Microsoft.SC-100.v2024-12-28.q107

Exam Code:	SC-100
Exam Name:	Microsoft Cybersecurity Architect
Certification Provider:	Microsoft
Free Question Number:	107
Version:	v2024-12-28
# of views:	6897
# of Questions views:	1973
https://www.dumpsfiles.com/files/Microsoft/SC-100/Microsoft.SC-100.v2024-12-28.q107	

NEW QUESTION: 1
You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.
You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.
What should you include in the recommendation?
A. Apply read-only locks on the storage accounts.
B. Set the AllowSharcdKeyAccess property to false.
C. Set the AllowBlobPublicAcccss property to false.
D. Configure automated key rotation.
Answer: A (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

NEW QUESTION: 2
Your company is moving a big data solution to Azure.
The company plans to use the following storage workloads:
* Azure Storage blob containers
* Azure Data Lake Storage Gen2
* Azure Storage file shares
* Azure Disk Storage
Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. Azure Disk Storage
B. Azure Storage blob containers
C. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Answer: B,D (LEAVE A REPLY)

Explanation

https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory

https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-acc

NEW QUESTION: 3

Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

A. Information Governance

B. eDiscovery

C. data loss prevention (DLP)

D. data classification content explorer

Answer: (SHOW ANSWER)

NEW QUESTION: 4

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer are a. NOTE Each correct selection is worth one point.

Answer:

NEW QUESTION: 5

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

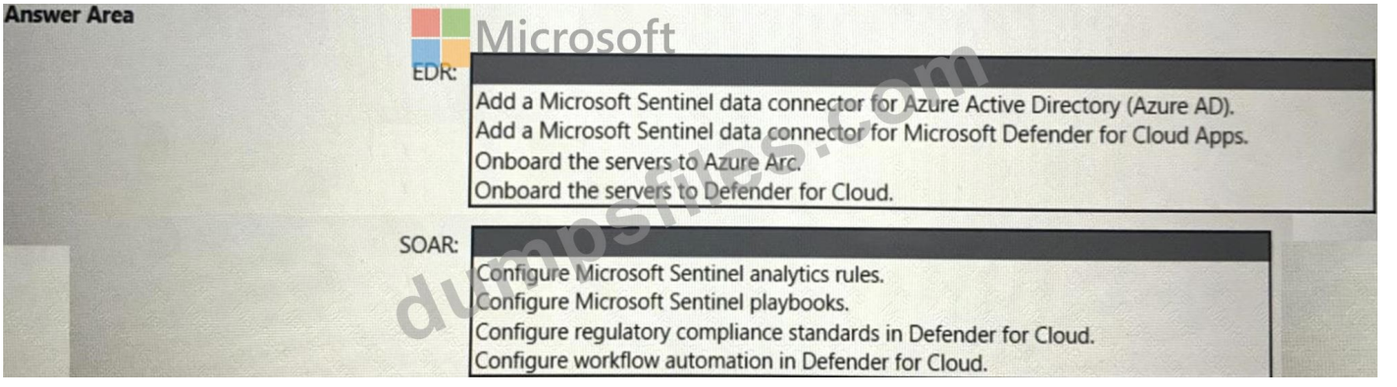
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

You plan to deploy Azure virtual machines that will run Windows Server.

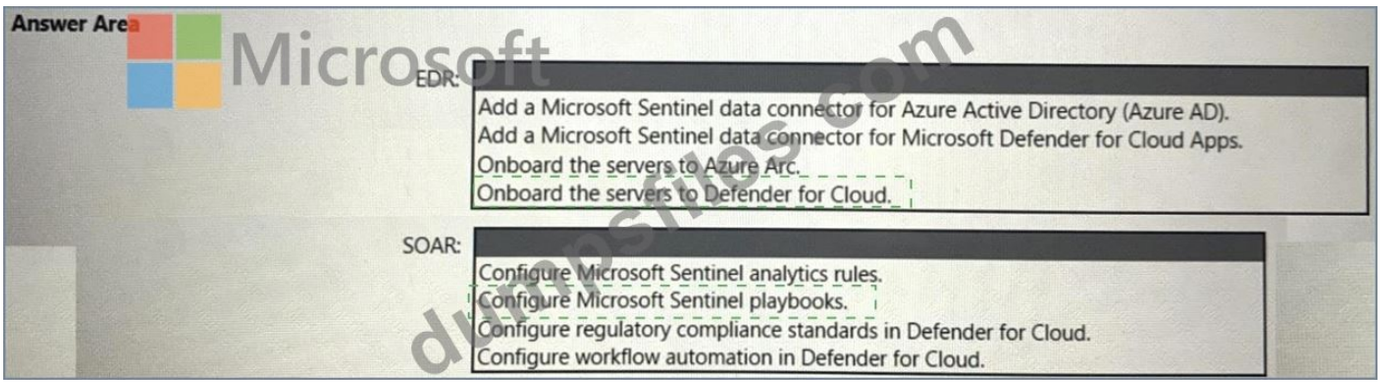
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation

NEW QUESTION: 6

Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 7

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and

continuous deployment (CI/CD) DevOps pipelines You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines.
What should recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

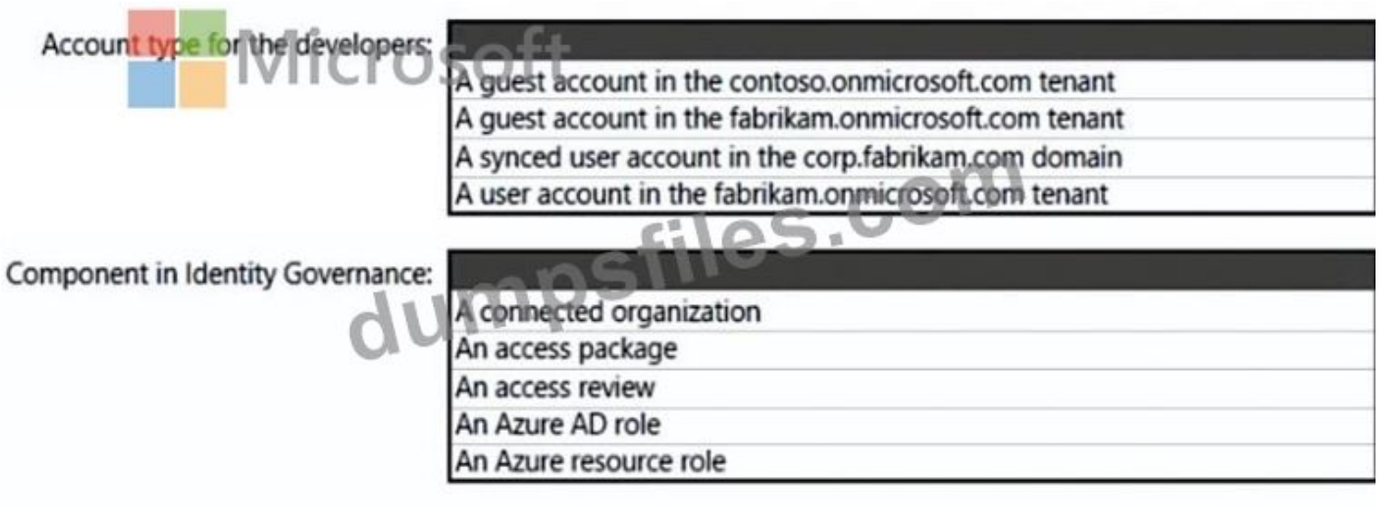
Answer:

NEW QUESTION: 8
You have a Microsoft 365 E5 subscription.
You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.
You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.
Which two components should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. data loss prevention (DLP) policies
B. sensitivity label policies
C. retention label policies
D. eDiscovery cases
Answer: B,D (LEAVE A REPLY)

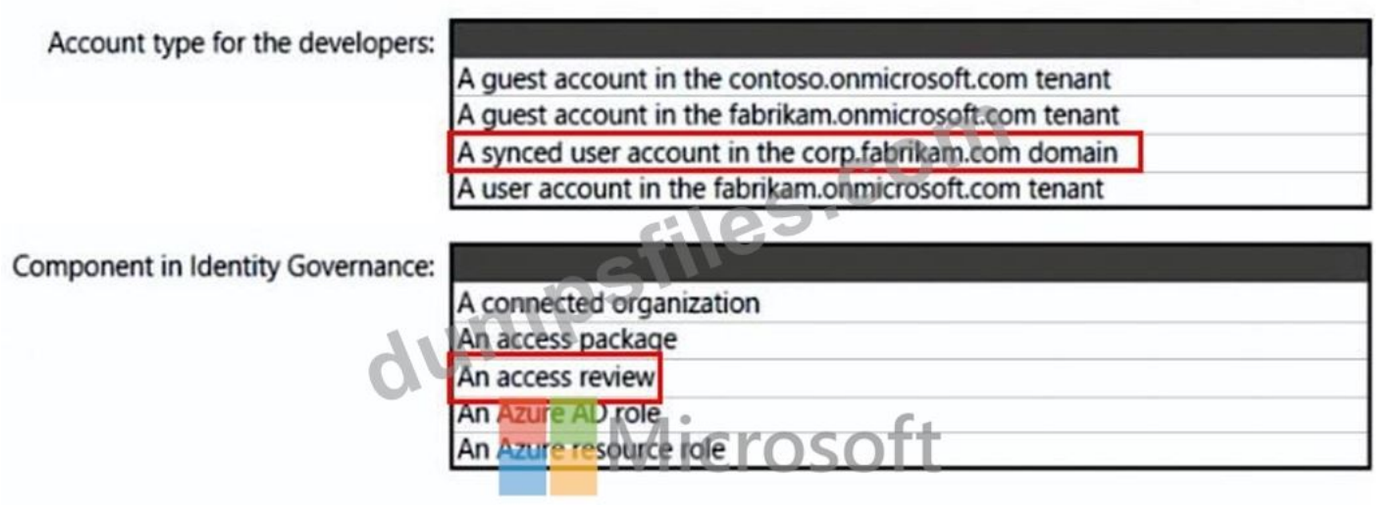
NEW QUESTION: 9
You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?
A. Microsoft Defender for Cloud Apps
B. insider risk management
C. Microsoft Information Protection
D. Azure Purview
Answer: C (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a
"Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as SalesForce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.

NEW QUESTION: 10
Your company has a Microsoft 365 E5 subscription.
The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online.
You need to recommend a solution to identify documents that contain sensitive information.
What should you include in the recommendation?
A. data loss prevention (DLP)
B. eDiscovery
C. data classification content explorer
D. Information Governance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
What should you create in Azure AD to meet the Contoso developer requirements?



Answer:



NEW QUESTION: 12

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attach surface.

What should you include in the recommendation?

A. Azure Firewall Premium

B. Azure Application Gateway Web Application Firewall (WAF)

C. network security groups (NSGs)

D. Azure Traffic Manager and application security groups

Answer: D (LEAVE A REPLY)

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection

NEW QUESTION: 13

Your company, named Contoso. Ltd... has an Azure AD tenant namedcontoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You

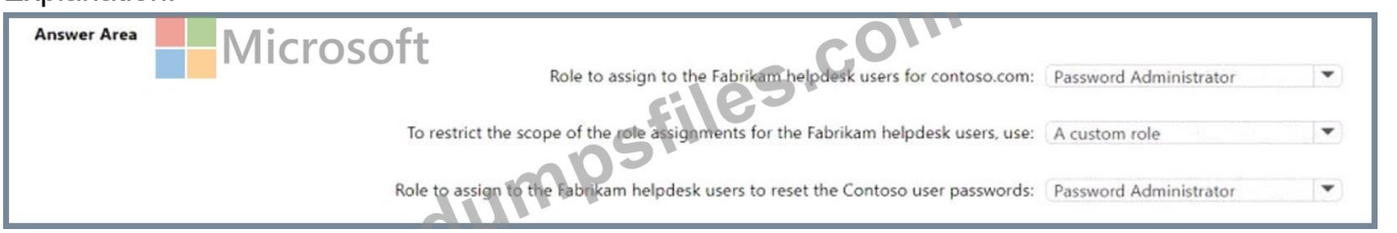
need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:

* Follow the principle of least privilege.
* Minimize administrative effort.

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

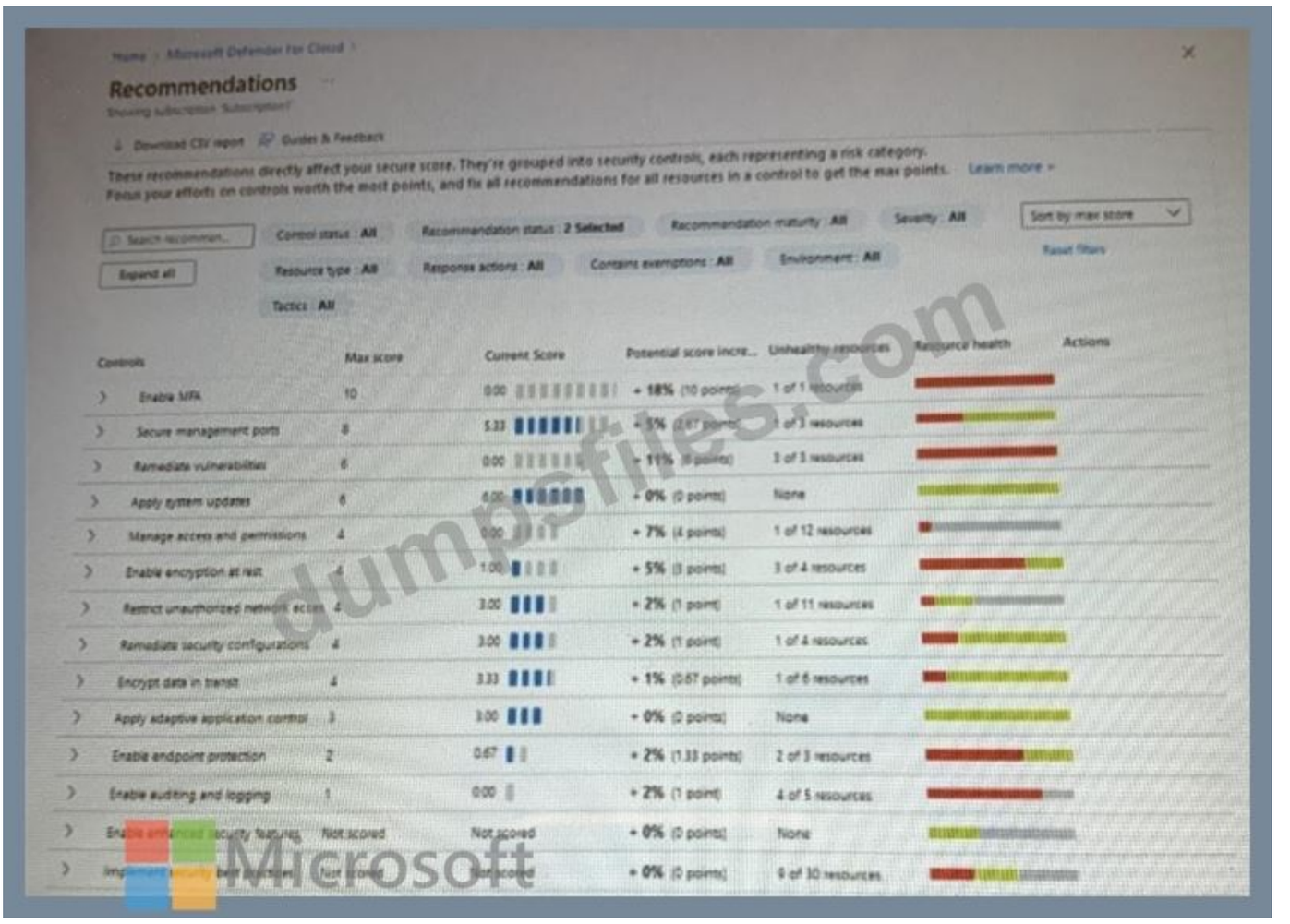
Answer:

Explanation:



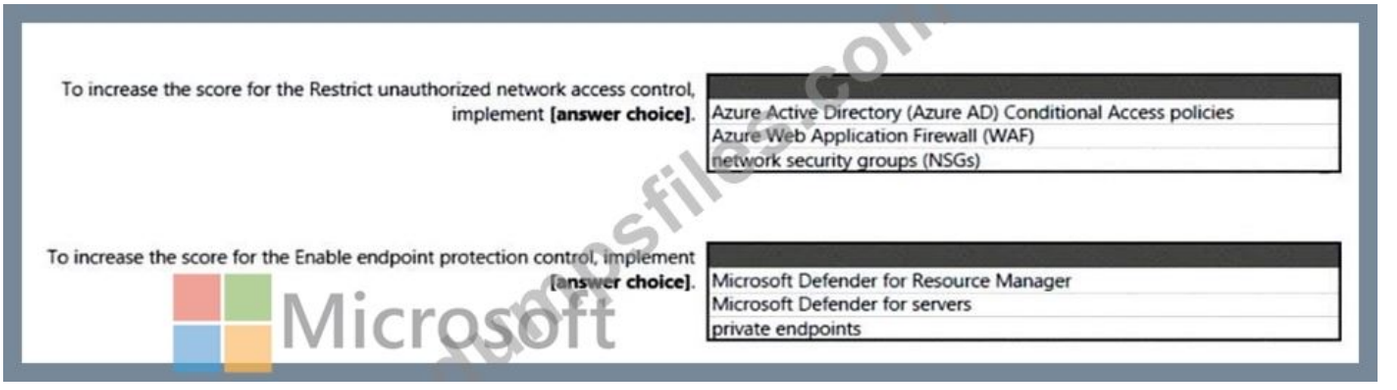
NEW QUESTION: 14

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

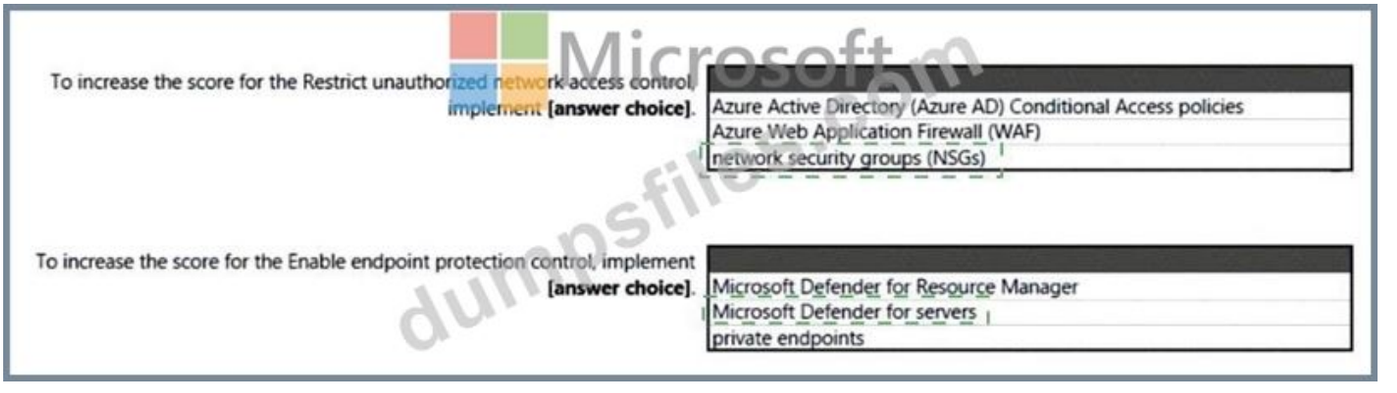


Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



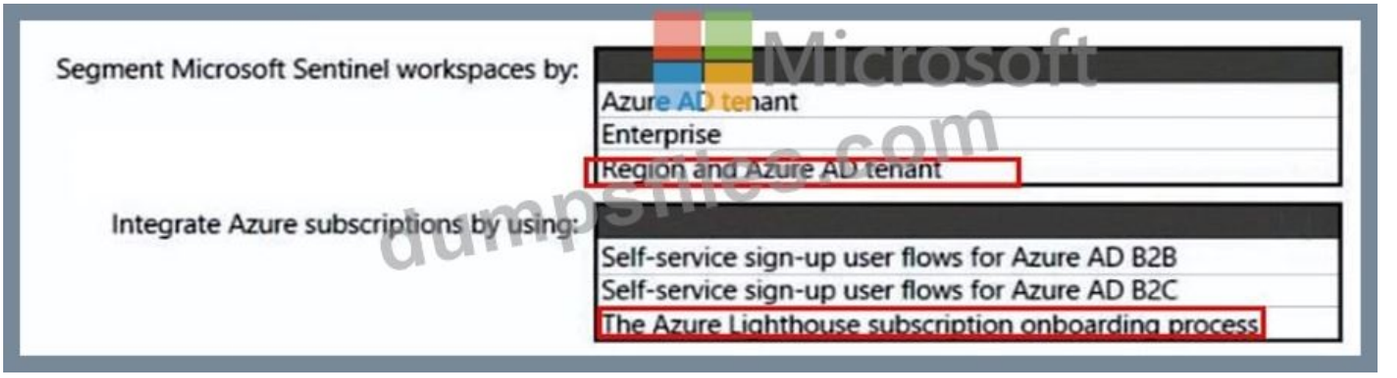
Answer:



Explanation
Selection 1: NSG Selection
Selection 2: Microsoft Defender for servers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION: 15
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:



NEW QUESTION: 16
You are designing a ransomware response plan that follows Microsoft Security Best Practices.
You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.
What should you include in the recommendation?
A. Microsoft Defender for Endpoint
B. Windows Defender Device Guard
C. BitLocker Drive Encryption (BitLocker)
D. Azure Files
E. protected folders
Answer: E (LEAVE A REPLY)

NEW QUESTION: 17
You have a Microsoft 365 subscription.
You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).
You need to recommend a solution that automatically restricts access to Microsoft Exchange Online.
SharePoint Online, and Teams m near-real-lime (NRT) in response to the following Azure AD events:
* A user account is disabled or deleted
* The password of a user is changed or reset.
* All the refresh tokens for a user are revoked
* Multi-factor authentication (MFA) is enabled for a user
Which two features should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. continuous access evaluation
B. Azure AD Application Proxy
C. Azure AD Privileged Identity Management (PIM)
D. Conditional Access
E. a sign-in risk policy
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 18
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation

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

NEW QUESTION: 19

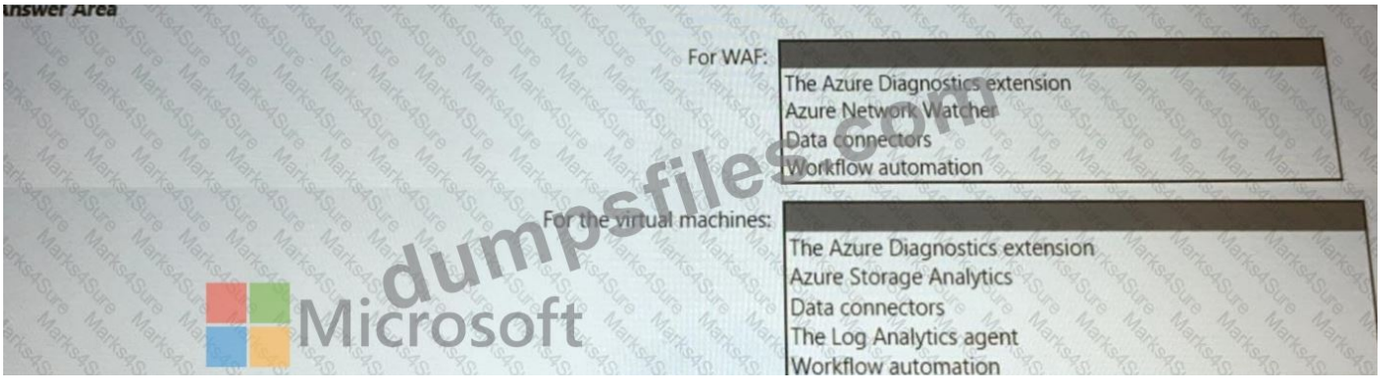
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.

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

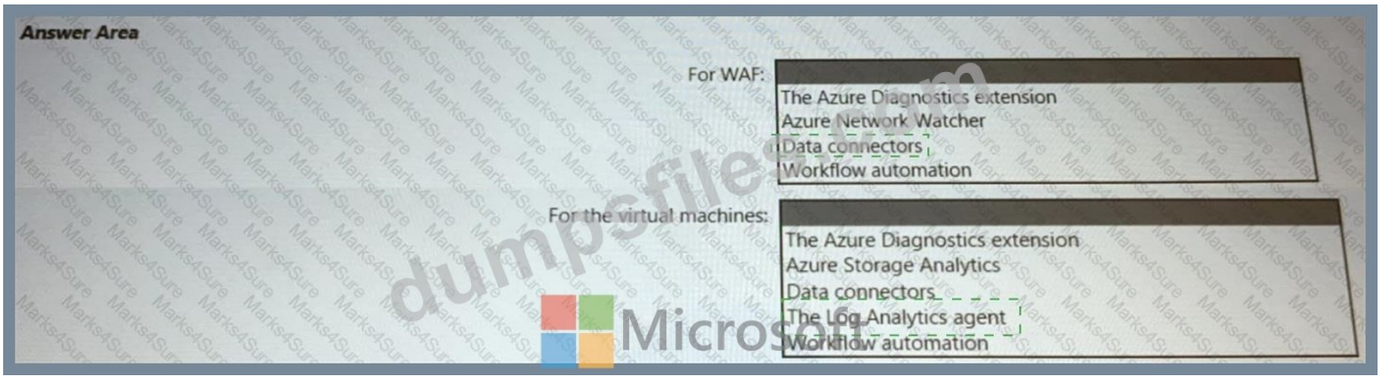
* Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
* Use Defender for Cloud to review alerts from the virtual machines.

What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE:

Each correct selection is worth one point.



