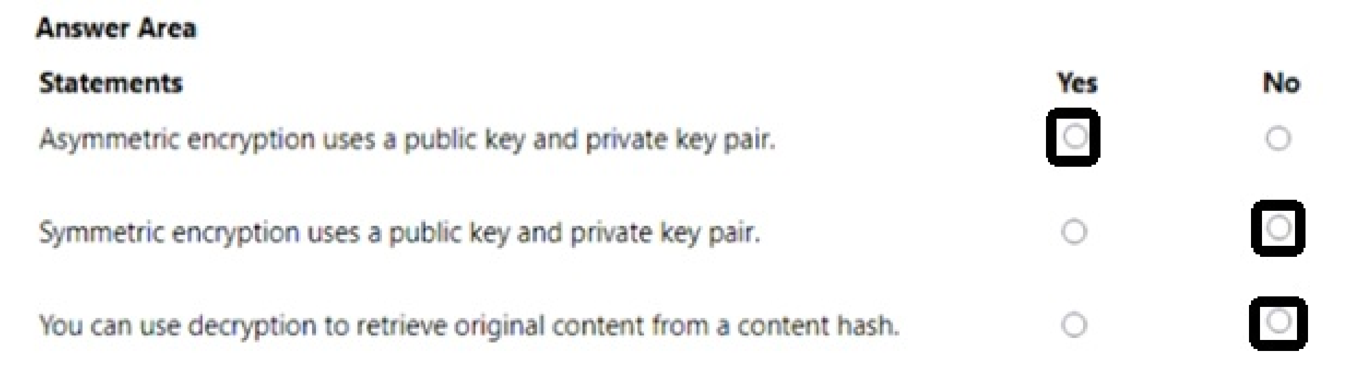
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Asymmetric encryption uses a public key and private key pair.	○	○
Symmetric encryption uses a public key and private key pair.	○	○
You can use decryption to retrieve original content from a content hash.	○	○

Answer:



Answer Area

Statements	Yes	No
Asymmetric encryption uses a public key and private key pair.	[✓ ○]	○
Symmetric encryption uses a public key and private key pair.	○	[✓ ○]
You can use decryption to retrieve original content from a content hash.	○	[✓ ○]

Explanation:

yes

no

no

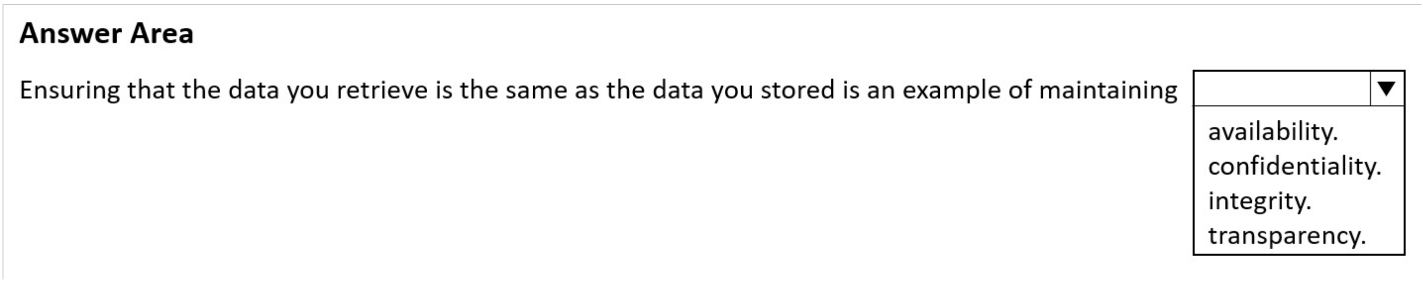
Question: 160

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

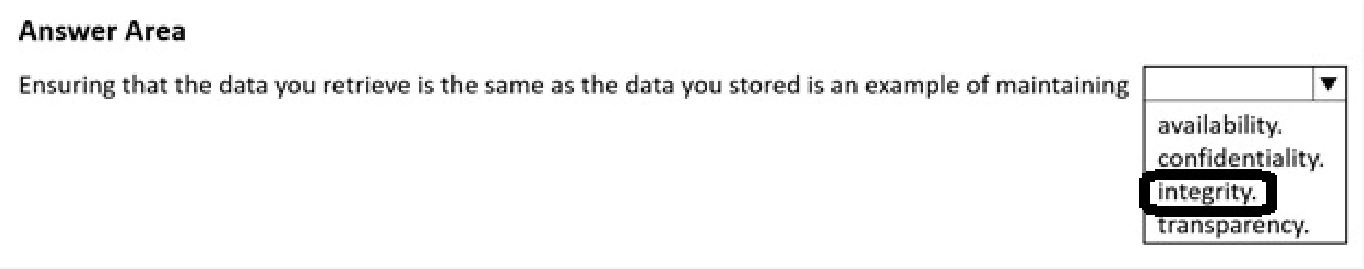


Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining ▼

availability.
confidentiality.
integrity.
transparency.

Answer:



Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining ▼

availability.
confidentiality.
[✓ integrity.]
transparency.

Explanation:

ensuring DATA is not altered....."Integrity"

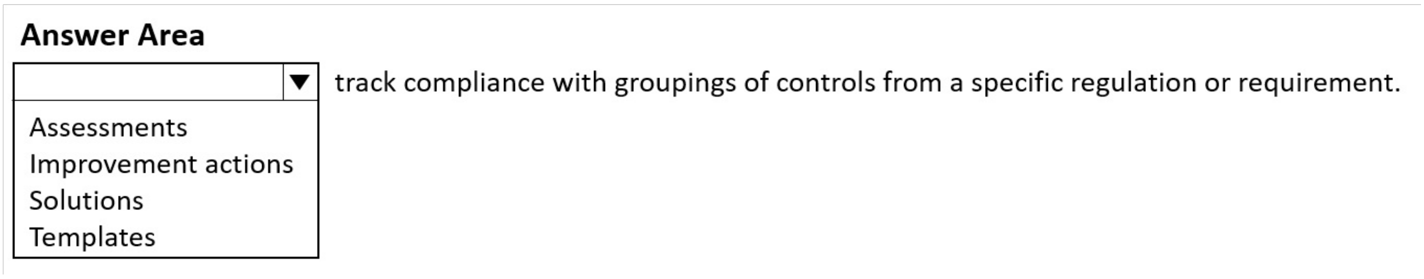
Question: 161

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

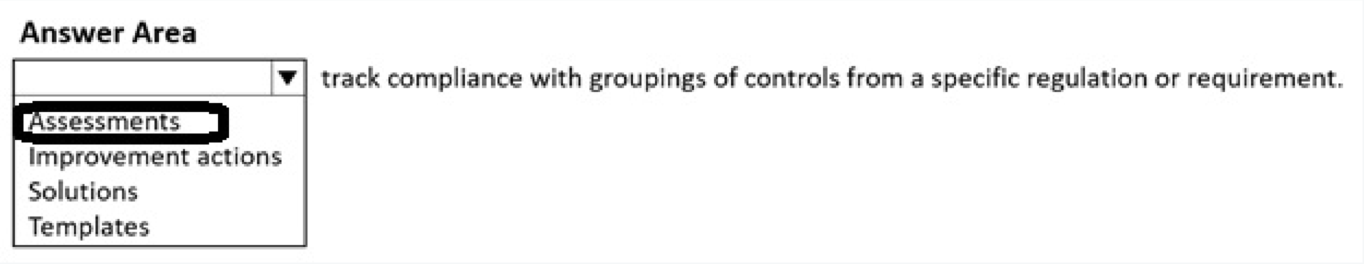


Answer Area

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

Assessments
Improvement actions
Solutions
Templates

Answer:



Answer Area

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

[✓ Assessments]
Improvement actions
Solutions
Templates

Question: 162

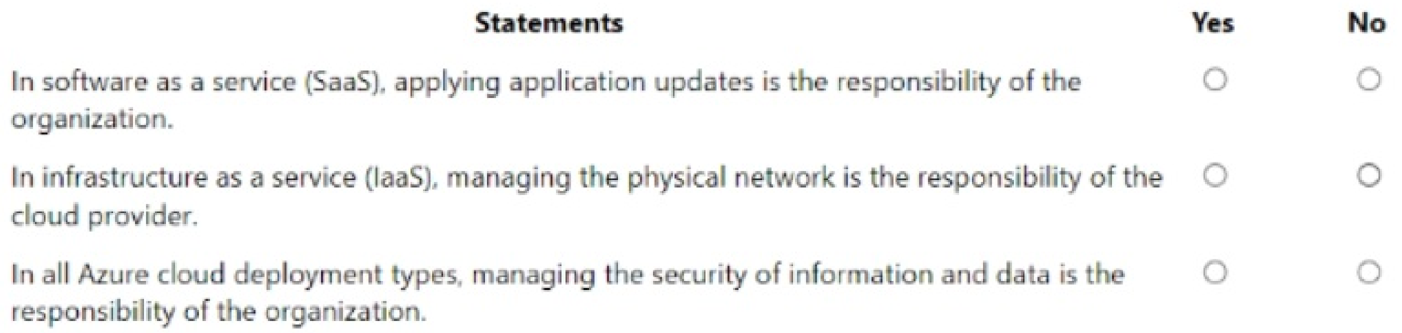
CertyIQ

HOTSPOT

-

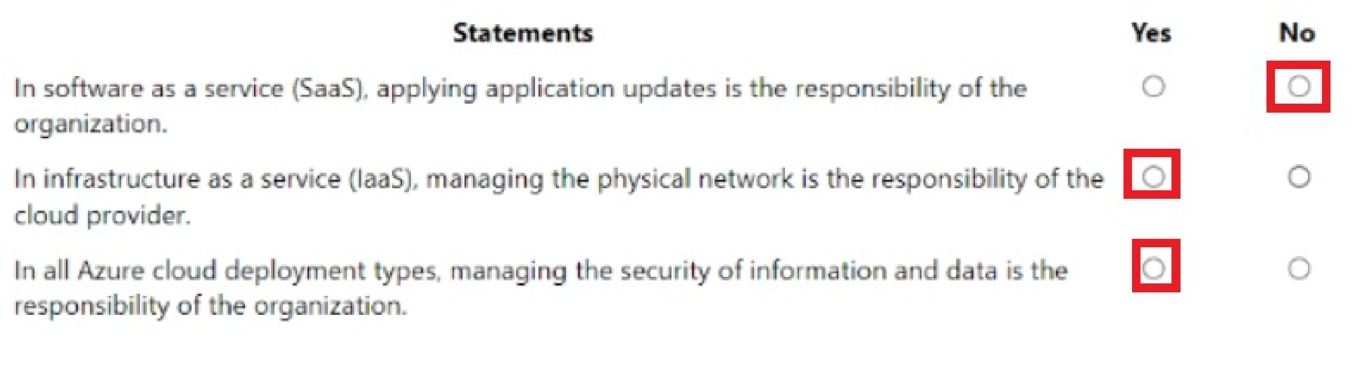
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



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

Answer:



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

Explanation:

NYY is the correct answer.

Question: 163 CertyIQ

What should you use to associate the same identity to more than one Azure virtual machine?

A.an Azure AD user account

B.a user-assigned managed identity

C.a system-assigned managed identity

D.an Azure AD security group

Answer: B

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-portal-windows-vmhttps://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-manage-user-assigned-managed-identities?pivots=identity-mi-methods-azp#manage-access-to-user-assigned-managed-identitieshttps://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-cli-windows-vm

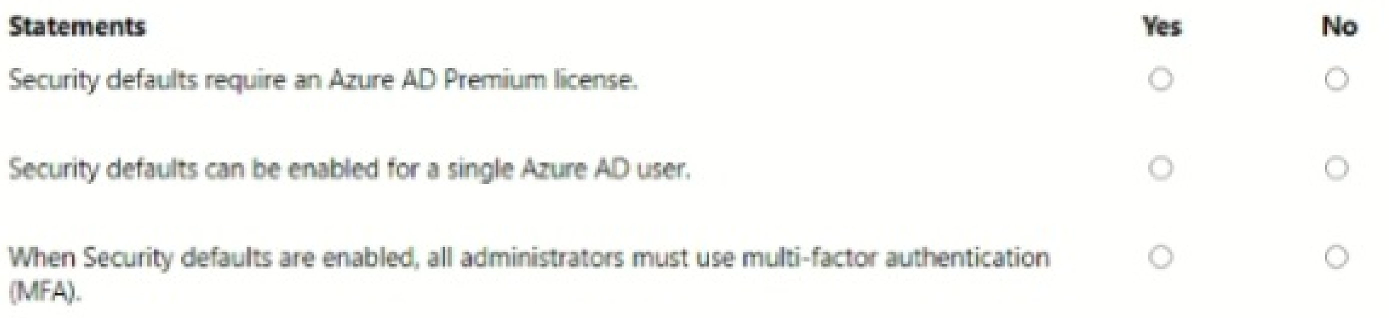
Question: 164 CertyIQ

HOTSPOT

-

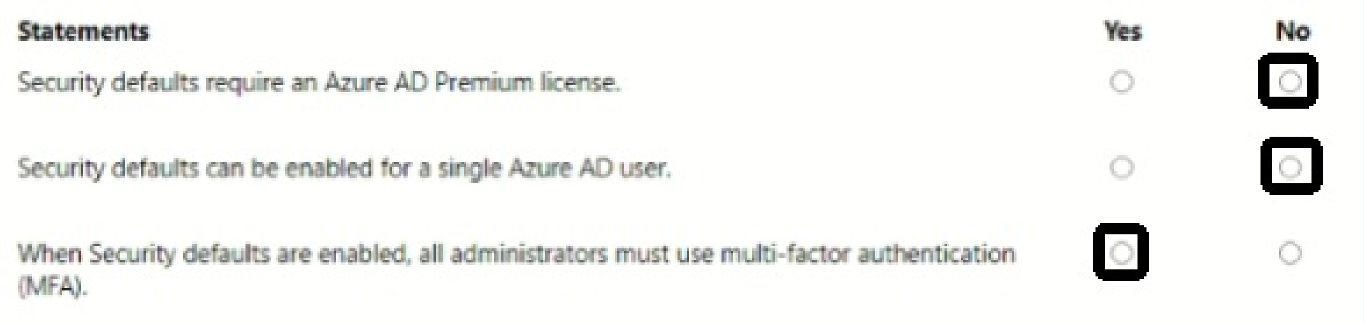
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



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

Answer:



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

Question: 165

Which three forms of verification can be used with Azure AD Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.

NOTE: Each correct answer is worth one point.

A.security questions

B.the Microsoft Authenticator app

C.SMS messages

D.a smart card

E.Windows Hello for Business

Answer: BCE

Explanation:

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

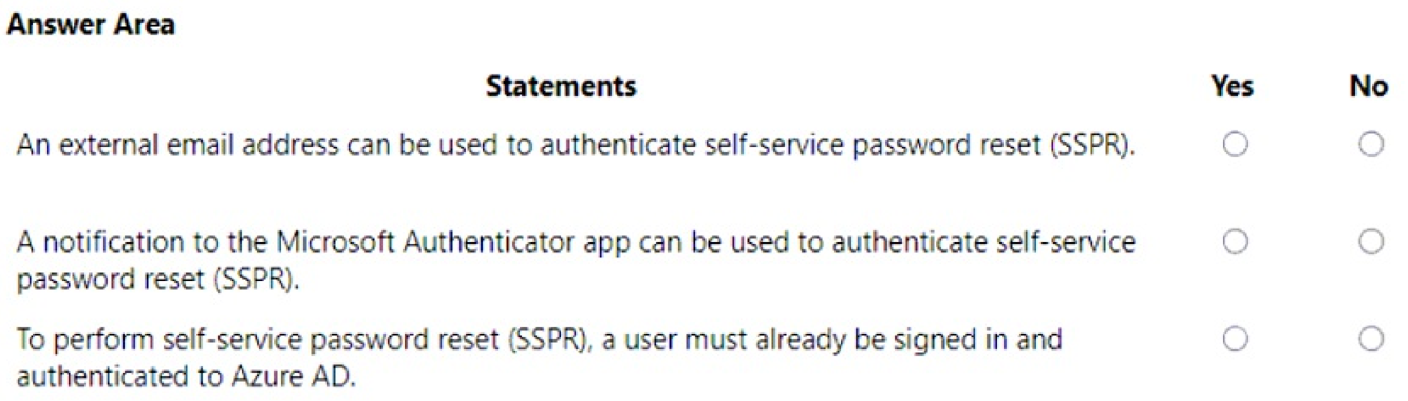
Question: 166

HOTSPOT

-

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

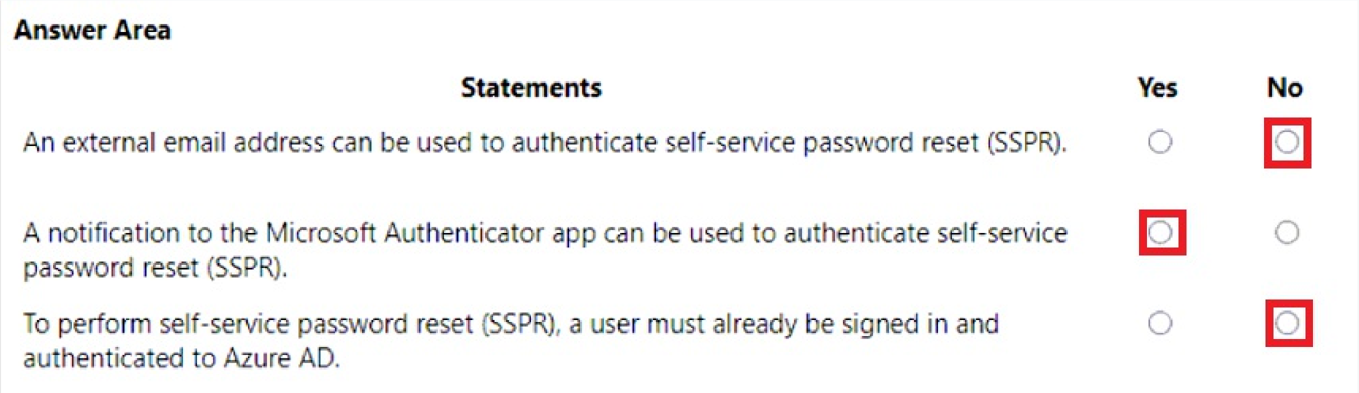
NOTE: Each correct selection is worth one point.



