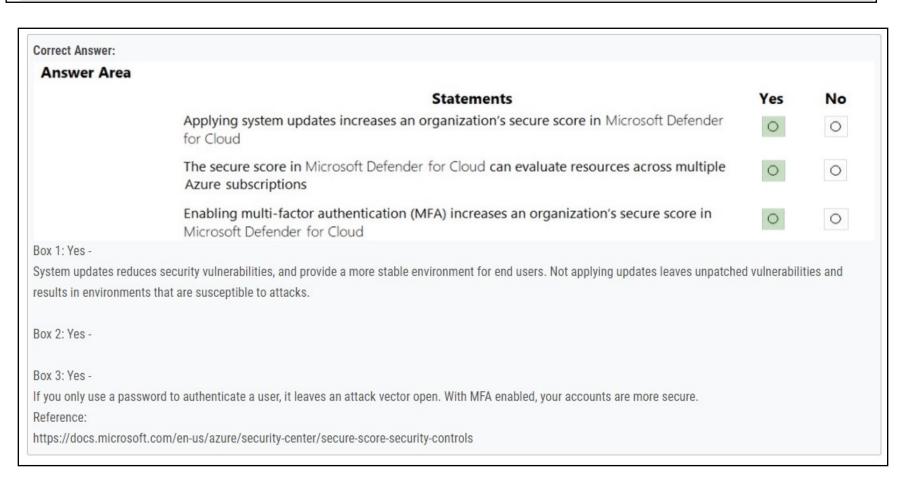
45 questions in 45 minutes

Question #1				Topic 1
HOTSPOT - For each of the following NOTE: Each correct selec Hot Area: Answer Area	statements, select Yes if the statement is true. Otherwise, select No. tion is worth one point.			
	Statements	Yes	No	
	All Azure Active Directory (Azure AD) license editions include the same features.	0	0	
10	You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	0	0	
,	You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	0	0	
Hide Solution 🗩	Discussion 30			
Correct Answer:				
Answer Area				
	Statements	Yes	No	
	All Azure Active Directory (Azure AD) license editions include the same features.	0	0	
	You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	0	0	
	You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	0	0	

6	Answer Area				
Correct Answer:	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.			
Reference: https://docs.micro	osoft.com/en-us/azure/cloud-adoption-framework/get-started	1/			



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

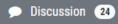
- A. Microsoft Secure Score
- B. Productivity Score
- C. Secure score in Azure Security Center
- D. Compliance score Most Voted

# Question #9 Topic 1

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 Most Voted
- D. the Azure Active Directory admin center





Correct Answer: C

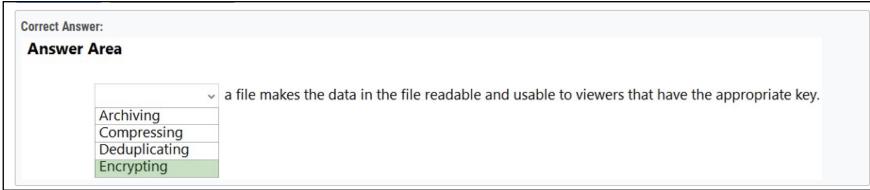
The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.

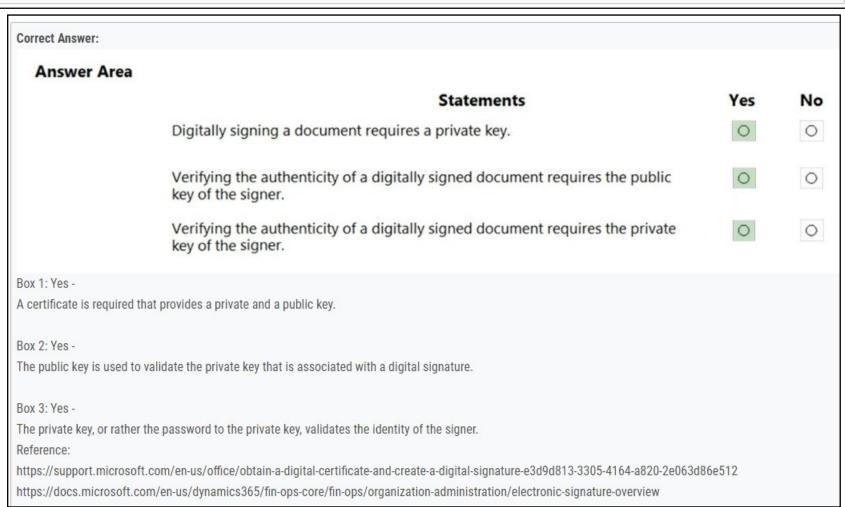
Reference:

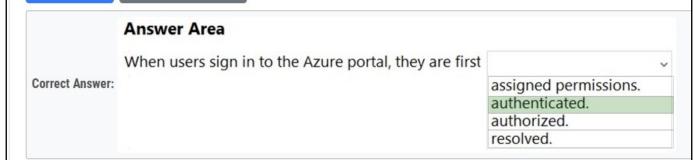
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal? view=o365-worldwide

Community vote distribution

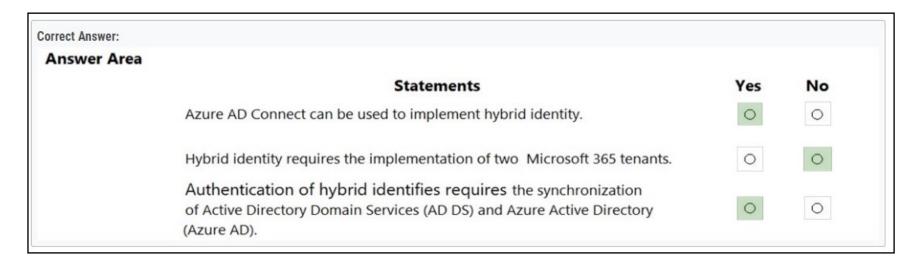
C (100%)











# 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.

### 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

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) Most Voted
- B. Azure Multi-Factor Authentication (MFA)
- C. Azure Active Directory (Azure AD) Identity Protection
- D. conditional access policies

### Question #29

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 Most Voted
- D. Azure AD Privileged Identity Management (PIM)

### **Correct 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.

Biometrics templates are stored locally on a device.

Reference:

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

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 Most Voled

B. managed identities

C. conditional access policies

D. Azure AD Identity Protection

	Answer Area		
	Statements	Yes	No
	Conditional access policies can use the device state as a signal.	0	0
Correct Answer:	Conditional access policies apply before first-factor authentication is complete.	0	0
	Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	0	0
Box 1: Yes -			
Box 2: No -			
Conditional Acce	ss policies are enforced after first-factor authentication is completed.		
Box 3: Yes -			
Reference:			
https://docs.micr	osoft.com/en-us/azure/active-directory/conditional-access/overview		

# 

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) Most Voted
- D. authentication method policies

### 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.

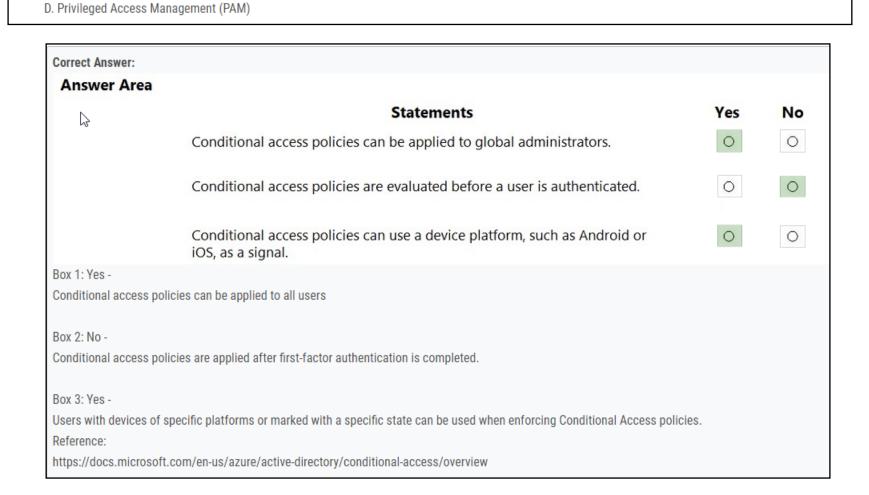
- A. text message (SMS) Most Voted
- B. Microsoft Authenticator app Most Voted
- C. email verification
- D. phone call Most Voted
- E. security question

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 Most Voted



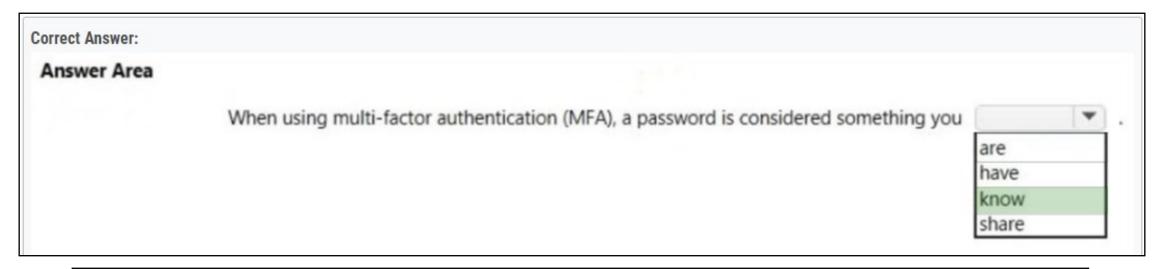
You have an Azure subscription.

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

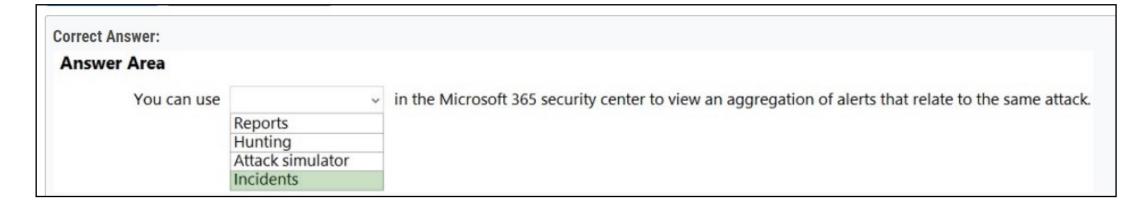
What should you use?

- 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) Most Voted

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

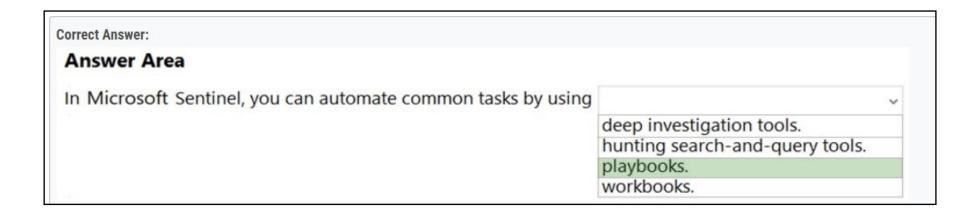




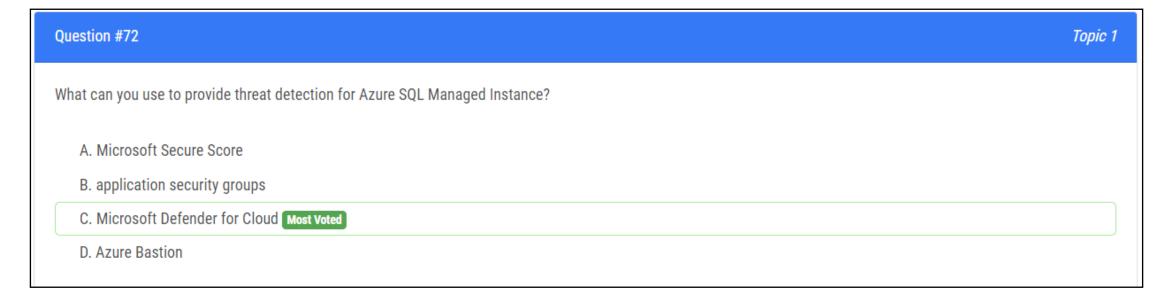


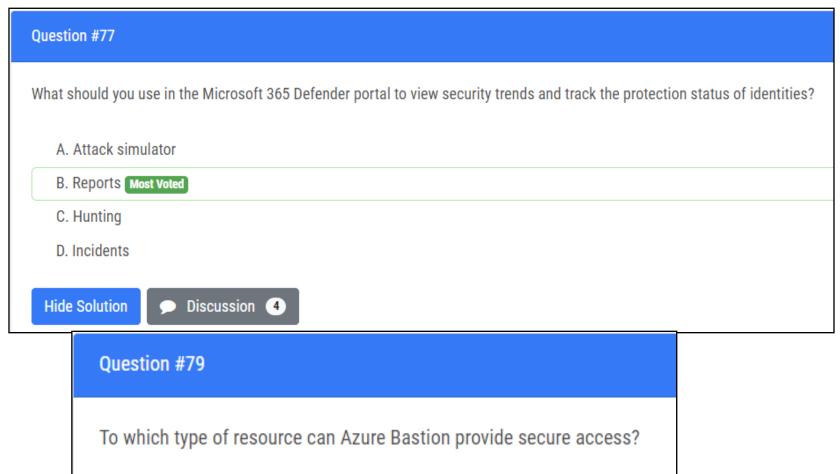
	Answer Area		
	Statements	Yes	No
Correct Answer:	Network security groups (NSGs) can deny inbound traffic from the internet.	0	0
	Network security groups (NSGs) can deny outbound traffic to the internet.	0	0
	Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	0	0
You can use an A	zure network security group to filter network traffic to and from Azure resources in an Azure virtua	al network. A	network s
security rules that	t allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure	e resources.	For each ru
and destination, p	oort, and protocol.		
Reference:			

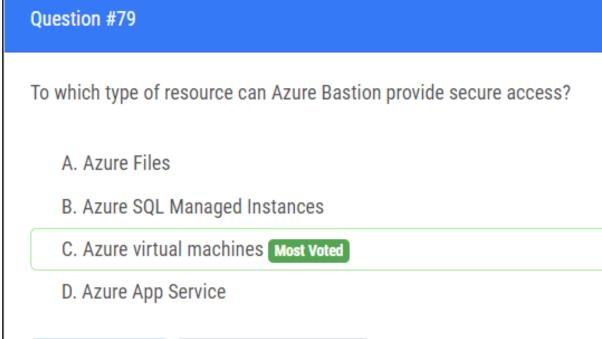
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

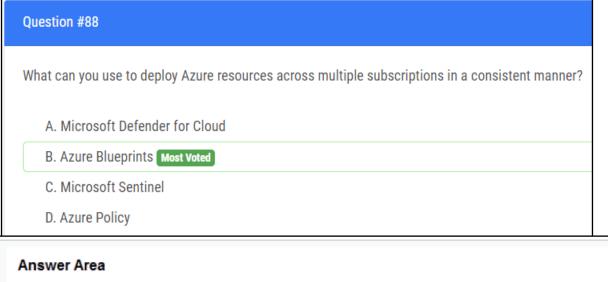


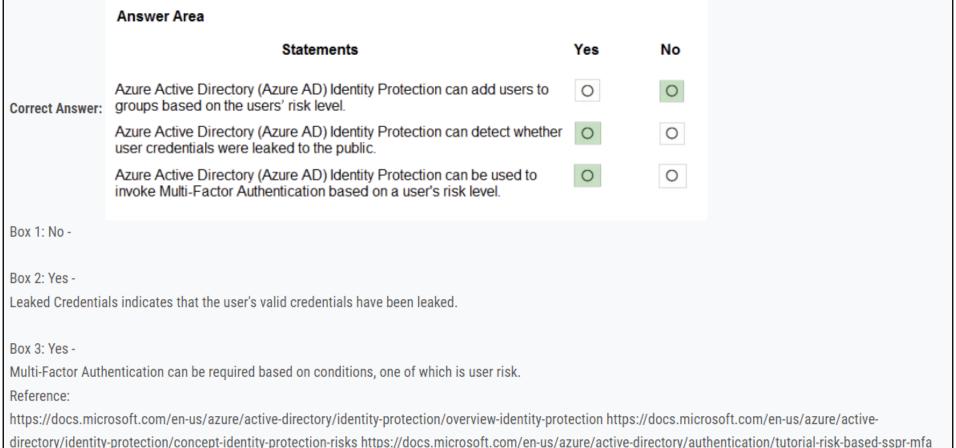
orrect Answer:			
Answer Area			
	Statements	Yes	No
	Microsoft Defender for Endpoint can protect Android devices.	0	0
	Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	0	0
	Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	0	0











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 Most Voted
- D. Alerts





# Correct Answer: C

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

## Correct Answer:

# **Answer Area**

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

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

# Reference:

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