Answer:



Explanation:

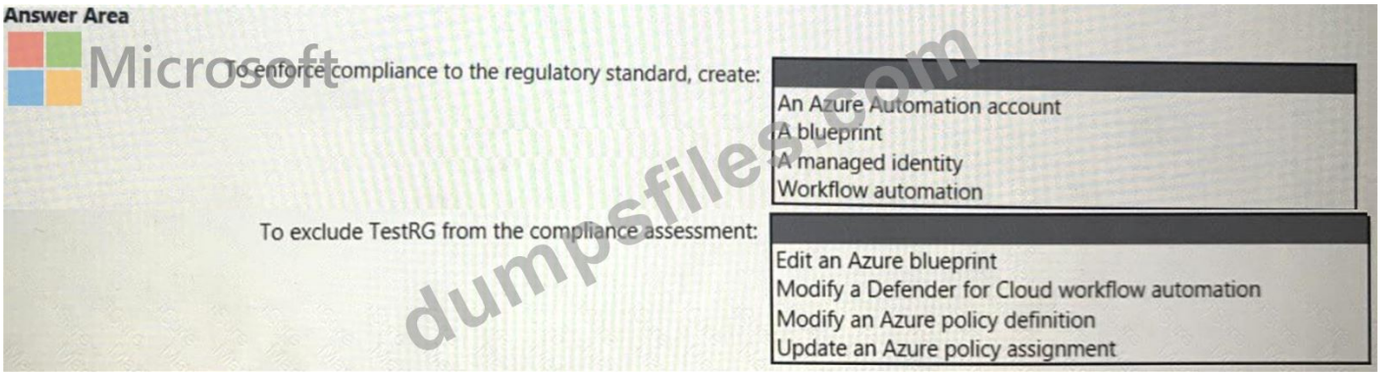
Graphical user interface Description automatically generated

NEW QUESTION: 20

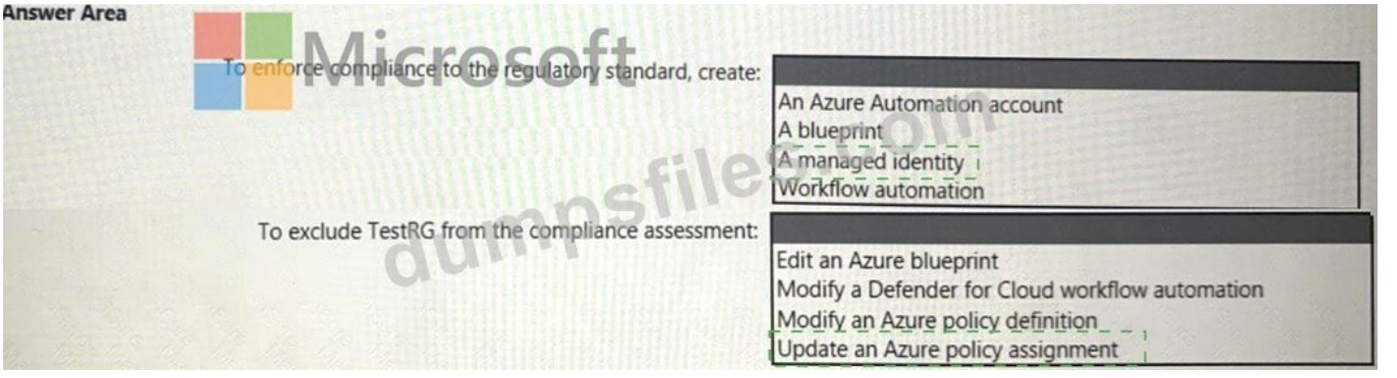
You need to recommend a solution to meet the compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation

NEW QUESTION: 21

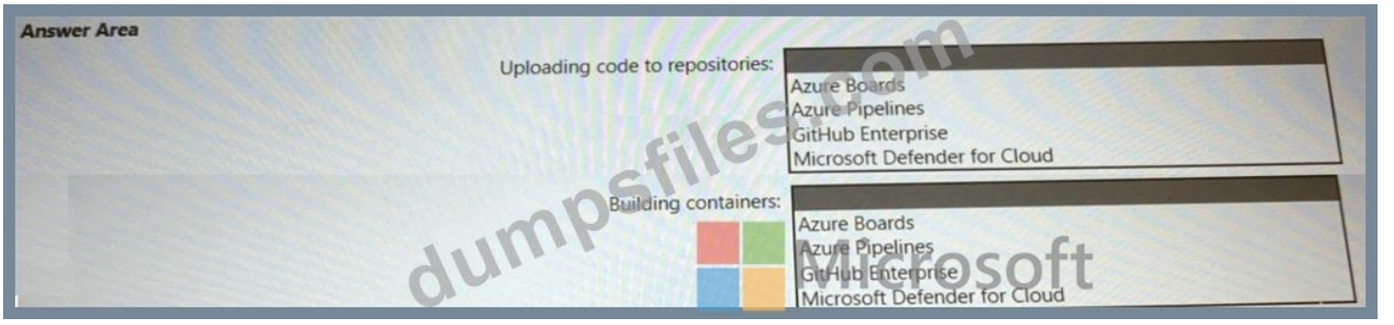
You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).

You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment

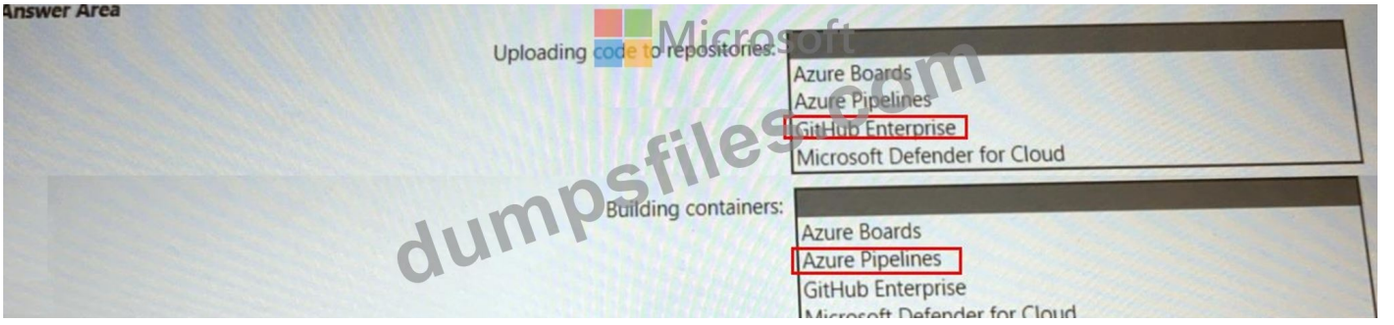
What should you include during the application design phase?

A. software decomposition by using Microsoft Visual Studio Enterprise
B. dynamic application security testing (DAST) by using Veracode
C. static application security testing (SAST) by using SonarQube
D. threat modeling by using the Microsoft Threat Modeling Tool
Answer: A (LEAVE A REPLY)

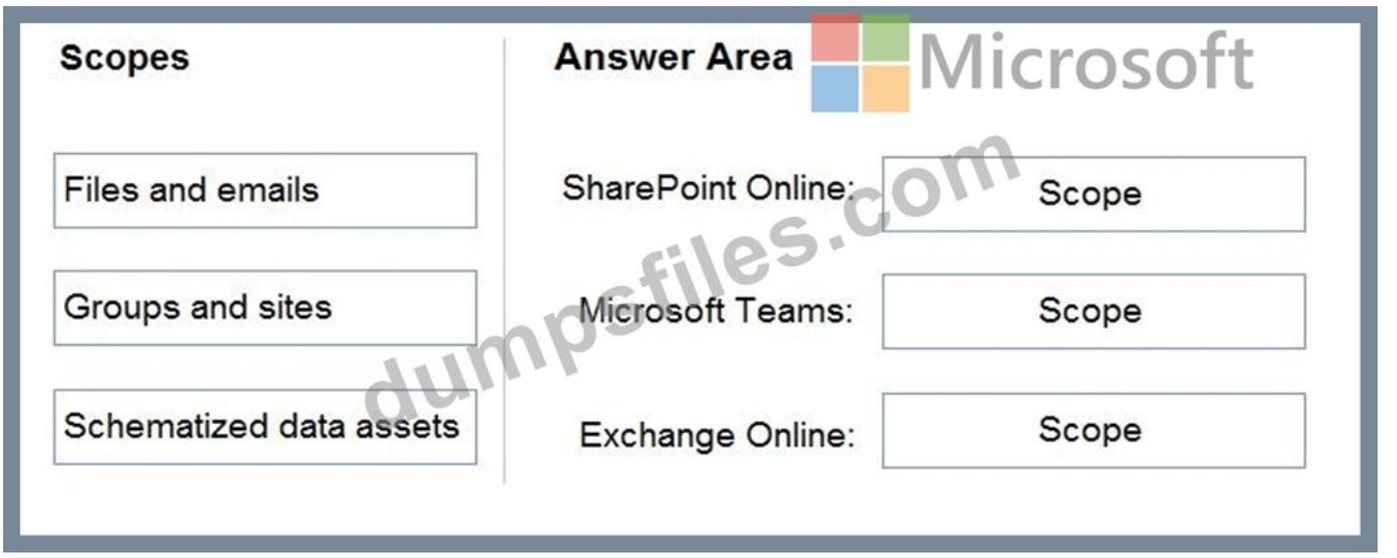
NEW QUESTION: 22
Your company has an Azure App Service plan that is used to deploy containerized web apps.
You are designing a secure DevOps strategy for deploying the web apps to the App Service plan.
You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:
Uploading the code to repositories Building containers
Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.



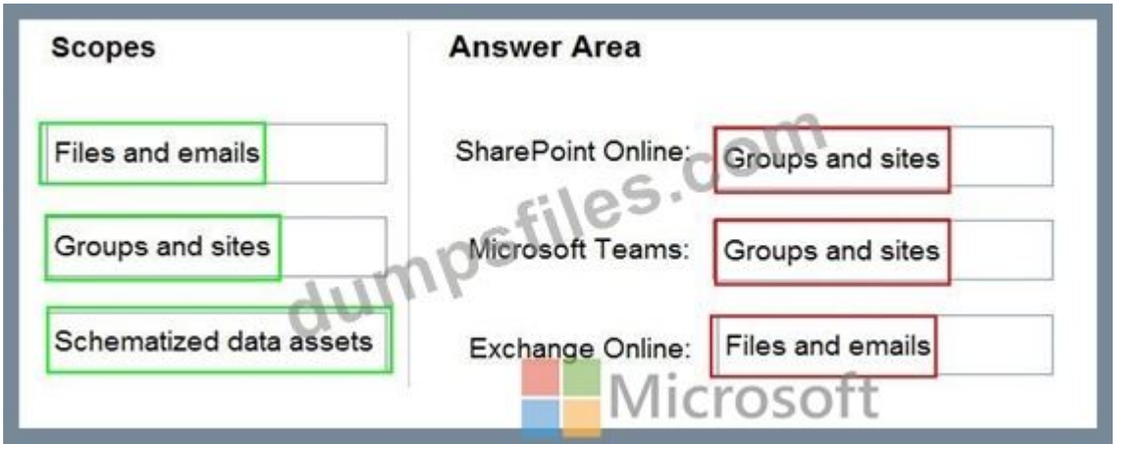
Answer:



NEW QUESTION: 23
Your company has Microsoft 365 E5 licenses and Azure subscriptions.
The company plans to automatically label sensitive data stored in the following locations:
* Microsoft SharePoint Online
* Microsoft Exchange Online
* Microsoft Teams
You need to recommend a strategy to identify and protect sensitive data.
Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 24

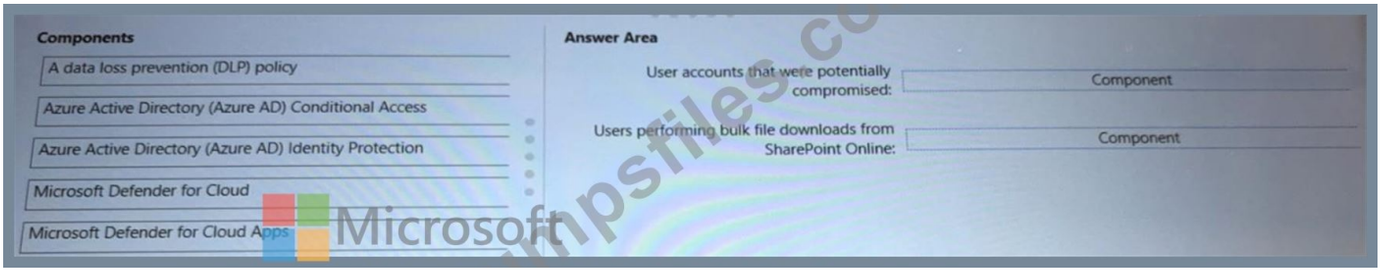
You have a Microsoft 365 subscription

You need to recommend a security solution to monitor the following activities:

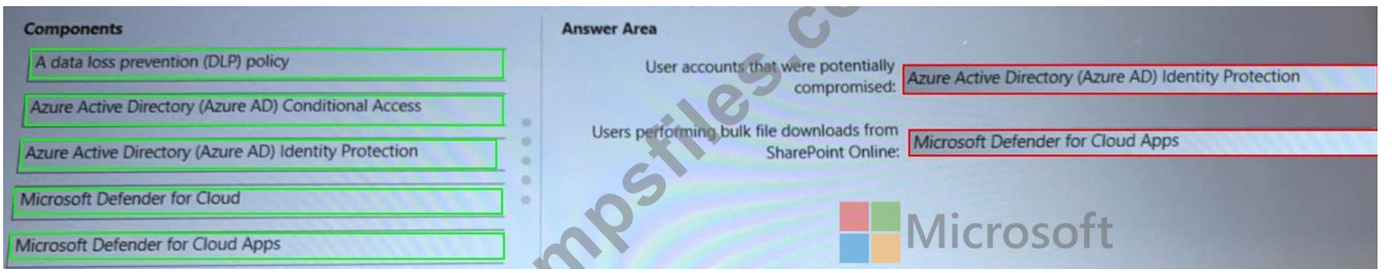
* User accounts that were potentially compromised

* Users performing bulk file downloads from Microsoft SharePoint Online What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each Correct selection is worth one Point.



Answer:



NEW QUESTION: 25

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

A. Transparent Data Encryption (TDE)

B. Always Encrypted

C. row-level security (RLS)

D. dynamic data masking

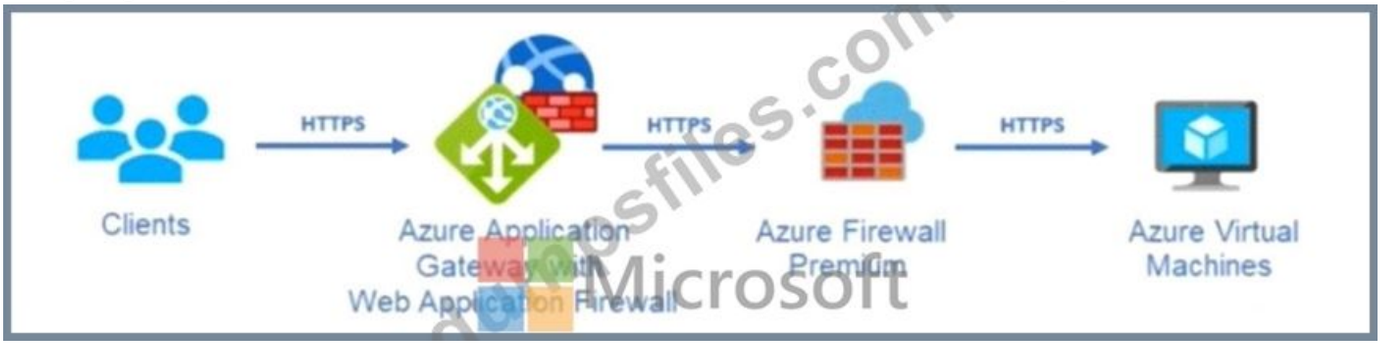
E. data classification

Answer: (SHOW ANSWER)

https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-enclaves

NEW QUESTION: 26

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.

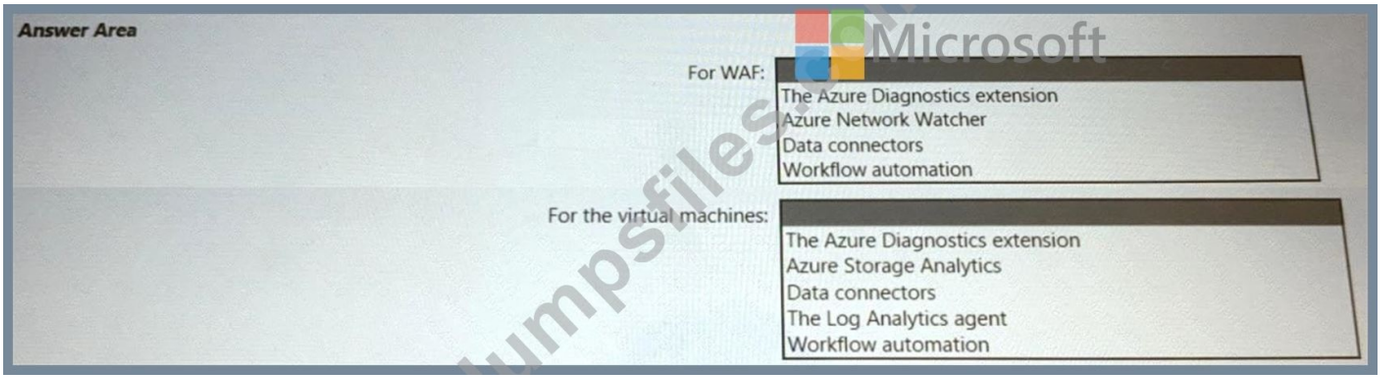


You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

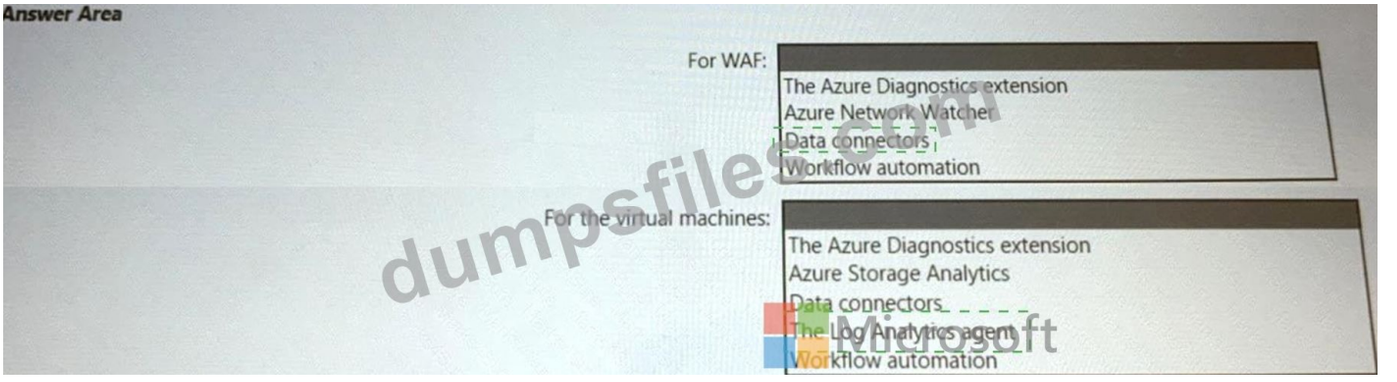
* Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
* Use Defender for Cloud to review alerts from the virtual machines.

What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE:

Each correct selection is worth one point.



Answer:



Explanation:

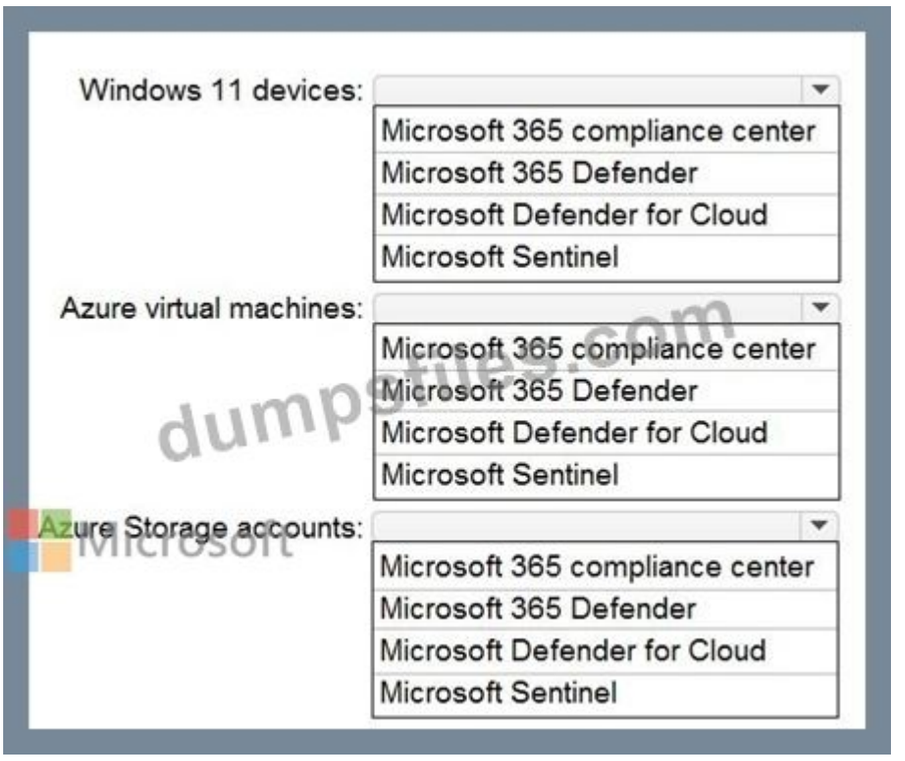
Graphical user interface Description automatically generated

NEW QUESTION: 27

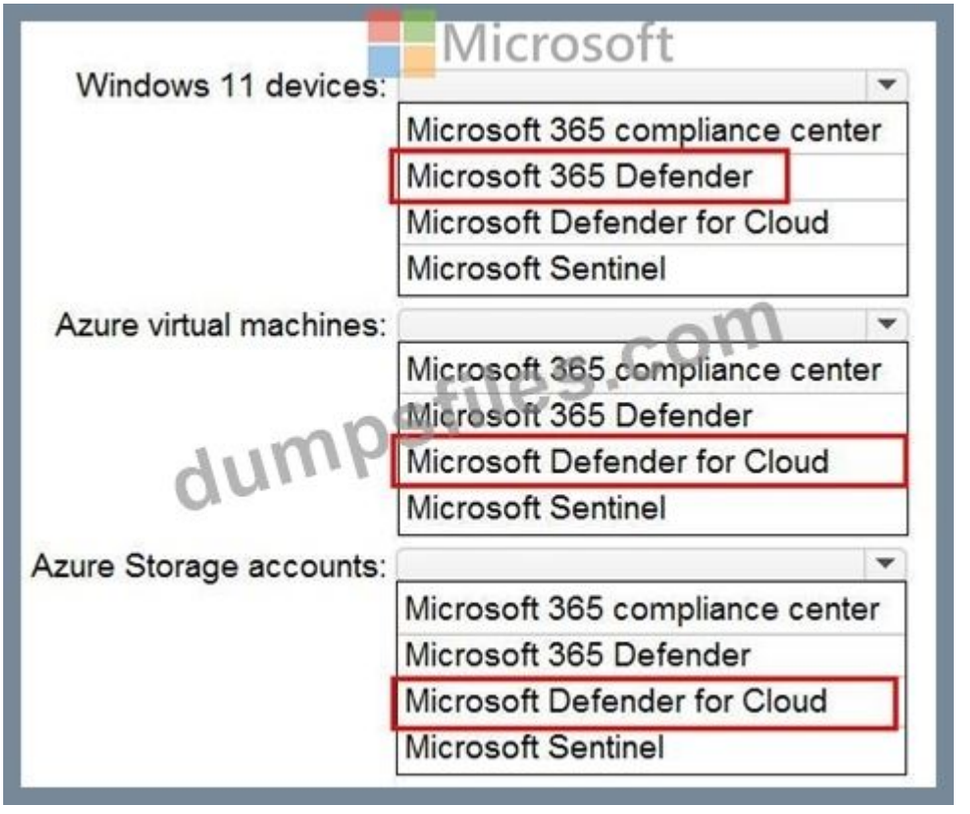
You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:

* Windows 11 devices managed by Microsoft Intune
* Azure Storage accounts
* Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.



Answer:

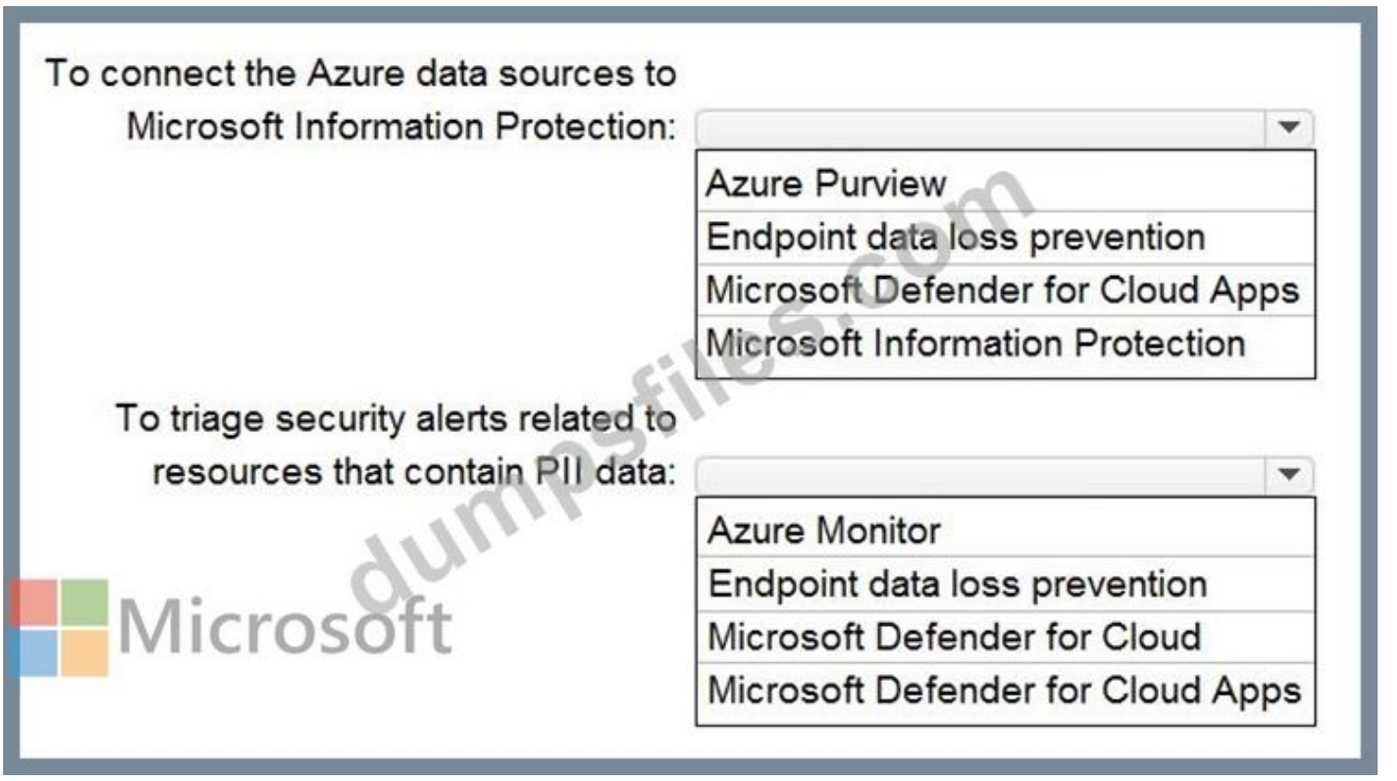


NEW QUESTION: 28

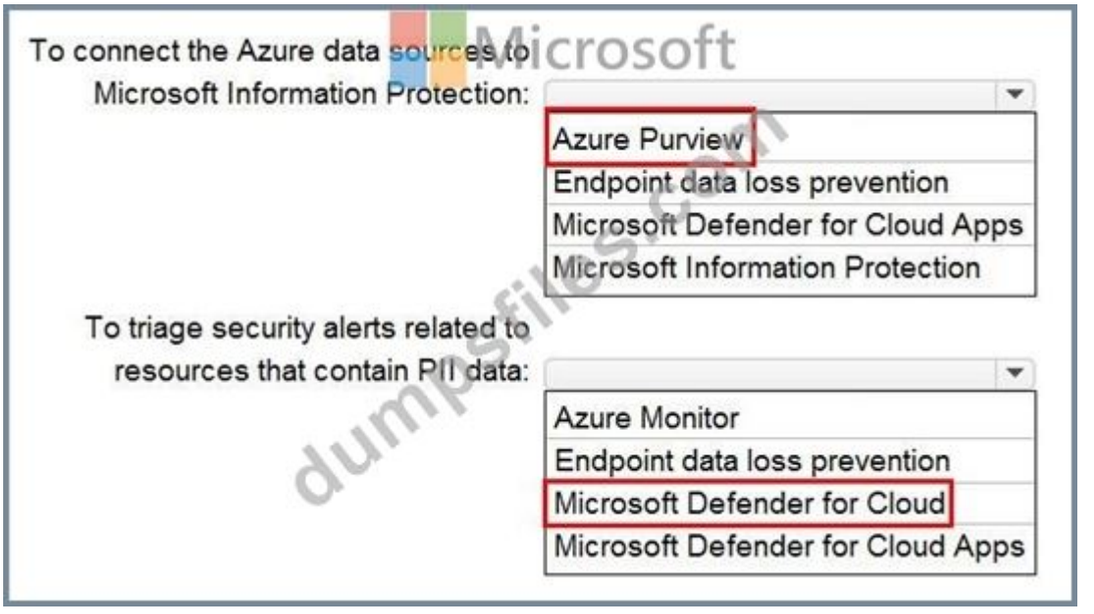
Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The company plans to use Microsoft Information Protection for the PII data store in Azure.