Answer 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:



Answer 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.	○	[✓ ○]

Explanation:

NO

because it only send by email an verification code to reset the password

Yes

NO

https://www.youtube.com/embed/rA8TvhNcCvQ?azure-portal=true

Question: 167 CertyIQ

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

A.Windows 10 and newer only

B.Windows 10 and newer and Android only

C.Windows 10 and newer and macOS only

D.Windows 10 and newer, Android, and macOS

Answer: C

Explanation:

Windows 10 and newer and macOS only.

Question: 168 CertyIQ

You have an Azure subscription that contains a Log Analytics workspace.

You need to onboard Microsoft Sentinel.

What should you do first?

A.Create a hunting query.
B.Correlate alerts into incidents.
C.Connect to your security sources.
D.Create a custom detection rule.

Answer: C

Explanation:

Connect to your security sources.

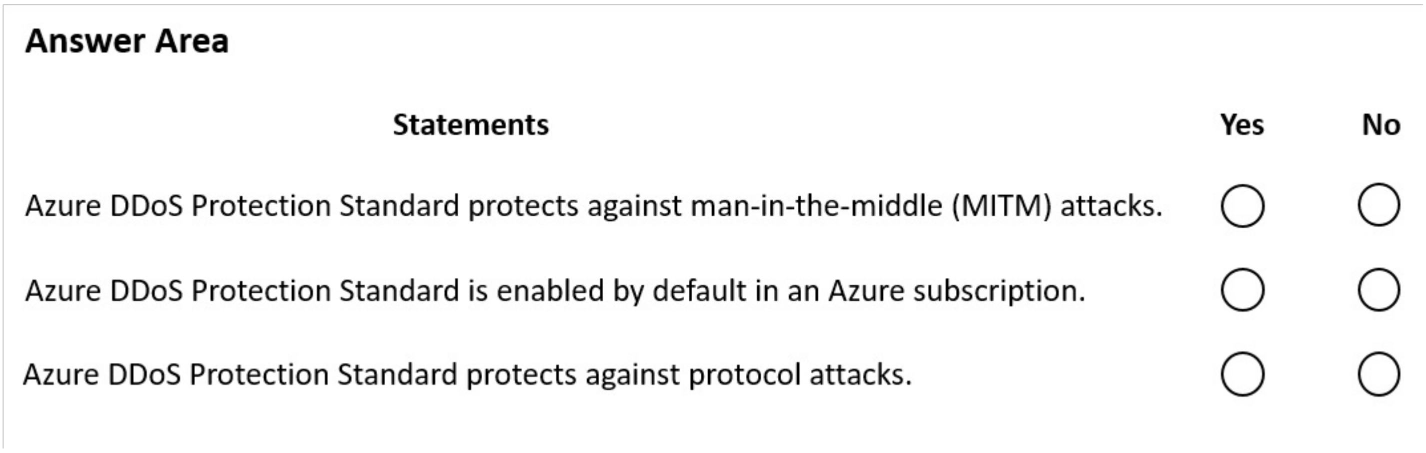
https://learn.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture

Question: 169 CertyIQ

HOTSPOT
-

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

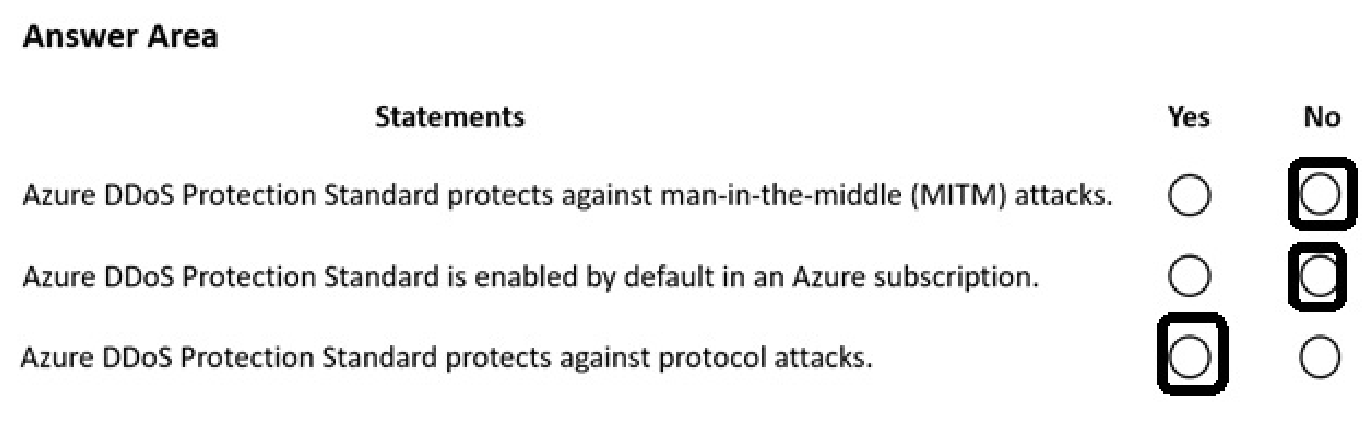
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	○	○
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	○	○
Azure DDoS Protection Standard protects against protocol attacks.	○	○

Answer:



Answer Area

Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	○	[✓ ○]
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	○	[✓ ○]
Azure DDoS Protection Standard protects against protocol attacks.	[✓ ○]	○

Explanation:

https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overviewhttps://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-features

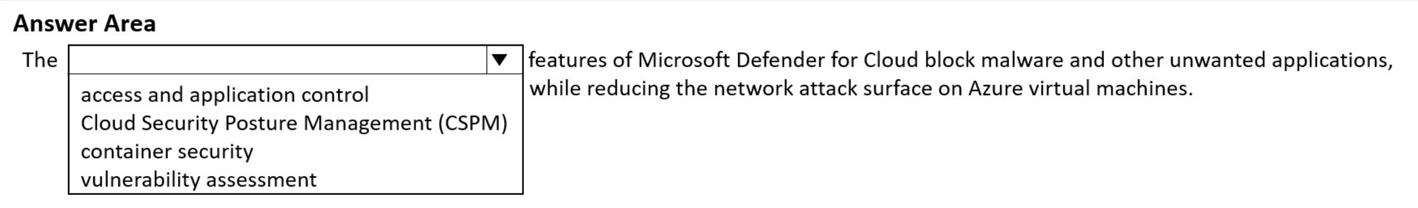
Question: 170

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

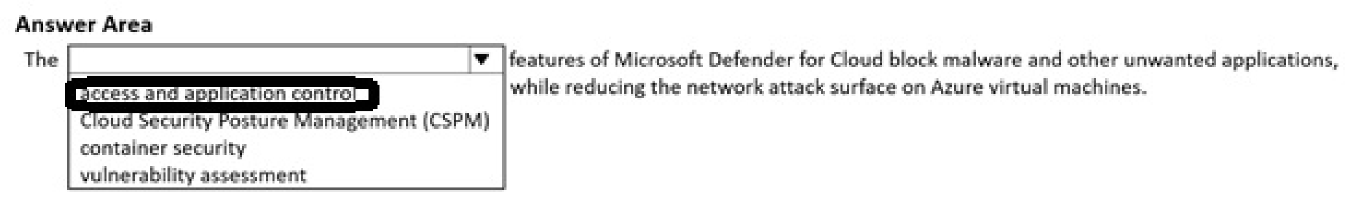


Answer Area

The ▼ features of Microsoft Defender for Cloud block malware and other unwanted applications, while reducing the network attack surface on Azure virtual machines.

- access and application control
- Cloud Security Posture Management (CSPM)
- container security
- vulnerability assessment

Answer:



Answer Area

The ▼ features of Microsoft Defender for Cloud block malware and other unwanted applications, while reducing the network attack surface on Azure virtual machines.

- [✓ access and application control]
- Cloud Security Posture Management (CSPM)
- container security
- vulnerability assessment

Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-appshttps://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controlshttps://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad

Question: 171

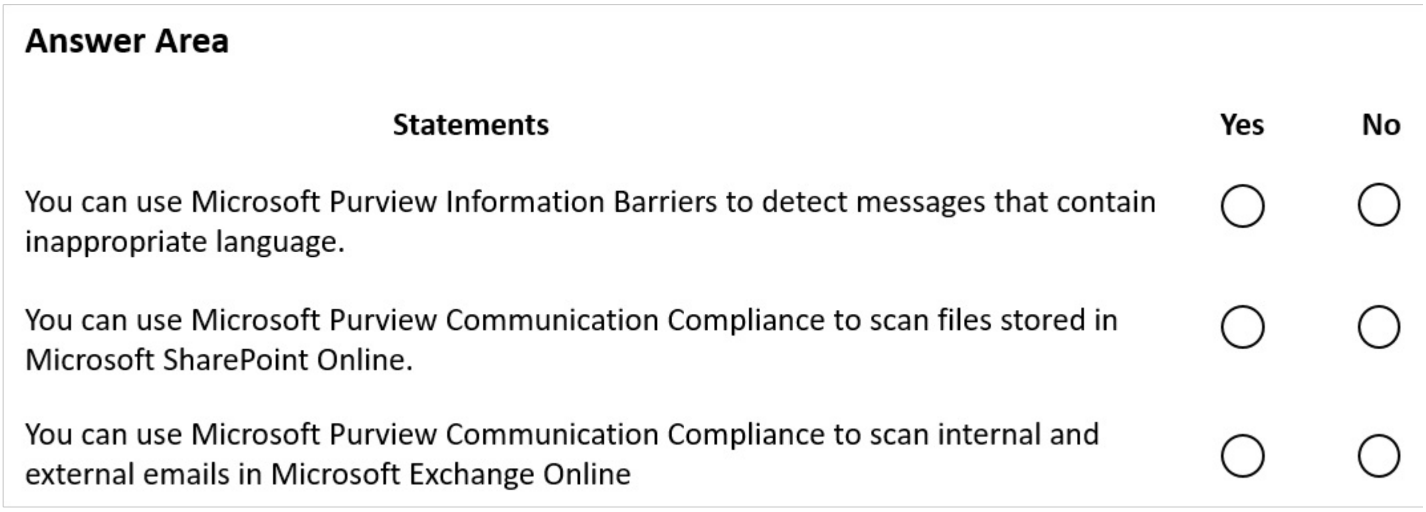
CertyIQ

HOTSPOT

-

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

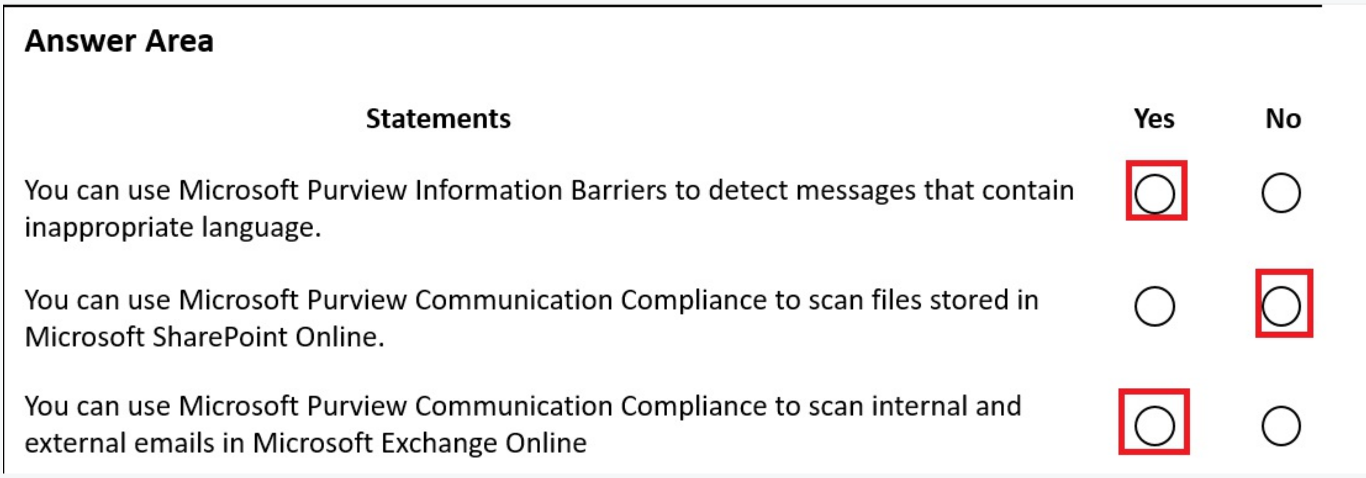
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
You can use Microsoft Purview Information Barriers to detect messages that contain inappropriate language.	○	○
You can use Microsoft Purview Communication Compliance to scan files stored in Microsoft SharePoint Online.	○	○
You can use Microsoft Purview Communication Compliance to scan internal and external emails in Microsoft Exchange Online	○	○

Answer:



Answer Area

Statements	Yes	No
You can use Microsoft Purview Information Barriers to detect messages that contain inappropriate language.	[✓ ○]	○
You can use Microsoft Purview Communication Compliance to scan files stored in Microsoft SharePoint Online.	○	[✓ ○]
You can use Microsoft Purview Communication Compliance to scan internal and external emails in Microsoft Exchange Online	[✓ ○]	○

Explanation:

YNY

https://learn.microsoft.com/en-us/microsoft-365/compliance/communication-compliance-policies?view=o365-worldwide

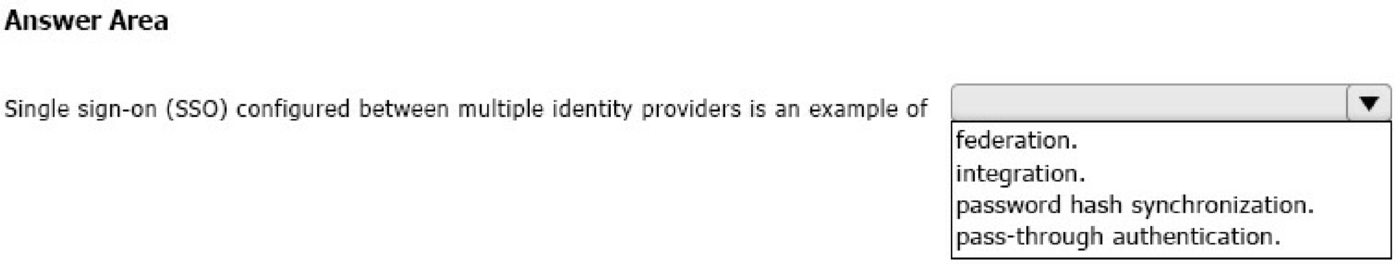
Question: 172

CertyIQ

HOTSPOT

-

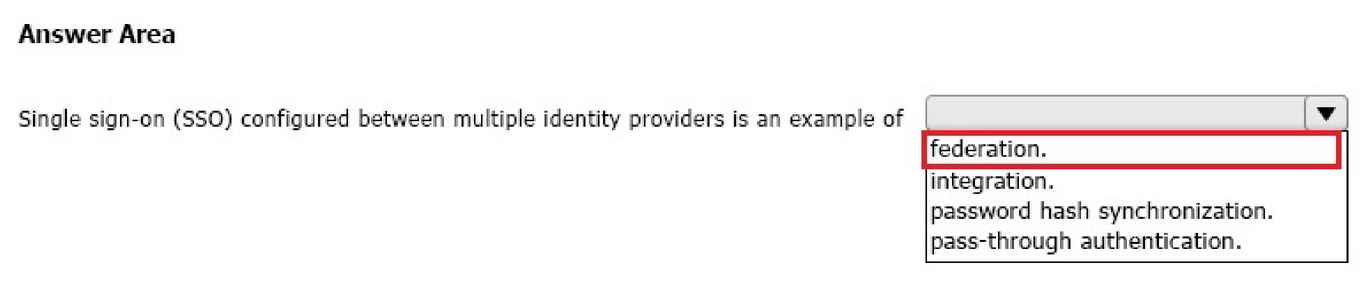
Select the answer that correctly completes the sentence.



Answer Area

Single sign-on (SSO) configured between multiple identity providers is an example of

Answer:



Answer Area

Single sign-on (SSO) configured between multiple identity providers is an example of

- federation.
- integration.
- password hash synchronization.
- pass-through authentication.

Explanation:

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

Question: 173

CertyIQ

You plan to move resources to the cloud.

You are evaluating the use of Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) cloud models.

You plan to manage only the data, user accounts, and user devices for a cloud-based app.

Which cloud model will you use?