You need to recommend a solution to discover PII data at risk in the Azure resources.

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



Answer:

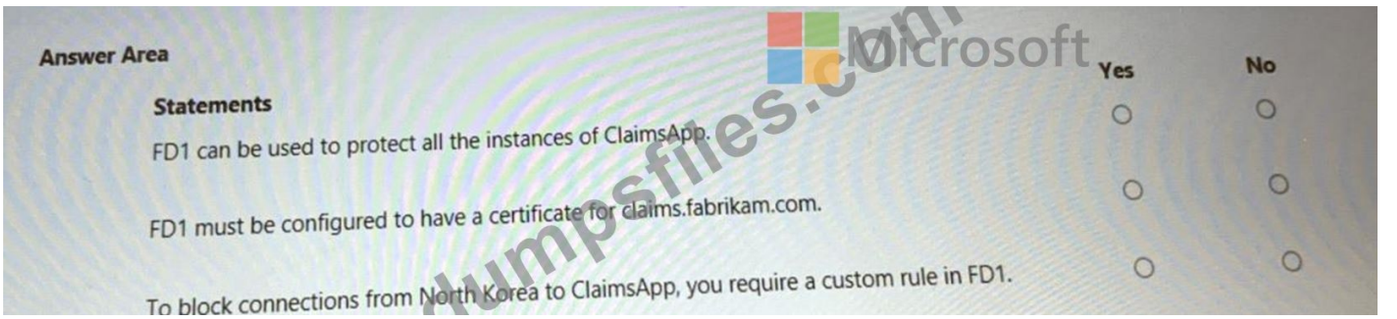


NEW QUESTION: 29

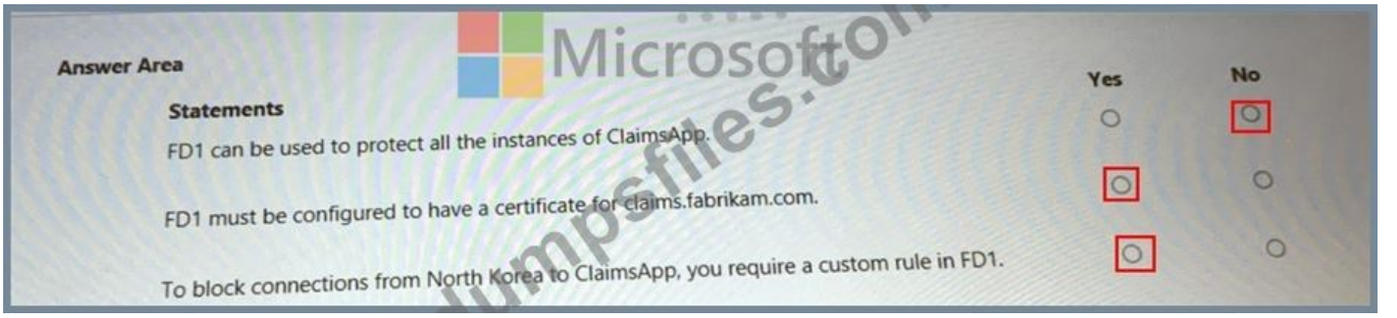
You are evaluating the security of ClaimsApp.

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:



NEW QUESTION: 30

You have Microsoft Defender for Cloud assigned to Azure management groups.

You have a Microsoft Sentinel deployment.

During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. threat intelligence reports in Defender for Cloud

B. Microsoft Sentinel notebooks

C. workload protections in Defender for Cloud

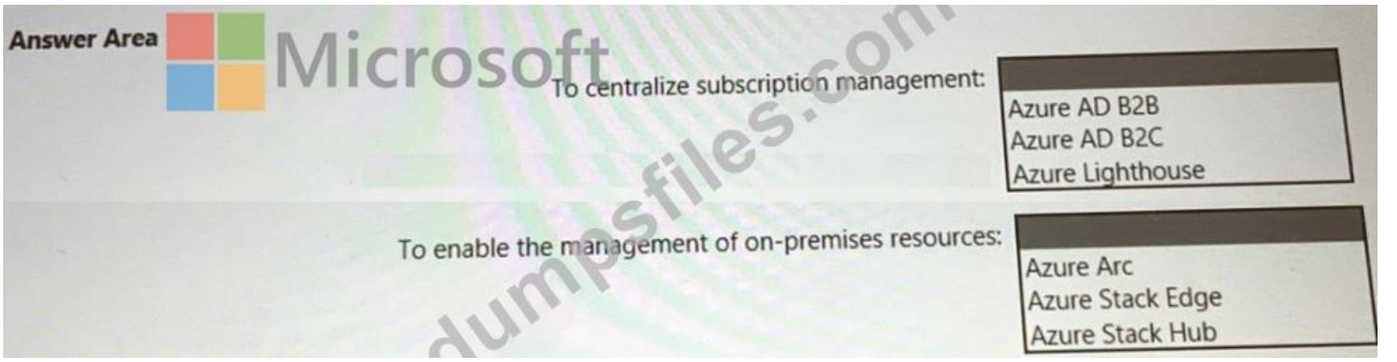
D. Microsoft Sentinel threat intelligence workbooks

Answer: C (LEAVE A REPLY)

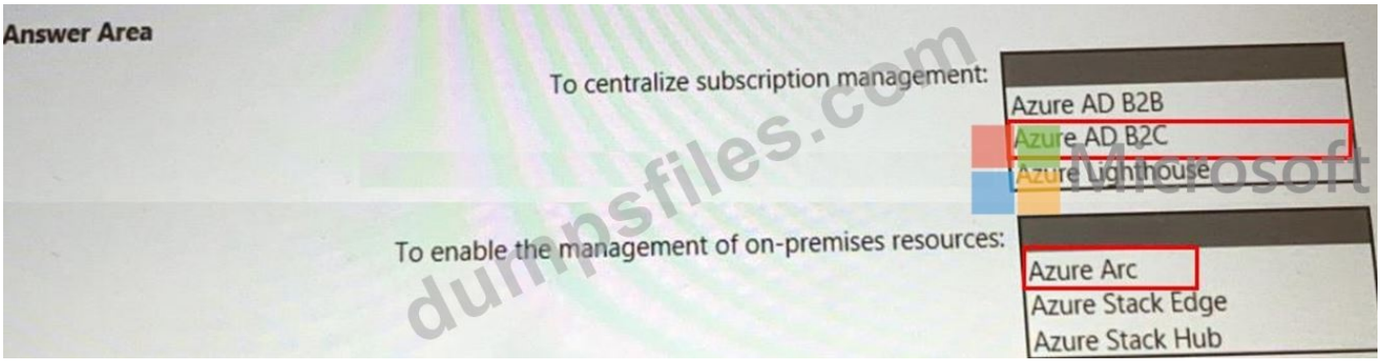
NEW QUESTION: 31

You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer are

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



Answer:



NEW QUESTION: 32
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend configuring gateway-required virtual network integration.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure

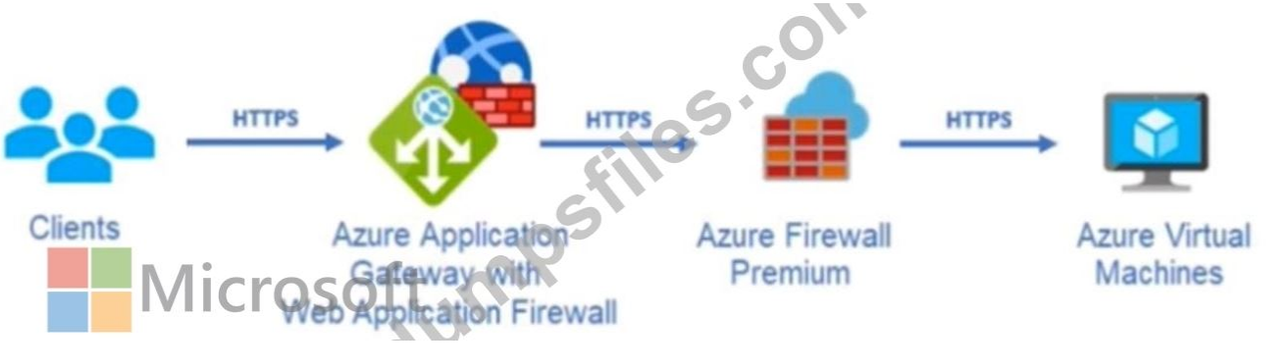
NEW QUESTION: 33
You have an operational model based on the Microsoft Cloud Adoption framework for Azure.
You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, database, files, and storage accounts.
What should you include in the recommendation?
A. security baselines in the Microsoft Cloud Security Benchmark
B. modern access control
C. network isolation

D. business resilience
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
You have a Microsoft 365 tenant.
Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:
* Users must be able to request access to App1 by using a self-service request.
* When users request access to App1, they must be prompted to provide additional information about their request.
* Every three months, managers must verify that the users still require access to Appl.
What should you include in the design?
A. Azure AD Application Proxy
B. connected apps in Microsoft Defender for Cloud Apps
C. Microsoft Entra Identity Governance
D. access policies in Microsoft Defender for Cloud Apps
Answer: C (LEAVE A REPLY)
a

NEW QUESTION: 35
You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.
You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.
What should you include in the recommendation?
A. Apply read-only locks on the storage accounts.
B. Set the AllowSharcdKeyAccess property to false.
C. Set the AllowBlobPublicAcccss property to false.
D. Configure automated key rotation.
Answer: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

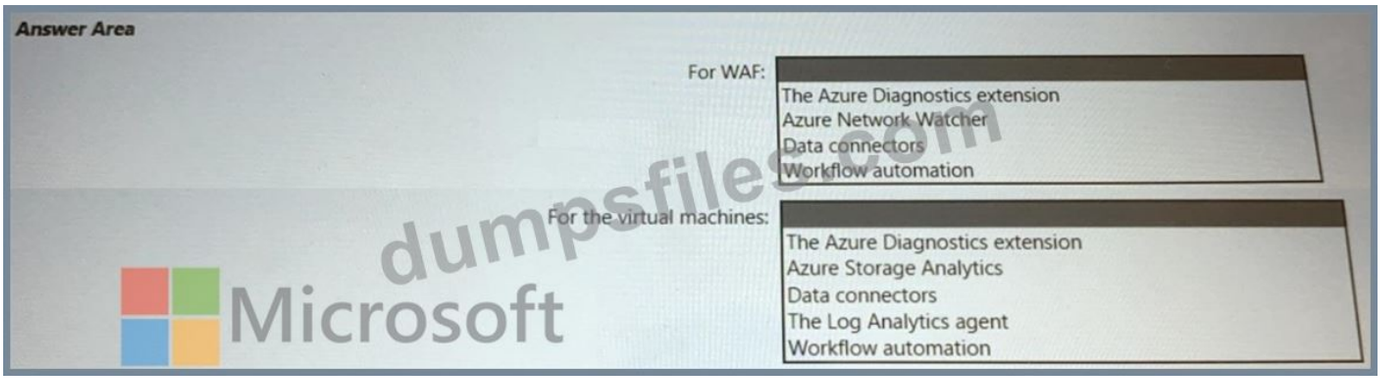
NEW QUESTION: 36
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



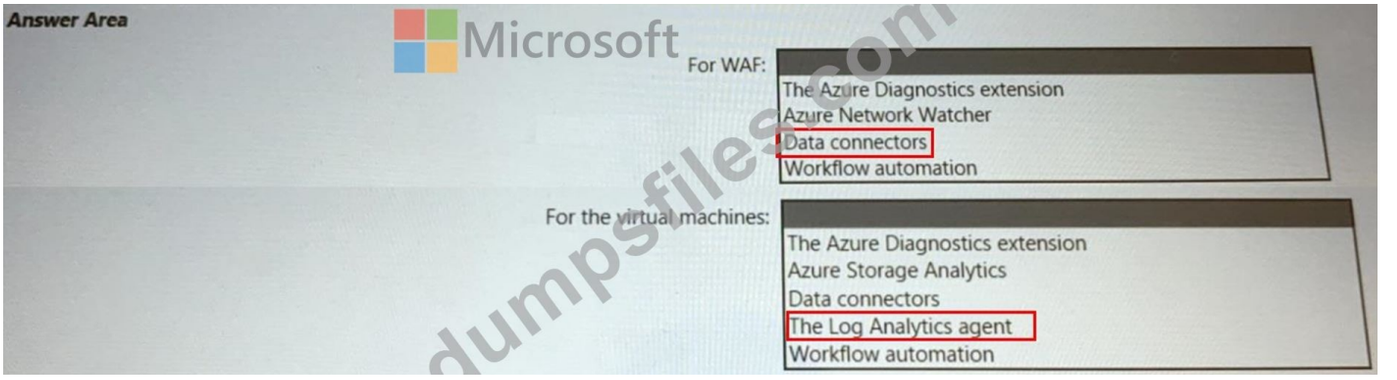
You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

* Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
* Use Defender for Cloud to review alerts from the virtual machines.

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



Answer:



NEW QUESTION: 37

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD) The customer plans to obtain an Azure subscription and provision several Azure resources.

You need to evaluate the customer's security environment.

What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

A. role-based authorization

B. Azure AD Privileged Identity Management (PIM)

C. resource-based authorization

D. Azure AD Multi-Factor Authentication

Answer: B (LEAVE A REPLY)

Explanation

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

https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing?rtc=1

NEW QUESTION: 38

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

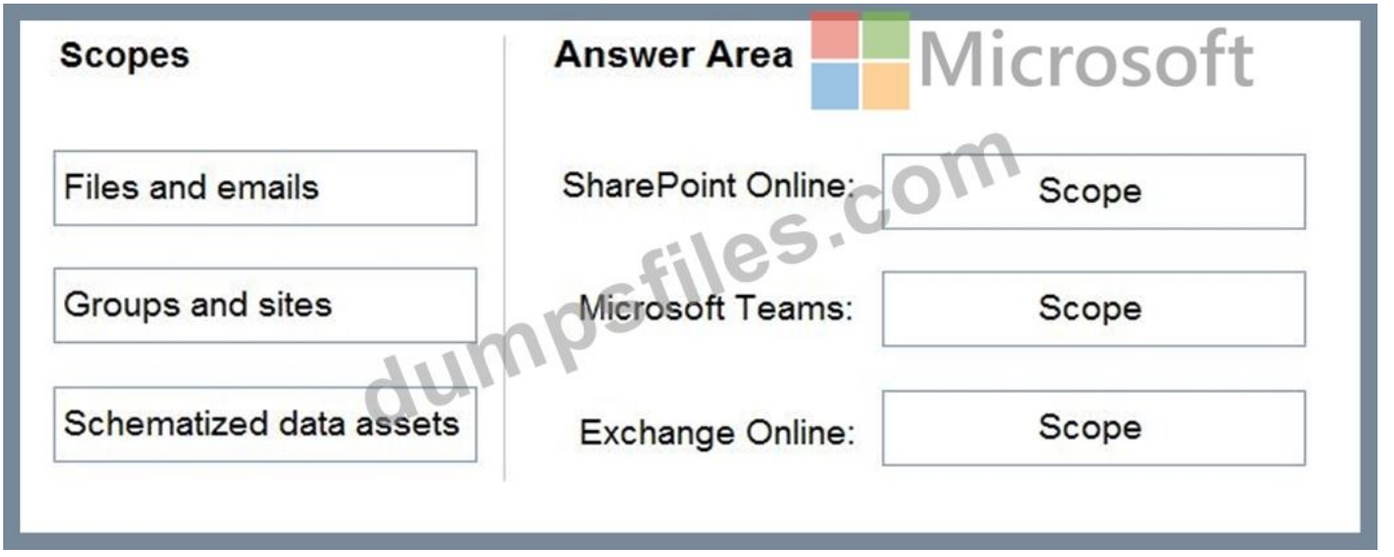
The company plans to automatically label sensitive data stored in the following locations:

* Microsoft SharePoint Online
* Microsoft Exchange Online
* Microsoft Teams

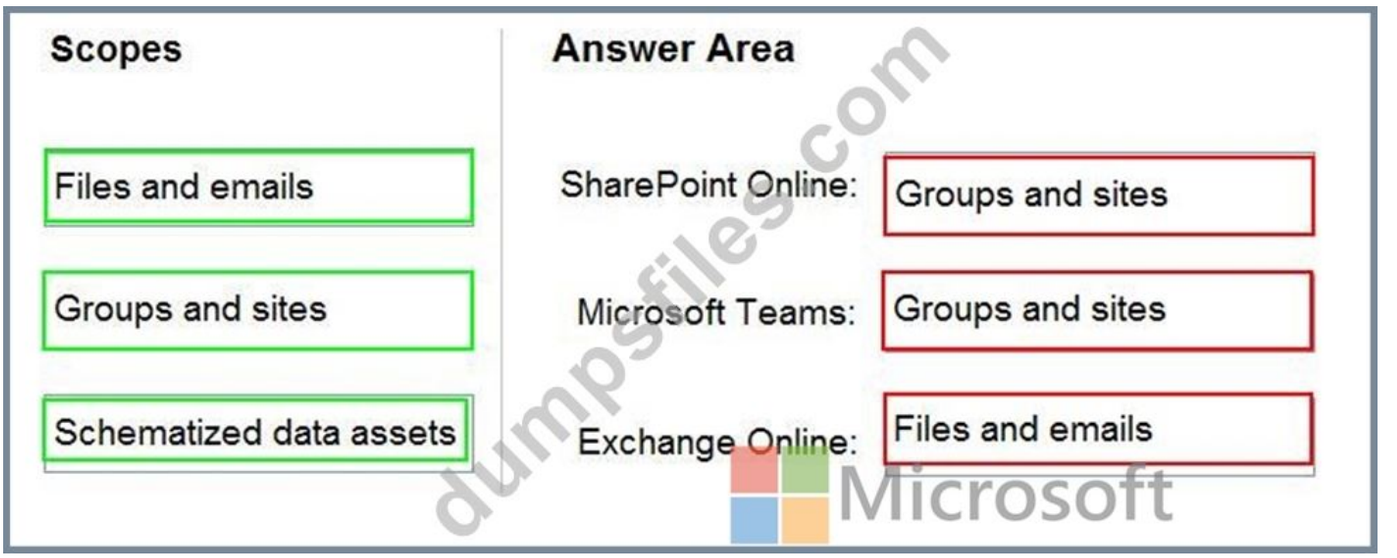
You need to recommend a strategy to identify and protect sensitive data.

Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



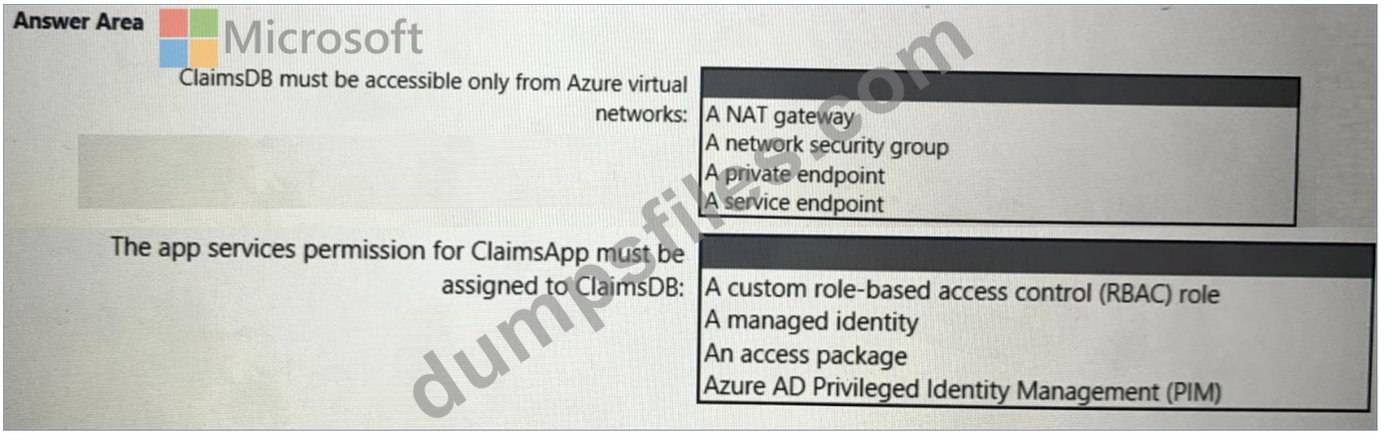
Answer:



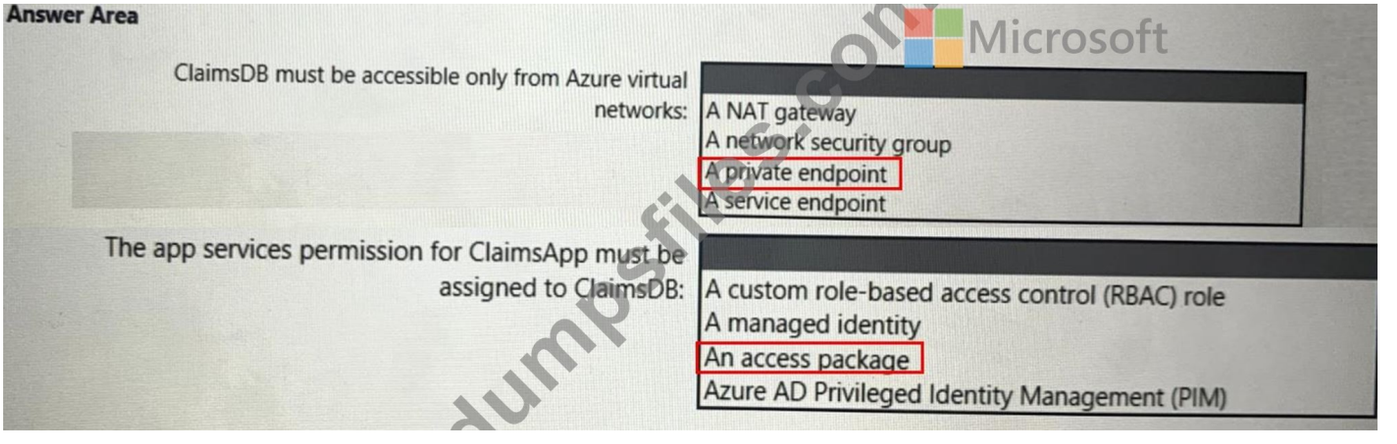
NEW QUESTION: 39

You need to recommend a solution to meet the requirements for connections to ClaimsDB. What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



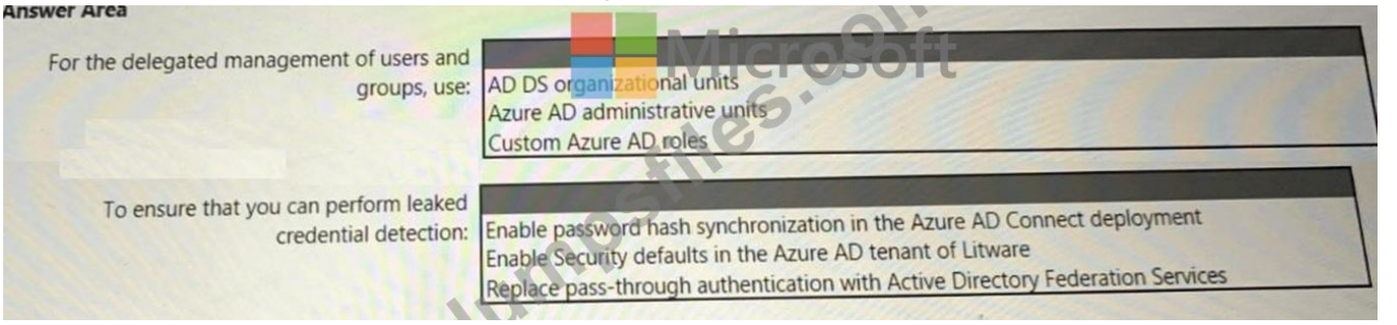
Answer:



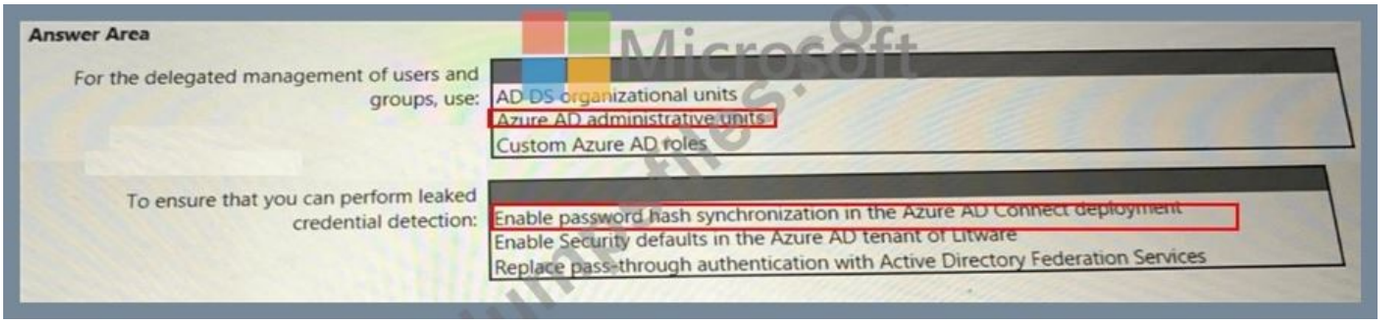
NEW QUESTION: 40

You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

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

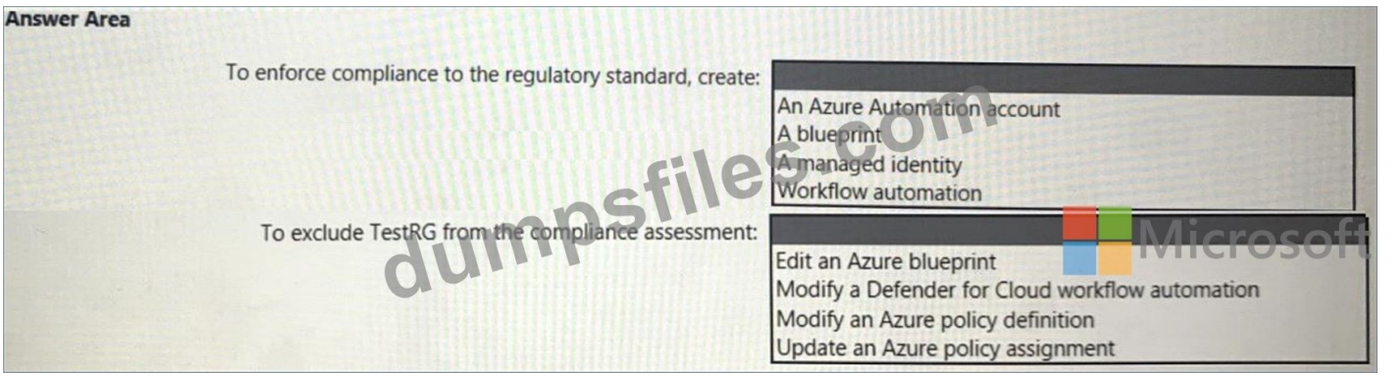


Answer:



NEW QUESTION: 41
Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.
A. Azure Active Directory (Azure AD Privileged Identity Management (PIM)
B. Azure Web Application Firewall (WAF)
C. Microsoft Defender for Cloud alerts
D. Microsoft Sentinel
E. Azure Firewall
Answer: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION: 42
You need to recommend a solution to meet the compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

NEW QUESTION: 43

You are designing the security architecture for a cloud-only environment.