A.SaaS

B.PaaS

C.IaaS

Answer: A

Explanation:

A is correcthttps://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibilityResponsibility always retained by the customer:- Information and Data- Devices (Mobile and PCs)- Accounts and Identities

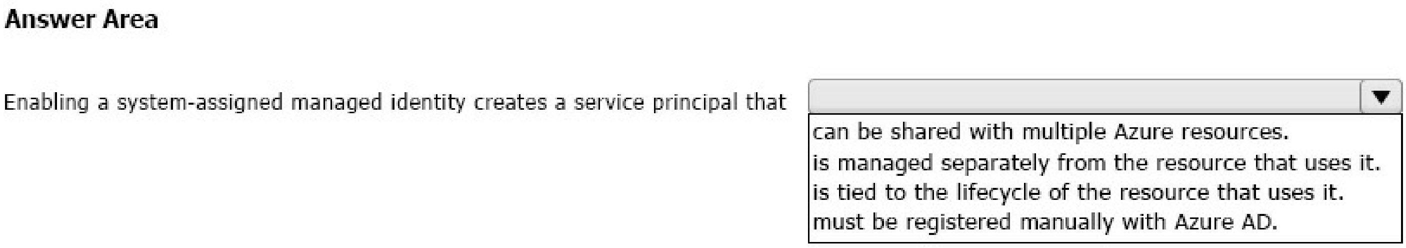
Question: 174

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

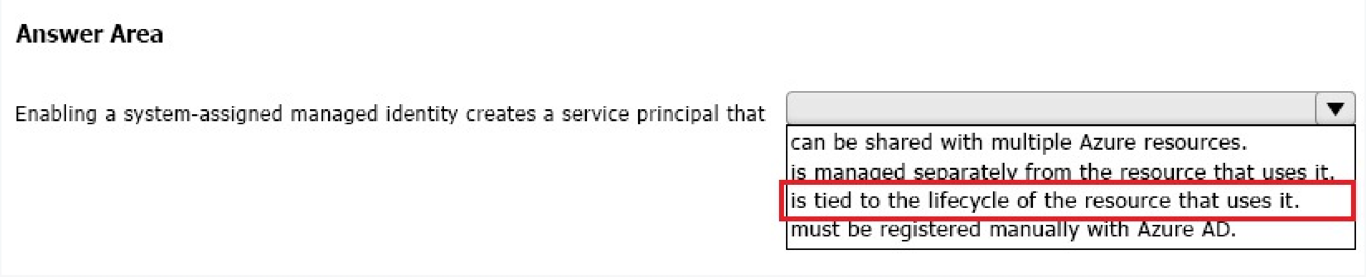


Answer Area

Enabling a system-assigned managed identity creates a service principal that

- can be shared with multiple Azure resources.
- is managed separately from the resource that uses it.
- is tied to the lifecycle of the resource that uses it.
- must be registered manually with Azure AD.

Answer:



Answer Area

Enabling a system-assigned managed identity creates a service principal that

- can be shared with multiple Azure resources.
- is managed separately from the resource that uses it.
- [✓ is tied to the lifecycle of the resource that uses it.]
- must be registered manually with Azure AD.

Question: 175

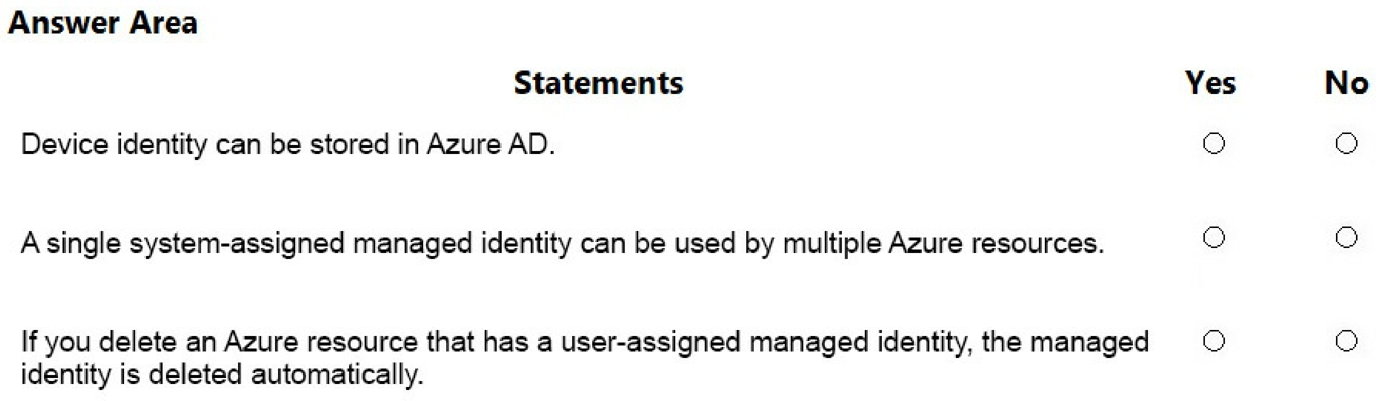
CertyIQ

HOTSPOT

-

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

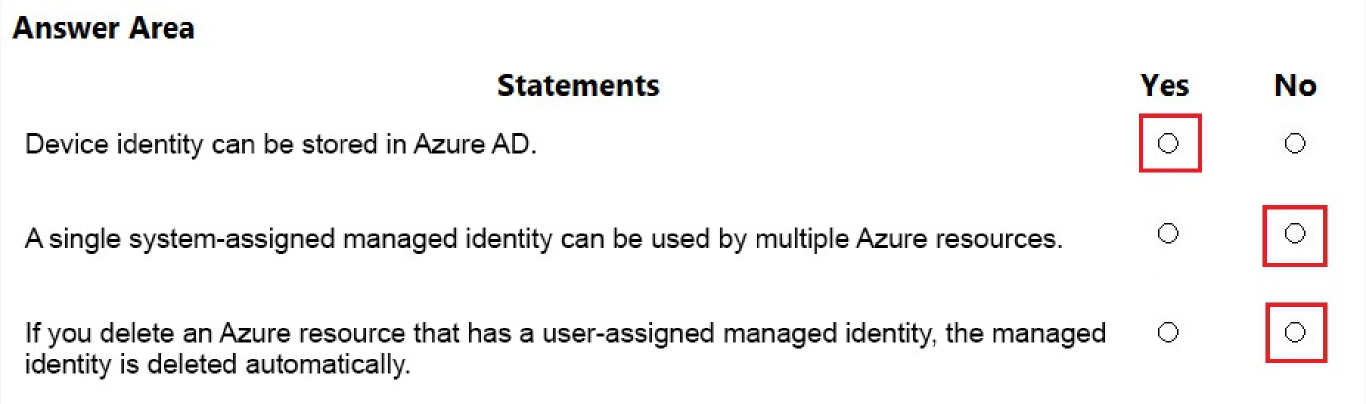
NOTE: Each correct selection is worth one point.



Answer Area

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

Answer:



Answer Area

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

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question: 176

CertyIQ

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

A.Adoption Score

B.Microsoft Secure Score

C.Secure score in Microsoft Defender for Cloud

D.Compliance score

Answer: D

Explanation:

Answer is correct

https://learn.microsoft.com/en-us/purview/compliance-score-calculation

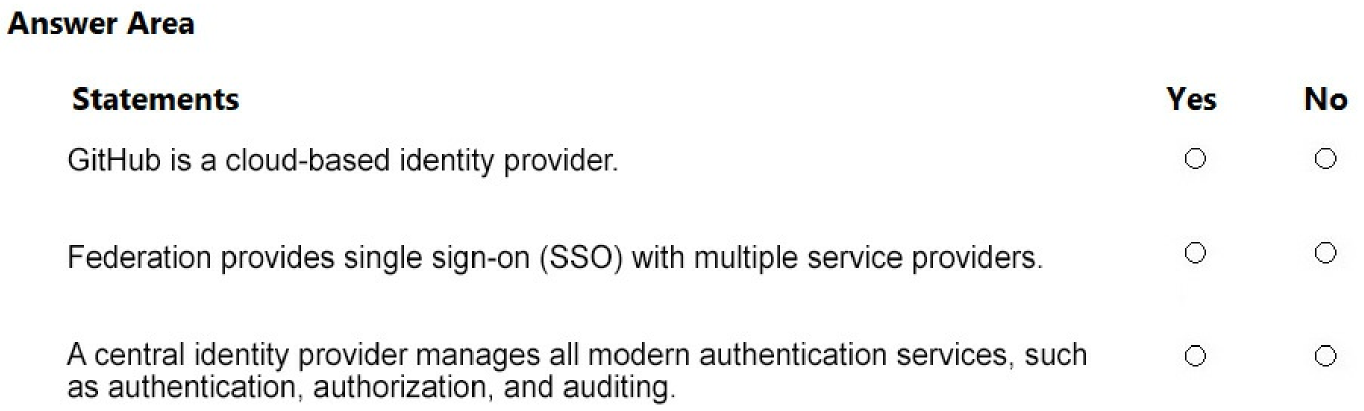
Question: 177

HOTSPOT

-

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

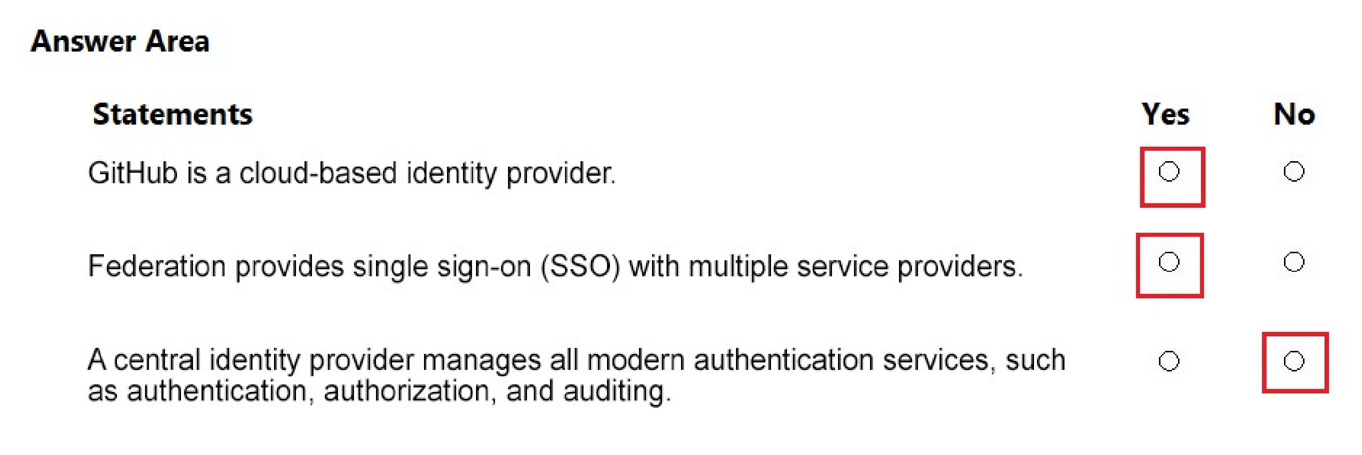
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	○	○
Federation provides single sign-on (SSO) with multiple service providers.	○	○
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	○	○

Answer:



Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	[✓ ○]	○
Federation provides single sign-on (SSO) with multiple service providers.	[✓ ○]	○
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	○	[✓ ○]

Explanation:

YYN. Git Hub can be used as Identity Provider.

Question: 178

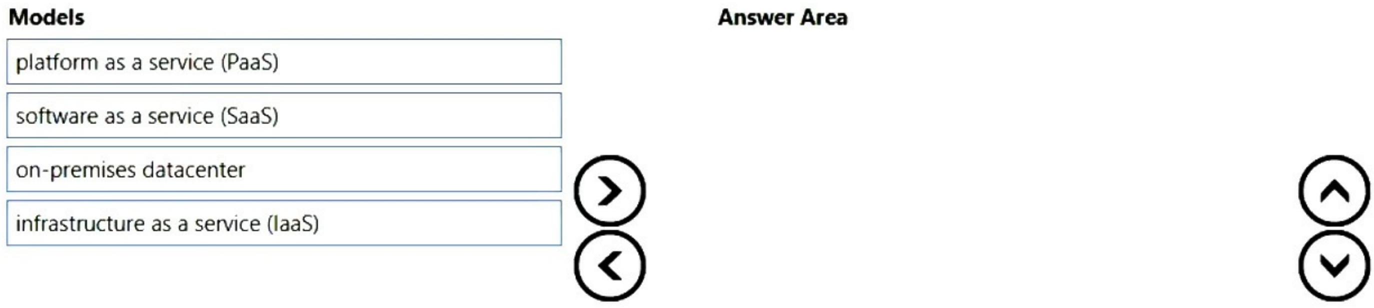
CertyIQ

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 to the least? To answer, move all models from the list of models to the answer area and arrange them in the correct order.

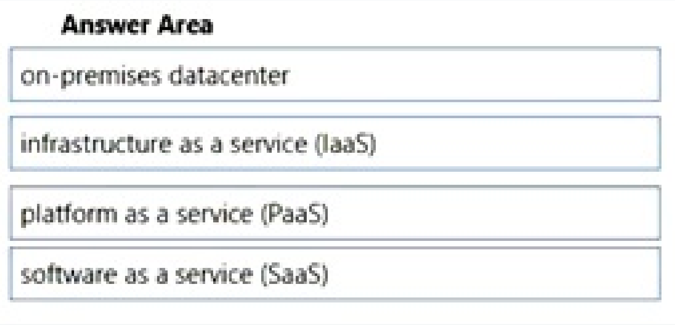


Models

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

Answer Area

Answer:



Answer Area

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

Explanation:

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

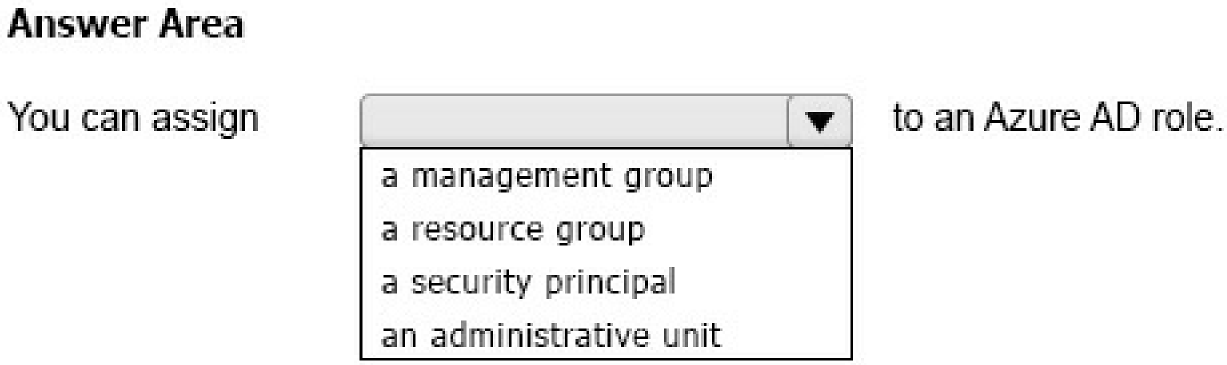
Question: 179

CertyIQ

HOTSPOT

-

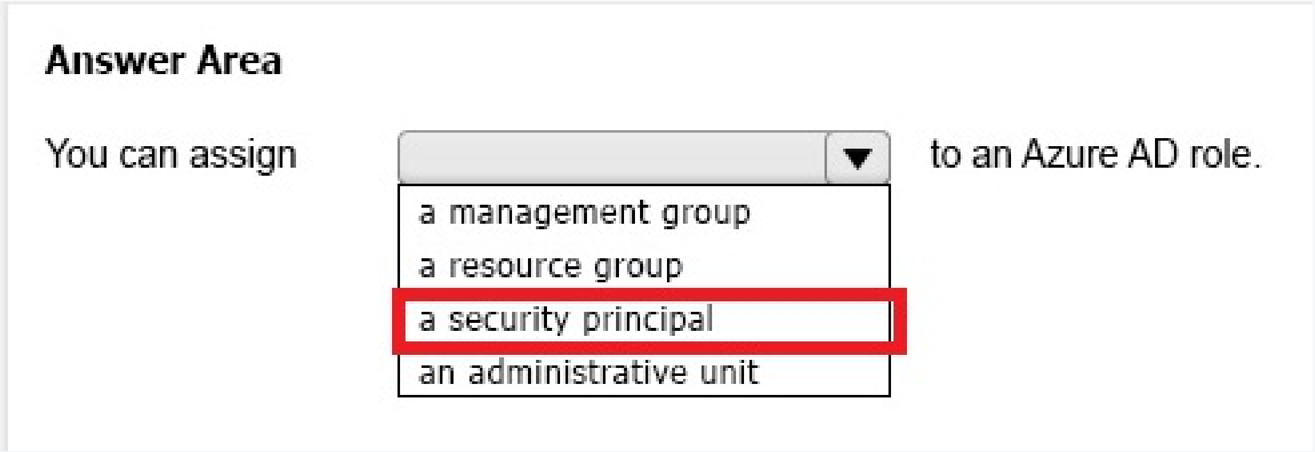
Select the answer that correctly completes the sentence.



Answer Area

You can assign [▼] to an Azure AD role.

Answer:



Answer Area

You can assign [▼] to an Azure AD role.

- a management group
- a resource group
- a security principal
- an administrative unit

Explanation:

Security Principal should be the correct answer.

https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Question: 180 CertyIQ

You have an Azure subscription.

You need to implement approval-based, time-bound role activation.

What should you use?

A.access reviews in Azure AD
B.Azure AD Privileged Identity Management (PIM)
C.Azure AD Identity Protection
D.Conditional access in Azure AD

Answer: B

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 181 CertyIQ

What should you use in the Microsoft 365 Defender portal to view security trends and track the protection status of identities?

A.Reports
B.Incidents
C.Hunting
D.Secure score

Answer: A

Explanation:

A is correct Keywords = trends and track = Reports

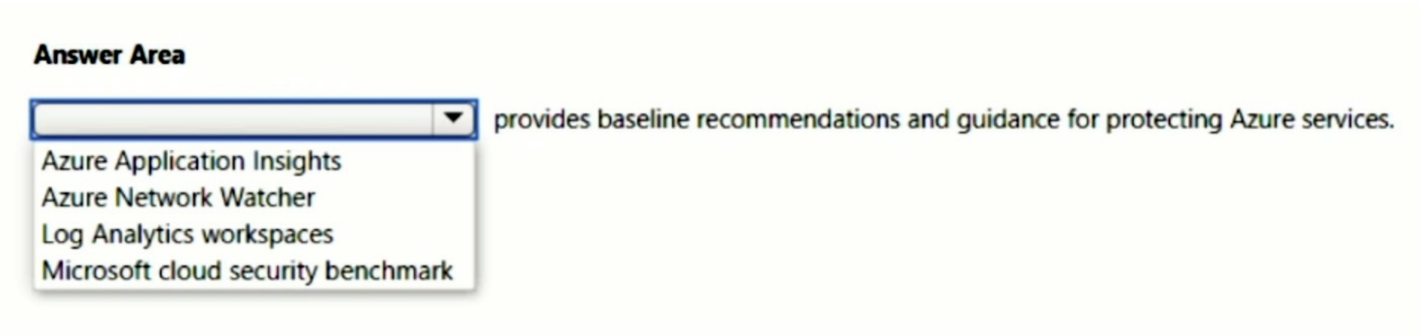
Question: 182

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

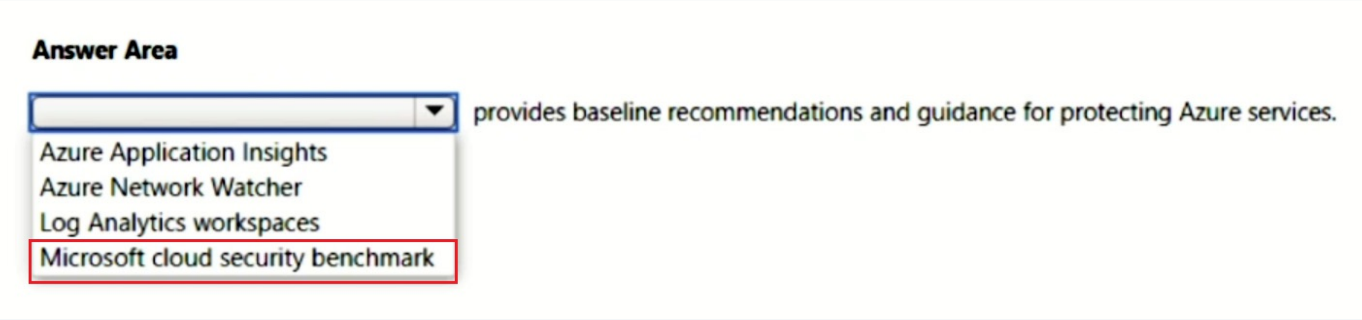


Answer Area

[▼] provides baseline recommendations and guidance for protecting Azure services.

Azure Application Insights
Azure Network Watcher
Log Analytics workspaces
Microsoft cloud security benchmark

Answer:



Answer Area

[▼] provides baseline recommendations and guidance for protecting Azure services.

Azure Application Insights
Azure Network Watcher
Log Analytics workspaces
Microsoft cloud security benchmark

Explanation:

https://learn.microsoft.com/en-us/security/benchmark/azure/overview

Question: 183

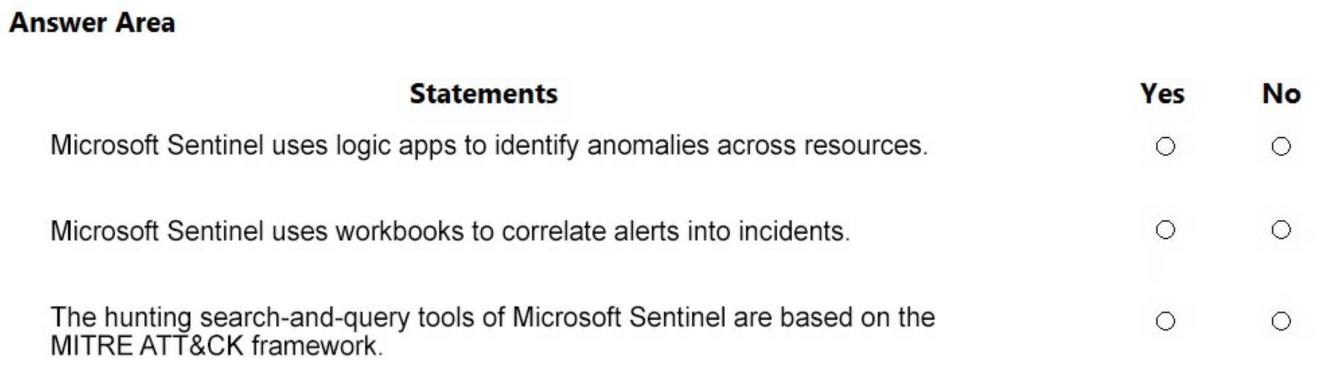
CertyIQ

HOTSPOT

-

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

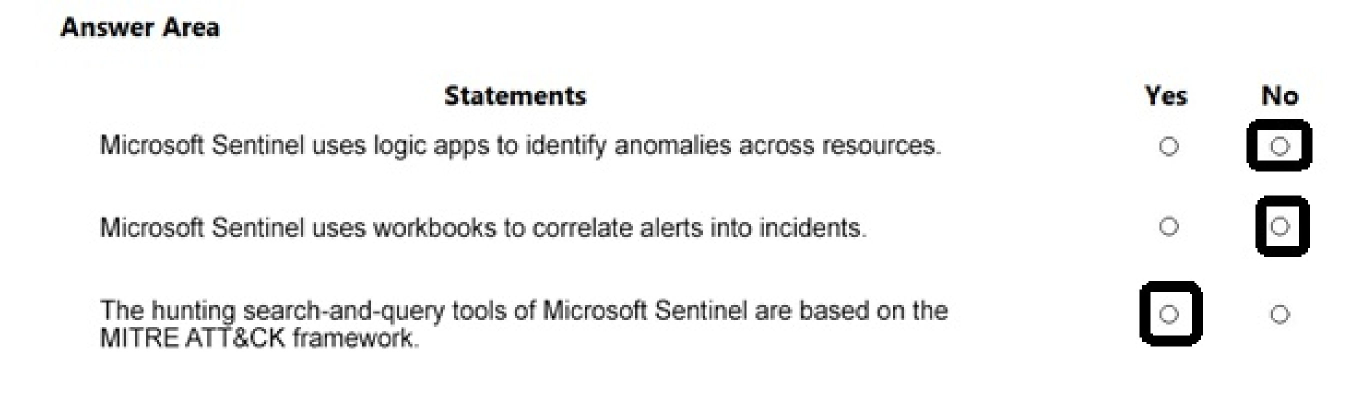
NOTE: Each correct selection is worth one point.



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:



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.	[✓ ○]	○

Explanation:

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

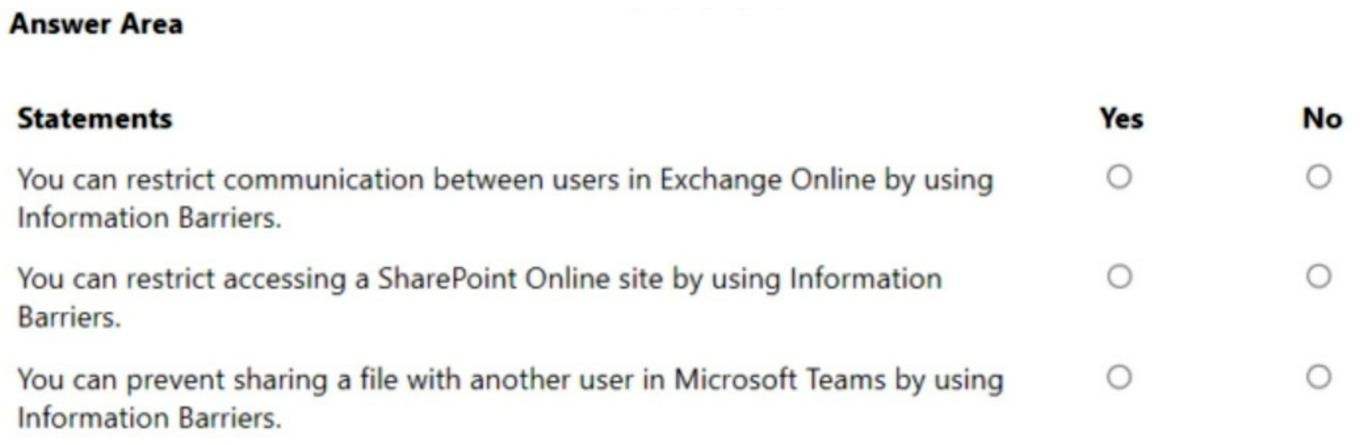
Question: 184 CertyIQ

HOTSPOT

-

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

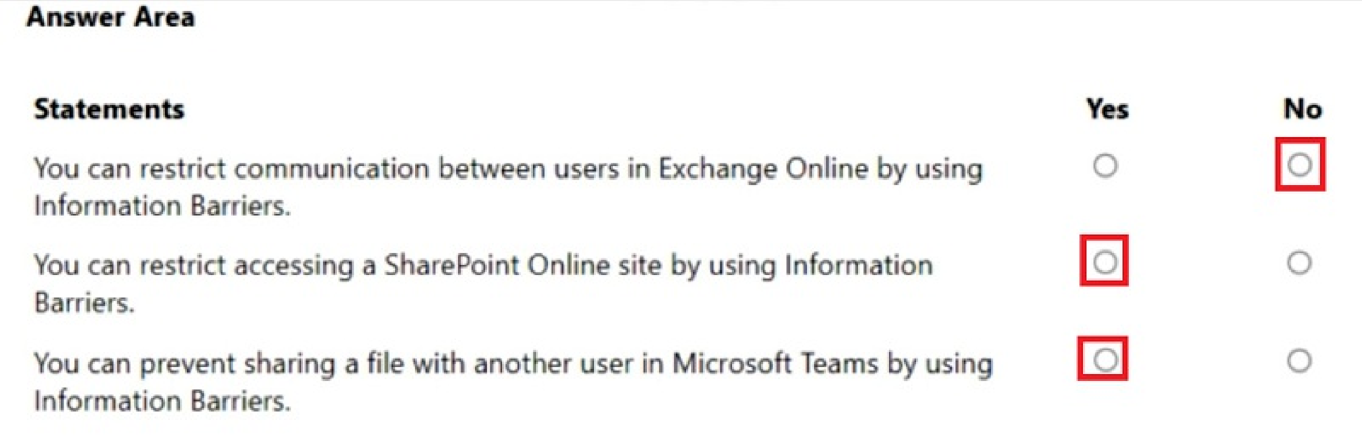
NOTE: Each correct selection is worth one point.



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:



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.	[✓ ○]	○

Explanation:

NYY You cannot restrict communication through Exchange/mail.

Question: 185 CertyIQ

Which portal contains the solution catalog?

A.Microsoft Purview compliance portal
B.Microsoft 365 Defender portal
C.Microsoft 365 admin center
D.Microsoft 365 Apps admin center

Answer: A

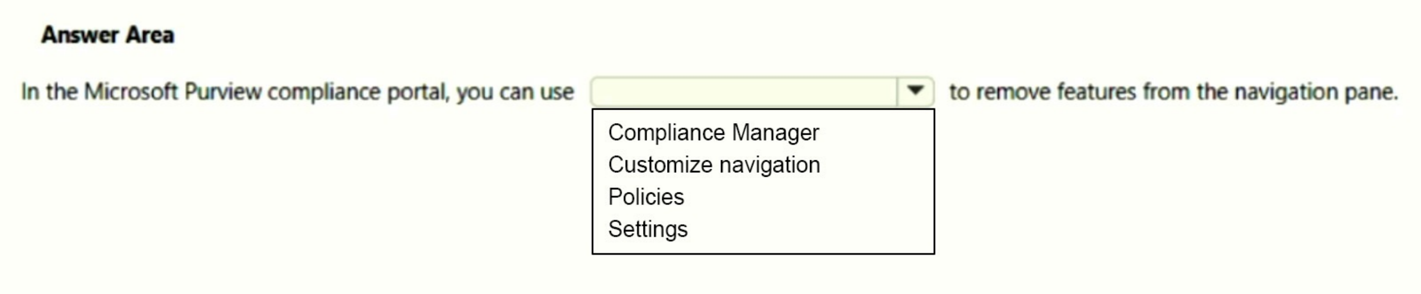
Explanation:

https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-solution-catalog?view=o365-worldwide

Question: 186 CertyIQ

HOTSPOT
-

Select the answer that correctly completes the sentence.

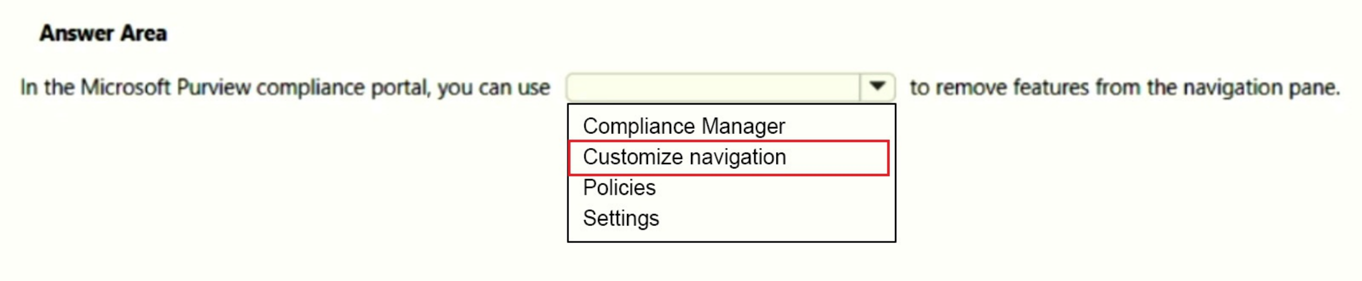


Answer Area

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

Compliance Manager
Customize navigation
Policies
Settings

Answer:



Answer Area

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

Compliance Manager
[✓ Customize navigation]
Policies
Settings

Explanation:

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

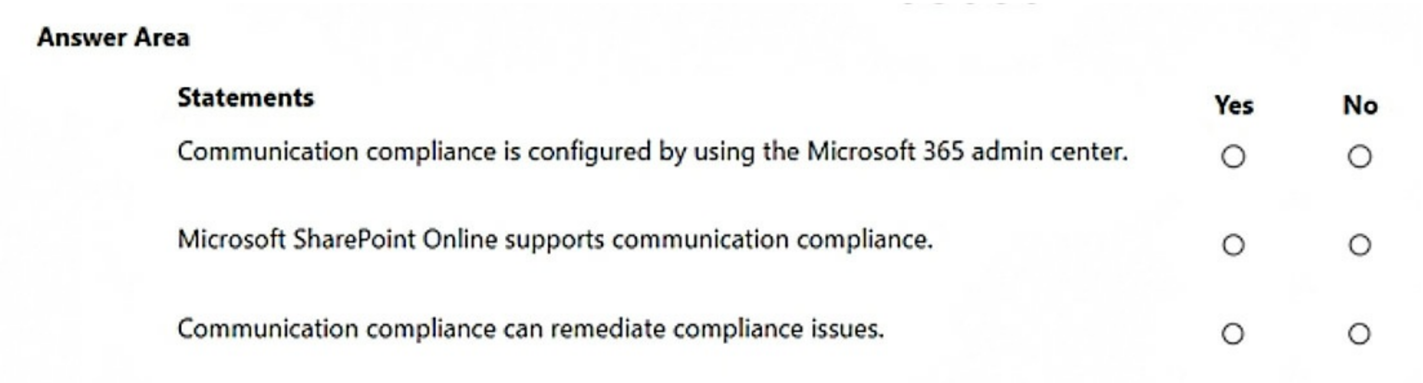
Question: 187 CertyIQ

HOTSPOT

-

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

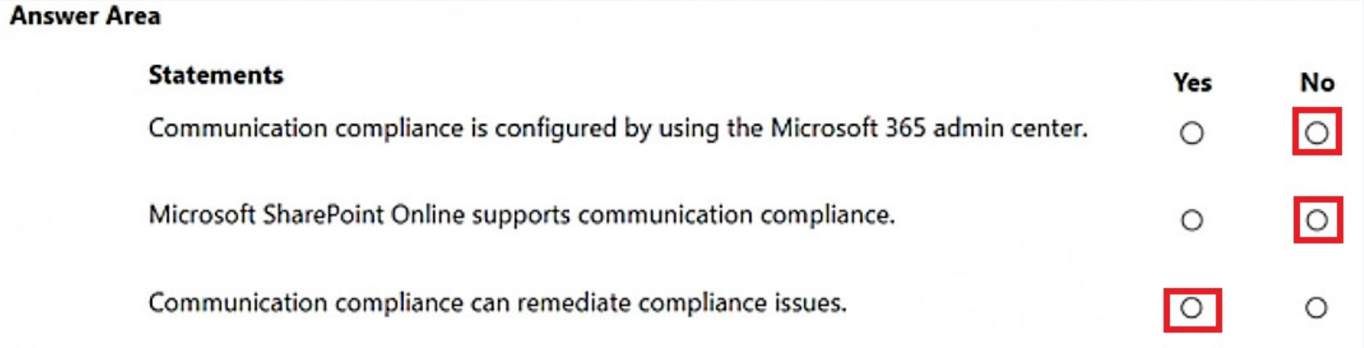
NOTE: Each correct selection is worth one point.