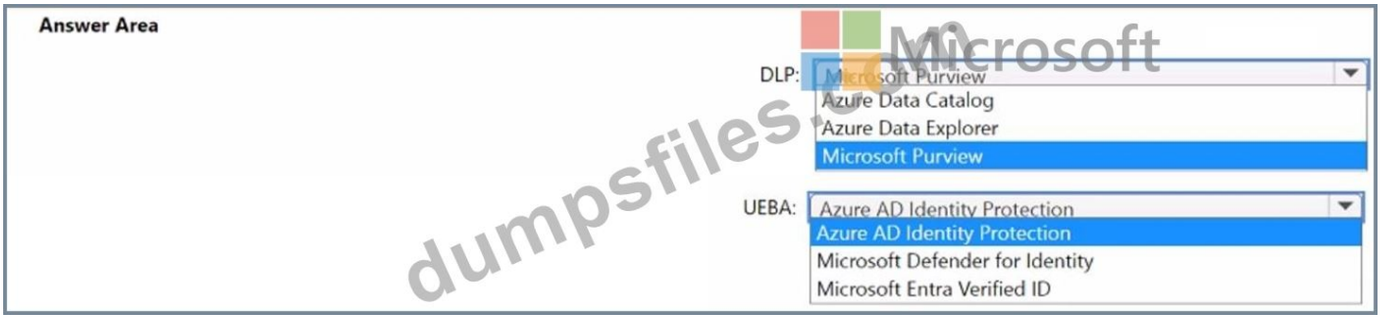
You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

* Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.

* Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

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

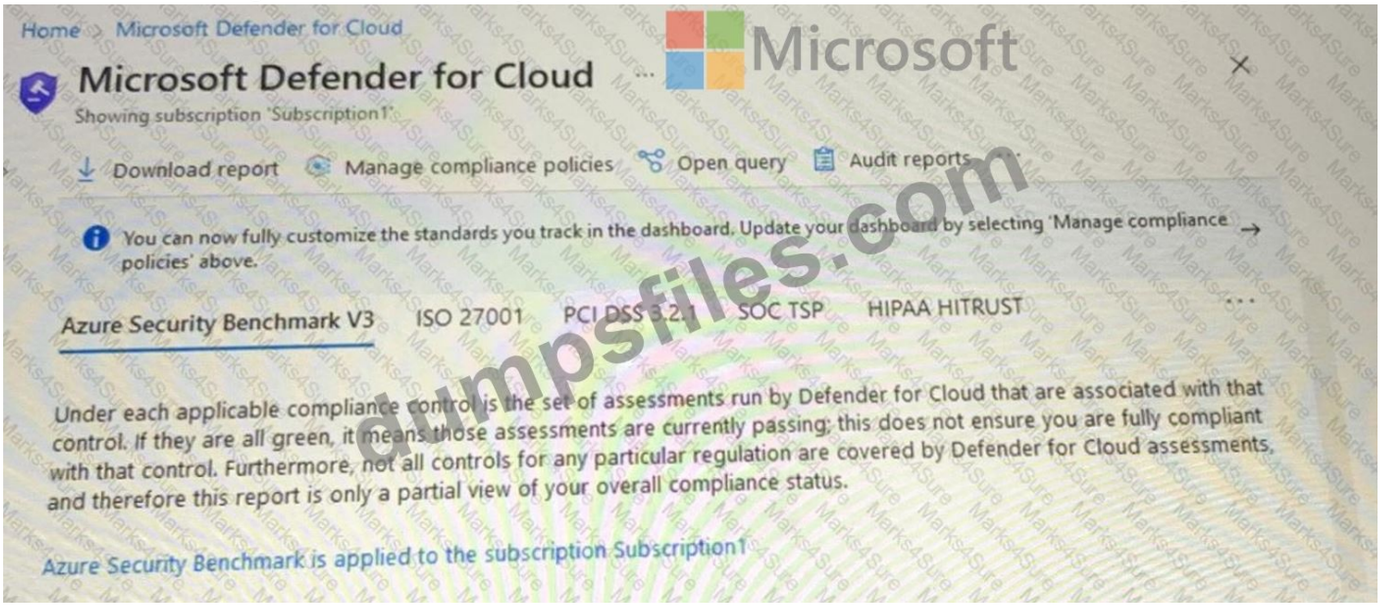


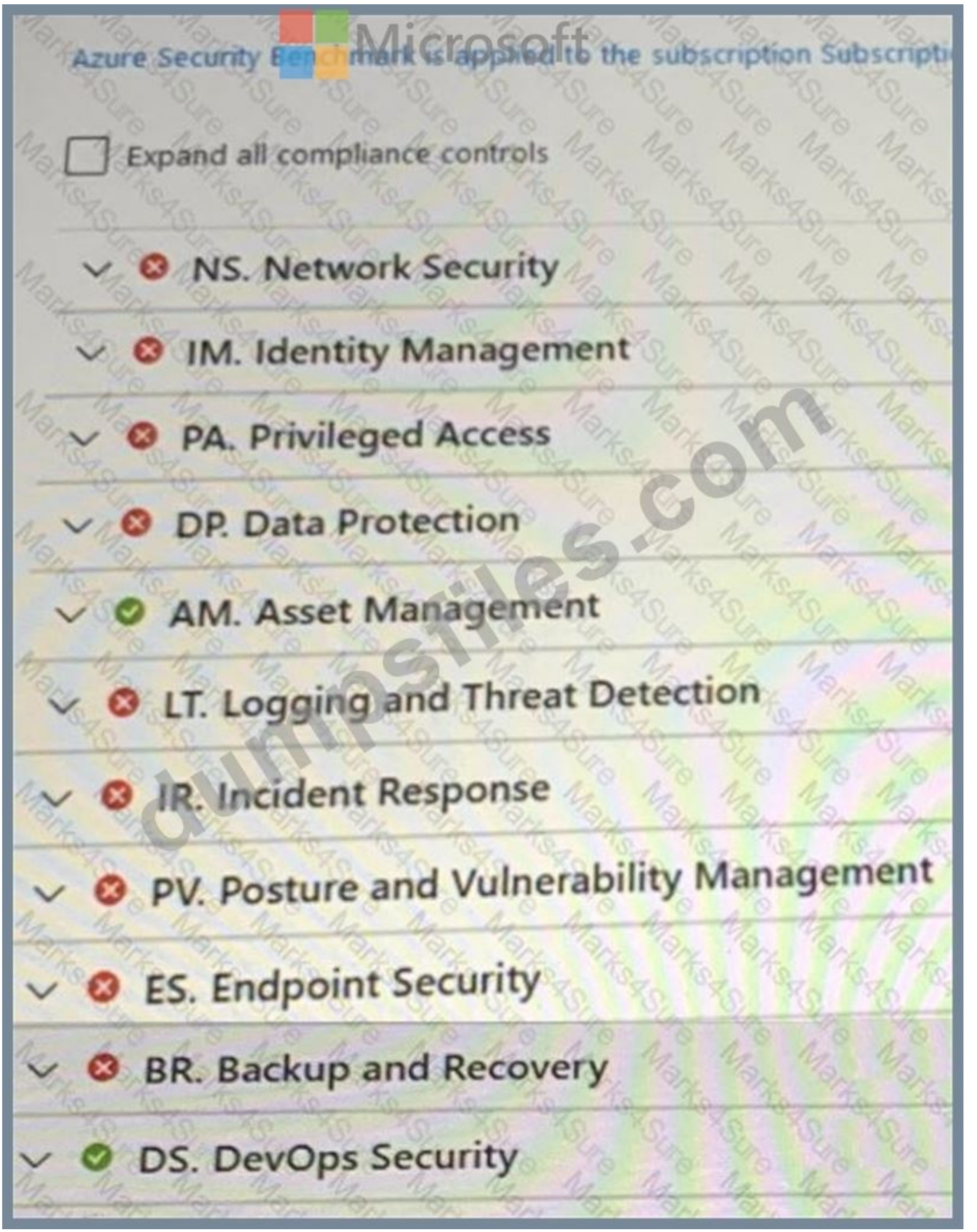
Answer:

NEW QUESTION: 44

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.





You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

A. Data Protection

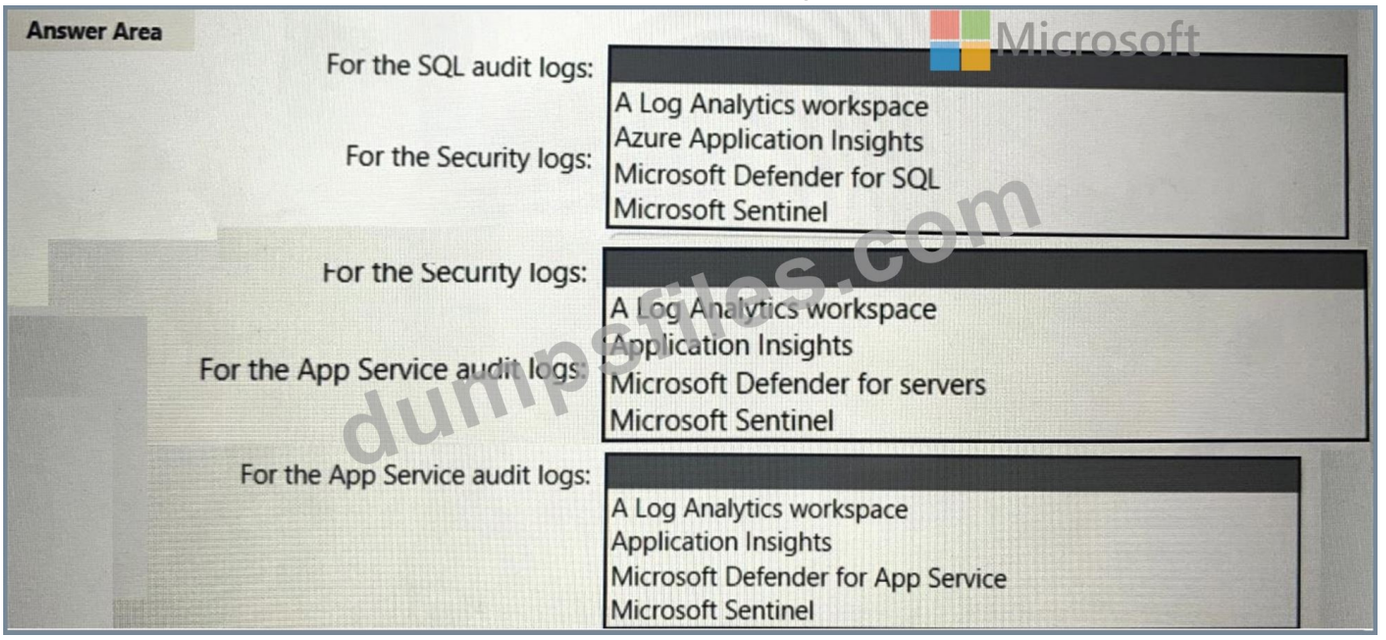
B. Incident Response

C. Posture and Vulnerability Management
D. Asset Management
E. Endpoint Security
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

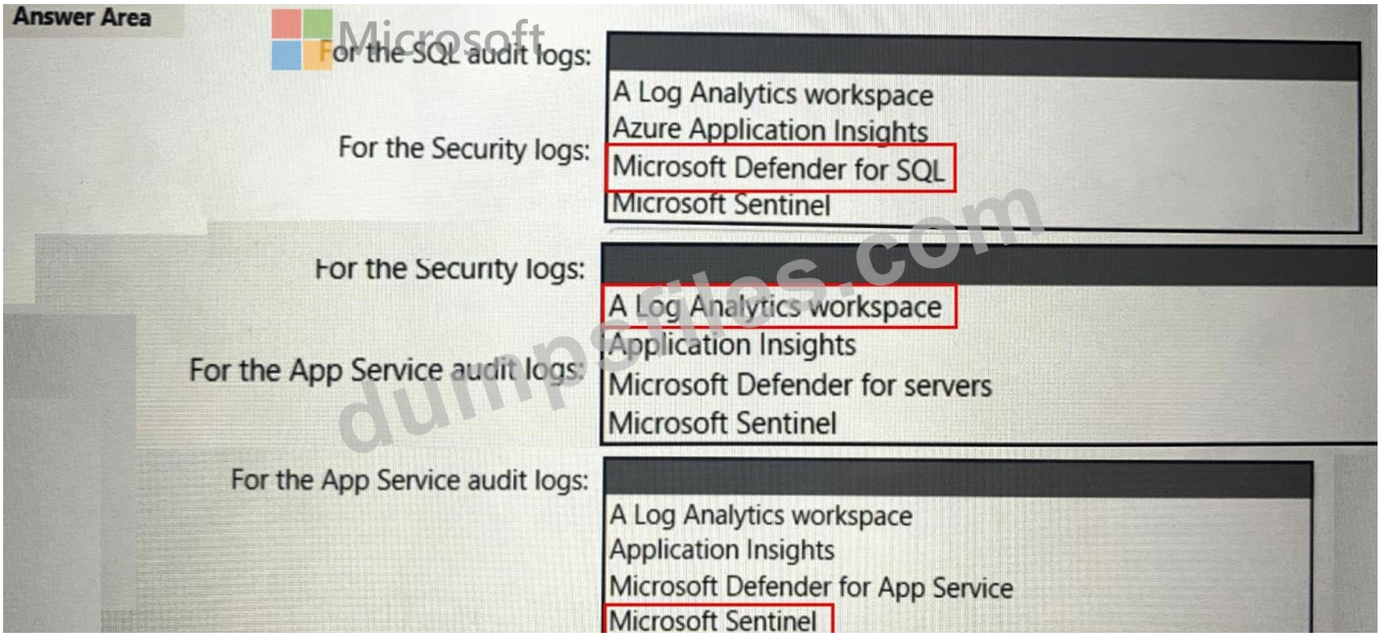
NEW QUESTION: 45
Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.
The company's security policy prevents the use of personal devices for accessing company data and applications.
You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.
What should you include in the recommendation?
A. Migrate the on-premises applications to cloud-based applications.
B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.
Answer: D (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop
https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cl

NEW QUESTION: 46
You are designing an auditing solution for Azure landing zones that will contain the following components:
* SQL audit logs for Azure SQL databases
* Windows Security logs from Azure virtual machines
* Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
* Log all privileged access.
* Retain logs for at least 365 days.
* Minimize costs.

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

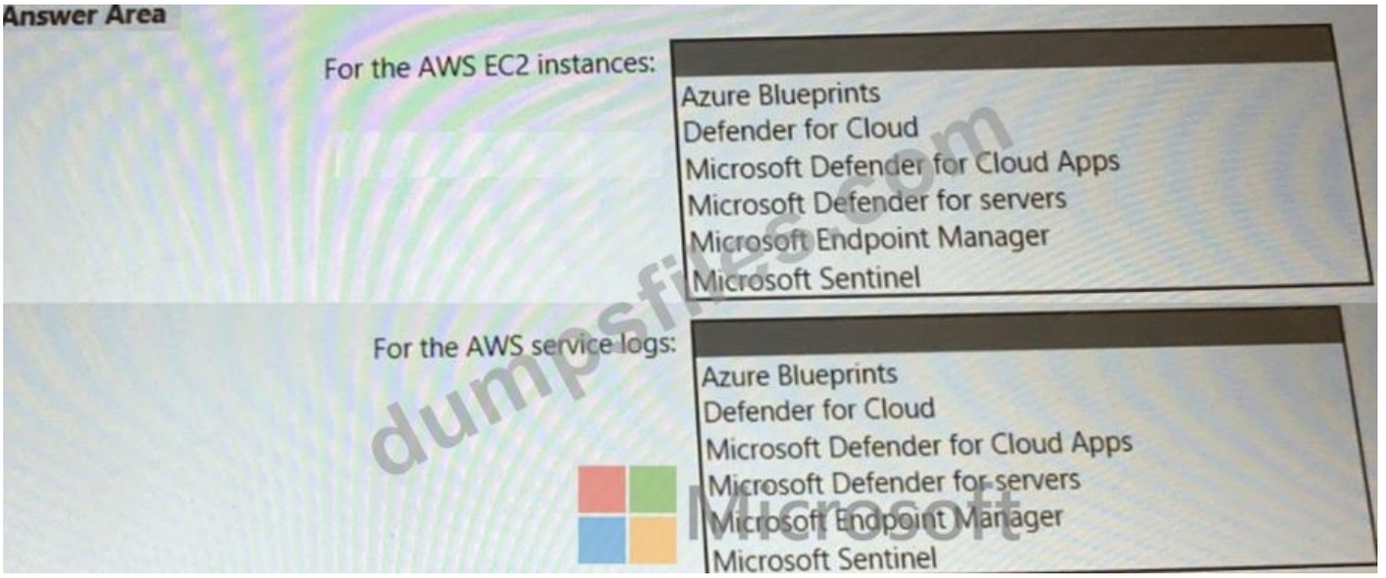


Answer:

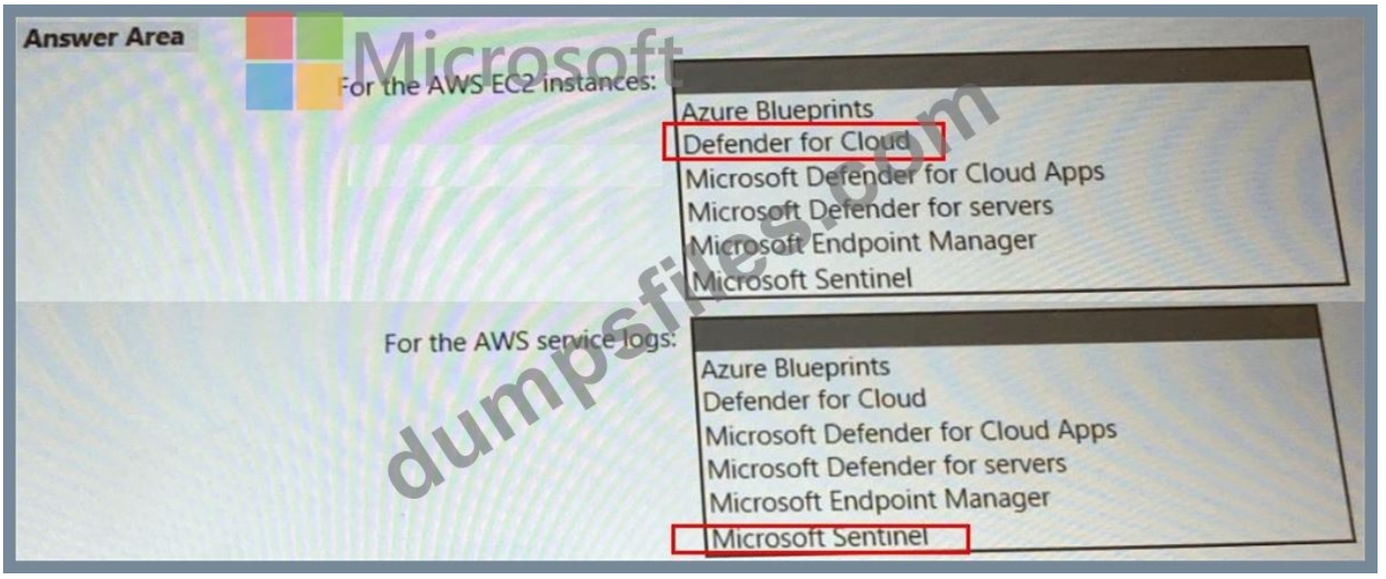


NEW QUESTION: 47

You need to recommend a solution to meet the AWS requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 48
You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.
What should you configure for each landing zone?
A. Azure DDoS Protection Standard
B. an Azure Private DNS zone
C. Microsoft Defender for Cloud
D. an ExpressRoute gateway
Answer: (SHOW ANSWER)
One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive.

Given the landing zone requirements of
1) "Use a DNS namespace of litware.com"
2) "Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints"

NEW QUESTION: 49
You are evaluating the security of ClaimsApp.
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:

OverView
Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.
On-premises Environment
The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.
Azure Environment
Fabrikam has the following Azure resources:
* An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com
* A single Azure subscription named Sub1
* A virtual network named Vnetl in the East US Azure region
* A virtual network named Vnet2 in the West Europe Azure region
* An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled
* A Microsoft Sentinel workspace
* An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

* 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
* A resource group named TestRG that is used for testing purposes only
* An Azure Virtual Desktop host pool that contains personal assigned session hosts All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-.
* An Azure AD tenant named contoso.onmicrosoft.com
* An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:
* Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
* Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
* Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification
* ClaimsApp will be deployed to Azure App Service instances that connect to Vnetl and Vnet2.
* Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
* ClaimsApp will access data in ClaimsDB.
* ClaimsDB must be accessible only from Azure virtual networks.
* The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:
* Azure DevTest labs will be used by developers for testing.
* All the application code must be stored in GitHub Enterprise.
* Azure Pipelines will be used to manage application deployments.

* All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.
Security Requirement
Fabrikam identifies the following security requirements:
* Internet-accessible applications must prevent connections that originate in North Korea.
* Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
* Administrators must connect to a secure host to perform any remote administration of the virtual machines.
The secure host must be provisioned from a custom operating system image.
AWS Requirements
Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.
* Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
* Ensure that the security administrators can query AWS service logs directly from the Azure environment.
Contoso Developer Requirements
Fabrikam identifies the following requirements for the Contoso developers;
* Every month, the membership of the ContosoDevelopers group must be verified.
* The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
* The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.
Compliance Requirement
Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

NEW QUESTION: 50
You have a Microsoft 365 E5 subscription.
You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.
You need to recommend a solution to prevent Personally Identifiable Information (Pll) from being shared.
Which two components should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. data loss prevention (DLP) policies
B. sensitivity label policies
C. retention label policies

D. eDiscovery cases

Answer: (SHOW ANSWER)

Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate. Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.

https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/

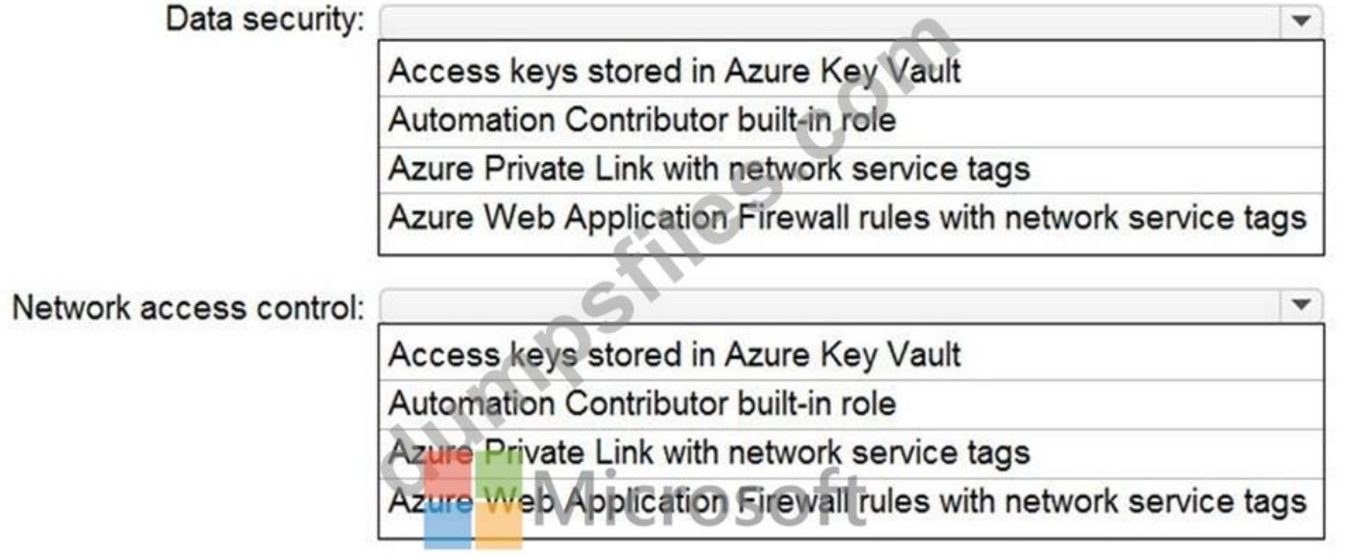
https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

NEW QUESTION: 51

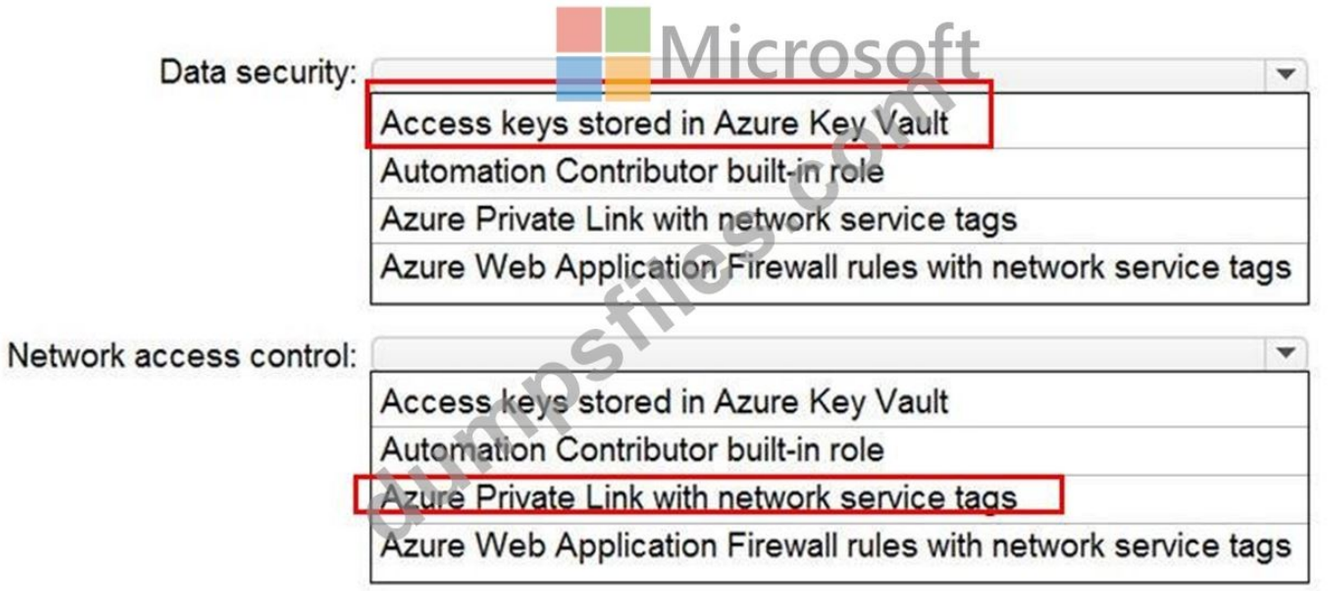
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

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



Answer:



NEW QUESTION: 52

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation? (Choose Two)

A. Onboard the virtual machines to Microsoft Defender for Endpoint.

B. Onboard the virtual machines to Azure Arc.

C. Create a device compliance policy in Microsoft Endpoint Manager.

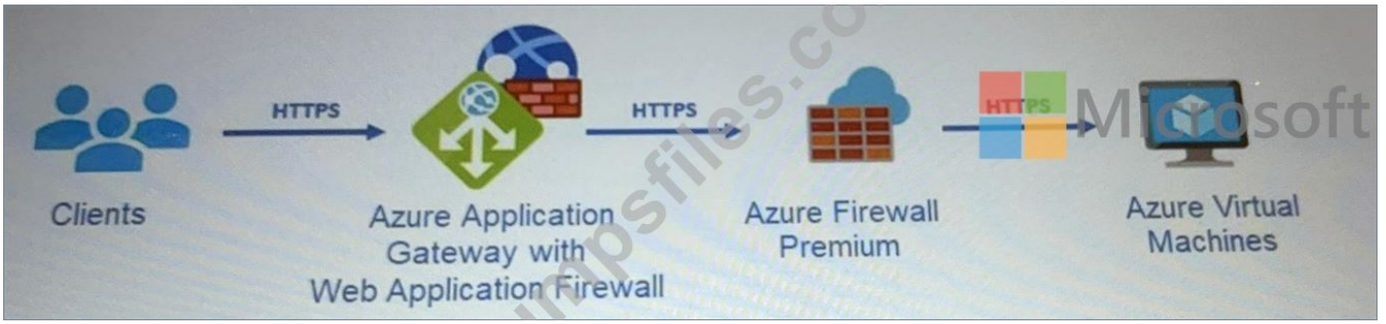
D. Enable the Qualys scanner in Defender for Cloud.

Answer: A,B (LEAVE A REPLY)

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-worldwide

NEW QUESTION: 53

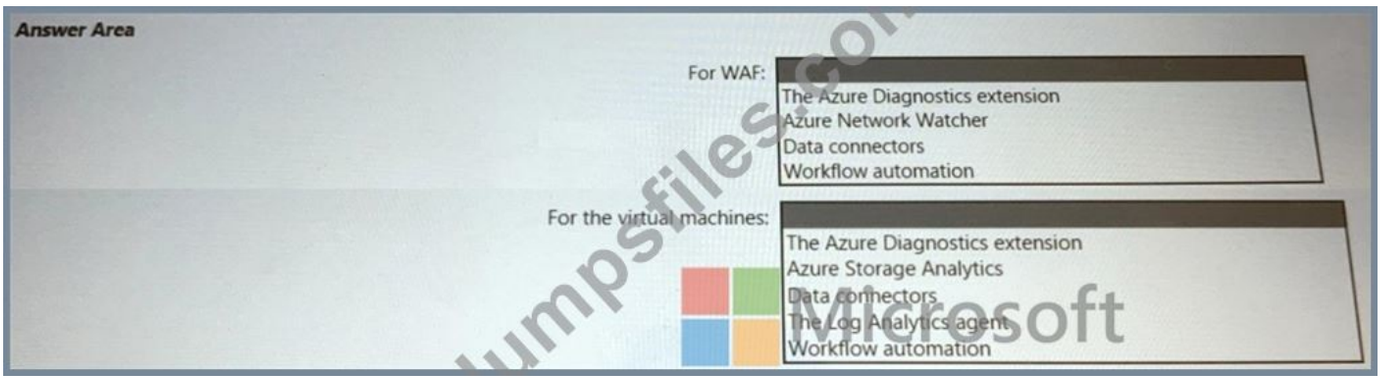
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



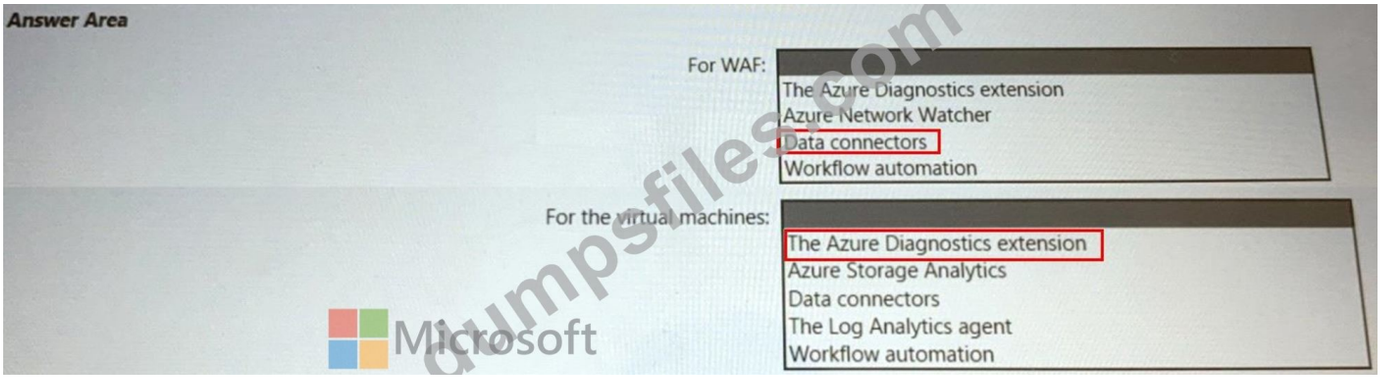
You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

* Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
* Use Defender for Cloud to review alerts from the virtual machines.

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



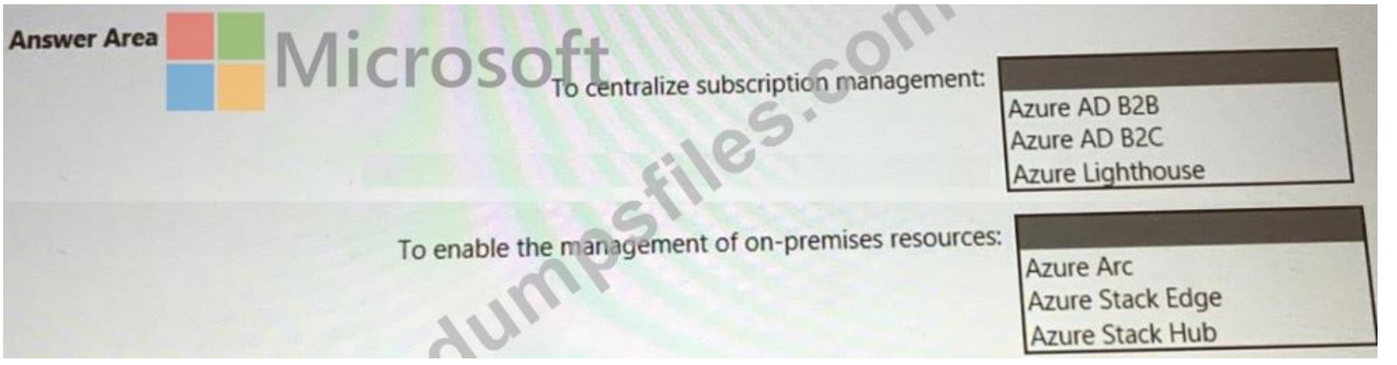
Answer:



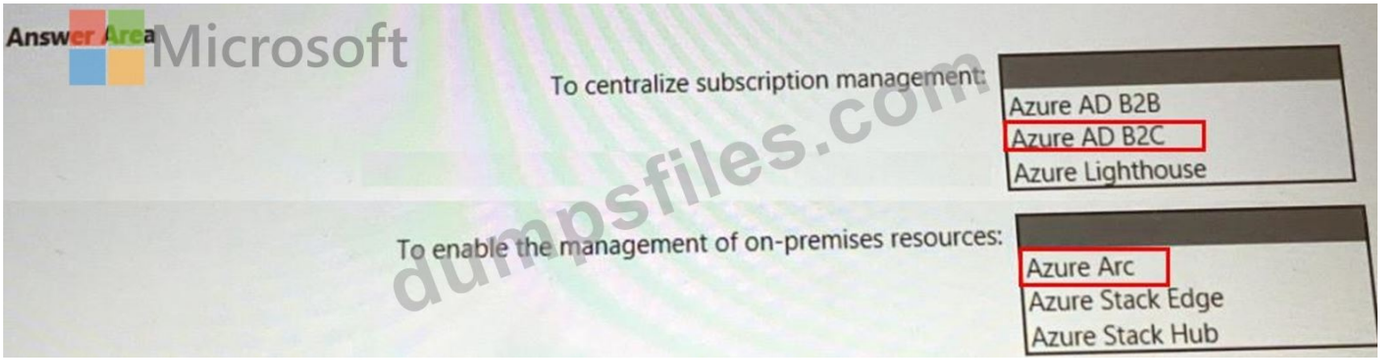
NEW QUESTION: 54

You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer are

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

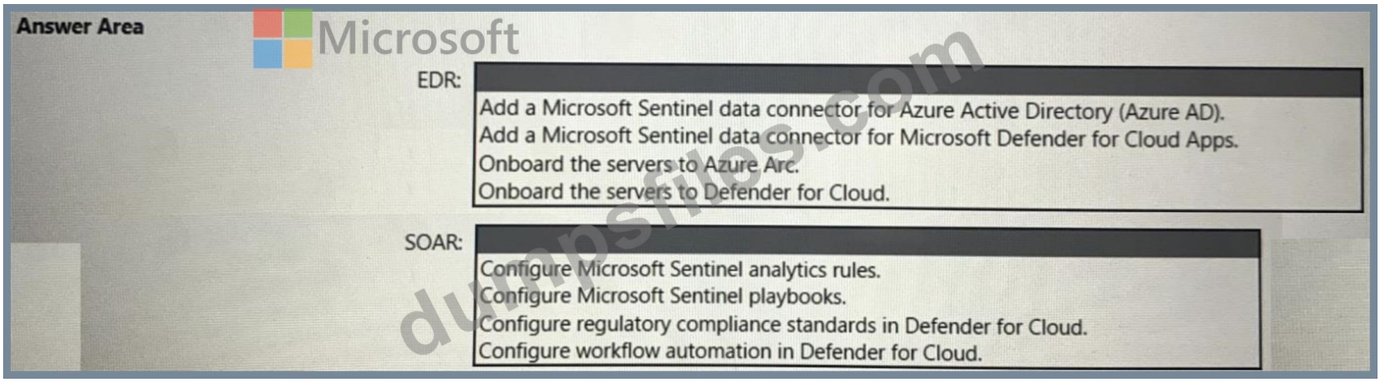


Answer:

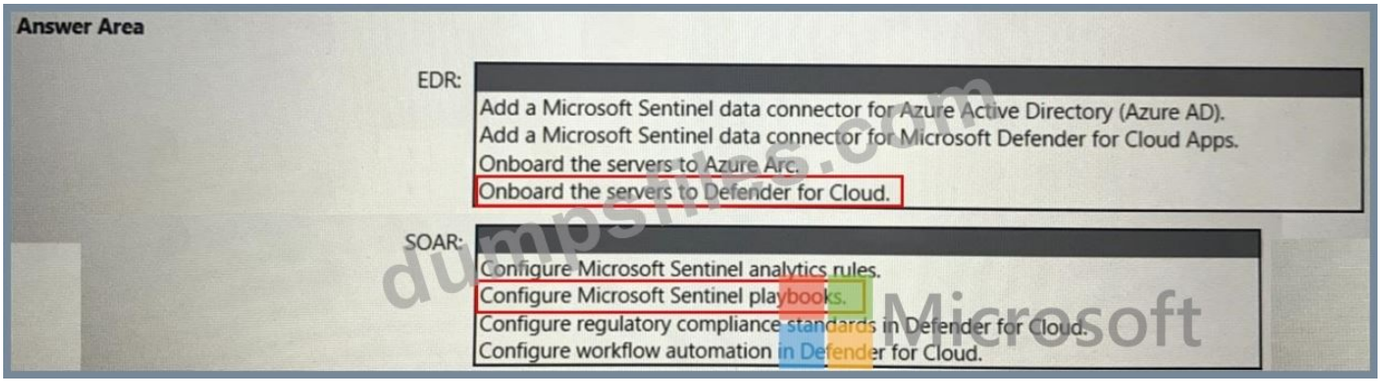


NEW QUESTION: 55

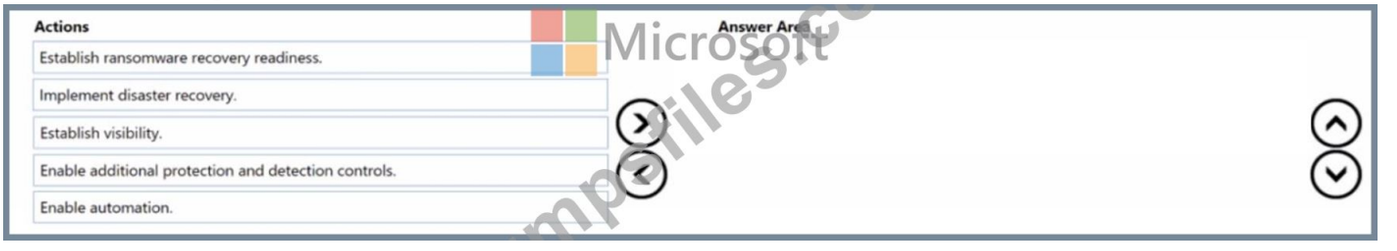
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.
You plan to deploy Azure virtual machines that will run Windows Server.
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.
How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



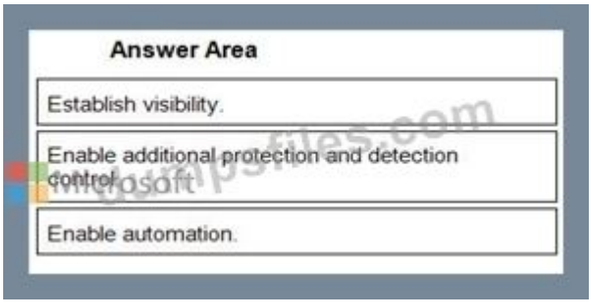
Answer:



NEW QUESTION: 56
You are designing a security operations strategy based on the Zero Trust framework.
You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).
Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer, move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.



Answer:



1 - Establish visibility.
2 - Enable additional protection and detection control.
3 - Enable automation.

NEW QUESTION: 57
A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions. You are evaluating the security posture of the customer.
You discover that the AKS resources are excluded from the secure score recommendations. You need to produce accurate recommendations and update the secure score.
Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. Configure auto provisioning.
B. Assign regulatory compliance policies.
C. Review the inventory.
D. Add a workflow automation.
E. Enable Defender plans.
Answer: A,E (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

NEW QUESTION: 58
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.
The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
* Prevent the remote users from accessing any other resources on the network.
* Support Azure Active Directory (Azure AD) Conditional Access.
* Simplify the end-user experience.
What should you include in the recommendation?

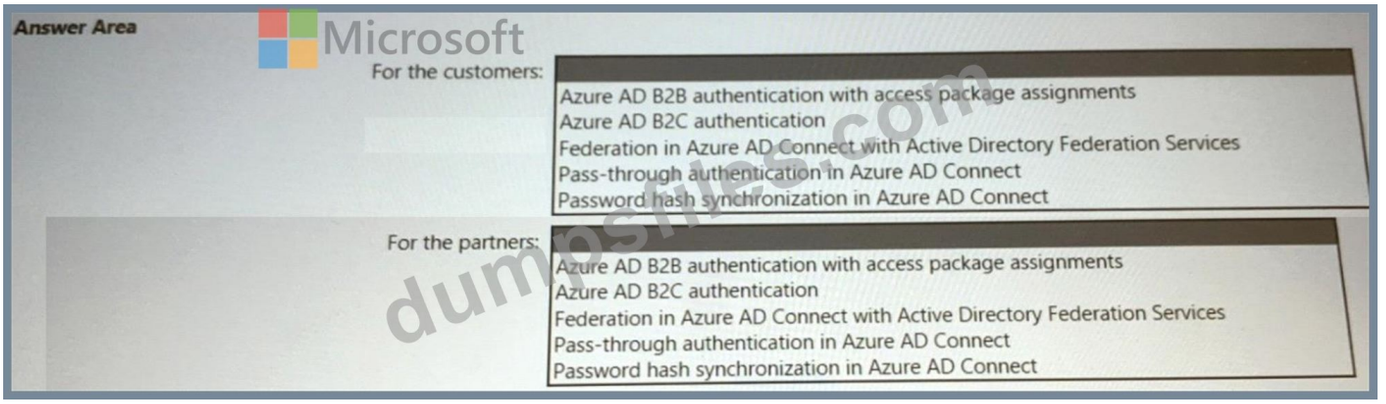
A. Azure Virtual WAN
B. web content filtering in Microsoft Defender for Endpoint
C. Microsoft Tunnel
D. Azure AD Application Proxy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
You are creating the security recommendations for an Azure App Service web app named App1.
App1 has the following specifications:
* Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
* Users will authenticate by using Azure Active Directory (Azure AD) user accounts.
You need to recommend an access security architecture for App1.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

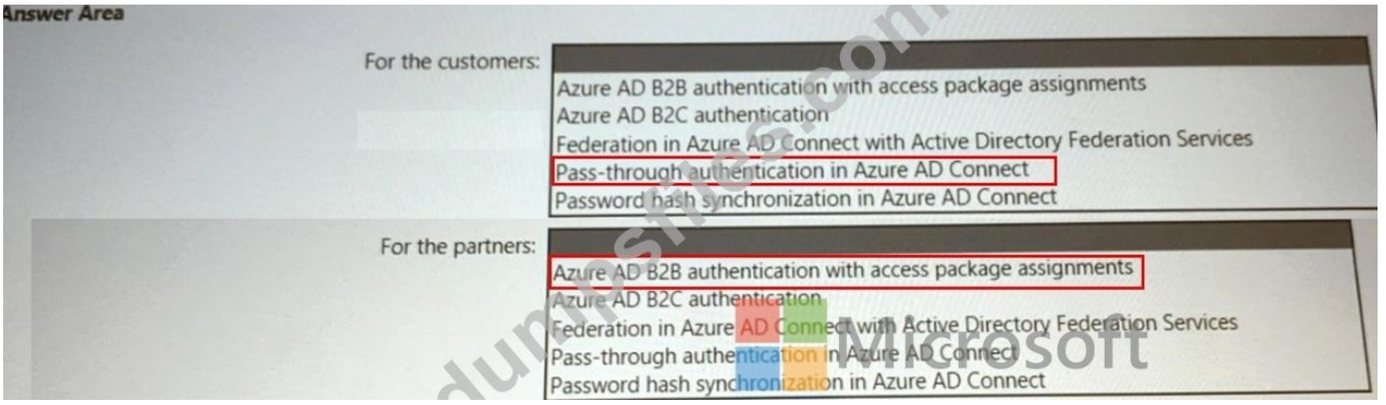
Answer:

NEW QUESTION: 60
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DSV You need to recommend an identity security strategy that meets the following requirements:
* Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website
* Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned
The solution must minimize the need to deploy additional infrastructure components. What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 61

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table.

The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

A. dynamic data masking

B. data classification

C. row-level security (RLS)

D. Transparent Data Encryption (TDE)

E. Always Encrypted

Answer: D (LEAVE A REPLY)

NEW QUESTION: 62

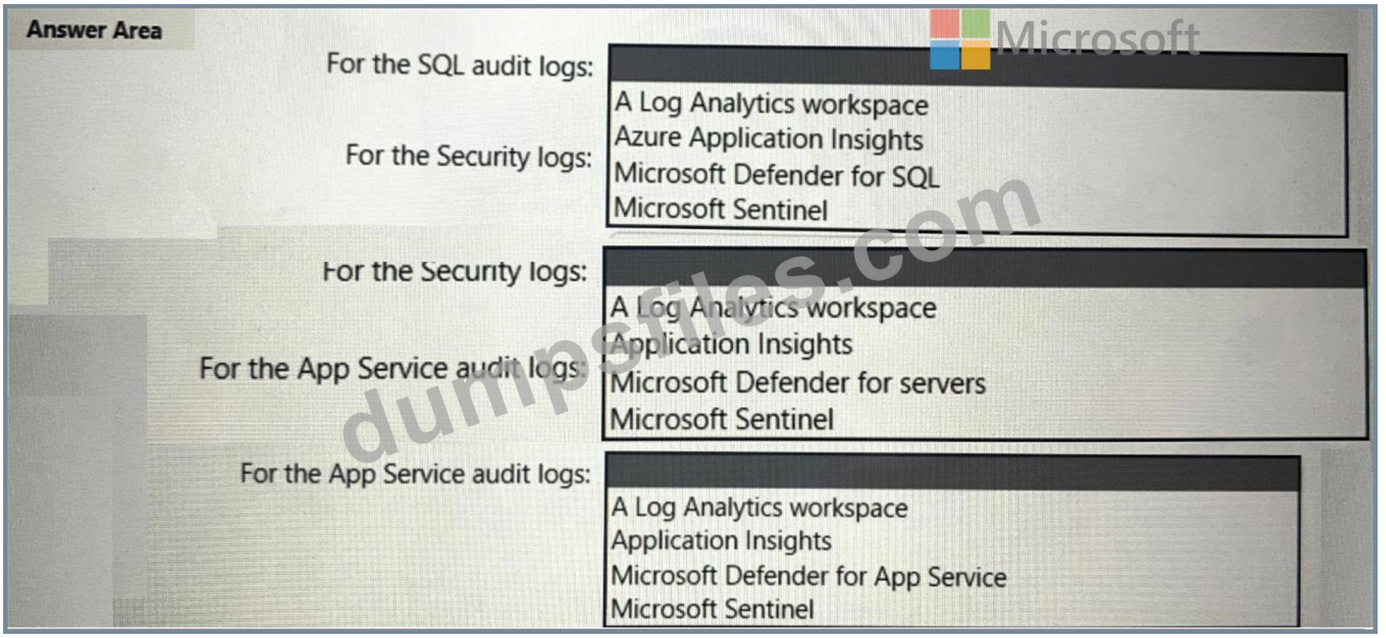
You are designing an auditing solution for Azure landing zones that will contain the following components:

* SQL audit logs for Azure SQL databases
* Windows Security logs from Azure virtual machines
* Azure App Service audit logs from App Service web apps

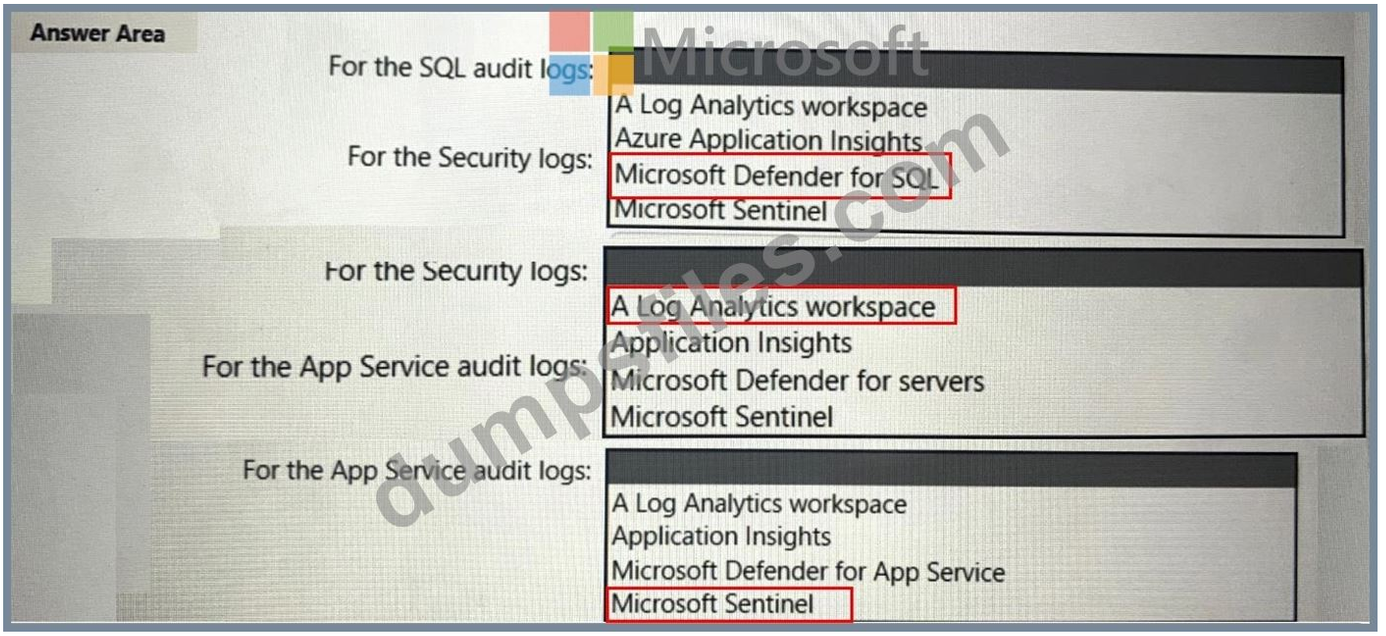
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:

* Log all privileged access.
* Retain logs for at least 365 days.
* Minimize costs.

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

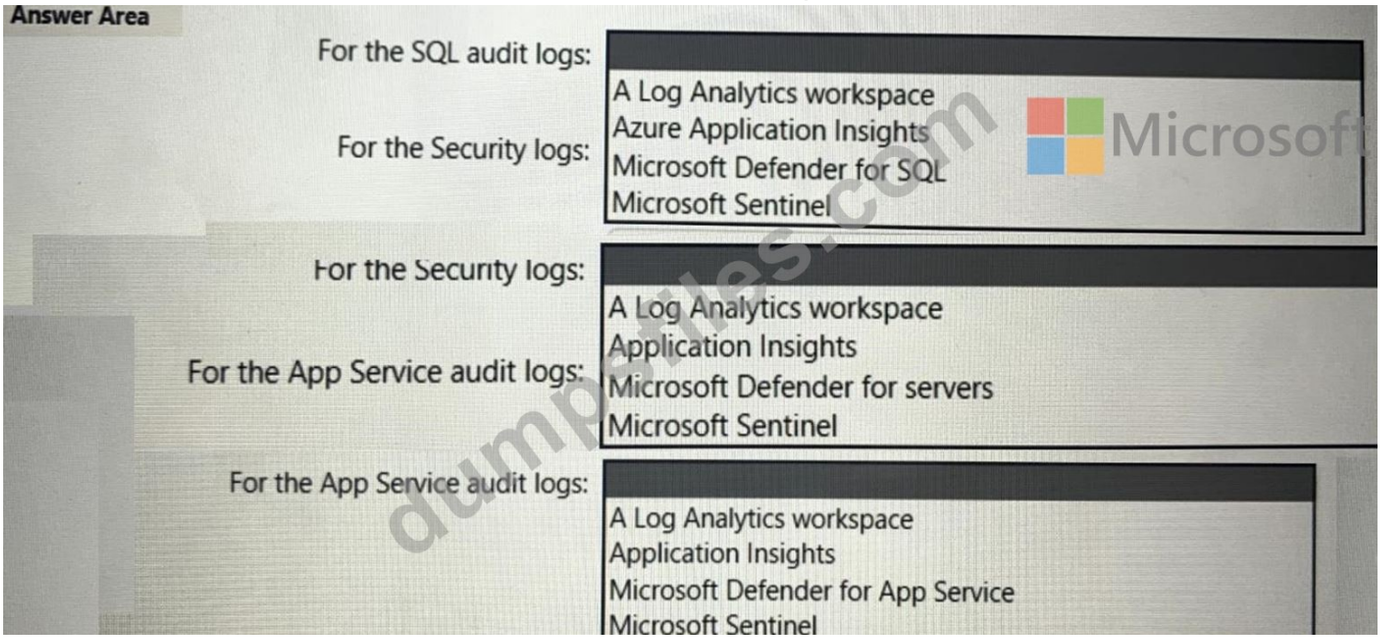


Answer:

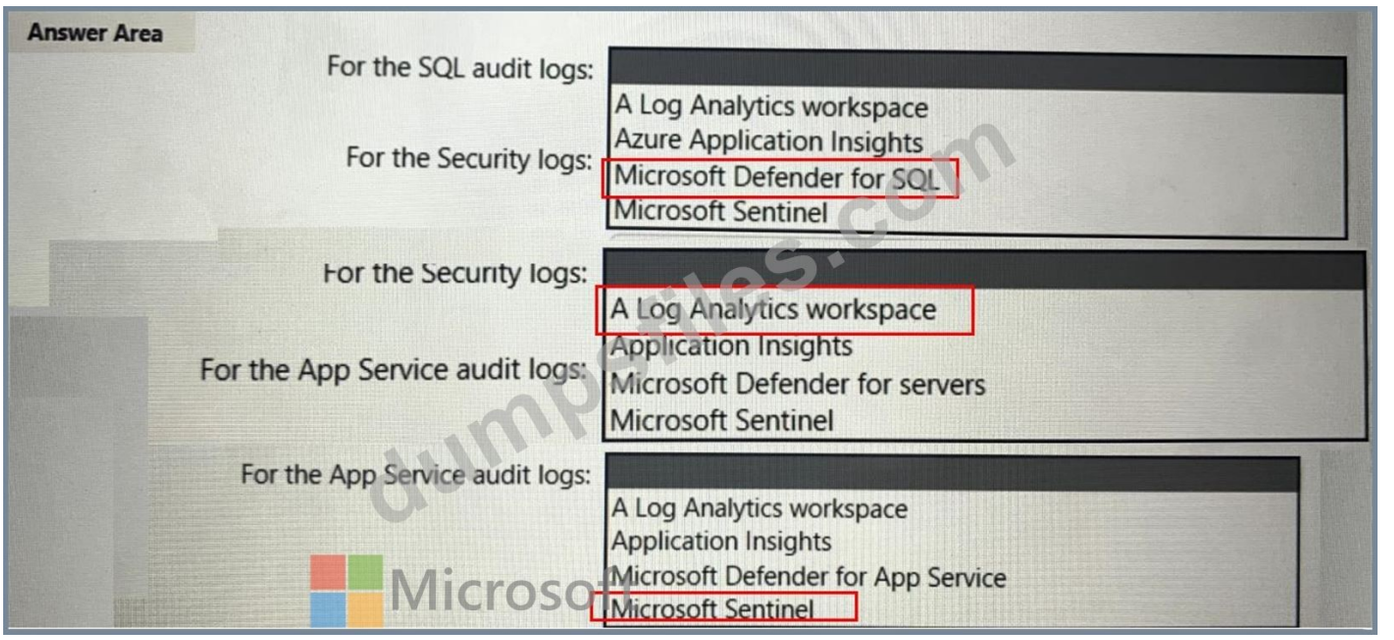


NEW QUESTION: 63
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?
A. From Defender for Cloud, review the secure score recommendations.
B. From Defender for Cloud, review the Azure security baseline for audit report.
C. From Defender for Cloud, enable Defender for Cloud plans.
D. From Defender for Cloud, add a regulatory compliance standard.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
You are designing an auditing solution for Azure landing zones that will contain the following components:
* SQL audit logs for Azure SQL databases
* Windows Security logs from Azure virtual machines
* Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
* Log all privileged access.
* Retain logs for at least 365 days.
* Minimize costs.
What should you include in the recommendation? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.