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:



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.	[✓ ○]	○

Explanation:

No

No

yes

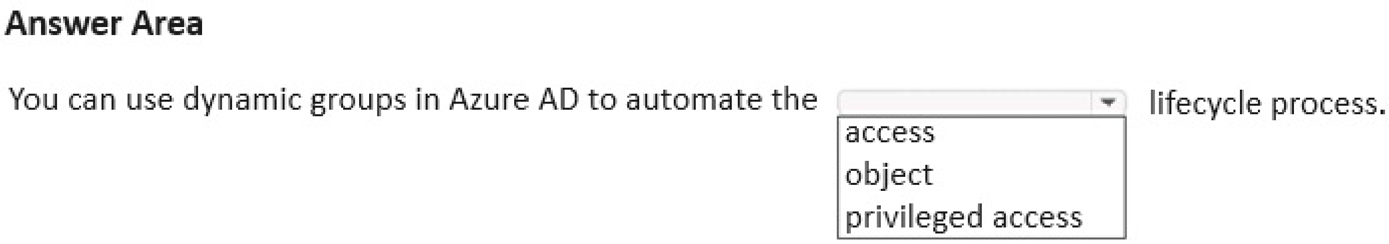
Question: 188

CertyIQ

HOTSPOT

-

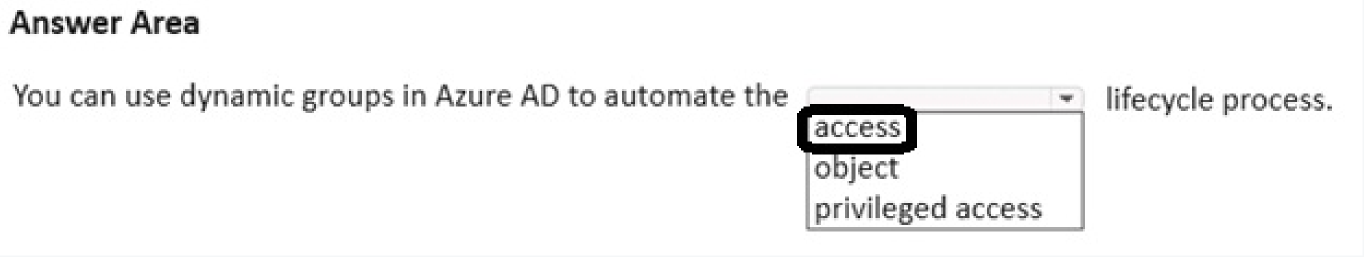
Select the answer that correctly completes the sentence.



Answer Area

You can use dynamic groups in Azure AD to automate the [▾] lifecycle process.

Answer:



Answer Area

You can use dynamic groups in Azure AD to automate the [✓ access] / object / privileged access lifecycle process.

Question: 189

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

A.1

B.2

C.3

D.4

Answer: B

Explanation:

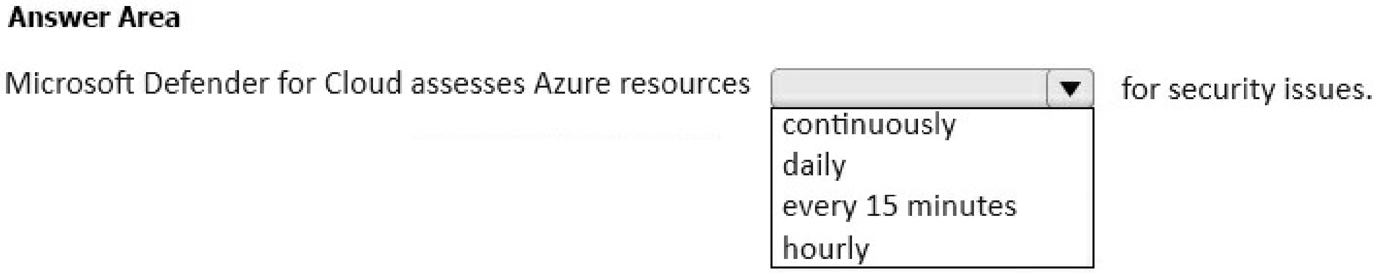
Correct answer is B:2.

Question: 190

HOTSPOT

-

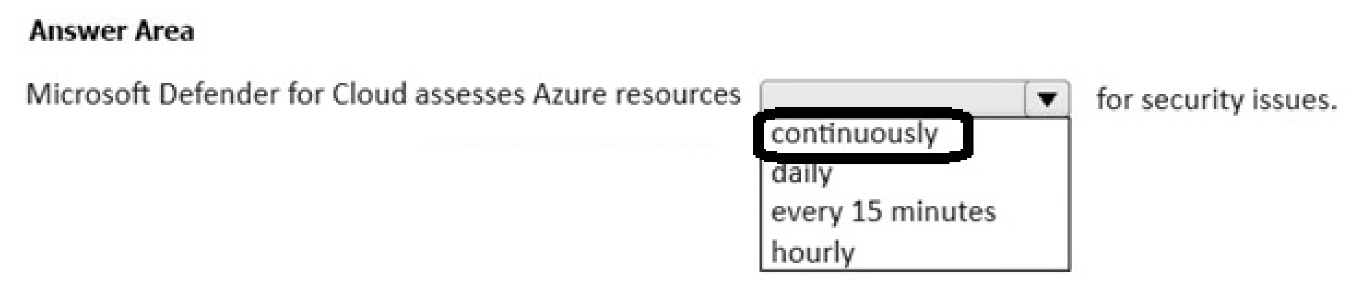
Select the answer that correctly completes the sentence.



Answer Area

Microsoft Defender for Cloud assesses Azure resources continuously / daily / every 15 minutes / hourly for security issues.

Answer:



Answer Area

Microsoft Defender for Cloud assesses Azure resources [✓ continuously] / daily / every 15 minutes / hourly for security issues.

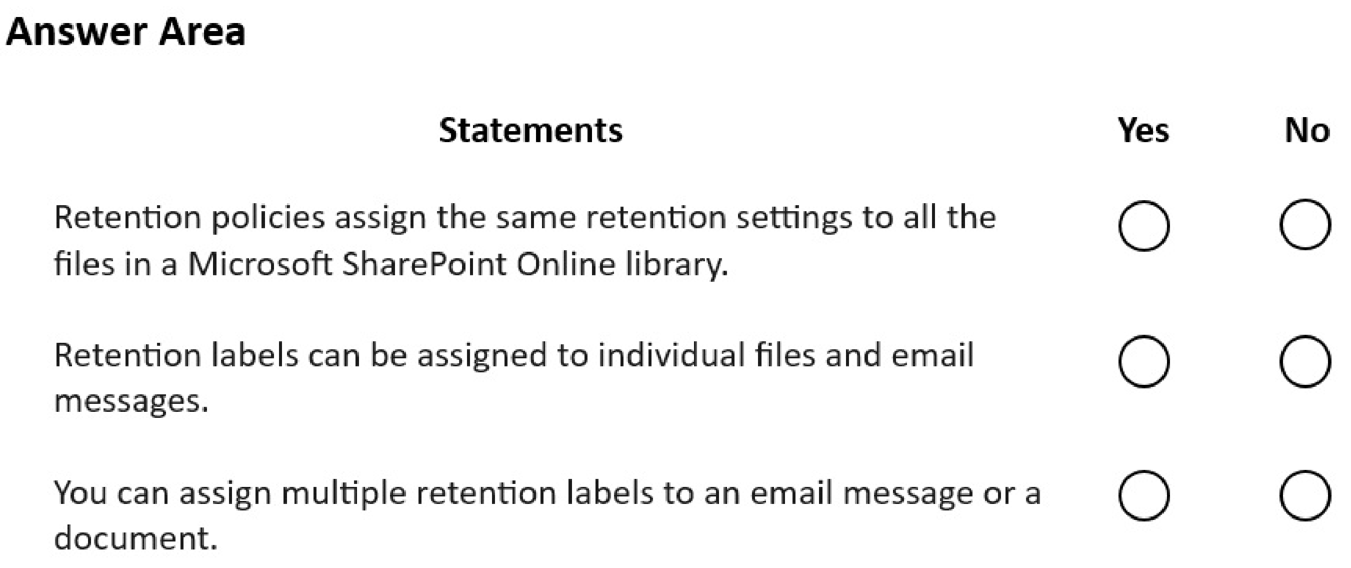
Question: 191

HOTSPOT

-

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

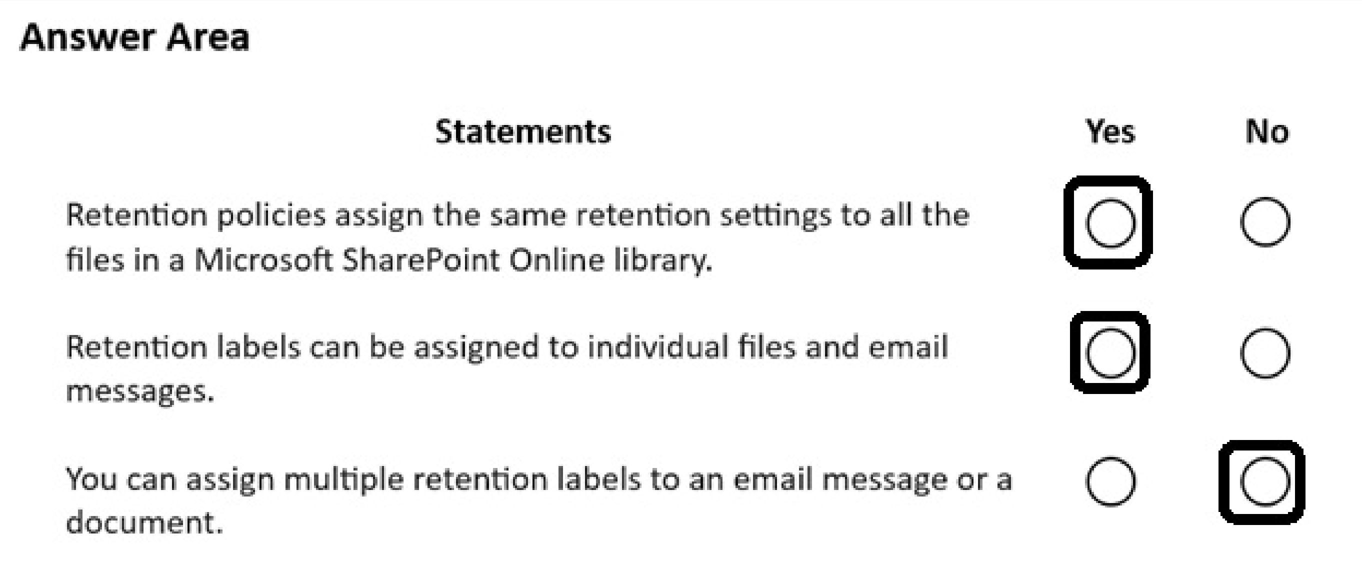
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Retention policies assign the same retention settings to all the files in a Microsoft SharePoint Online library.	○	○
Retention labels can be assigned to individual files and email messages.	○	○
You can assign multiple retention labels to an email message or a document.	○	○

Answer:



Answer Area

Statements	Yes	No
Retention policies assign the same retention settings to all the files in a Microsoft SharePoint Online library.	[✓ ○]	○
Retention labels can be assigned to individual files and email messages.	[✓ ○]	○
You can assign multiple retention labels to an email message or a document.	○	[✓ ○]

Explanation:

Yes

Yes

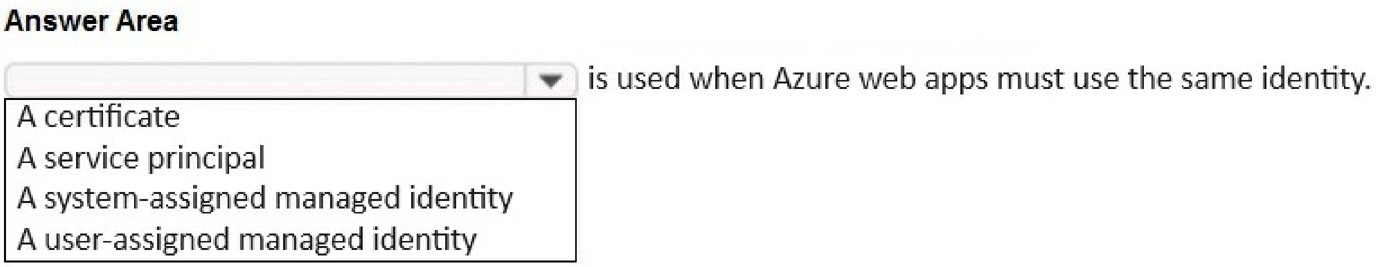
No

Question: 192 CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

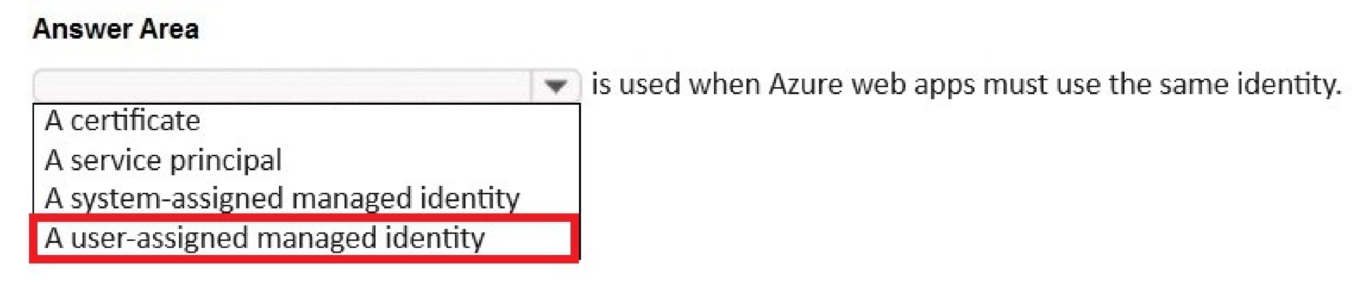


Answer Area

▼ is used when Azure web apps must use the same identity.

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

Answer:



Answer Area

▼ is used when Azure web apps must use the same identity.

- A certificate
- A service principal
- A system-assigned managed identity
- [✓ A user-assigned managed identity]

Explanation:

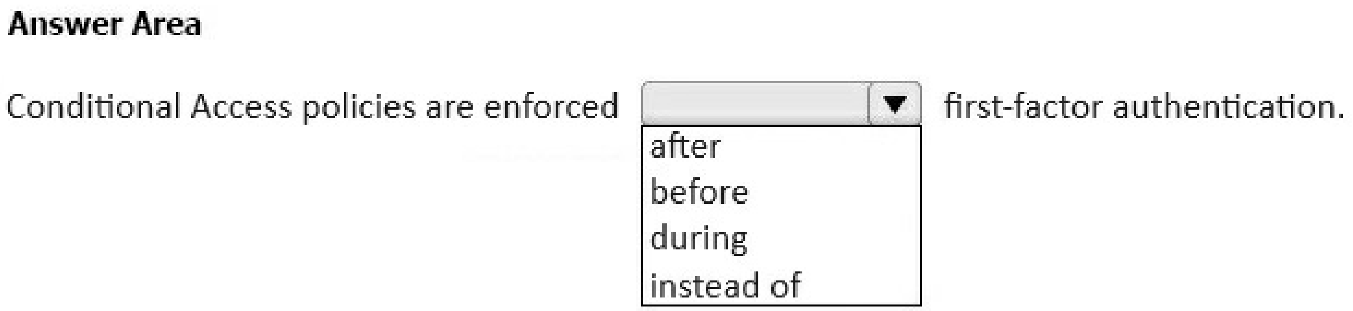
A user assigned managed identity.

Question: 193 CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

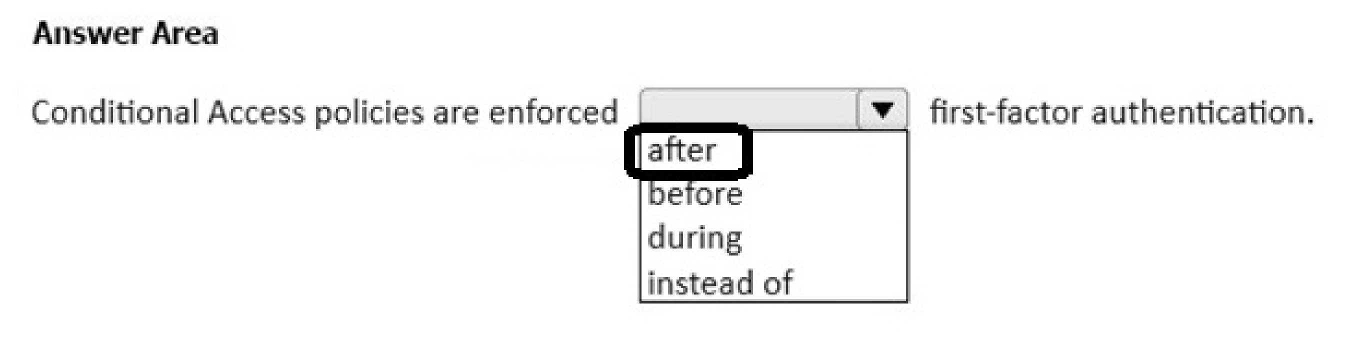


Answer Area

Conditional Access policies are enforced ▼ first-factor authentication.

- after
- before
- during
- instead of

Answer:



Answer Area

Conditional Access policies are enforced ▼ first-factor authentication.

- [✓ after]
- before
- during
- instead of

Question: 194

CertyIQ

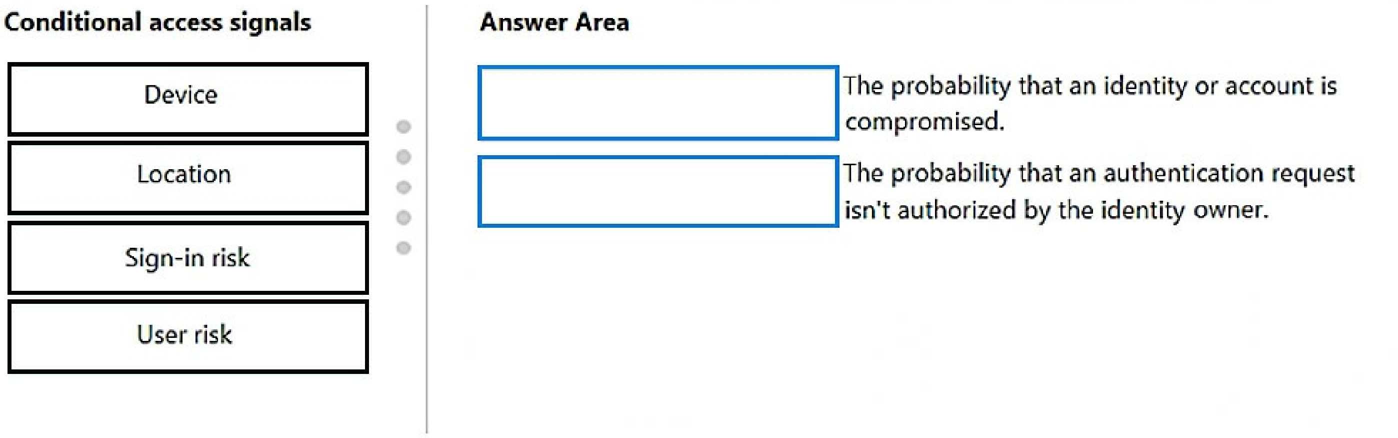
DRAG DROP

-

Match the types of Conditional Access signals to the appropriate definitions.