Answer:

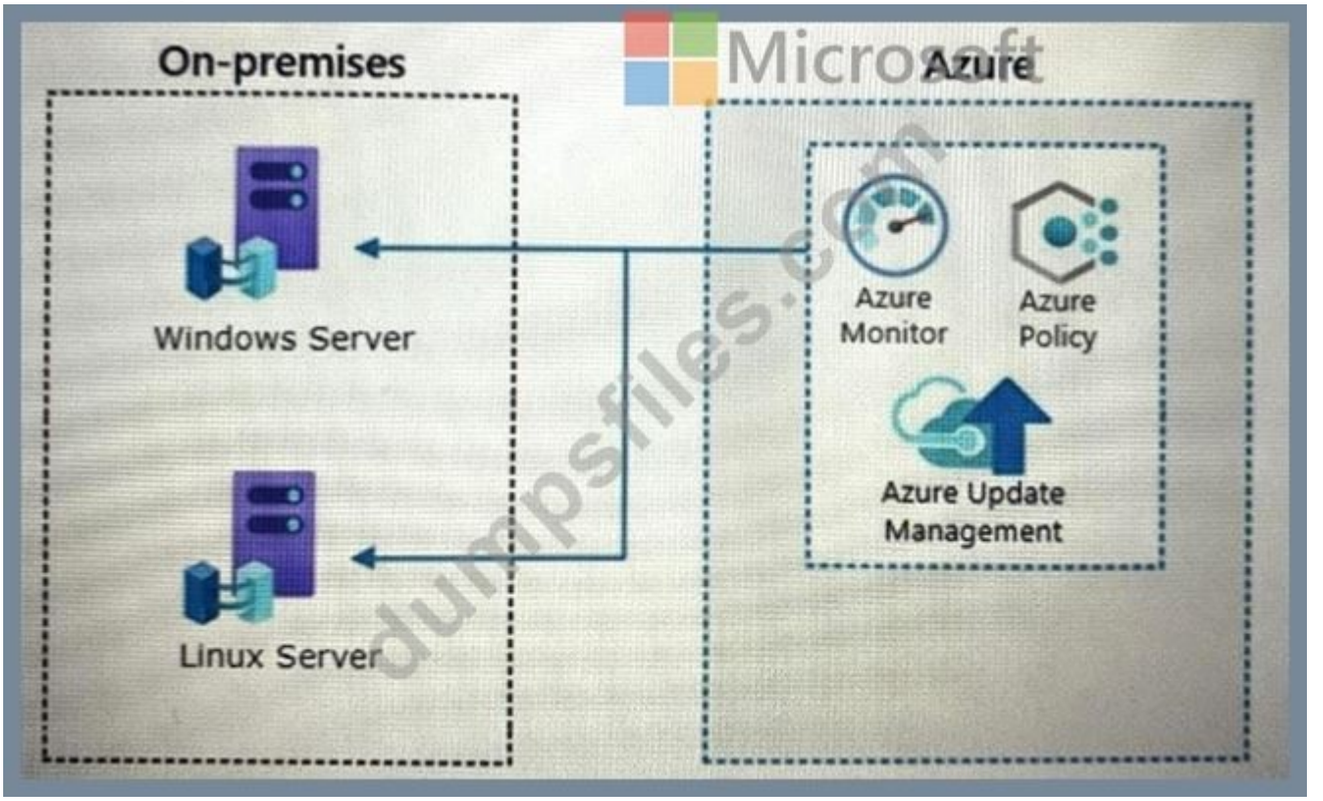


NEW QUESTION: 65

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:

* Govern virtual machines and servers across multiple environments.

* Enforce standards for all the resources across all the environment across the Azure policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

A. Azure VPN Gateway

B. guest configuration in Azure Policy

C. on-premises data gateway

D. Azure Bastion

E. Azure Arc

Answer: (SHOW ANSWER)

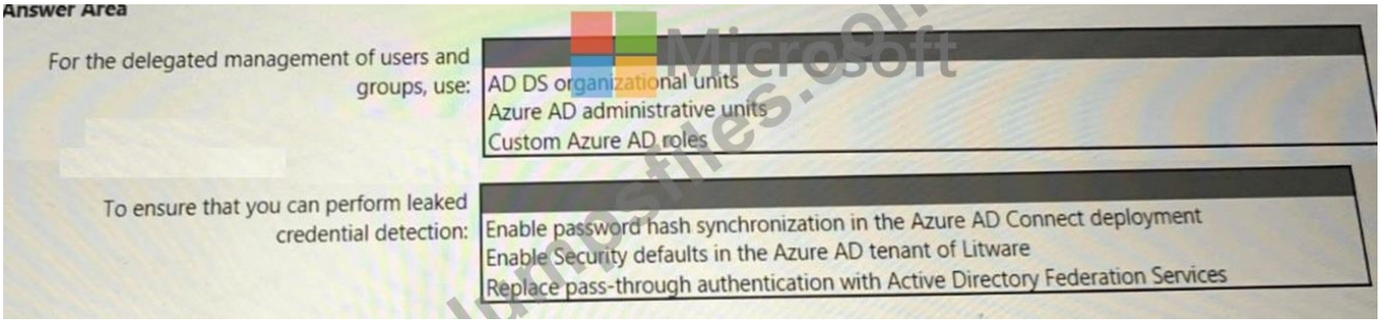
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

NEW QUESTION: 66

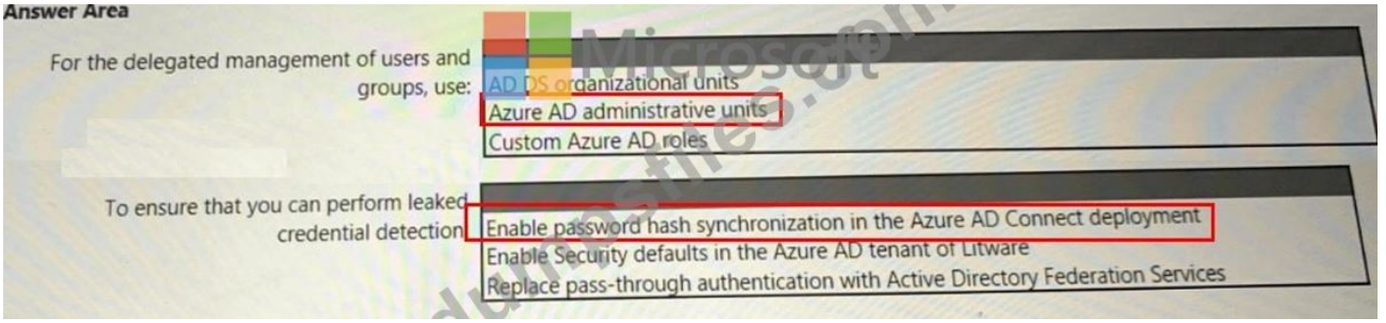
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 67

You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers.

In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Registry

B. Linux containers deployed to Azure Kubernetes Service (AKS)

C. Windows containers deployed to Azure Container Registry

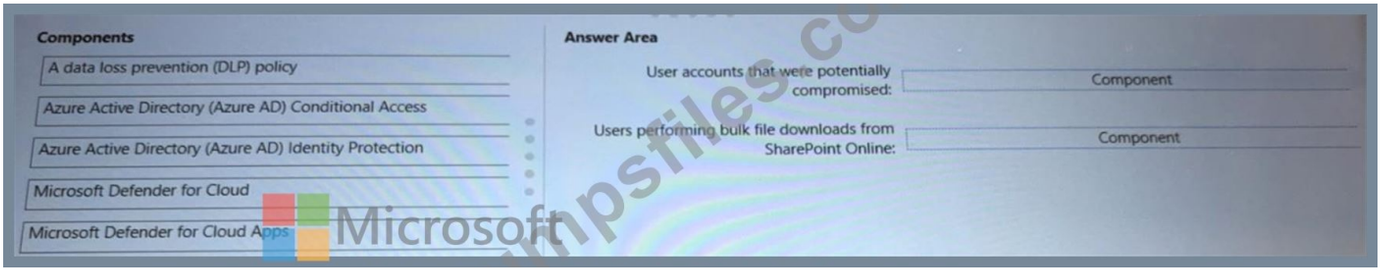
D. Windows containers deployed to Azure Kubernetes Service (AKS)

E. Linux containers deployed to Azure Container Instances

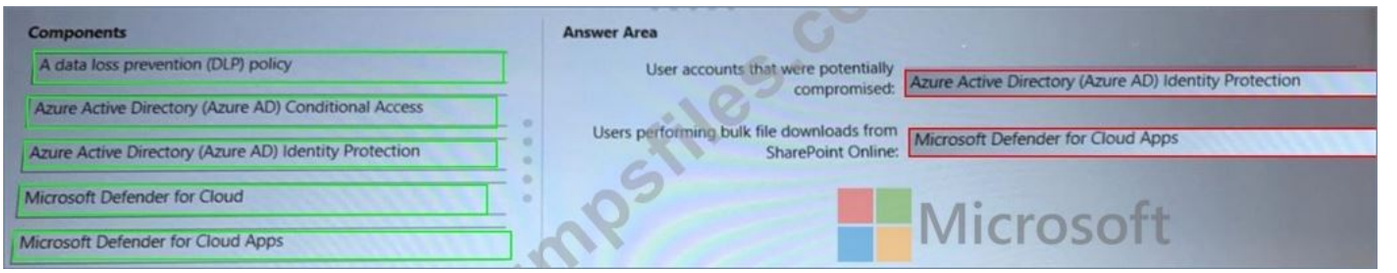
Answer: A,B (LEAVE A REPLY)
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-security-requirements-for-containers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabilities-for-running-images

NEW QUESTION: 68
Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:
* Minimizes manual intervention by security operation analysts
* Supports Waging alerts within Microsoft Teams channels
What should you include in the strategy?
A. data connectors
B. playbooks
C. workbooks
D. KQL
Answer: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

NEW QUESTION: 69
You have a Microsoft 365 subscription
You need to recommend a security solution to monitor the following activities:
* User accounts that were potentially compromised
* Users performing bulk file downloads from Microsoft SharePoint Online What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each Correct selection is worth one Point.



Answer:



NEW QUESTION: 70

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The company plans to use Microsoft Information Protection for the PII data store in Azure.

You need to recommend a solution to discover PII data at risk in the Azure resources.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

NEW QUESTION: 71

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance. Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID. Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

NEW QUESTION: 72

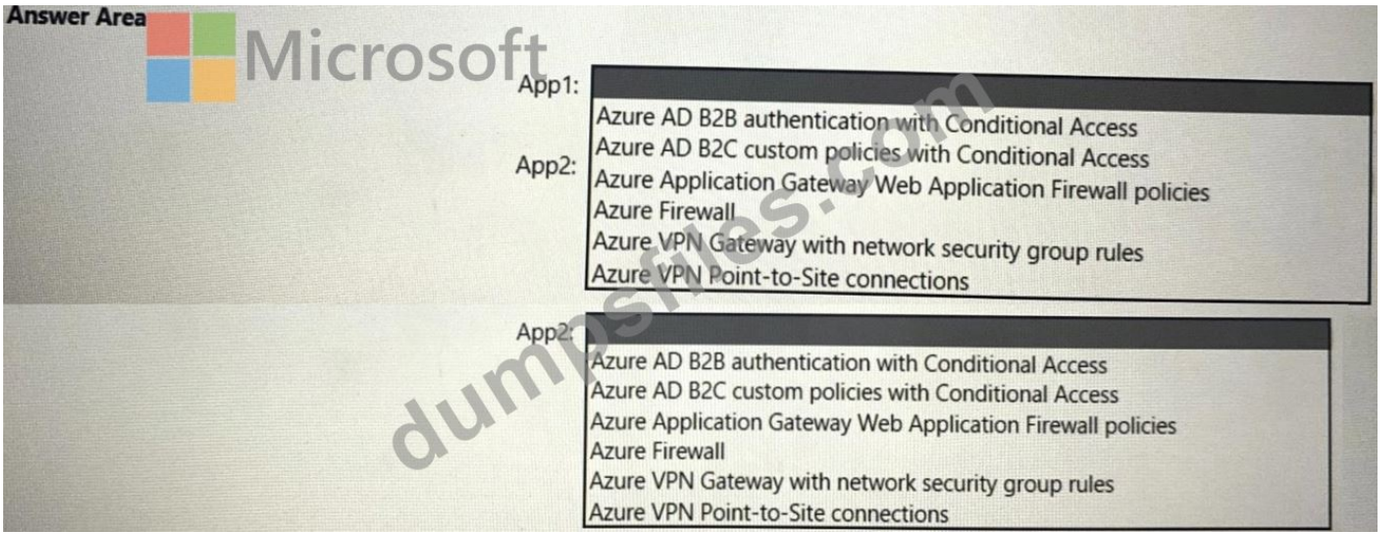
You have an Azure subscription. The subscription contains 100 virtual machines that run Windows Server.

The virtual machines are managed by using Azure Policy and Microsoft Defender for Servers.
You need to enhance security on the virtual machines. The solution must meet the following requirements:
* Ensure that only apps on an allowlist can be run.
* Require administrators to confirm each app added to the allowlist.
* Automatically add unauthorized apps to a blocklist when an attempt is made to launch the app.
* Require administrators to approve an app before the app can be moved from the blocklist to the allowlist.
What should you include in the solution?
A. admin consent settings for enterprise applications in Azure AD
B. app governance in Microsoft Defender for Cloud Apps
C. adaptive application controls in Defender for Servers
D. a compute policy in Azure Policy
Answer: C (LEAVE A REPLY)

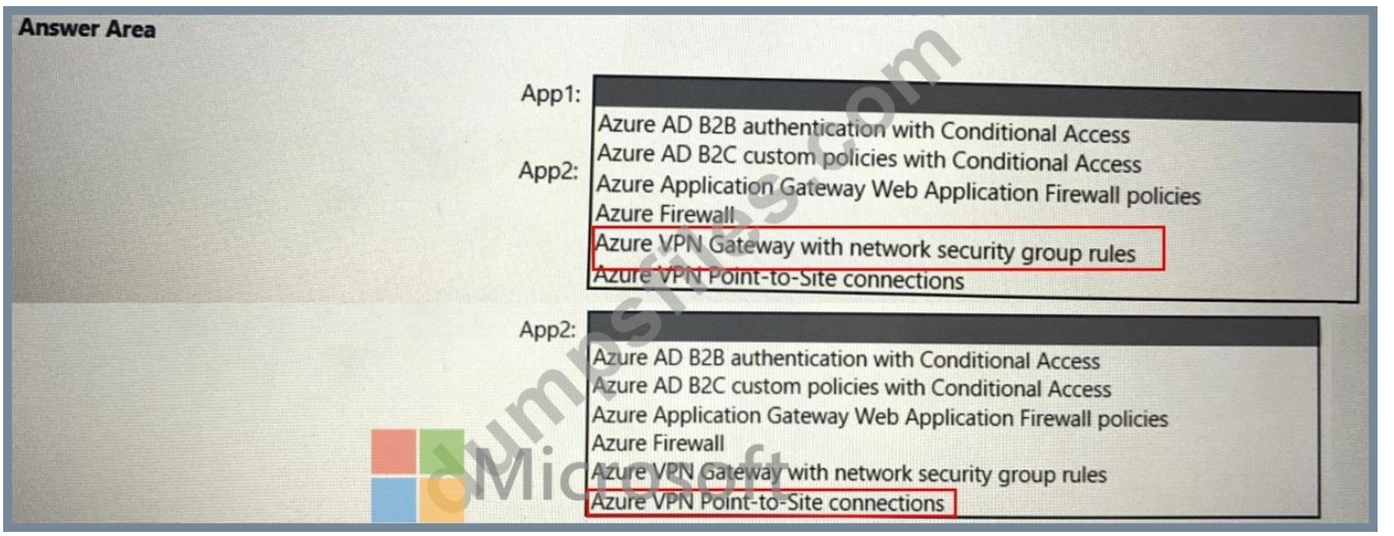
NEW QUESTION: 73
You have a hybrid cloud infrastructure.
You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 74

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?

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

B. From Defender for Cloud, review the secure score recommendations.

C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

D. From Defender for Cloud, enable Defender for Cloud plans.

Answer: (SHOW ANSWER)

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulat

NEW QUESTION: 75

Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

* Minimizes manual intervention by security operation analysts

* Supports Waging alerts within Microsoft Teams channels

What should you include in the strategy?

A. data connectors

B. playbooks

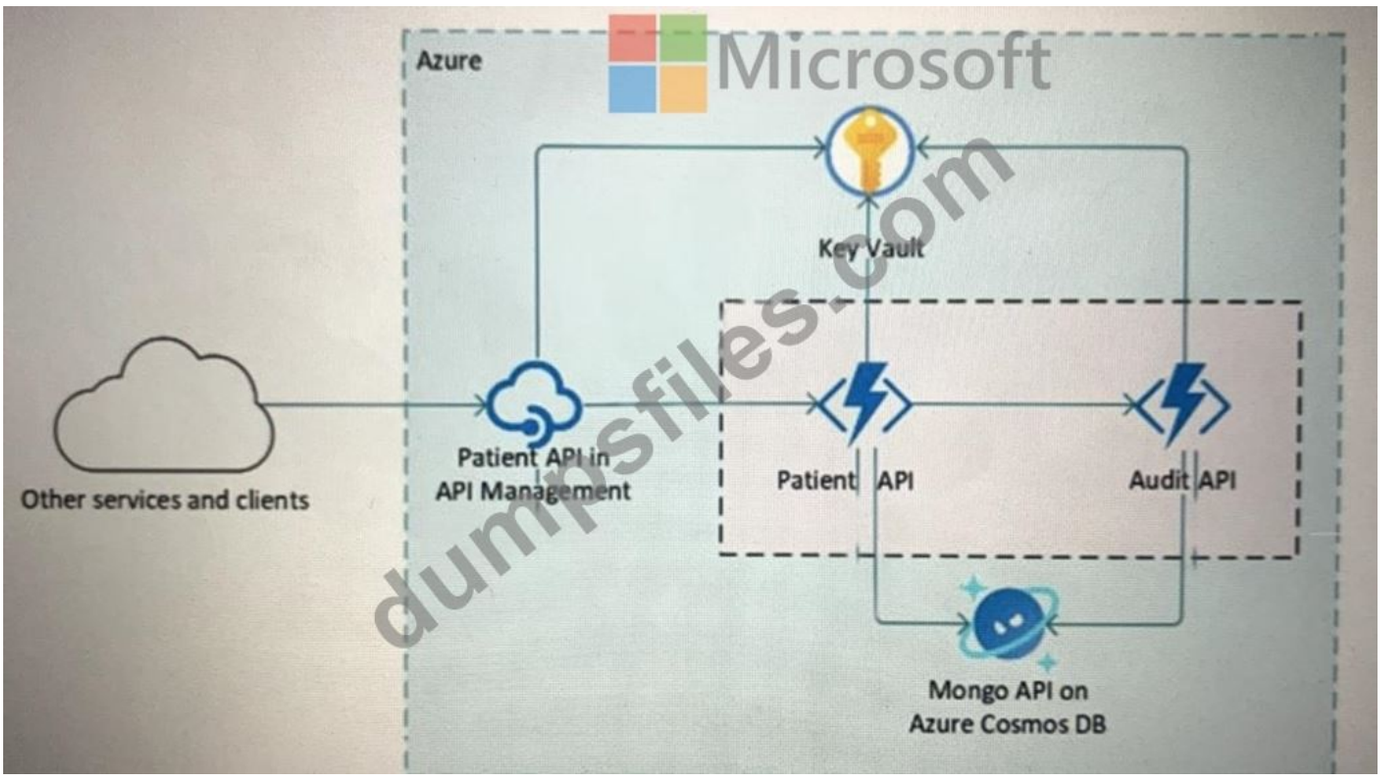
C. KQL

D. workbooks

Answer: D (LEAVE A REPLY)

NEW QUESTION: 76

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



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

A. Azure Active Directory (Azure AD) enterprise applications

B. an Azure App Service Environment (ASE)

C. Azure service endpoints

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

Answer: B (LEAVE A REPLY)

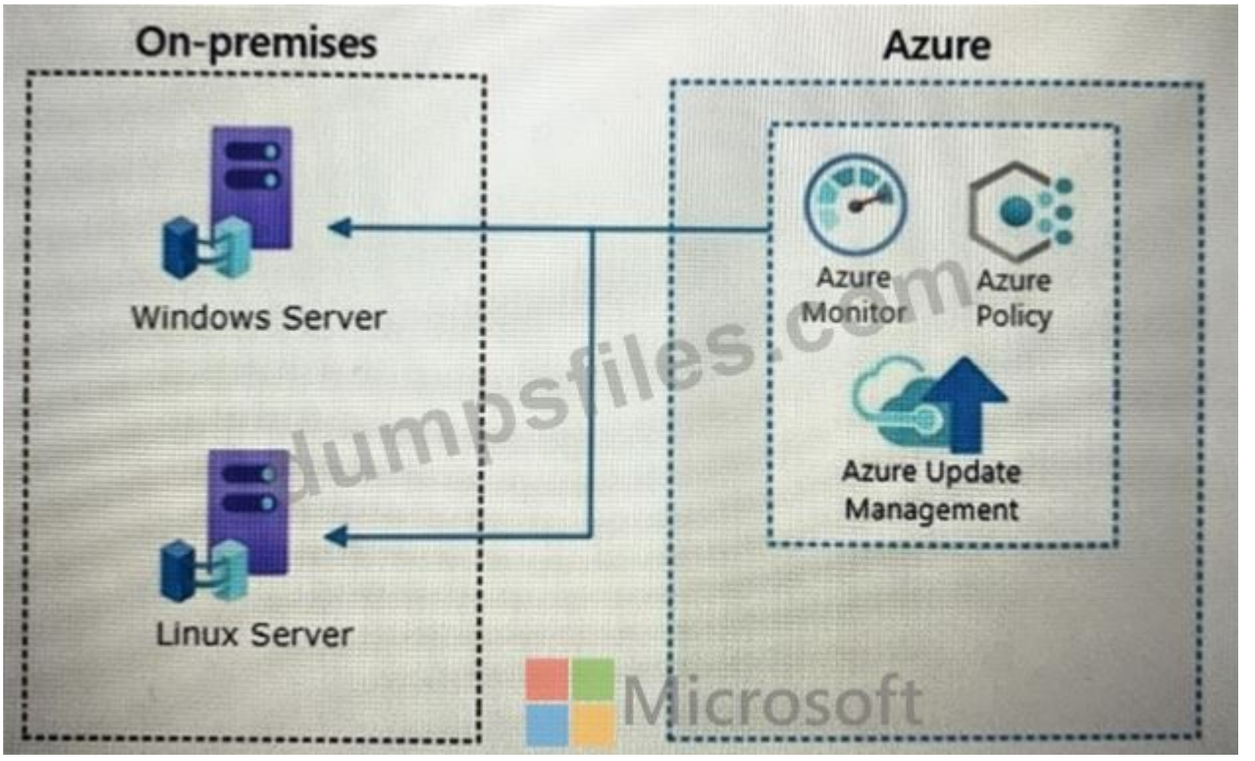
App Service environments (ASEs) are appropriate for application workloads that require:
Very high scale,Isolation and secure network access,High memory utilization.This capability can host your:
Windows web apps,Linux web apps
Docker containers,Mobile apps
Functions
https://docs.microsoft.com/en-us/azure/app-service/environment/overview

NEW QUESTION: 77

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.



NOTE Each correct selection is worth one point.

A. on-premises data gateway

B. Azure VPN Gateway

C. guest configuration in Azure Policy

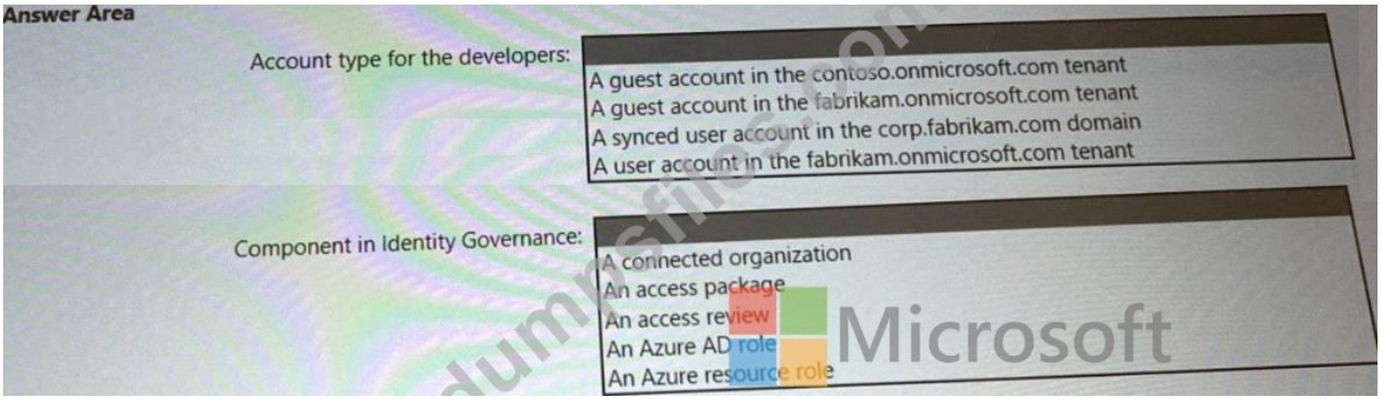
D. Azure Arc

E. Azure Bastion

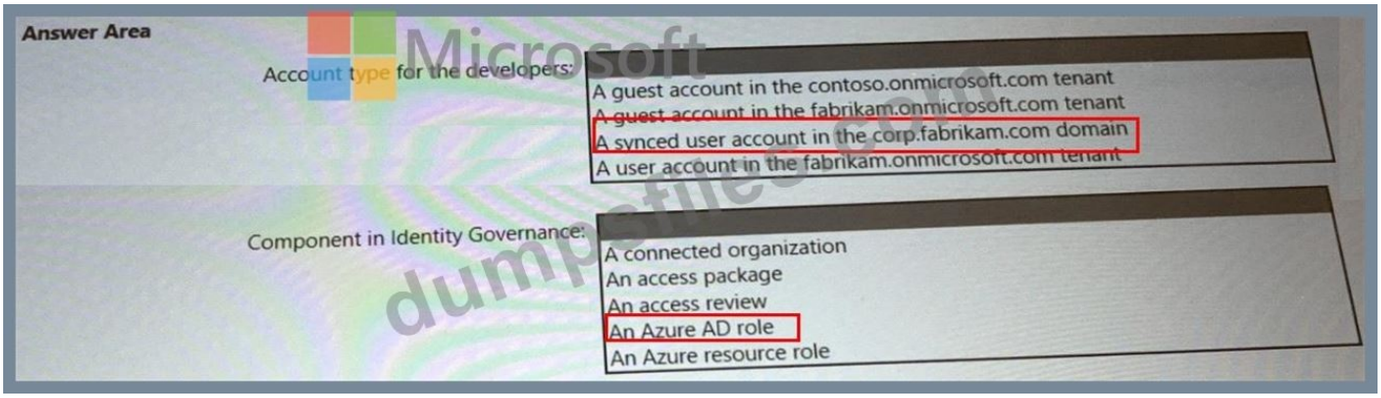
Answer: (SHOW ANSWER)

NEW QUESTION: 78

What should you create in Azure AD to meet the Contoso developer requirements?