To answer, drag the appropriate Conditional Access signal type from the column on the left to its definition on the right. Each signal type may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.



Conditional access signals

Device

Location

Sign-in risk

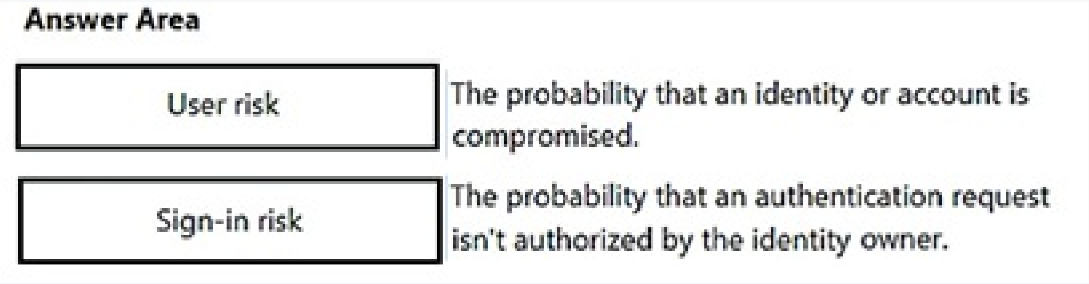
User risk

Answer Area

The probability that an identity or account is compromised.

The probability that an authentication request isn't authorized by the identity owner.

Answer:



Answer Area

User risk	The probability that an identity or account is compromised.
Sign-in risk	The probability that an authentication request isn't authorized by the identity owner.

Explanation:

User risk.

Sign-in risk.

Question: 195

CertyIQ

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

A.insider risk management

B.Compliance Manager

C.communication compliance

D.eDiscovery

Answer: A

Explanation:

Correct answer is A:insider risk management.

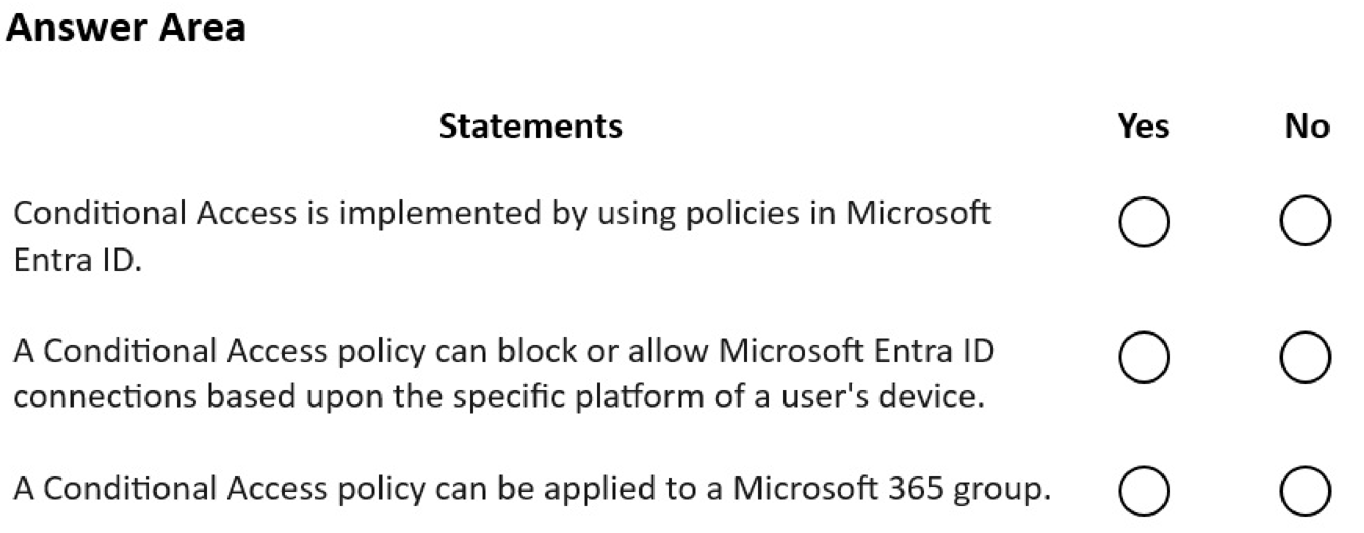
Question: 196 CertyIQ

HOTSPOT

-

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

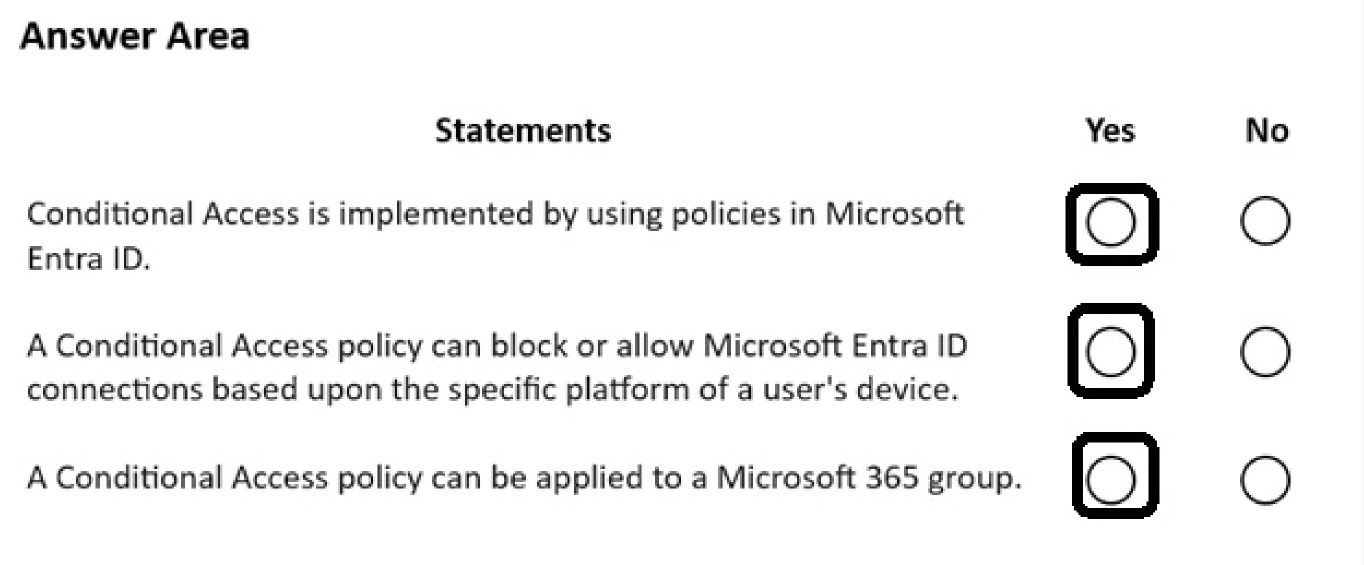
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Conditional Access is implemented by using policies in Microsoft Entra ID.	○	○
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device.	○	○
A Conditional Access policy can be applied to a Microsoft 365 group.	○	○

Answer:



Answer Area

Statements	Yes	No
Conditional Access is implemented by using policies in Microsoft Entra ID.	[✓ ○]	○
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device.	[✓ ○]	○
A Conditional Access policy can be applied to a Microsoft 365 group.	[✓ ○]	○

Explanation:

yes

yes

yes

Question: 197 CertyIQ

Which solution performs security assessments and automatically generates alerts when a vulnerability is found?

A.cloud security posture management (CSPM)
B.DevSecOps
C.cloud workload protection platform (CWPP)
D.security information and event management (SIEM)

Answer: A

Explanation:

A is correct.Microsoft Cloud Security Posture Management (CSPM) is indeed a service that performs security assessments and can generate alerts when vulnerabilities are found.Also right would be:The Microsoft solution that performs security assessments and automatically generates alerts when a vulnerability is found is Microsoft Defender Vulnerability Management.

Question: 198 CertyIQ

What can you use to protect against malicious links sent in email messages, chat messages, and channels?

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

Answer: B

Explanation:

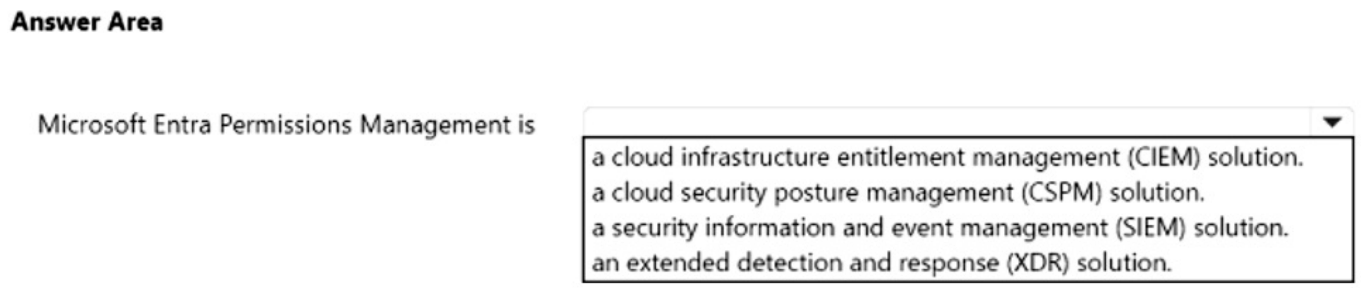
To protect against malicious links in email messages, chat messages, and channels, Microsoft offers Safe Links in Microsoft Defender for Office 365. This feature provides URL scanning and rewriting of inbound email messages during mail flow, and time-of-click verification of URLs and links in email messages, Teams, and supported Office 365 apps.

Question: 199 CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

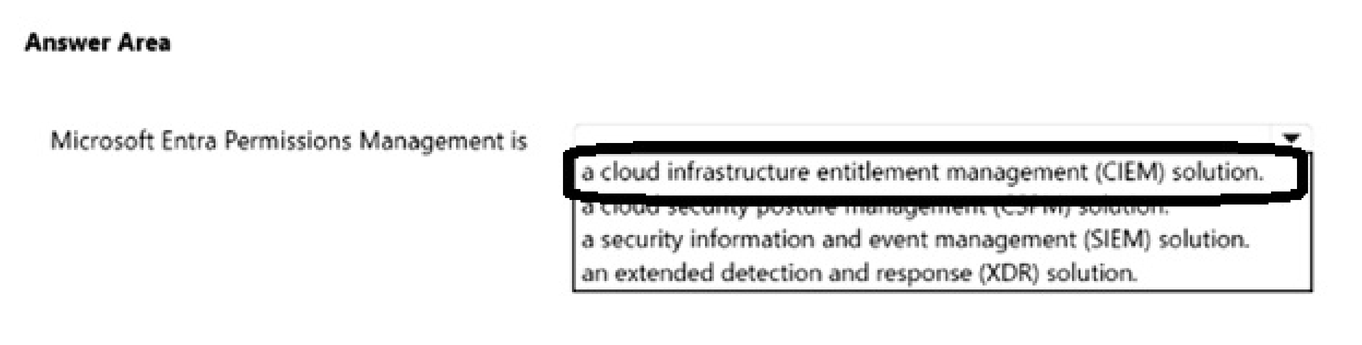


Answer Area

Microsoft Entra Permissions Management is

a cloud infrastructure entitlement management (CIEM) solution.
a cloud security posture management (CSPM) solution.
a security information and event management (SIEM) solution.
an extended detection and response (XDR) solution.

Answer:



Answer Area

Microsoft Entra Permissions Management is

[✓ a cloud infrastructure entitlement management (CIEM) solution.]
a cloud security posture management (CSPM) solution.
a security information and event management (SIEM) solution.
an extended detection and response (XDR) solution.

Explanation:

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities (users and workloads), actions, and resources across cloud infrastructures.

" https://learn.microsoft.com/en-us/entra/permissions-management/

Question: 200

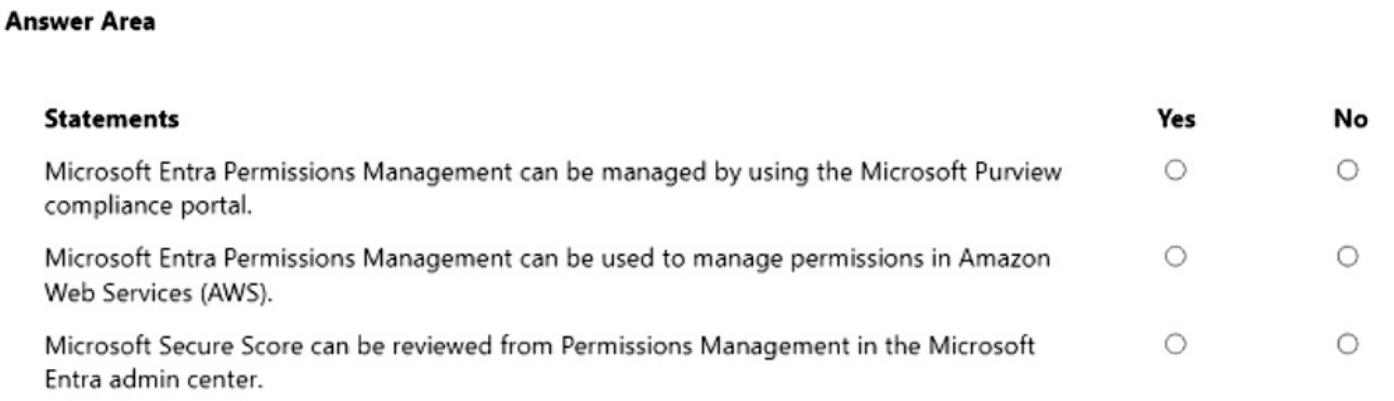
CertyIQ

HOTSPOT

-

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

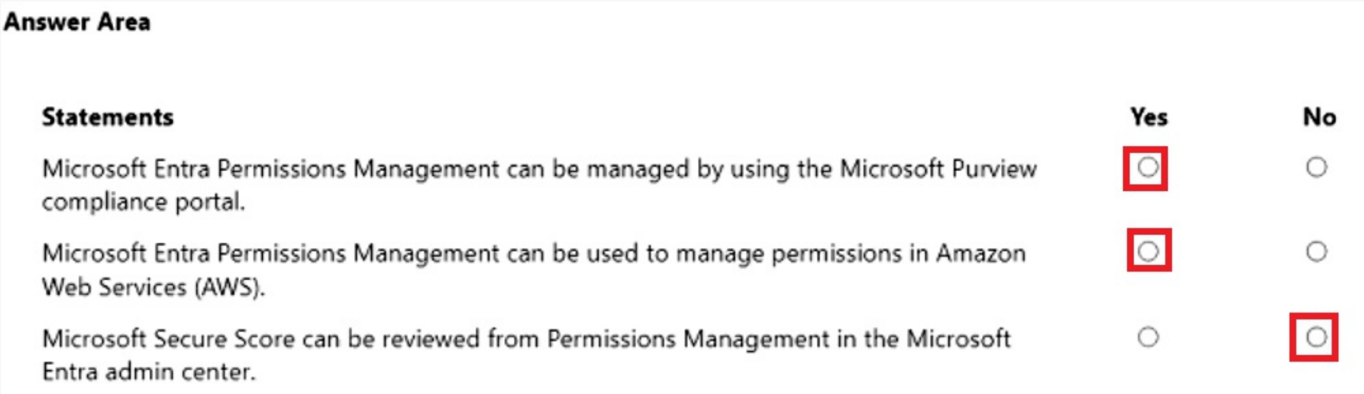
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Microsoft Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	○	○
Microsoft Entra Permissions Management can be used to manage permissions in Amazon Web Services (AWS).	○	○
Microsoft Secure Score can be reviewed from Permissions Management in the Microsoft Entra admin center.	○	○

Answer:



Answer Area

Statements	Yes	No
Microsoft Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	[✓ ○]	○
Microsoft Entra Permissions Management can be used to manage permissions in Amazon Web Services (AWS).	[✓ ○]	○
Microsoft Secure Score can be reviewed from Permissions Management in the Microsoft Entra admin center.	○	[✓ ○]

Explanation:

YES, Microsoft Entra permissions management can be managed by using the Microsoft Purview compliance portal[1]. The portal supports directly managing permissions for users who perform tasks within Microsoft Purview, including data security, data governance, and risk and compliance solutions.

YES, Microsoft Entra Permissions Management can indeed be used to manage permissions in AWS.

NO, Microsoft Secure Score is not reviewed from Permissions Management in the Microsoft Entra admin center. Permissions Management is a separate feature within Microsoft Entra that provides visibility into permissions across multicloud infrastructures

Question: 201

Which service includes Microsoft Secure Score for Devices?

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

Answer: B

Explanation:

Microsoft Defender for Endpoint.

Question: 202

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

A.the Microsoft 365 admin center
B.Azure Cost Management + Billing
C.Microsoft Service Trust Portal
D.the Microsoft Purview compliance portal

Answer: C

Explanation:

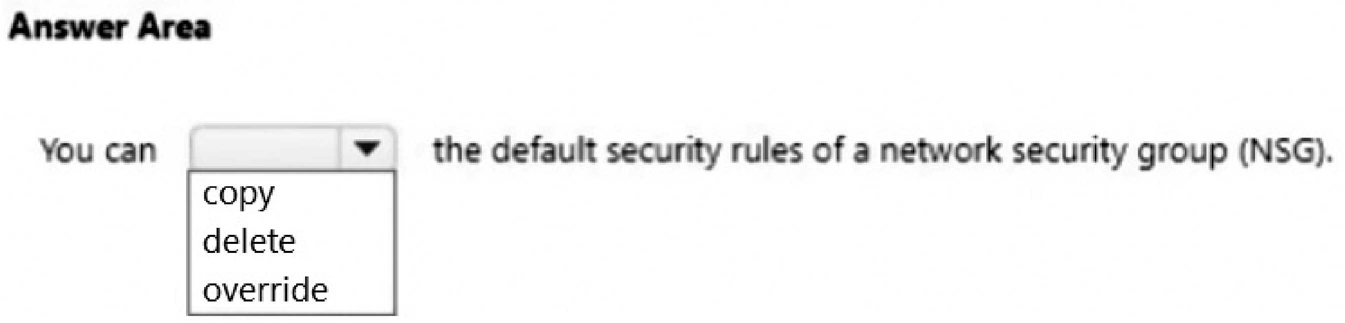
Reference:

https://servicetrust.microsoft.com/

Question: 203

HOTSPOT
-

Select the answer that correctly completes the sentence.

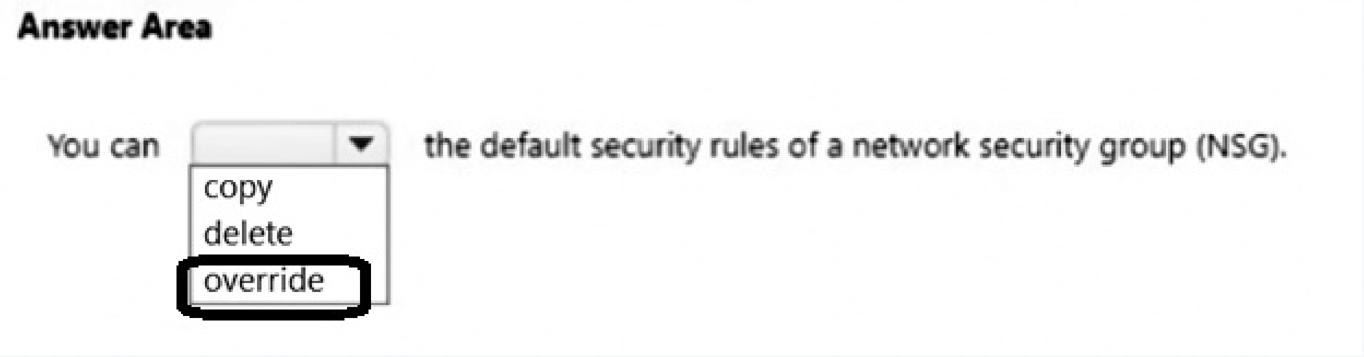


Answer Area

You can [▼] the default security rules of a network security group (NSG).

- copy
- delete
- override

Answer:



Answer Area

You can [▼] the default security rules of a network security group (NSG).

- copy
- delete
- [✓ override]

Question: 204 CertyIQ

You have an Azure subscription that contains a Log Analytics workspace.

You need to onboard Microsoft Sentinel.

What should you do first?

A.Create a hunting query.

B.Correlate alerts into incidents.

C.Connect to your data sources.

D.Create a custom detection rule.

Answer: C

Explanation:

Connect to your data sources.

Question: 205 CertyIQ

What is Azure Key Vault used for?

A.to deploy a cloud-based network security service that protects Azure virtual network resources

B.to protect cloud-based applications from cyber threats and vulnerabilities

C.to safeguard cryptographic keys and other secrets used by cloud apps and services

D.to provide secure and seamless RDP/SSH connectivity to Azure virtual machines via TLS from the Azure portal

Answer: C

Explanation:

to safeguard cryptographic keys and other secrets used by cloud apps and services.

Question: 206 CertyIQ

When a user authenticates by using passwordless sign-in, what should the user select in the Microsoft Authenticator app?

A.an answer to a security question

B.a number

C.an alphanumeric key

D.a passphrase

Answer: B

Explanation:

Correct answer is B:a number.

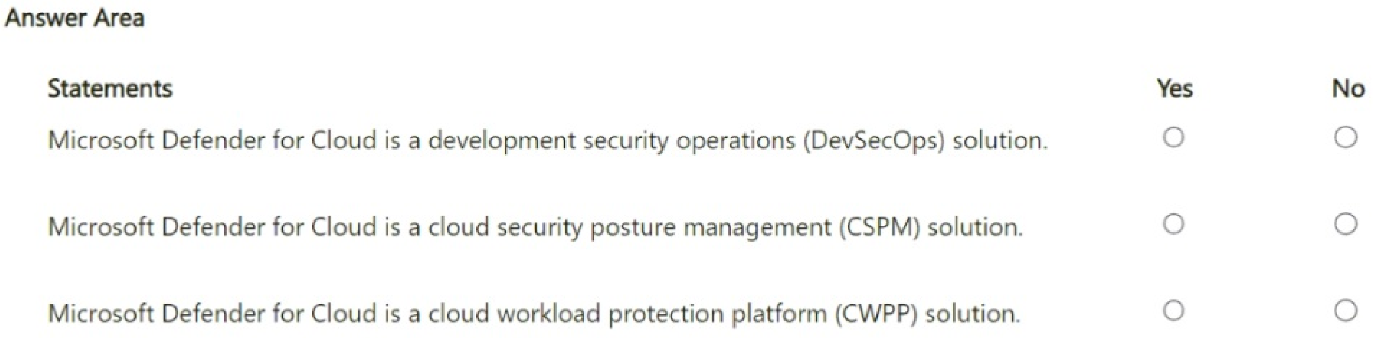
Question: 207 CertyIQ

HOTSPOT

-

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

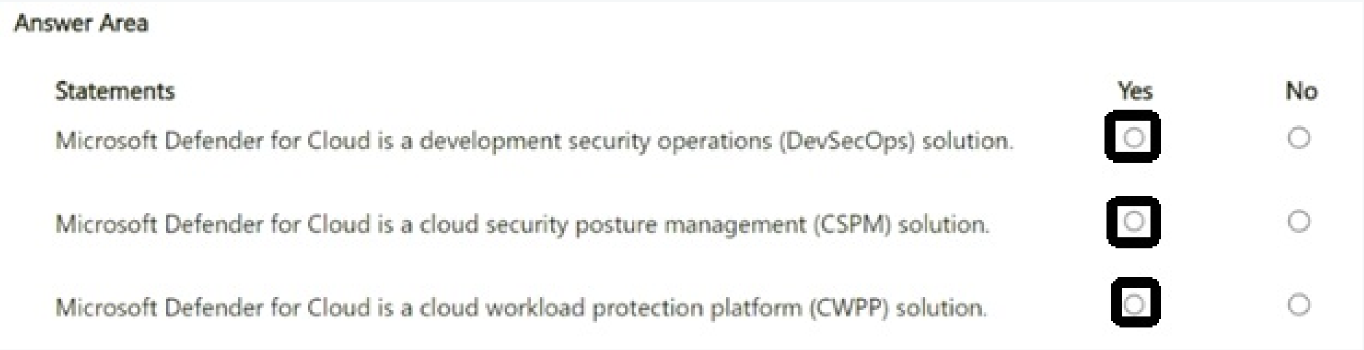
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Microsoft Defender for Cloud is a development security operations (DevSecOps) solution.	○	○
Microsoft Defender for Cloud is a cloud security posture management (CSPM) solution.	○	○
Microsoft Defender for Cloud is a cloud workload protection platform (CWPP) solution.	○	○

Answer:



Answer Area

Statements	Yes	No
Microsoft Defender for Cloud is a development security operations (DevSecOps) solution.	[✓ ○]	○
Microsoft Defender for Cloud is a cloud security posture management (CSPM) solution.	[✓ ○]	○
Microsoft Defender for Cloud is a cloud workload protection platform (CWPP) solution.	[✓ ○]	○

Explanation:

Yes

Yes

Yes

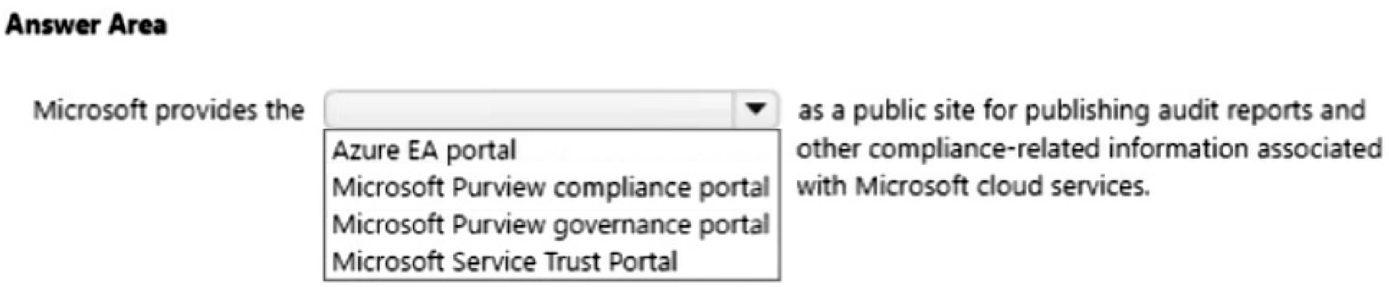
Question: 208

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

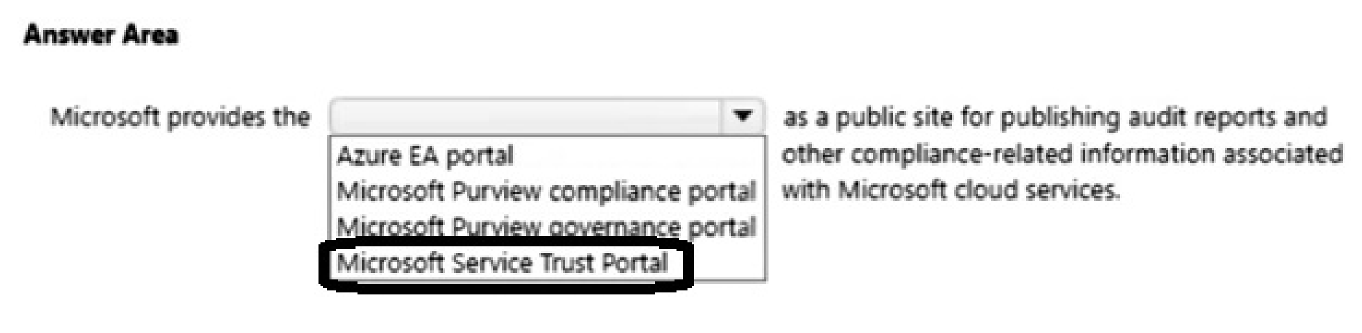


Answer Area

Microsoft provides the [dropdown] 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:



Answer Area

Microsoft provides the [dropdown] 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]

Explanation:

Reference:

https://learn.microsoft.com/en-us/purview/get-started-with-service-trust-portal

Question: 209

CertyIQ

What feature supports email as a method of authenticating users?

A.Microsoft Entra ID Protection

B.Microsoft Entra Multi-Factor Authentication (MFA)

C.self-service password reset (SSPR)

D.Microsoft Entra Password Protection

Answer: C

Explanation:

Answer is Self-Service Password Reset (SSPR)Self-service password reset allows users to reset their passwords using various methods, including email verification. This helps improve security and user convenience by enabling users to recover access to their accounts without needing to contact IT support.Microsoft Multi-Factor Authentication (MFA) does not support email as a method for the second factor of authentication. Instead, MFA typically supports methods such as:Authentication apps (like Microsoft Authenticator)SMS text messagesPhone callsSecurity keys (like FIDO2 devices)While email can be used for account recovery or notifications, it is not considered a secure second factor in the context of MFA.

Question: 210 CertyIQ

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

Answer: B

Explanation:

Reference:

https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

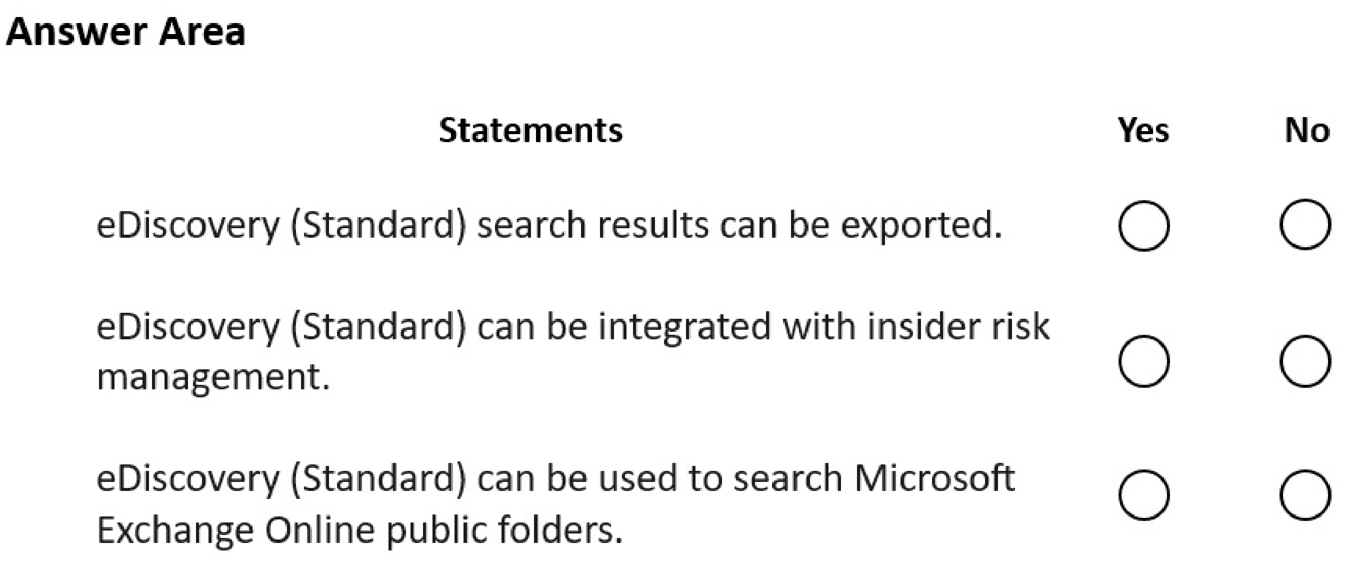
Question: 211 CertyIQ

HOTSPOT

-

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

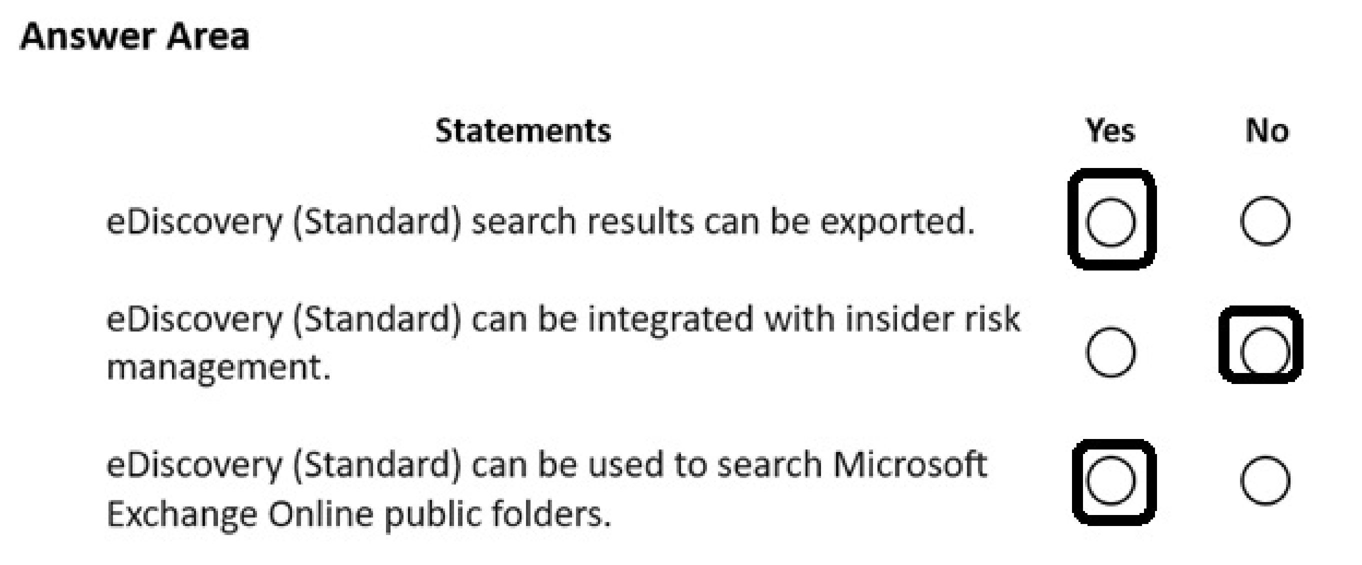
NOTE: Each correct selection is worth one point.