Answer:



NEW QUESTION: 79

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware.

The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Endpoint reports the endpoints as compliant.

B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. The client access tokens are refreshed.

Answer: (SHOW ANSWER)

https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-

https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

NEW QUESTION: 80

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

NEW QUESTION: 81

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?
A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, review the secure score recommendations.
C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
D. From Defender for Cloud, enable Defender for Cloud plans.
Answer: C (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulat

NEW QUESTION: 82
You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?
A. Azure Logics Apps
B. Azure Event Hubs
C. Azure Functions apps
D. Azure Monitor webhooks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83
Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.
A. Azure Firewall
B. Azure Web Application Firewall (WAF)
C. Microsoft Defender for Cloud alerts
D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)
E. Microsoft Sentinel
Answer: (SHOW ANSWER)
Topic 1, Litware, inc.
Existing Environment
Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD D%) forest named Utvvare.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash

synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.
The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.
Planned Changes
Litware plans to implement the following changes:
* Create a management group hierarchy for each Azure AD tenant.
* Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.
* Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.
Business Requirements
Litware identifies the following business requirements:
* Minimize any additional on-premises infrastructure.
* Minimize the operational costs associated with administrative overhead.
Hybrid Requirements
Litware identifies the following hybrid cloud requirements:
* Enable the management of on-premises resources from Azure, including the following:
* Use Azure Policy for enforcement and compliance evaluation.
* Provide change tracking and asset inventory.
* Implement patch management.
* Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.
Microsoft Sentinel Requirements
Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAK) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOQ by using Microsoft Sentinel.
Identity Requirements
Litware identifies the following identity requirements:
* Detect brute force attacks that directly target AD DS user accounts.
* Implement leaked credential detection in the Azure AD tenant of Litware.
* Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
* Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for.
* The management of group properties, membership, and licensing
* The management of user properties, passwords, and licensing
* The delegation of user management based on business units.
Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:

* insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
* Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
* Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:
* Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
* Provide a secure score scoped to the landing zone.
* Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
* Minimize the possibility of data exfiltration.
* Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
* Be created in a dedicated subscription.
* Use a DNS namespace of litware.com.

Application Security Requirements

Litware identifies the following application security requirements:
* Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
* Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

NEW QUESTION: 84

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

A. Azure Monitor webhooks
B. Azure Logics Apps
C. Azure Event Hubs
D. Azure Functions apps

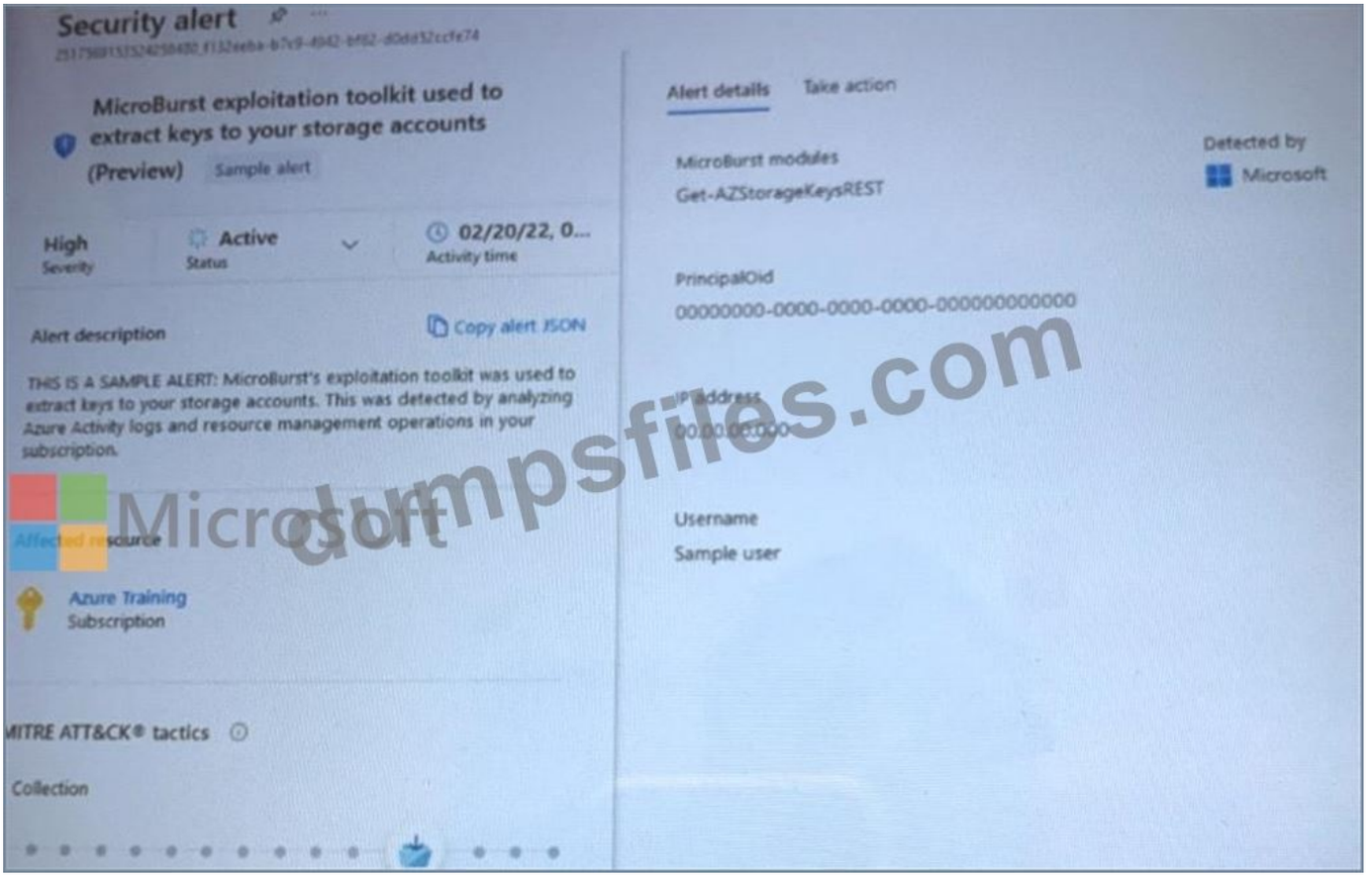
Answer: (SHOW ANSWER)

Explanation

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.Note: Azure Logic

Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems.
With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

NEW QUESTION: 85
You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



After remediating the threat which policy definition should you assign to prevent the threat from reoccurring?
A. Storage account public access should be disallowed
B. Storage accounts should prevent shared key access
C. Azure Key Vault Managed HSM should have purge protection enabled
D. Storage account keys should not be expired
Answer: A (LEAVE A REPLY)

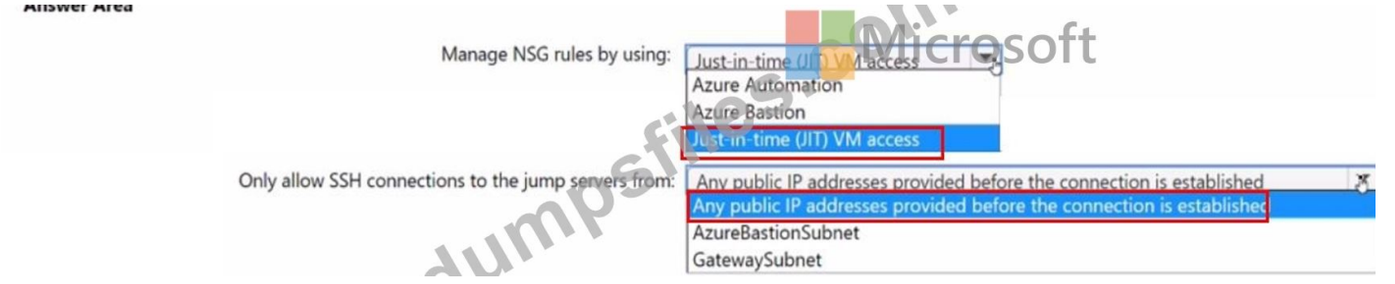
NEW QUESTION: 86
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect f personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG) You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:

* Ensure that each time the support staff connects to a jump server; they must request access to the server.
* Ensure that only authorized support staff can initiate SSH connections to the jump servers.
* Maximize protection against brute-force attacks from internal networks and the internet.
* Ensure that users can only connect to the jump servers from the internet.
* Minimize administrative effort

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



NEW QUESTION: 87

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Security Assertion Markup Language (SAML)

B. NTLMv2

C. certificate-based authentication

D. Kerberos

Answer: A,D (LEAVE A REPLY)

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

NEW QUESTION: 88

Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

A. Information Governance
B. data loss prevention (DLP)
C. data classification content explorer
D. eDiscovery
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
You have Microsoft Defender for Cloud assigned to Azure management groups.
You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. workload protections in Defender for Cloud
B. threat intelligence reports in Defender for Cloud
C. Microsoft Sentinel notebooks
D. Microsoft Sentinel threat intelligence workbooks
Answer: B,D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION: 90
You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements.
What should you recommend as part of the landing zone deployment?

A. a VNet-to-VNet connection
B. forced tunneling
C. service chaining
D. local network gateways
Answer: (SHOW ANSWER)

NEW QUESTION: 91
You need to recommend a solution to meet the security requirements for the virtual machines.
What should you include in the recommendation?

A. an Azure Bastion host

B. a network security group (NSG)
C. just-in-time (JIT) VM access
D. Azure Virtual Desktop
Answer: (SHOW ANSWER)
The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image." https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image

NEW QUESTION: 92
Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

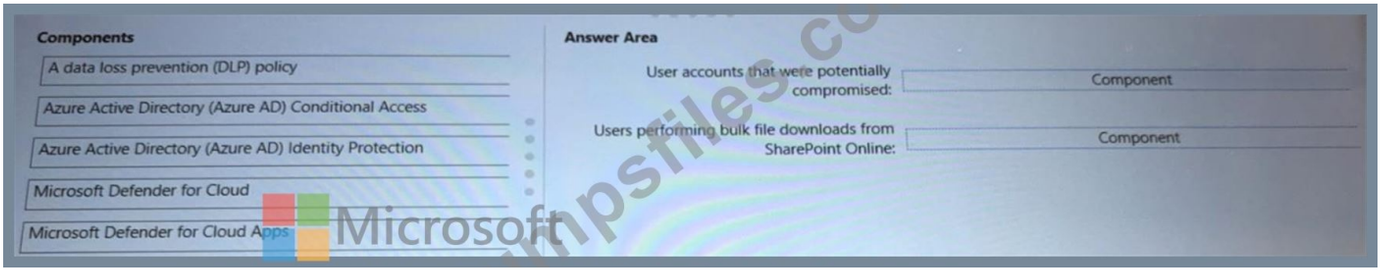
You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?
A. 1
B. 2
C. 3
D. 4
E. 5
Answer: C (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

NEW QUESTION: 93
You have a Microsoft 365 subscription
You need to recommend a security solution to monitor the following activities:

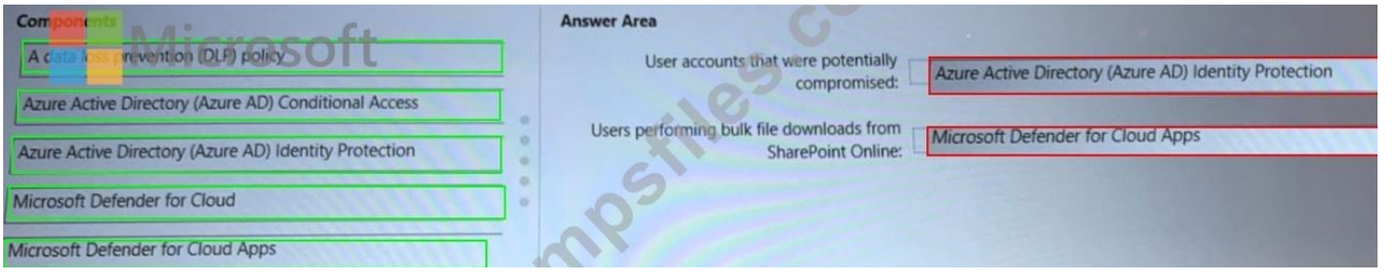
* User accounts that were potentially compromised
* Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each Correct selection is worth one Point.



Answer:



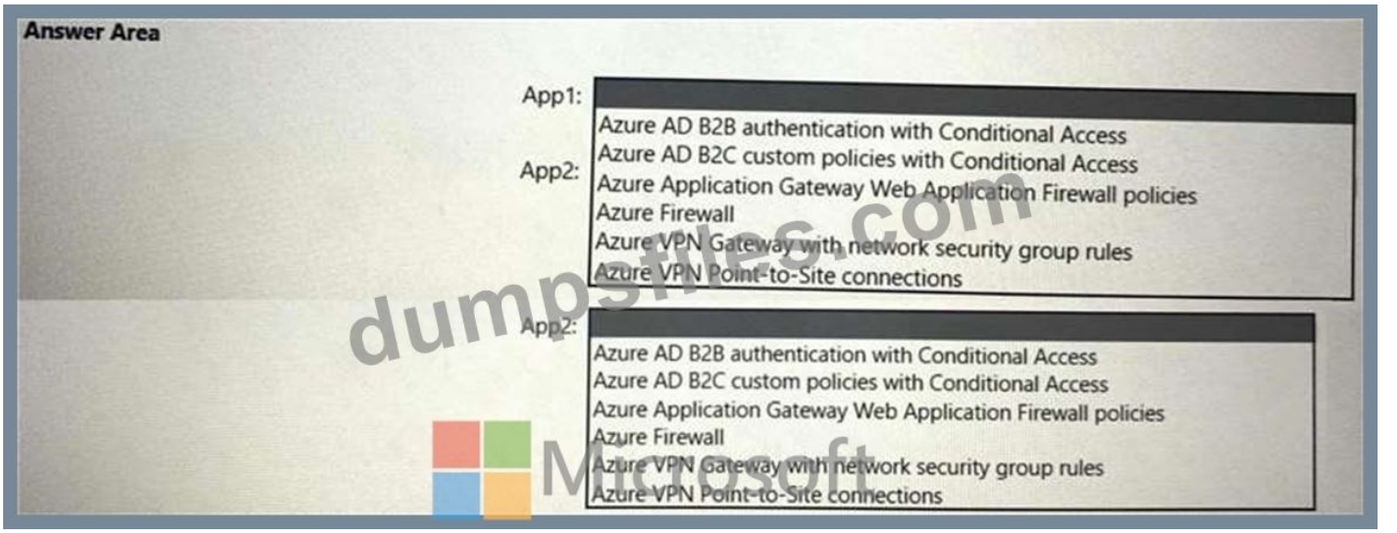
NEW QUESTION: 94

You have a hybrid cloud infrastructure.

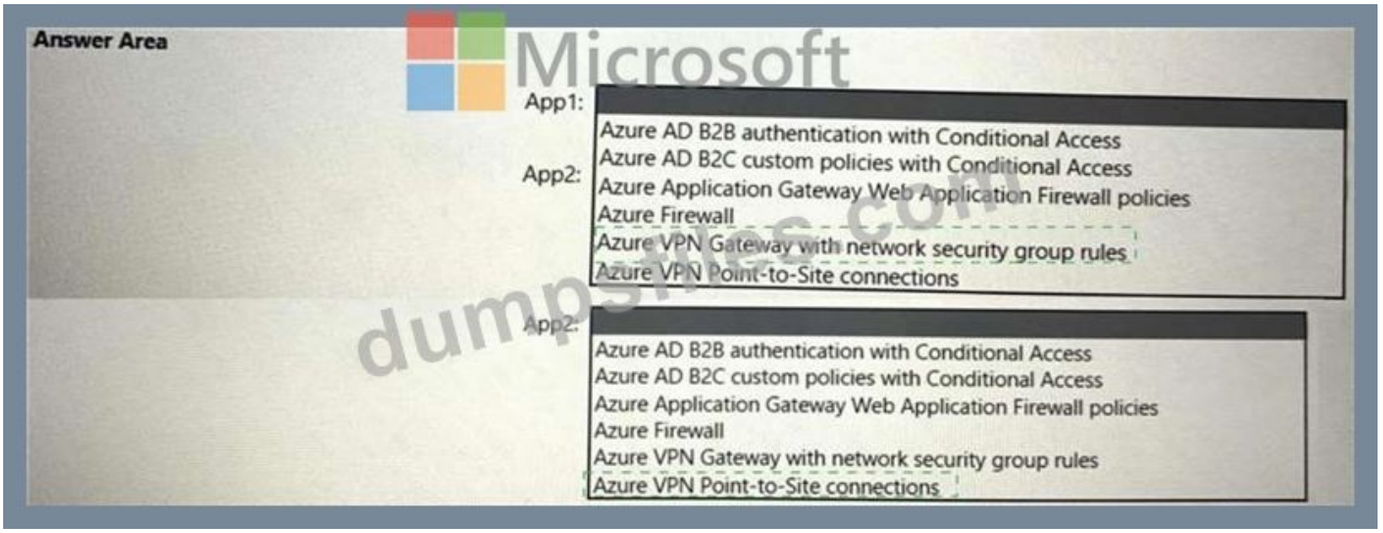
You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



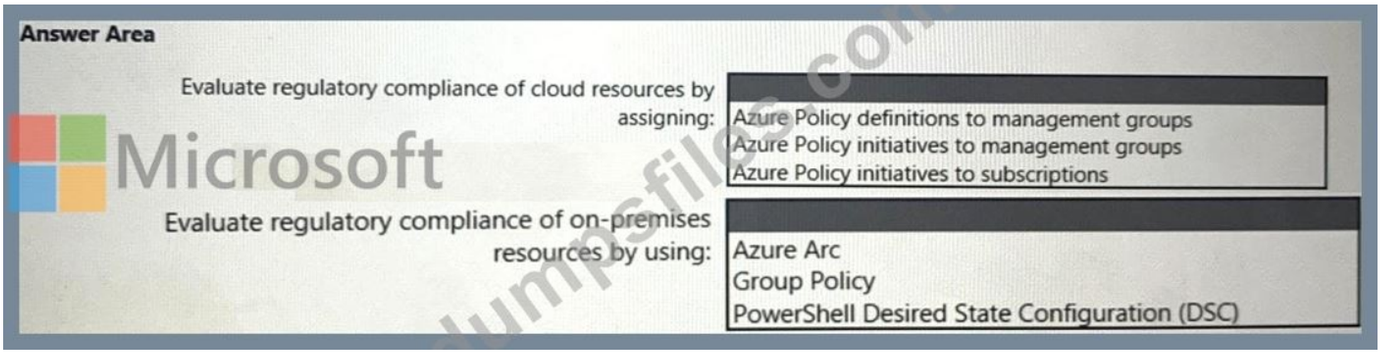
NEW QUESTION: 95

You need to recommend a solution to evaluate regulatory compliance across the entire managed environment.

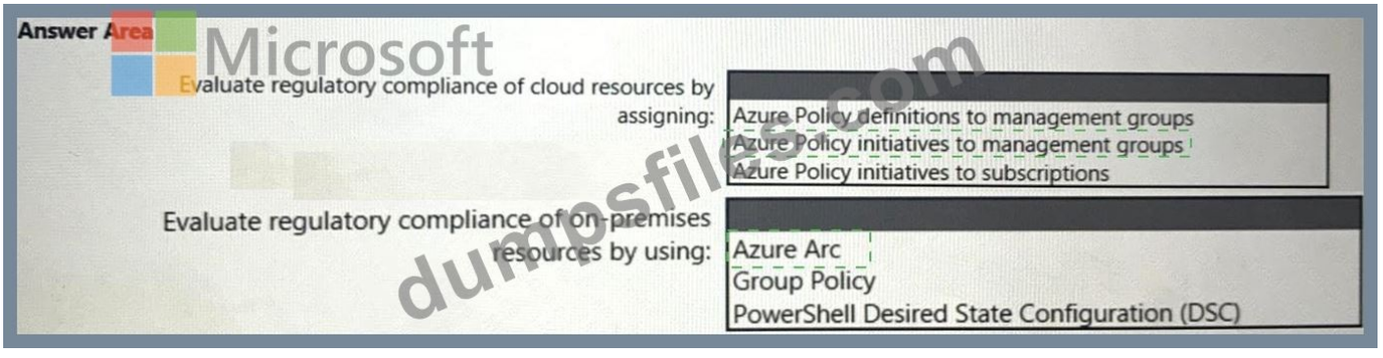
The solution must meet the regulatory compliance requirements and the business requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



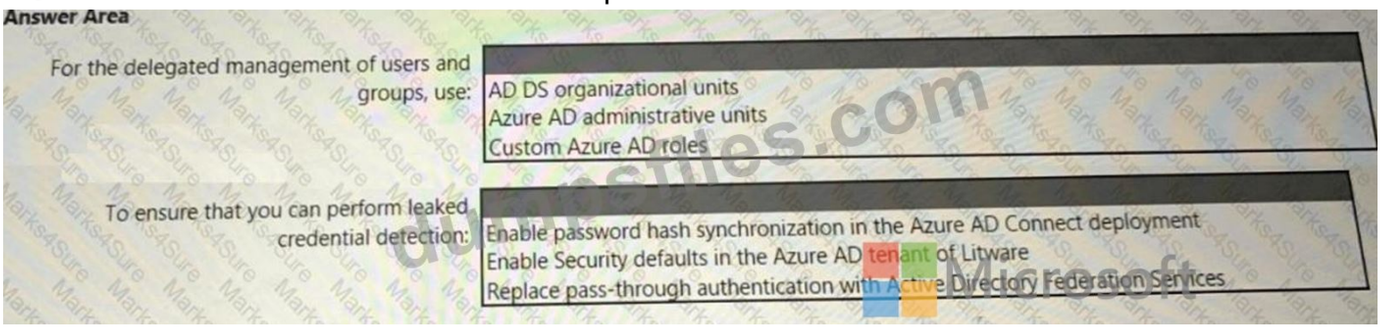
Explanation:

NEW QUESTION: 96

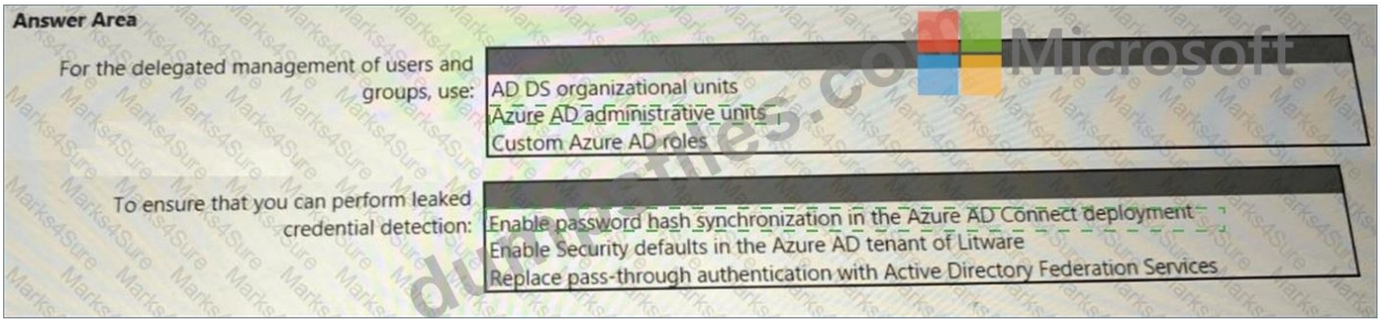
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



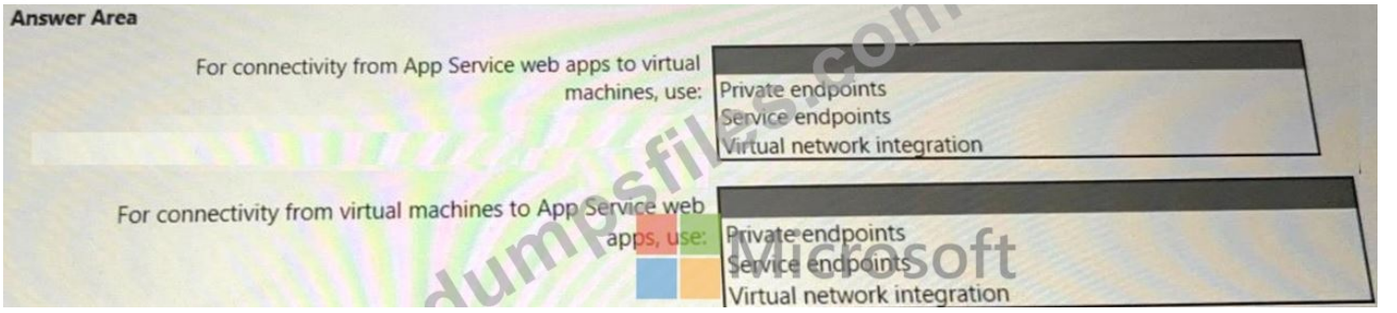
Answer:



Explanation:

NEW QUESTION: 97

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer are a. NOTE Each correct selection is worth one point.



Answer:

NEW QUESTION: 98

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines.

If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

B. adaptive application controls in Defender for Cloud

C. Azure Security Benchmark compliance controls m Defender for Cloud

D. app protection policies in Microsoft Endpoint Manager

Answer: B (LEAVE A REPLY)

https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute-recommendatio

NEW QUESTION: 99

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.

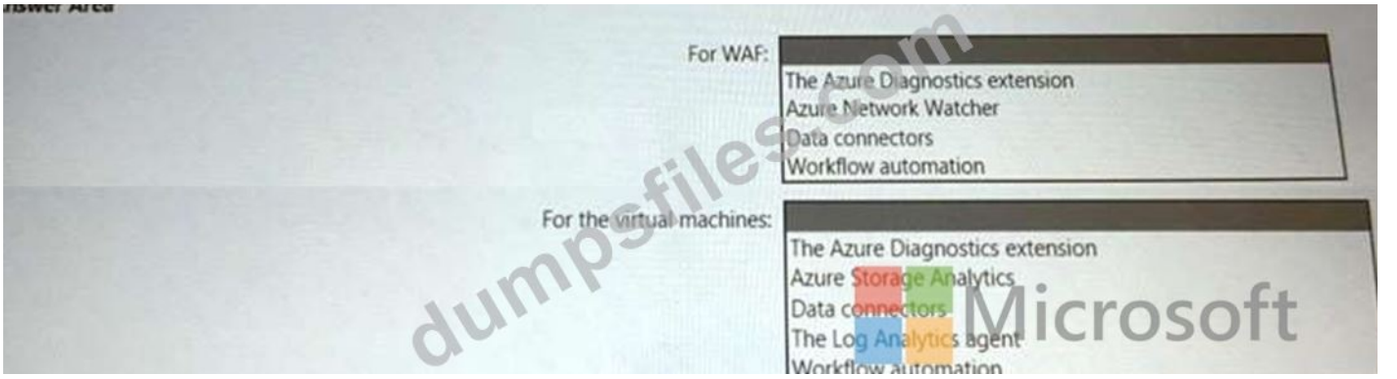
You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

* Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.