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:



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.	[✓ ○]	○

Explanation:

Yes, No, Yes

Integration with Insider Risk Management requires eDiscovery (Premium)

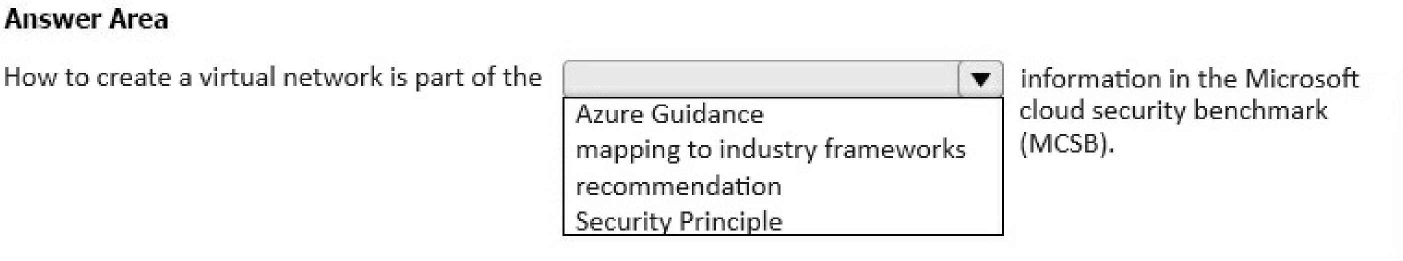
Question: 212

CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

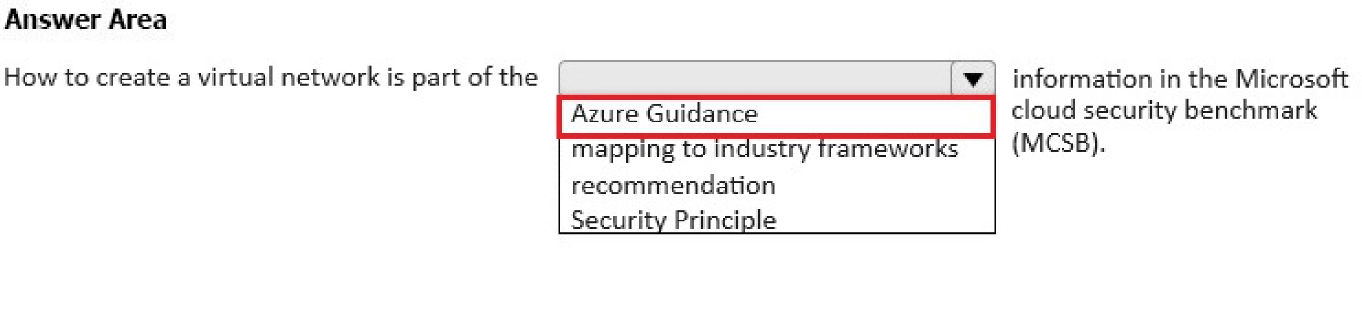


Answer Area

How to create a virtual network is part of the [▼] information in the Microsoft cloud security benchmark (MCSB).

- Azure Guidance
- mapping to industry frameworks
- recommendation
- Security Principle

Answer:



Answer Area

How to create a virtual network is part of the [▼] information in the Microsoft cloud security benchmark (MCSB).

- [✓ Azure Guidance]
- mapping to industry frameworks
- recommendation
- Security Principle

Explanation:

Reference:

https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security

Question: 213 CertyIQ

Which two actions can you perform by using Azure Key Vault? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.Store secrets.
B.Store Azure Resource Manager (ARM) templates.
C.Implement network security groups (NSGs).
D.Implement Azure DDoS Protection.
E.Store keys.

Answer: AE

Explanation:

A.Store secrets.

E.Store keys.

Reference:

https://learn.microsoft.com/en-us/azure/key-vault/general/overview

Question: 214 CertyIQ

Which feature is included in Microsoft Entra ID Governance?

A.Identity Protection
B.Privileged Identity Management
C.Permissions Management
D.Verifiable credentials

Answer: B

Explanation:

Privileged Identity Management (PIM).

Reference:

https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

Question: 215 CertyIQ

What should you create to search and export content preserved in an eDiscovery hold?

A.a Microsoft SharePoint Online site
B.a case

C.a Microsoft Exchange Online public folder
D.Azure Files

Answer: B

Explanation:

Correct answer is B:a case.

Refrence:

https://learn.microsoft.com/en-us/purview/ediscovery-create-holds

Question: 216

Which Microsoft Purview data classification type supports the use of regular expressions?

A.exact data match (EDM)
B.fingerprint classifier
C.sensitive information types (SITs)
D.trainable classifier

Answer: C

Explanation:

Sensitive Information Types .

Reference:

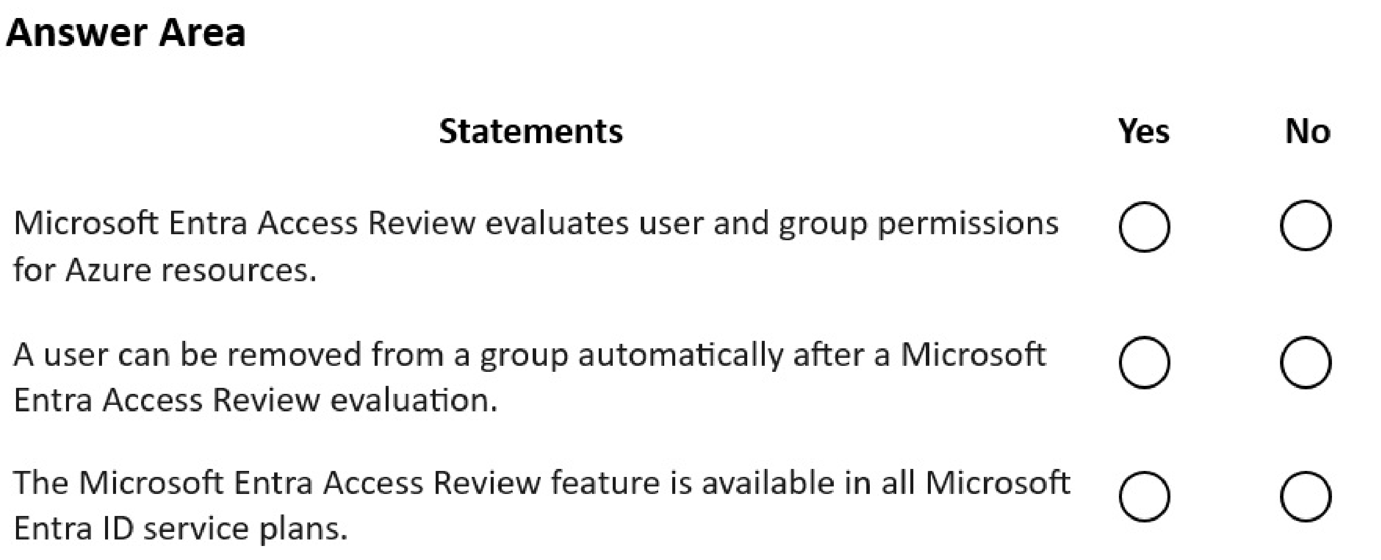
https://learn.microsoft.com/en-us/purview/dlp-policy-learn-about-regex-use

Question: 217

HOTSPOT
-

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

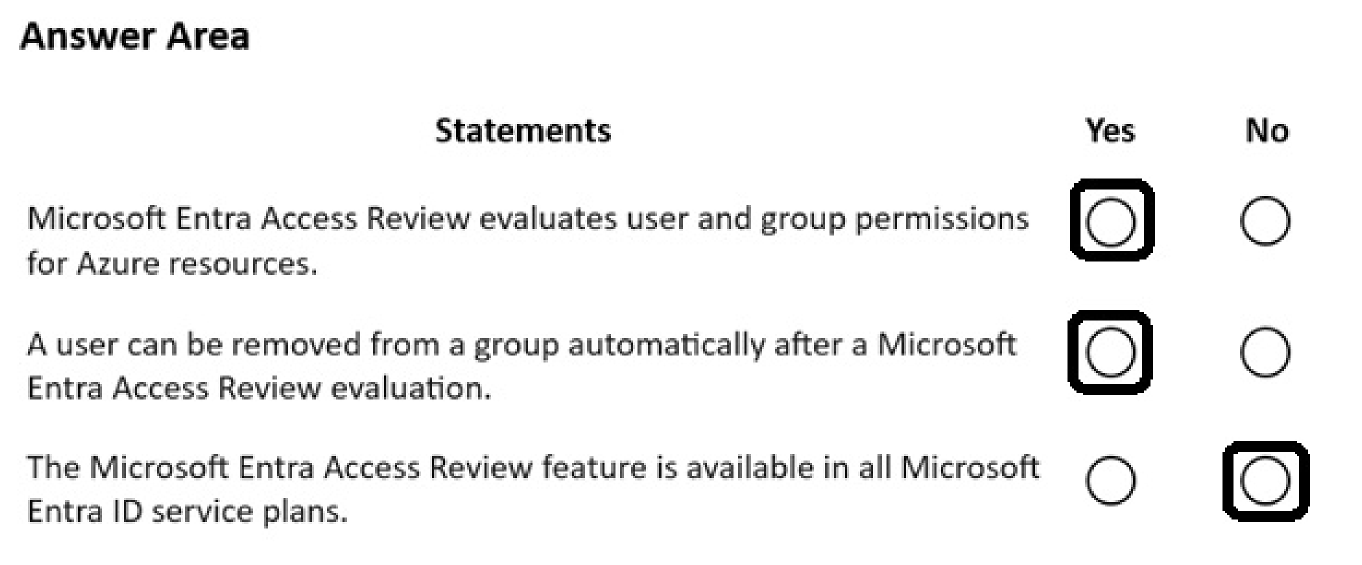
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Microsoft Entra Access Review evaluates user and group permissions for Azure resources.	○	○
A user can be removed from a group automatically after a Microsoft Entra Access Review evaluation.	○	○
The Microsoft Entra Access Review feature is available in all Microsoft Entra ID service plans.	○	○

Answer:



Answer Area

Statements	Yes	No
Microsoft Entra Access Review evaluates user and group permissions for Azure resources.	[✓ ○]	○
A user can be removed from a group automatically after a Microsoft Entra Access Review evaluation.	[✓ ○]	○
The Microsoft Entra Access Review feature is available in all Microsoft Entra ID service plans.	○	[✓ ○]

Explanation:

Yes

Yes

No

Reference:

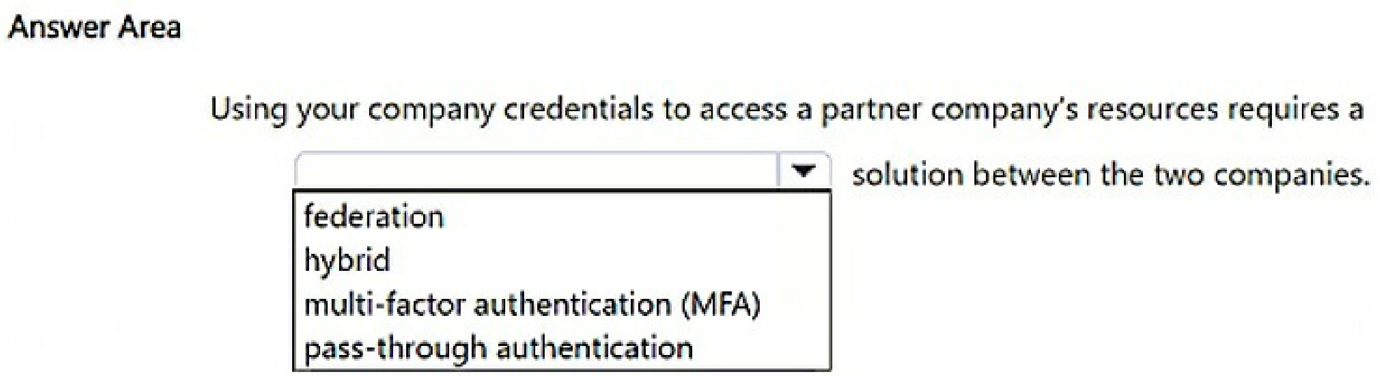
https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

Question: 218 CertyIQ

HOTSPOT

-

Select the answer that correctly completes the sentence.

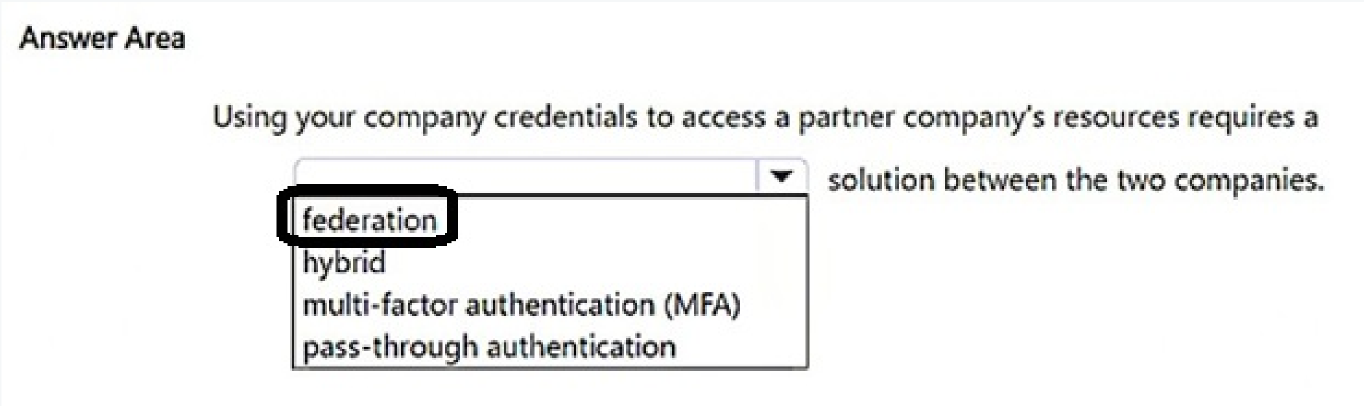


Answer Area

Using your company credentials to access a partner company's resources requires a [dropdown] solution between the two companies.

- federation
- hybrid
- multi-factor authentication (MFA)
- pass-through authentication

Answer:



Answer Area

Using your company credentials to access a partner company's resources requires a [dropdown] solution between the two companies.

- [✓ federation]
- hybrid
- multi-factor authentication (MFA)
- pass-through authentication

Explanation:

Reference:

https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b

Question: 219 CertyIQ

Which two types of devices can be managed by using Endpoint data loss prevention (Endpoint DLP)? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.Windows 11

B.Linux

C.iOS

D.macOS

E.Android

Answer: AD

Explanation:

A.Windows 11

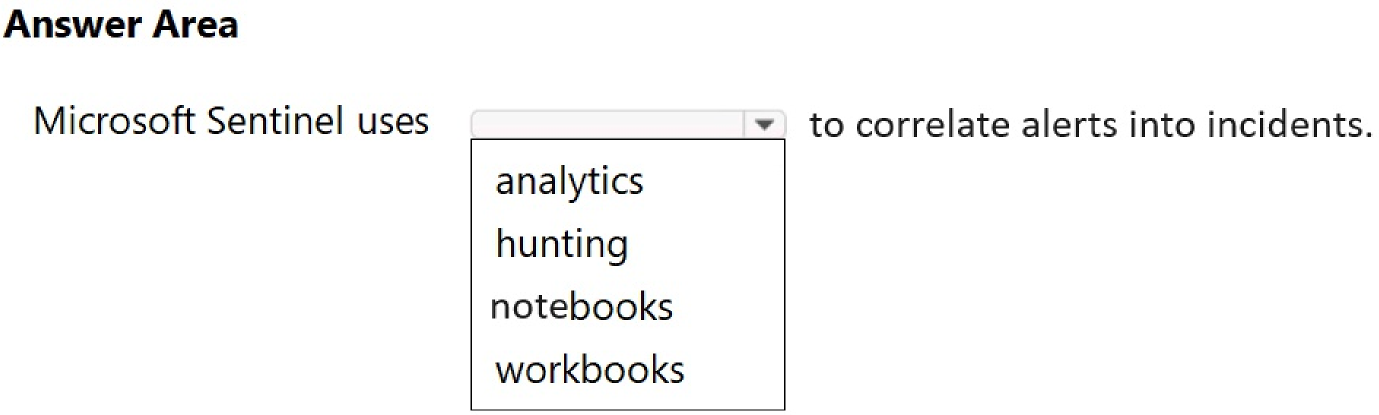
D.macOS

Question: 220

HOTSPOT

-

Select the answer that correctly completes the sentence.

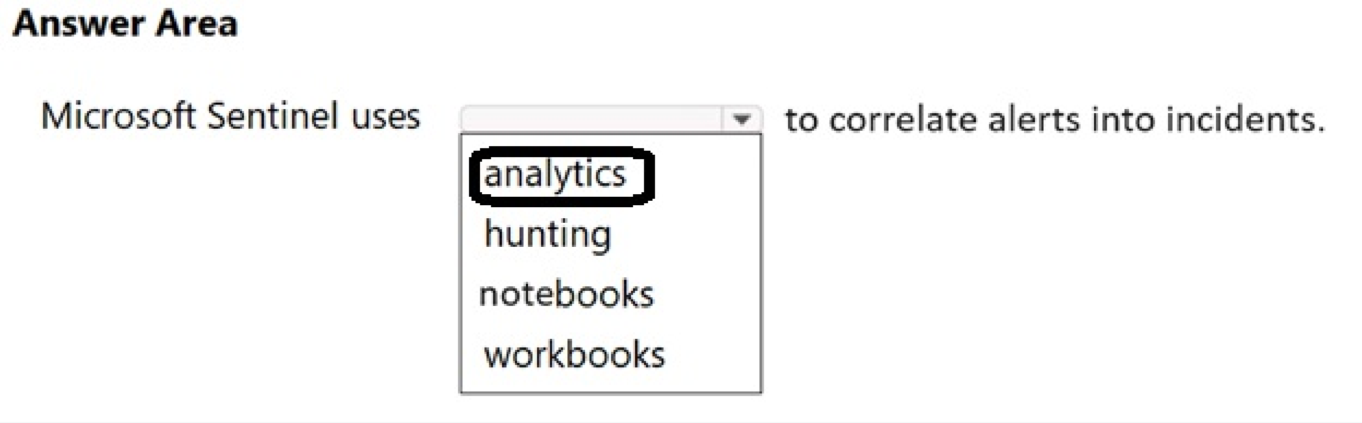


Answer Area

Microsoft Sentinel uses ▼ to correlate alerts into incidents.

- analytics
- hunting
- notebooks
- workbooks

Answer:



Answer Area

Microsoft Sentinel uses ▼ to correlate alerts into incidents.

- [✓ analytics]
- hunting
- notebooks
- workbooks

Explanation:

Reference:

https://learn.microsoft.com/en-us/answers/questions/25694/what-are-incidents-in-azure-sentinel-and-how-are-t

Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.
Your insights can help me improve our writing and better understand our readers.

Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam
Keep your head up, stay positive, and go show that exam what you're made of!

Feedback

More Papers

Total: **220 Questions**

Link: https://certyiq.com/papers/microsoft/sc-900