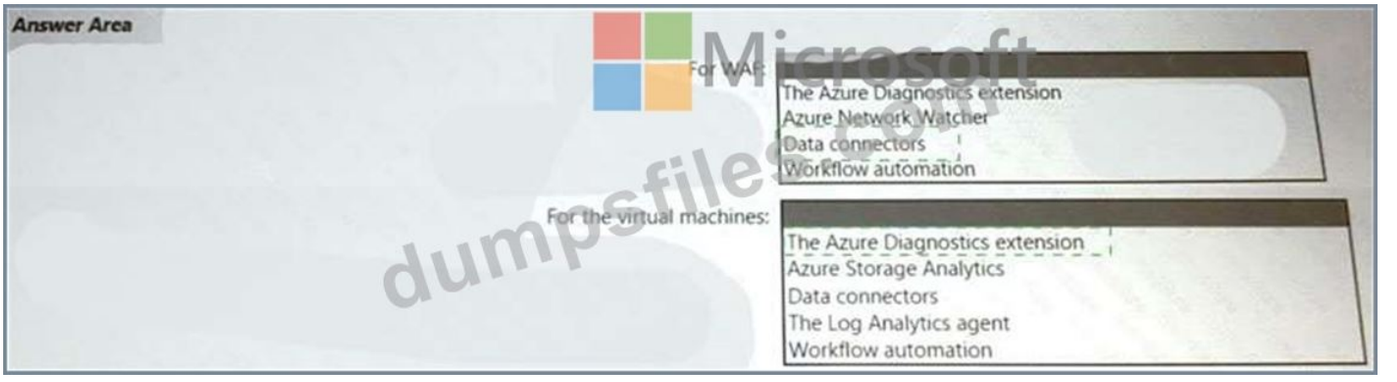
* Use Defender for Cloud to review alerts from the virtual machines.

What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE:

Each correct selection is worth one point.

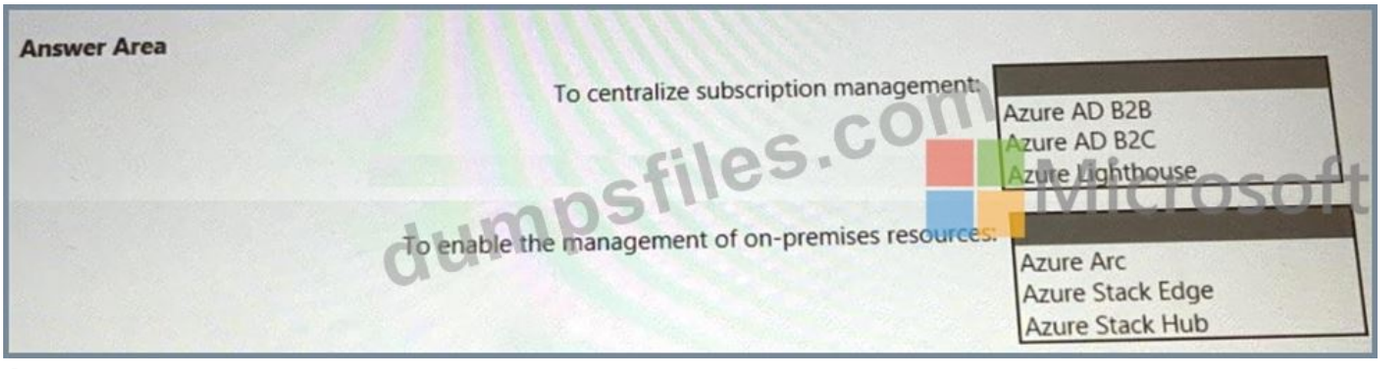


Answer:

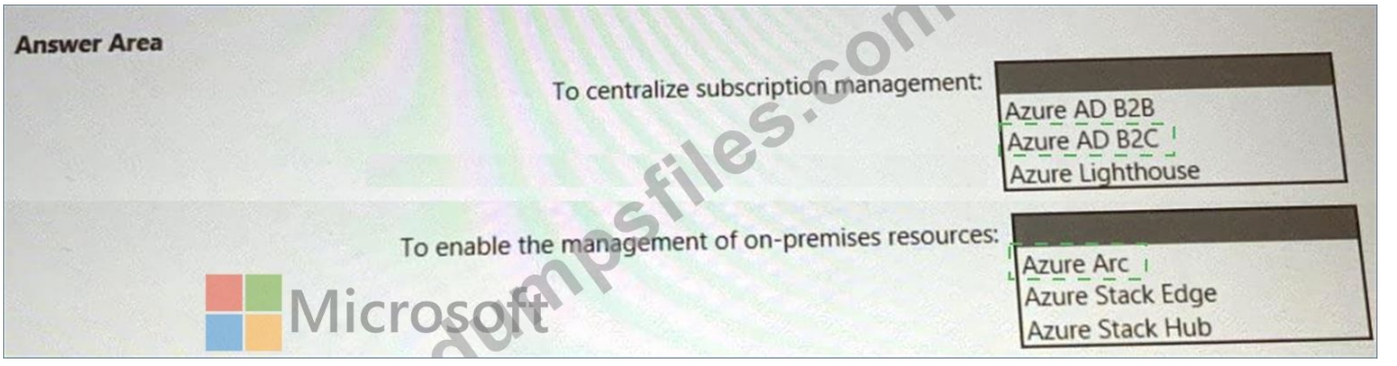


NEW QUESTION: 100

You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

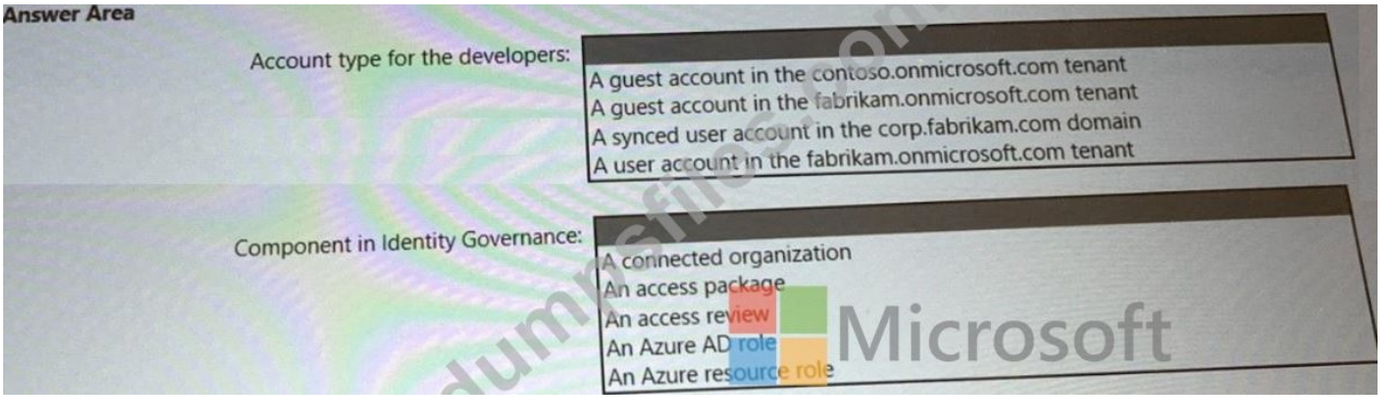


Answer:

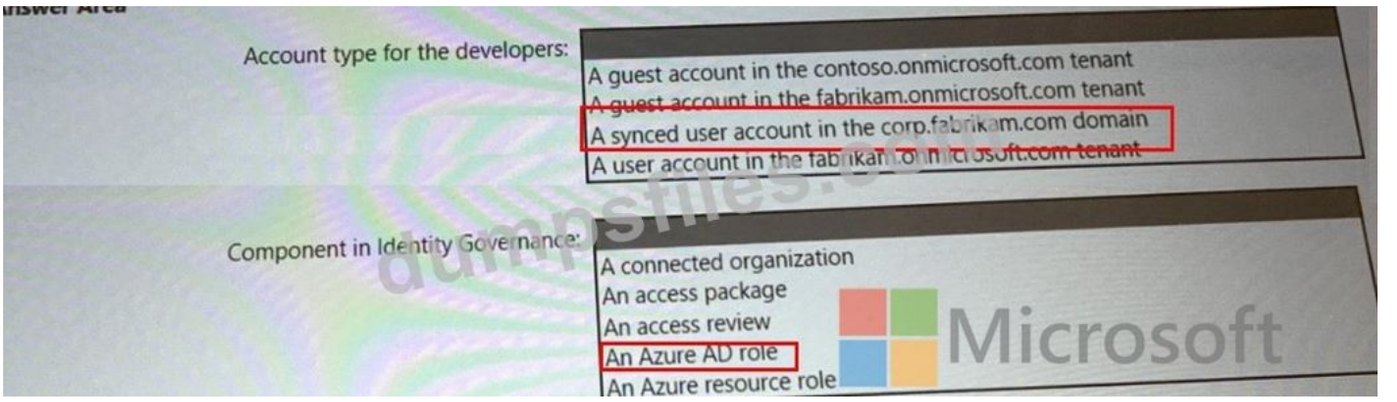


Explanation:

NEW QUESTION: 101
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling adaptive network hardening.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
JIT:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-st Adaptive Network Hardening:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify

NEW QUESTION: 102
What should you create in Azure AD to meet the Contoso developer requirements?


Answer:

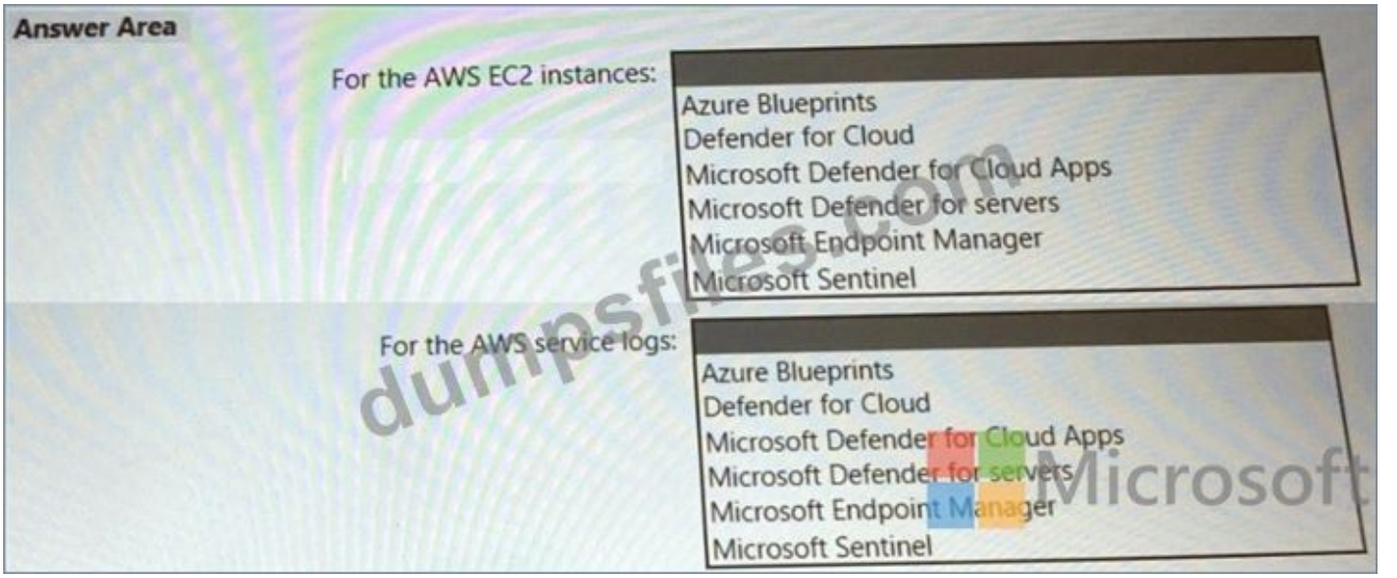


NEW QUESTION: 103

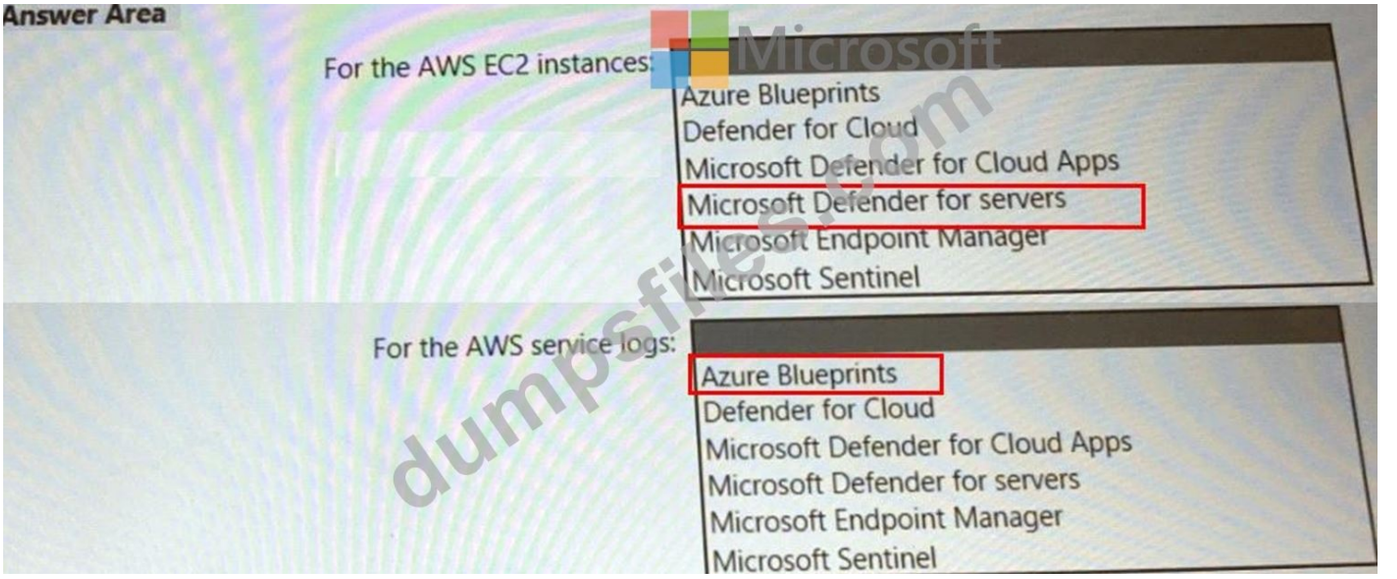
You need to recommend a solution to meet the AWS requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

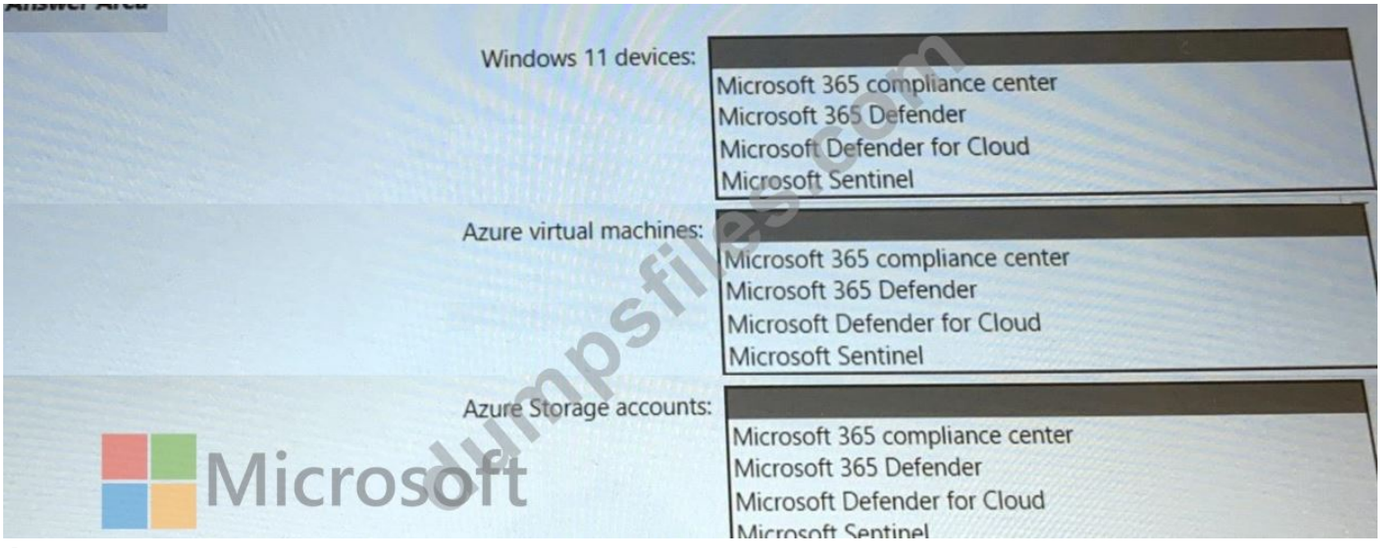


Answer:

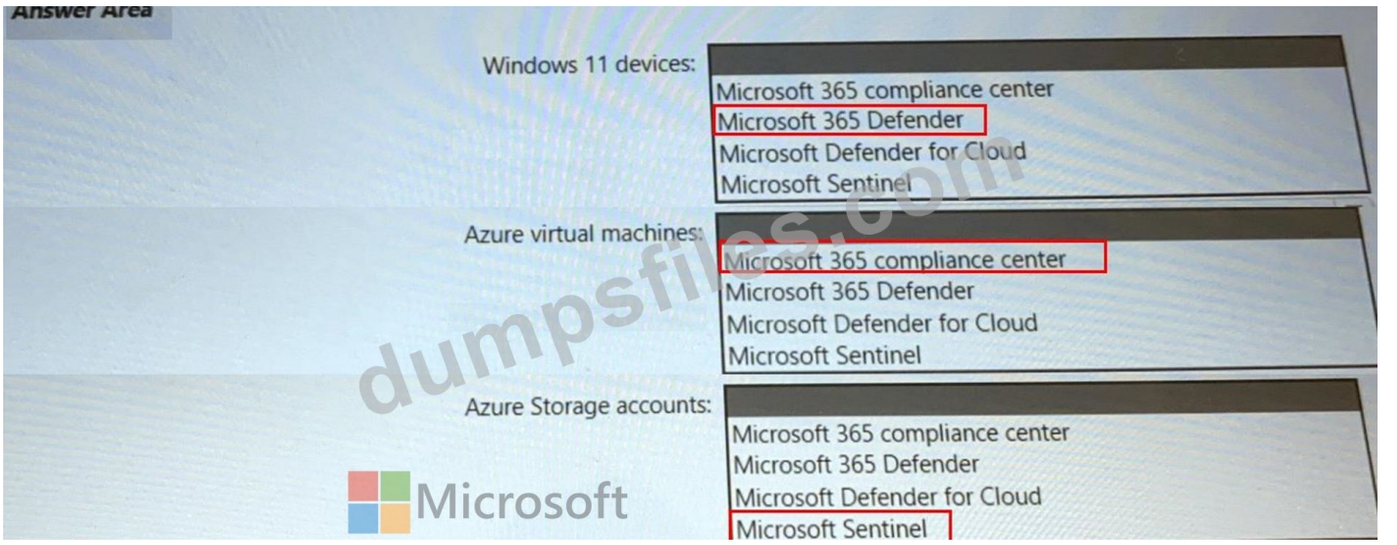


NEW QUESTION: 104
You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers.
In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. Windows containers deployed to Azure Kubernetes Service (AKS)
B. Windows containers deployed to Azure Container Registry
C. Linux containers deployed to Azure Container Registry
D. Linux containers deployed to Azure Kubernetes Service (AKS)
E. Linux containers deployed to Azure Container Instances
Answer: (SHOW ANSWER)

NEW QUESTION: 105
You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:
* Windows 11 devices managed by Microsoft Intune
* Azure Storage accounts
* Azure virtual machines
What should you use to evaluate the components? To answer, select the appropriate options in the answer area.



Answer:

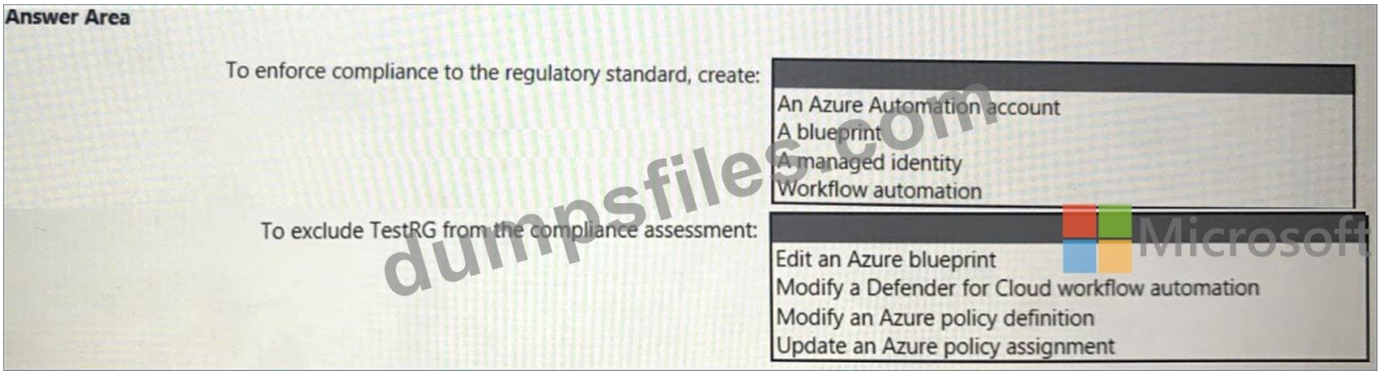


NEW QUESTION: 106

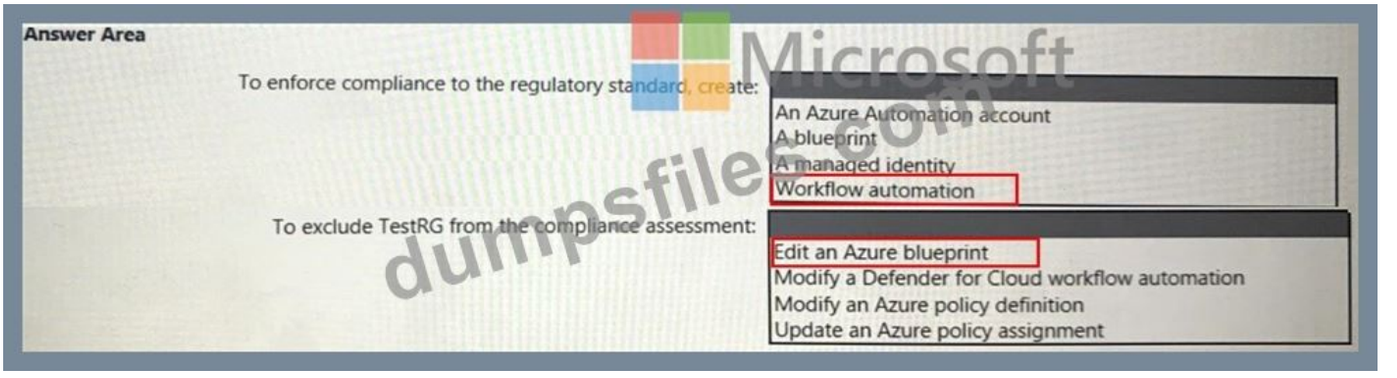
You need to recommend a solution to meet the compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 107

Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

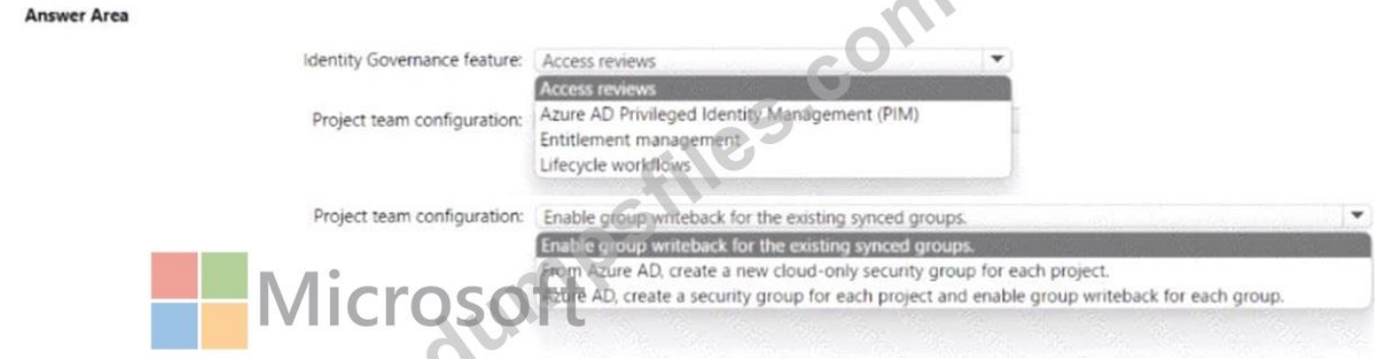
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

You need to recommend an Azure AD identity Governance solution that meets the following requirements:

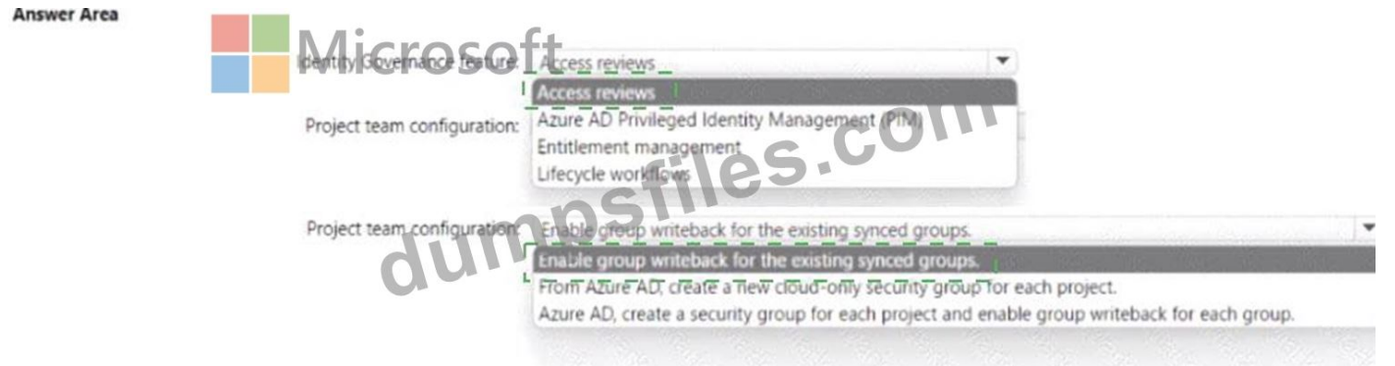
* Project managers must verify that their project group contains only the current members of their project team
* The members of each project team must only have access to the resources of the project to which they are assigned
* Users must be removed from a project group automatically if the project manager has MOT verified the group s membership for 30 days.
* Administrative effort must be minimized.

What should you include in the recommendation? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation: