Microsoft.SC-100.v2023-01-12.q126

Exam Code:	SC-100
Exam Name:	Microsoft Cybersecurity Architect
Certification Provider:	Microsoft
Free Question Number:	126
Version:	v2023-01-12
# of views:	1575
# of Questions views:	3492
https://www.dumpsfiles.com/files/Microsoft/SC-100/Microsoft.SC-100.v2023-01-12.q126	

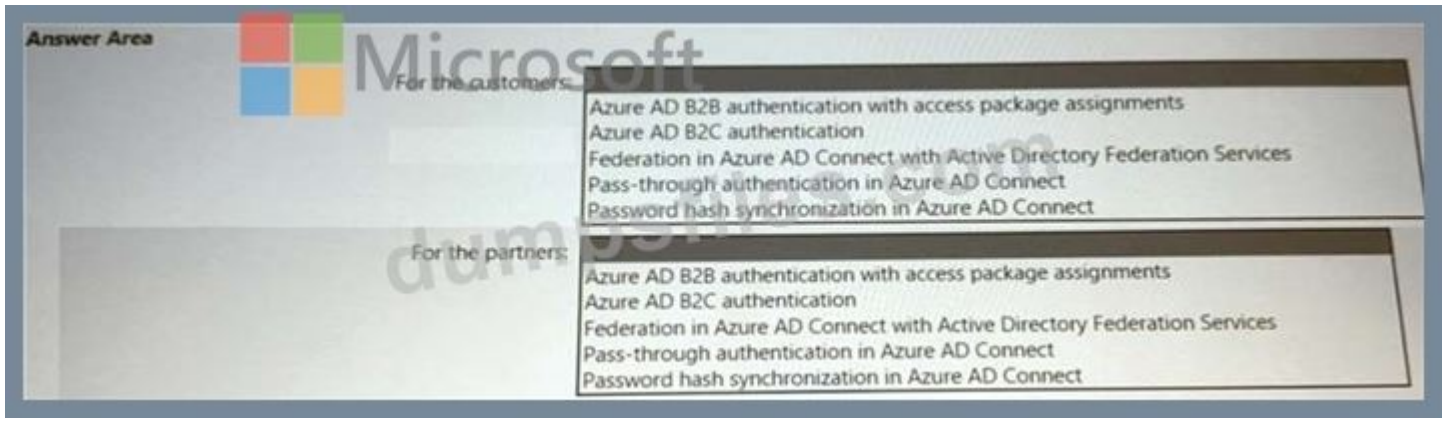
NEW QUESTION: 1
You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

Answer:

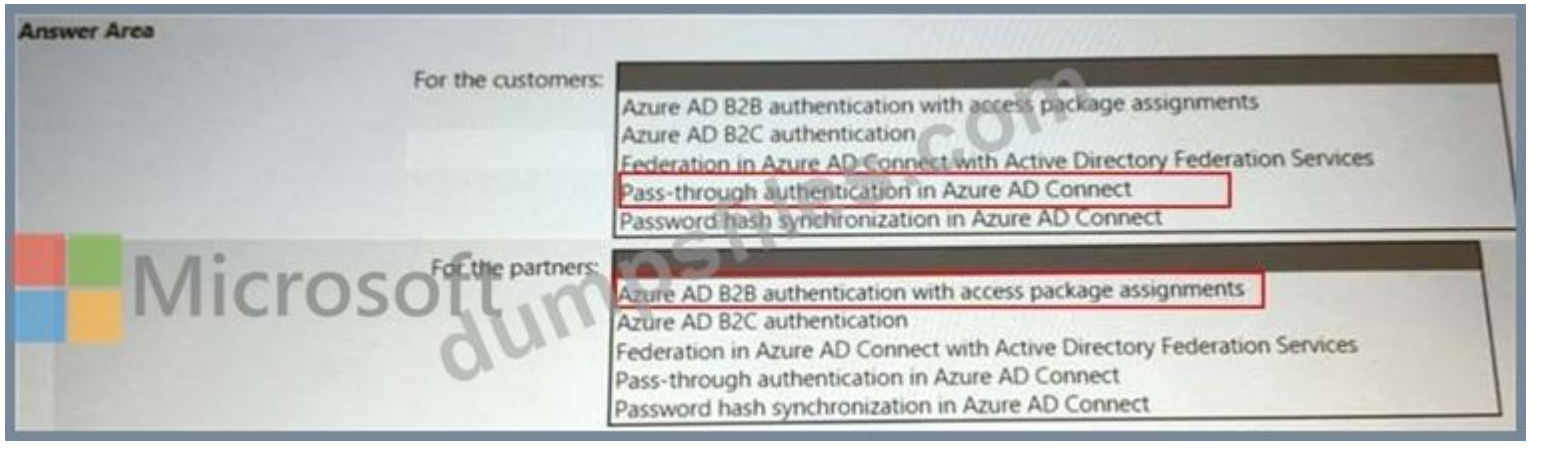
NEW QUESTION: 2
Your company has devices that run either Windows 10, Windows 11, or Windows Server.
You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?
A. Local Group Policy Object (LGPO)

B. Windows Autopilot
C. Microsoft Intune
D. Policy Analyzer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
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.



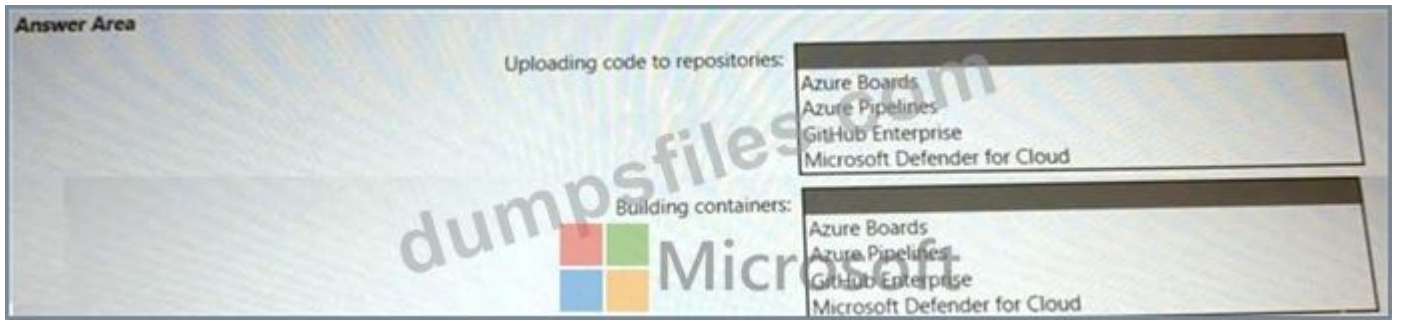
Answer:



NEW QUESTION: 4
You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts. You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts. Which two configurations should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Enable Microsoft Defender for Identity.
B. Send the Azure Cosmos DB logs to a Log Analytics workspace.
C. Disable local authentication for Azure Cosmos DB.

D. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.
E. Enable Microsoft Defender for Cosmos DB.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 5
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.



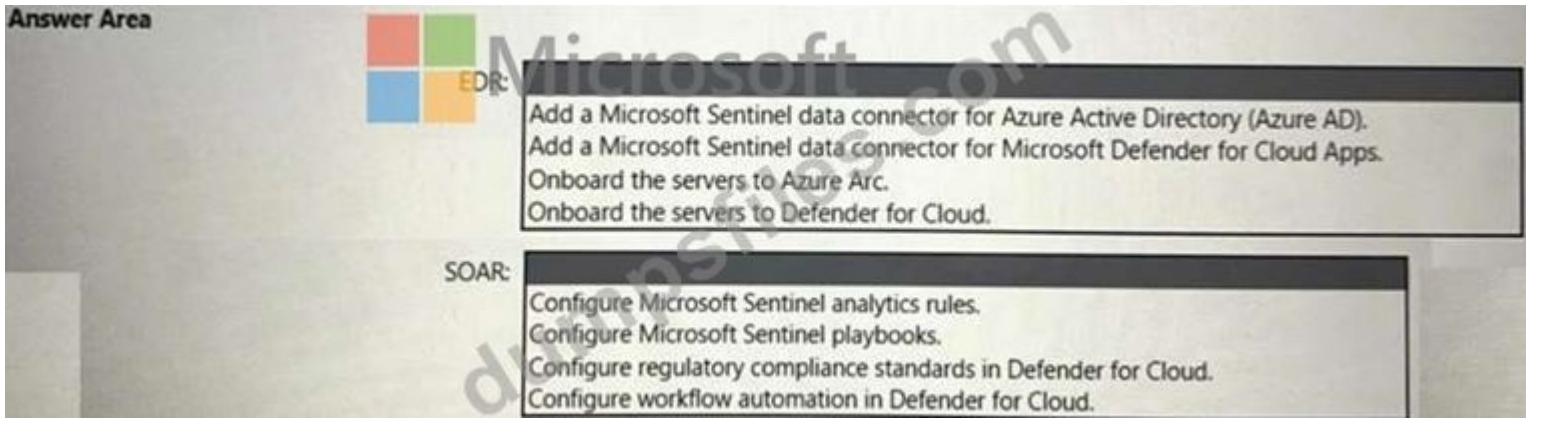
Answer:

Explanation

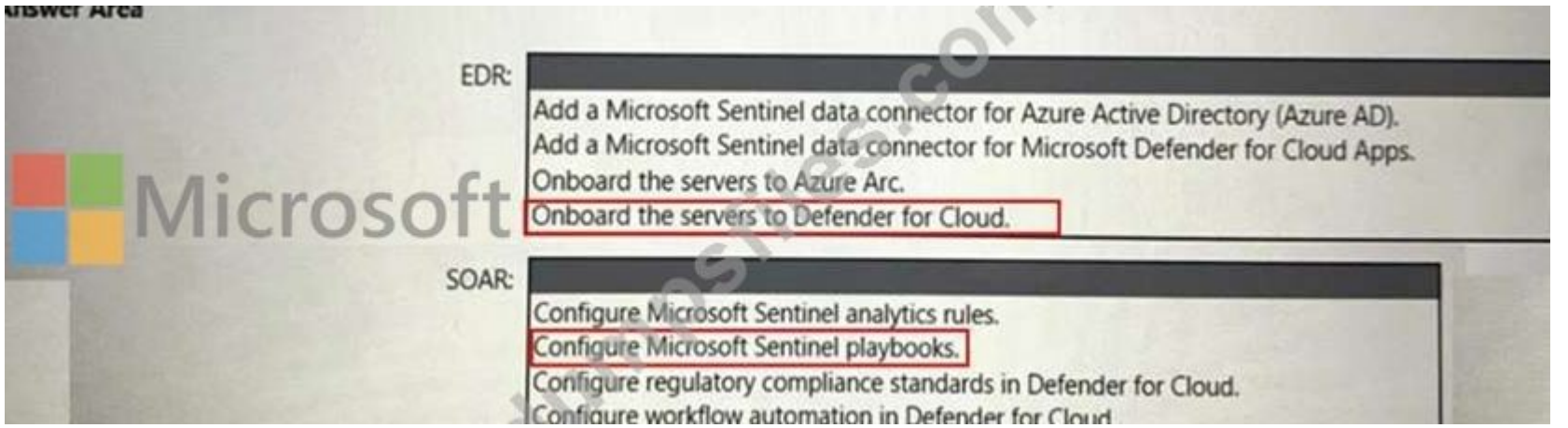
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec
https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-contai

NEW QUESTION: 6
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: 7
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.
You need to recommend a solution for the customer. The solution must minimize costs.
What should you include in the recommendation?
A. Microsoft Defender for Cloud
B. Microsoft Sentinel
C. Microsoft Defender for Cloud Apps
D. Microsoft 365 Defender
Answer: (SHOW ANSWER)

NEW QUESTION: 8
You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. 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: 9

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)

Explanation

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

NEW QUESTION: 10

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. 2

B. 5

C. 1

D. 3

E. 4

Answer: C (LEAVE A REPLY)

NEW QUESTION: 11

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 Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes

B. No

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12

You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:

* Encrypt cardholder data by using encryption keys managed by the company.
* Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.

B. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.

D. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM

Answer: (SHOW ANSWER)

NEW QUESTION: 13

You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts. You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts. Which two configurations should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable Microsoft Defender for Cosmos DB.

B. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.

C. Disable local authentication for Azure Cosmos DB.

D. Enable Microsoft Defender for Identity.

E. Send the Azure Cosmos DB logs to a Log Analytics workspace.

Answer: B,E (LEAVE A REPLY)

Explanation

https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs

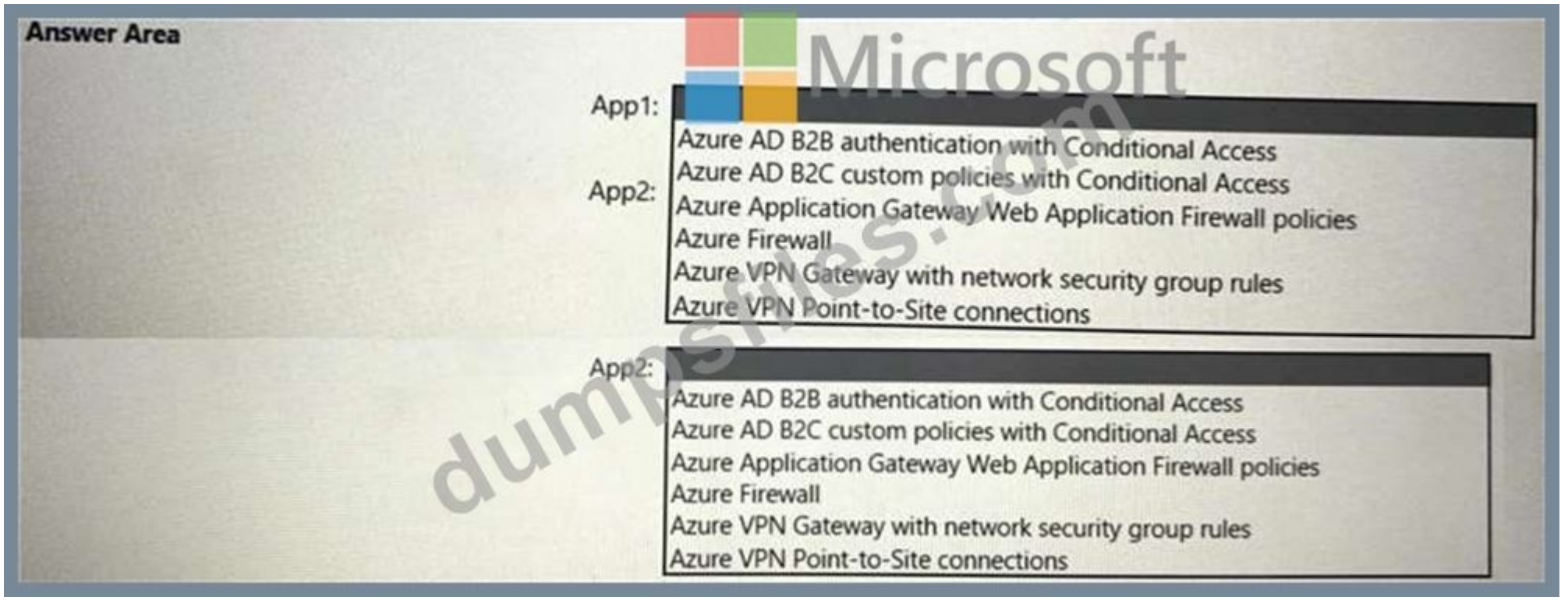
NEW QUESTION: 14

You have a hybrid cloud infrastructure.

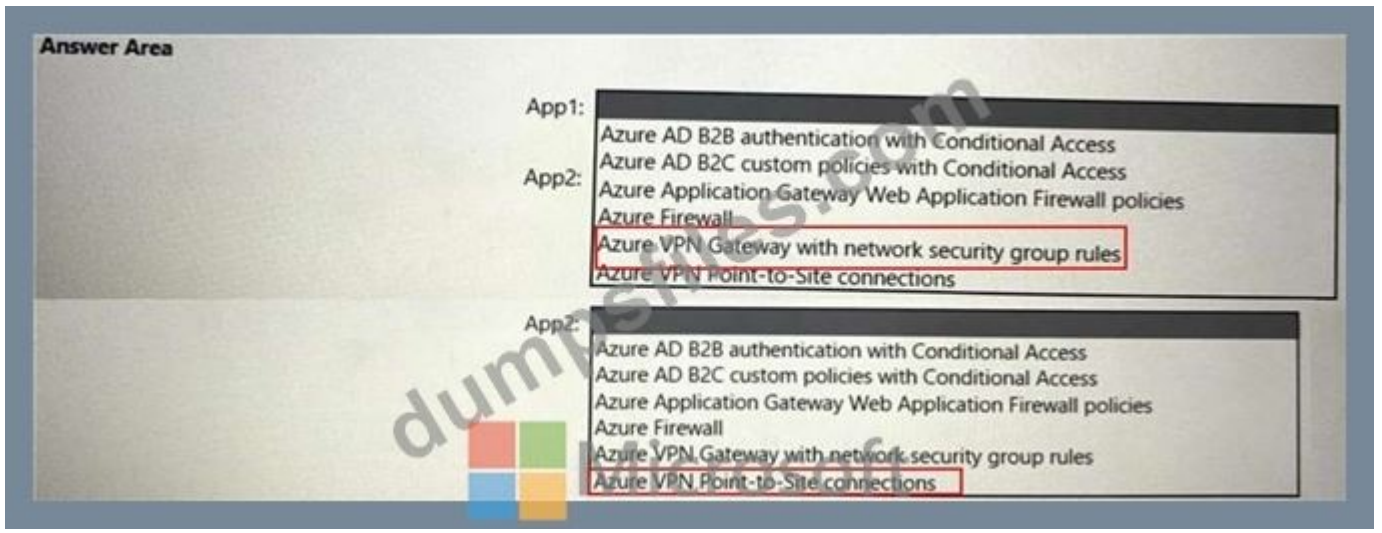
You plan to deploy the Azure applications shown in the following table.

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: 15

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and hunt for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs.

What should you include in the recommendation?

A. Microsoft Sentinel

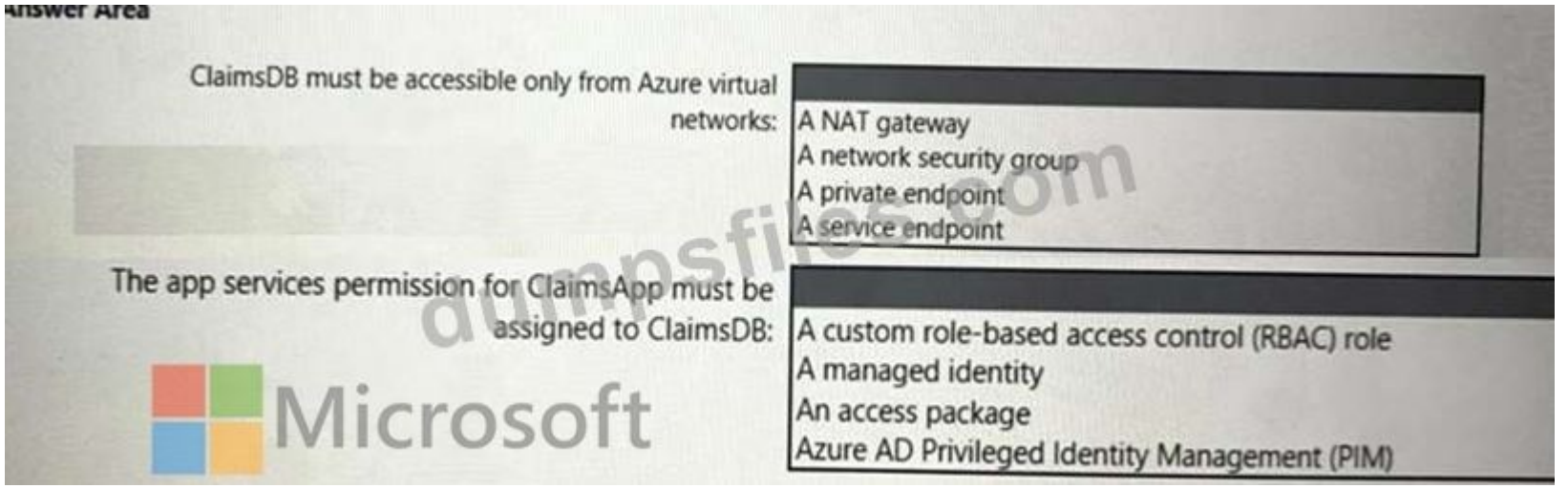
B. Microsoft Defender for Cloud Apps

C. Microsoft 365 Defender

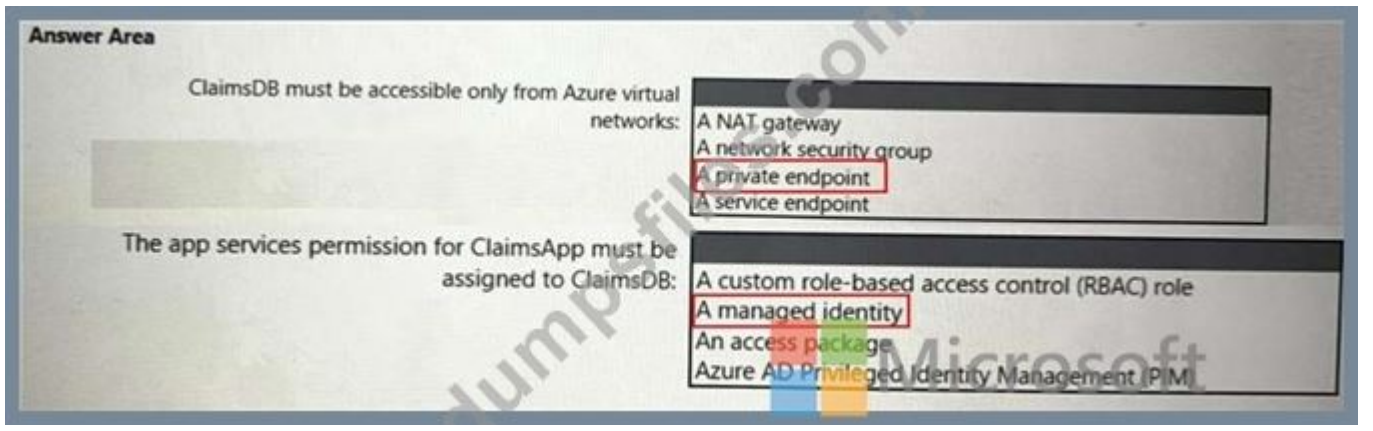
D. Microsoft Defender for Cloud

Answer: A (LEAVE A REPLY)

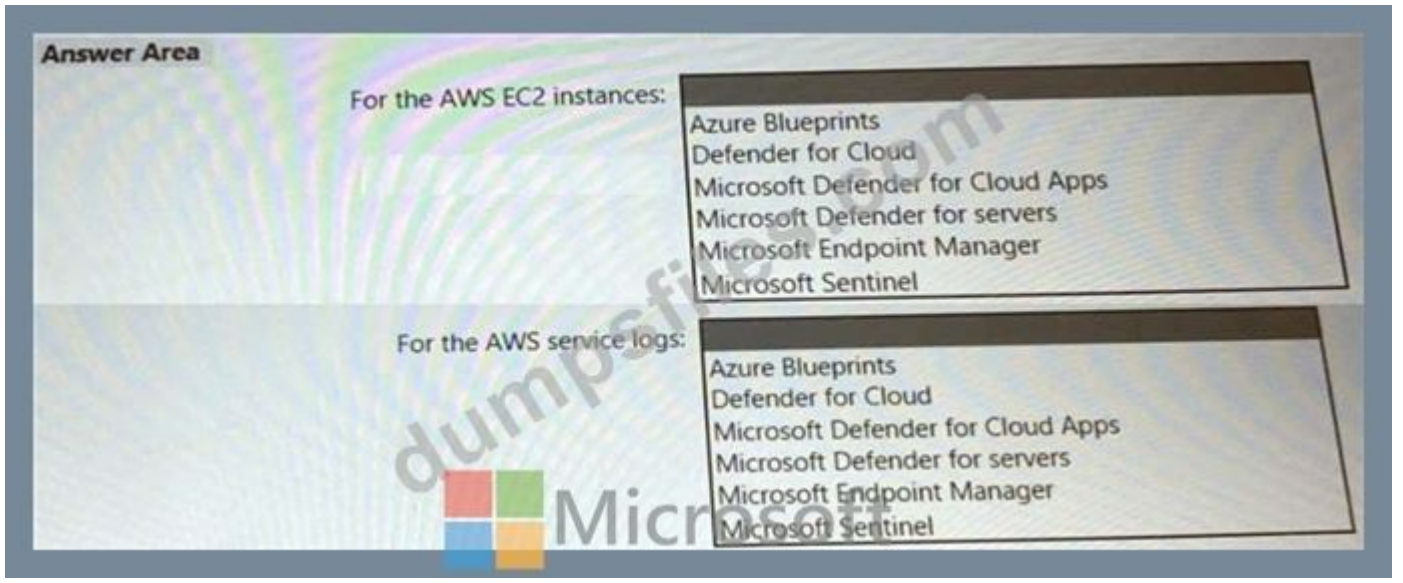
NEW QUESTION: 16
You need to recommend a solution to meet the requirements for connections to ClaimsDB.
What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



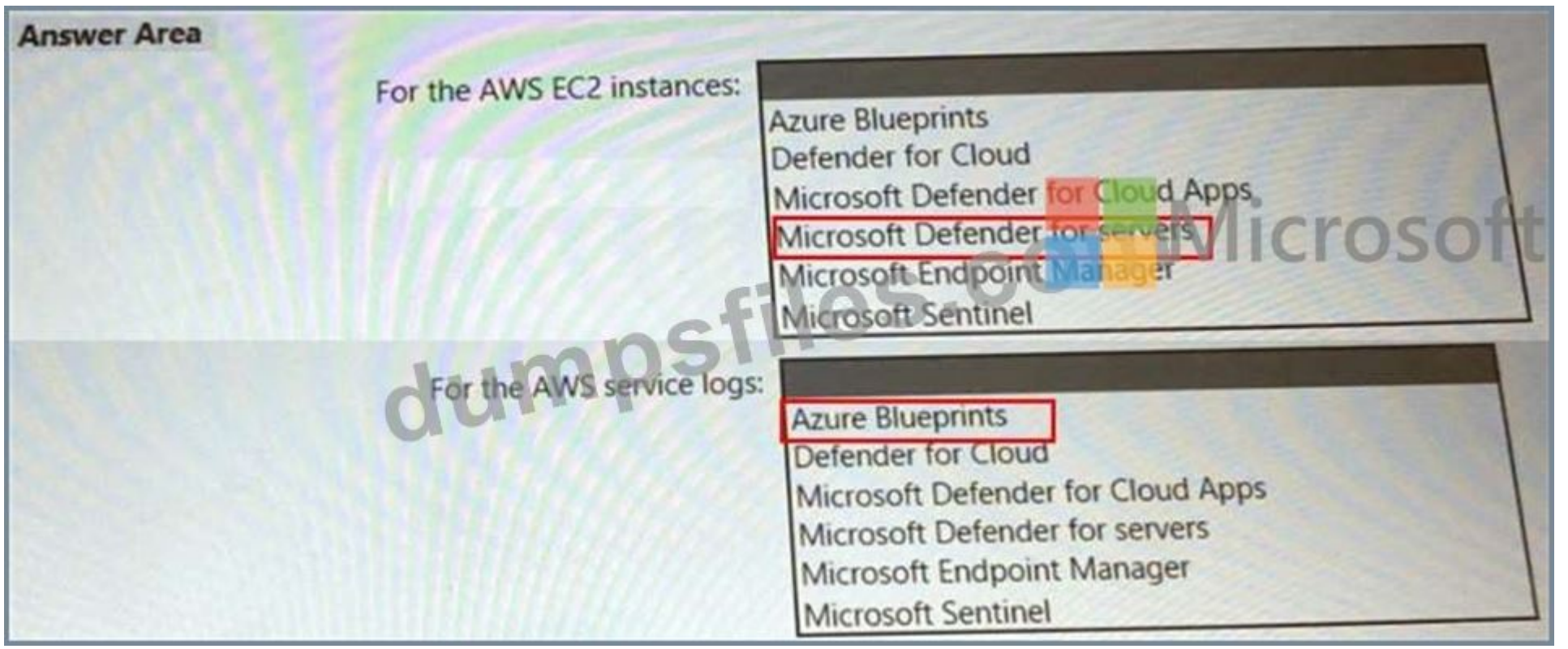
Answer:



NEW QUESTION: 17
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:



Topic 1, Fabrikam, Inc

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: 18

Your company plans to provision blob storage by using an Azure Storage account The blob storage will be accessible from 20 application sewers on the internet. You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

A. managed rule sets in Azure Web Application Firewall (WAF) policies
B. firewall rules for the storage account
C. inbound rules in Azure Firewall
D. inbound rules in network security groups (NSGs)
E. service tags in network security groups (NSGs)
Answer: D (LEAVE A REPLY)

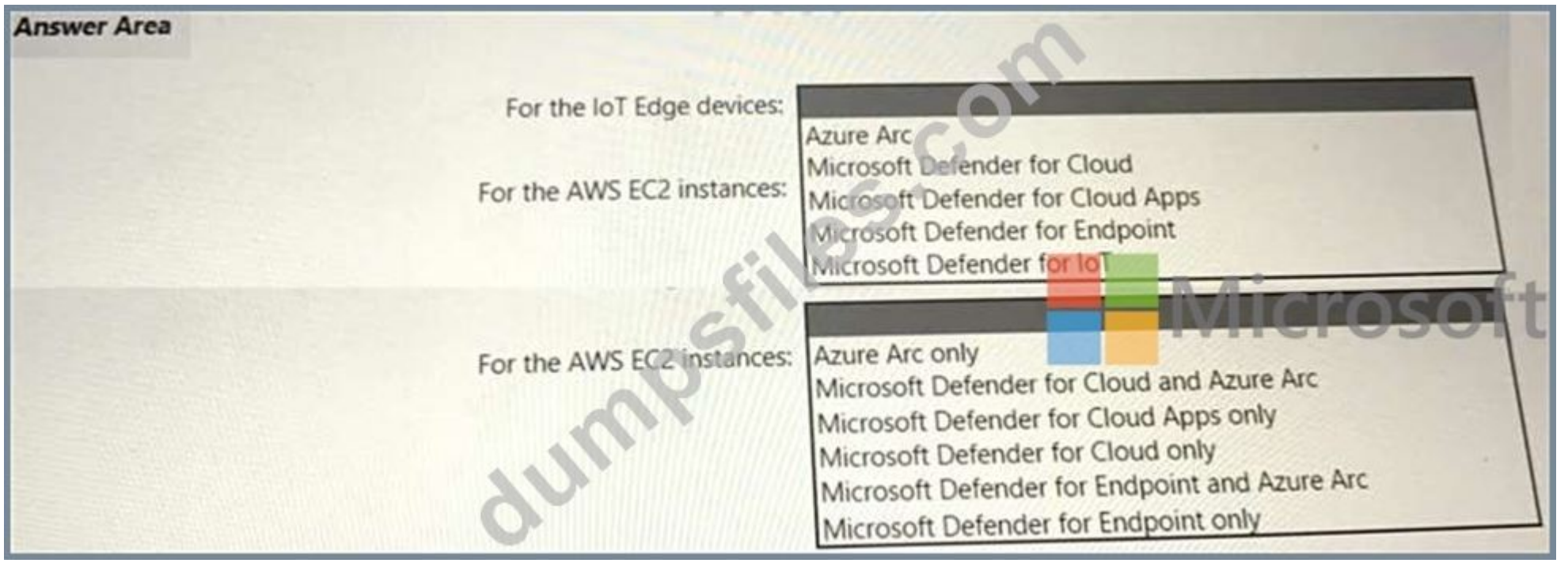
NEW QUESTION: 19

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

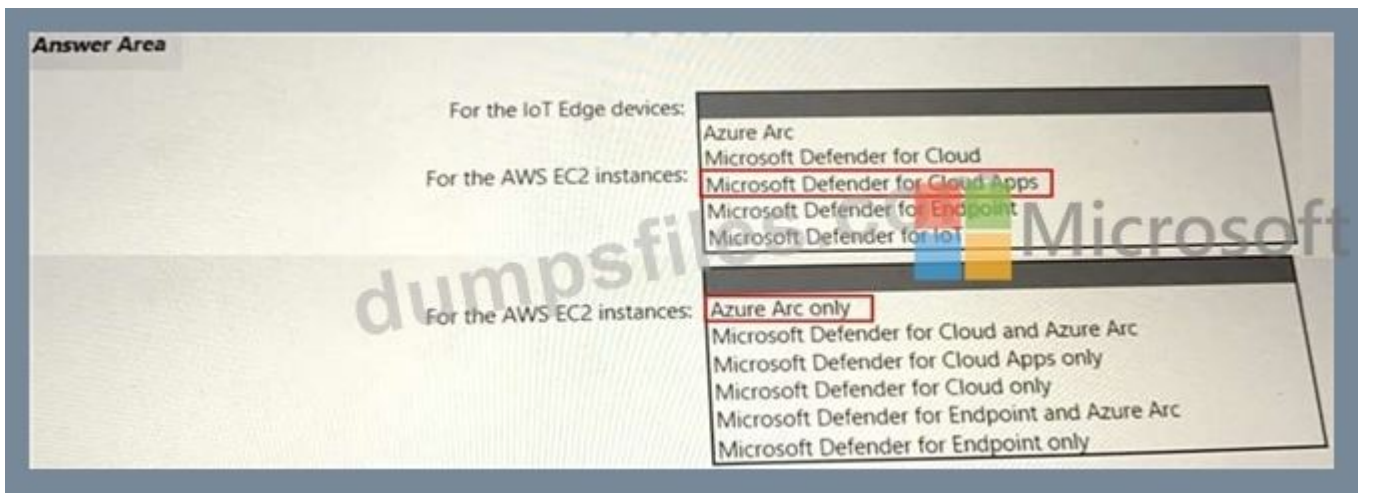
* Azure loT Edge devices
* AWS EC2 instances

Which services 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: 20

You are designing the encryption standards for data at rest for an Azure resource You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).

Does this meet the goal?

A. No

B. Yes

Answer: (SHOW ANSWER)

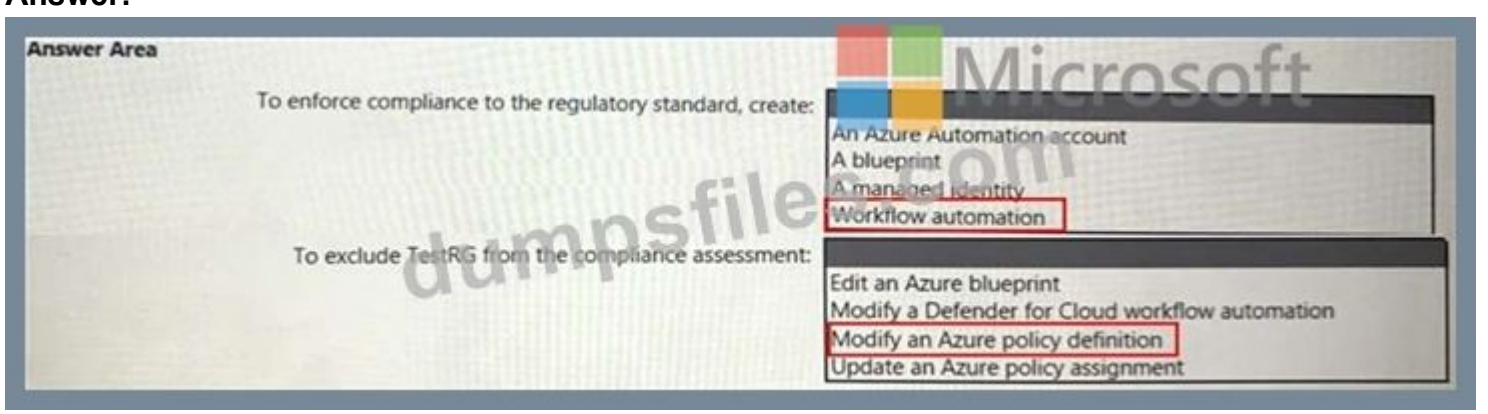
NEW QUESTION: 21

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:

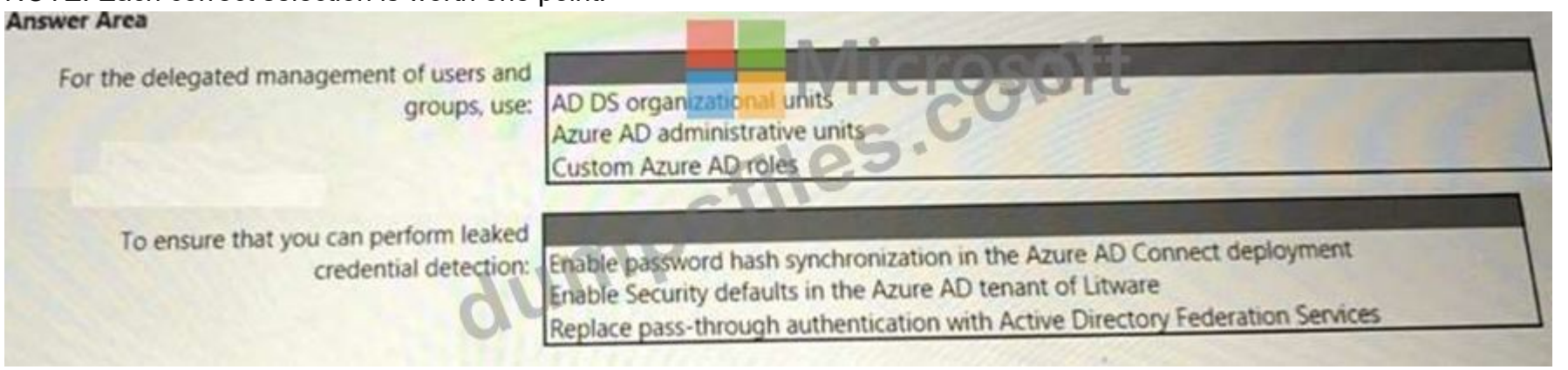


NEW QUESTION: 22

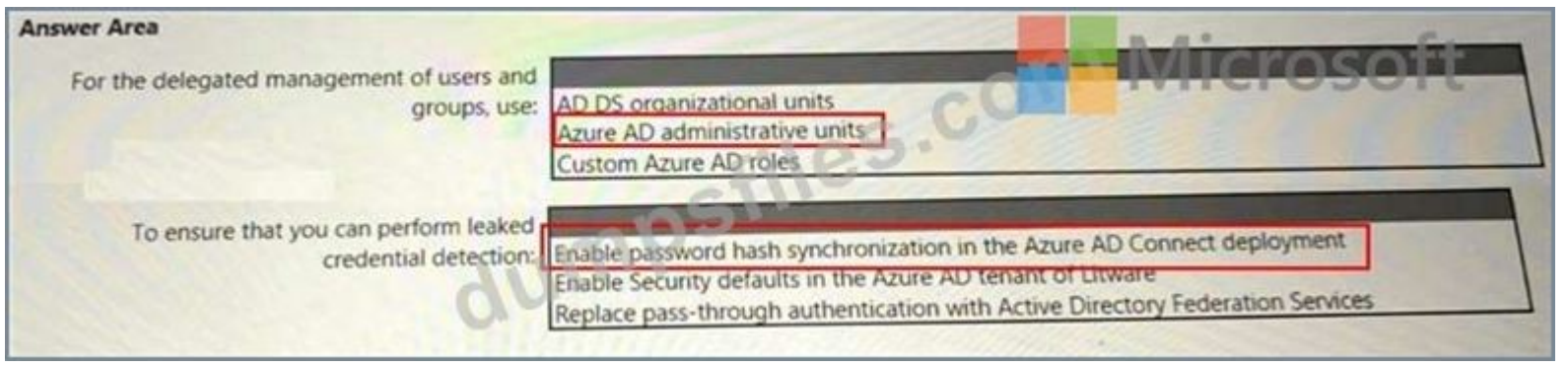
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.



Answer:



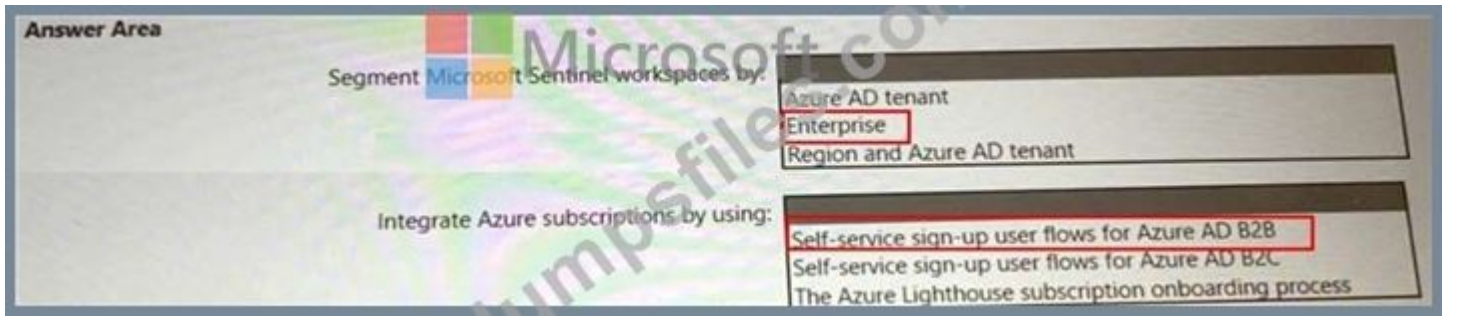
NEW QUESTION: 23

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: 24

You are creating the security recommendations for an Azure App Service web app named App1.

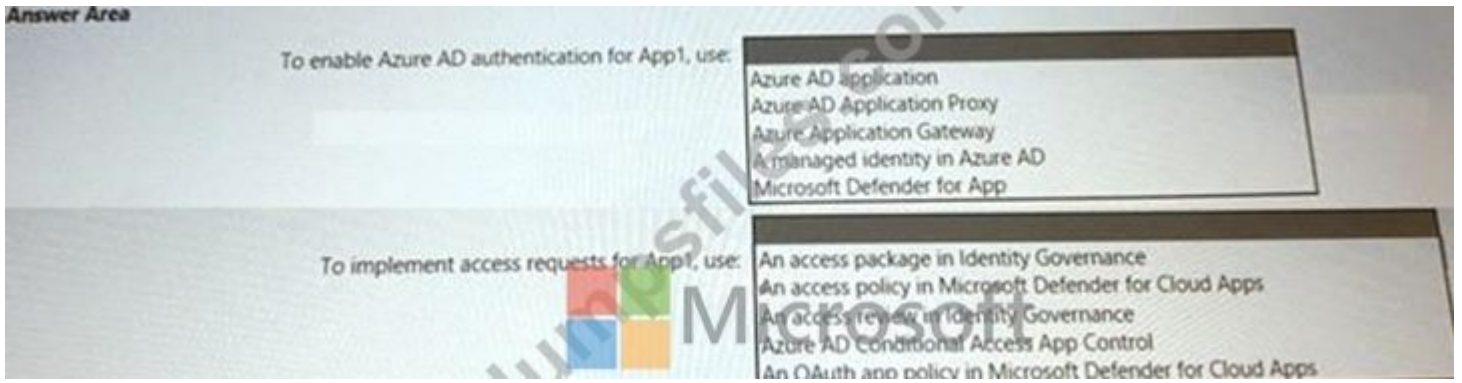
App1 has the following specifications:

* 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.

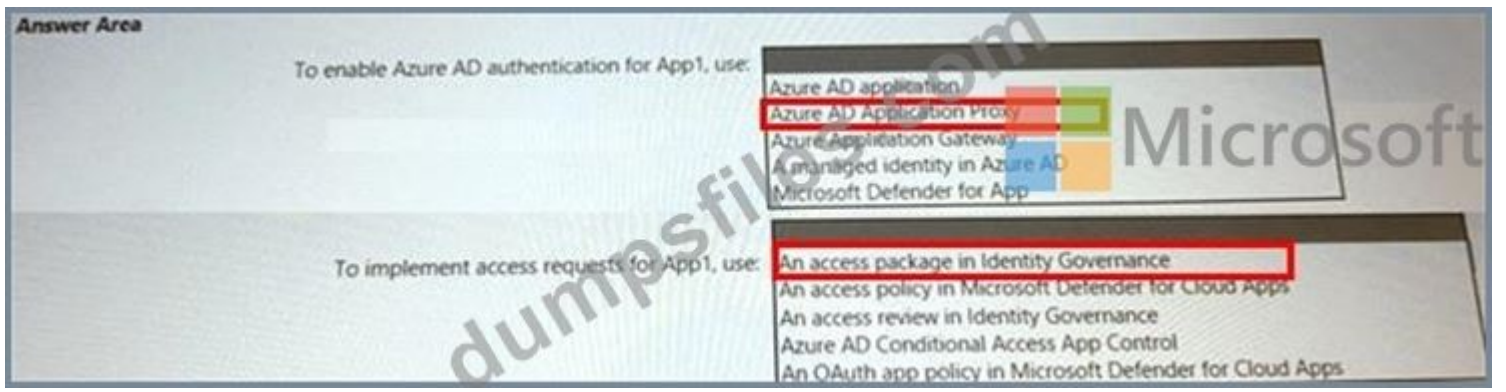
You need to recommend an access security architecture for App1.

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

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

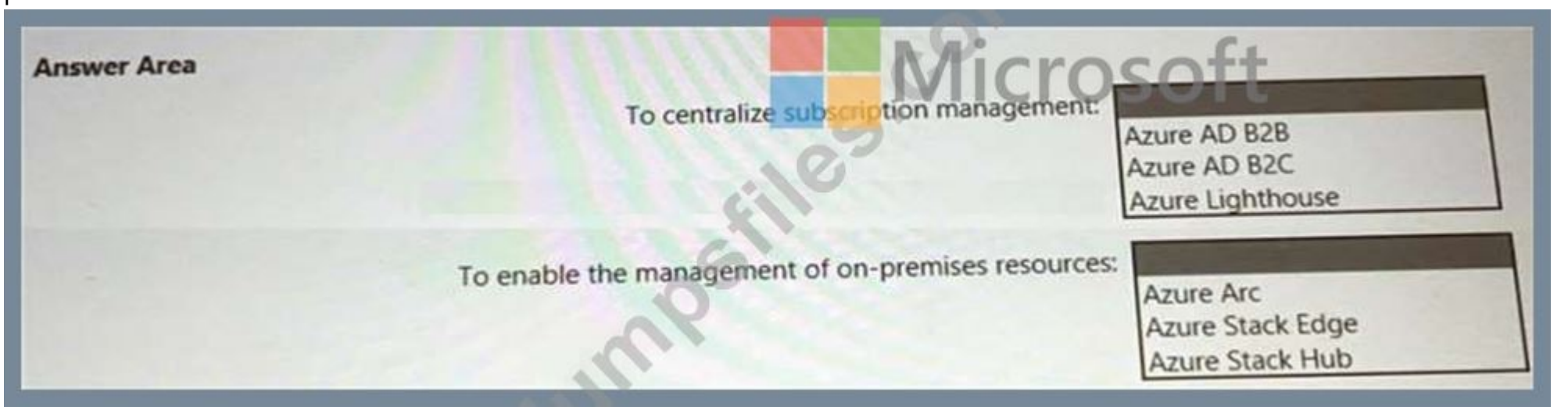


Answer:

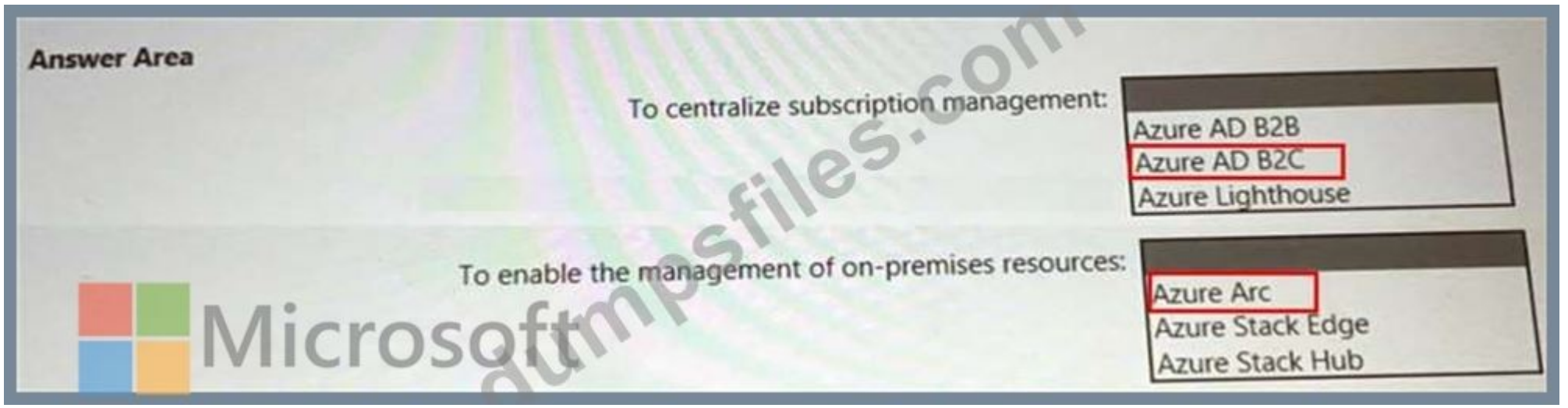


NEW QUESTION: 25

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: 26

Your company has an office in Seattle.

The company has two Azure virtual machine scale sets hosted on different virtual networks.

The company plans to contract developers in India.

You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal.

The solution must meet the following requirements:

* Prevent exposing the public IP addresses of the virtual machines.
* Provide the ability to connect without using a VPN.
* Minimize costs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Deploy Azure Bastion to one virtual network.

B. Deploy Azure Bastion to each virtual network.

C. Enable just-in-time VM access on the virtual machines.

D. Create a hub and spoke network by using virtual network peering.

E. Create NAT rules and network rules in Azure Firewall.

Answer: A,D (LEAVE A REPLY)

Explanation

https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

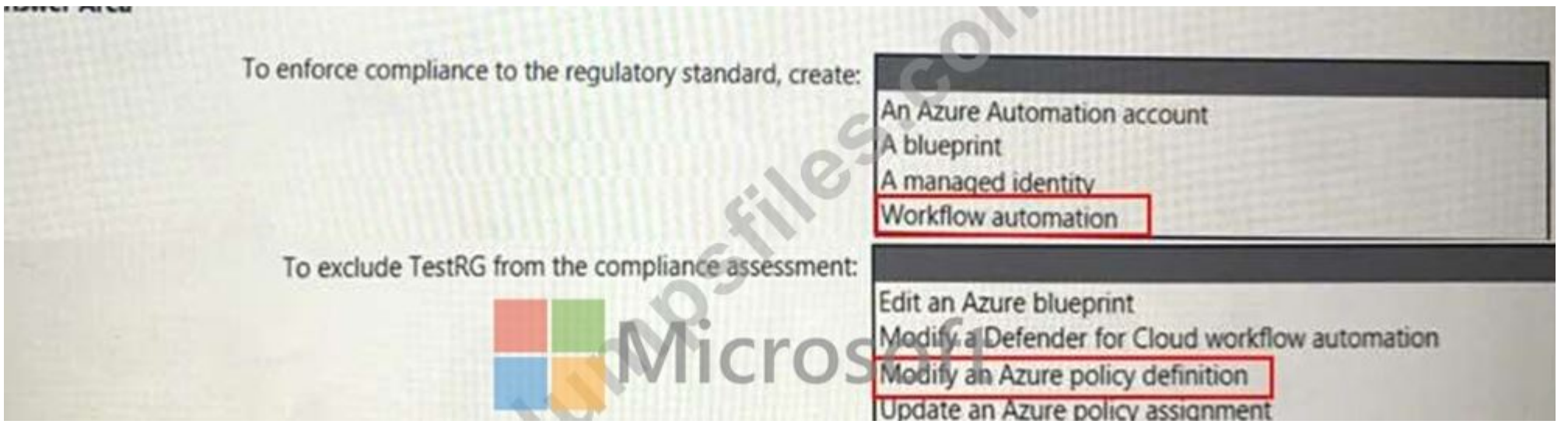
NEW QUESTION: 27

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: 28

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

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 (LEAVE A REPLY)

Topic 2, 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.

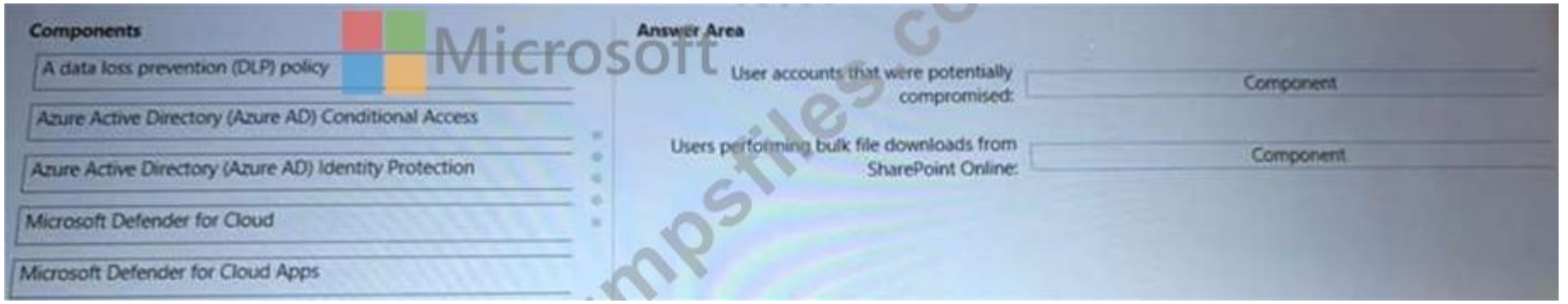
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

* Be created in a dedicated subscription.
* Use a DNS namespace of litware.com.

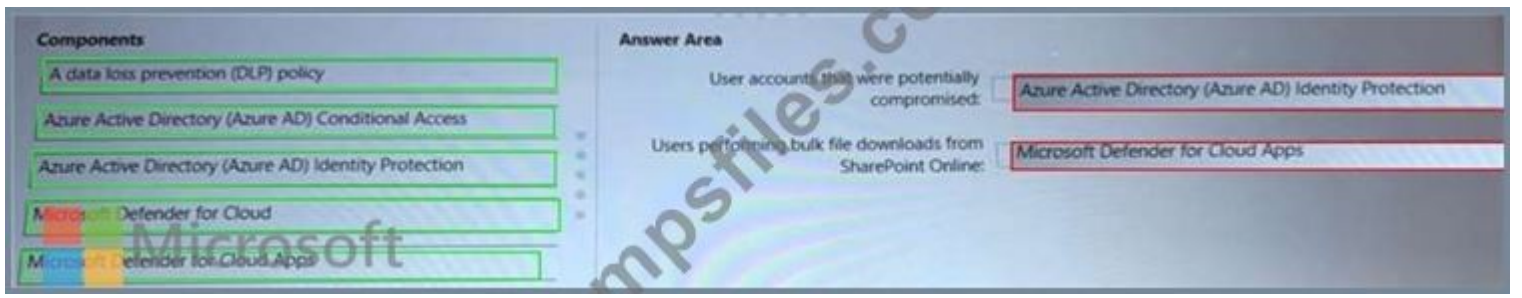
Application Security Requirements

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: 29
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:



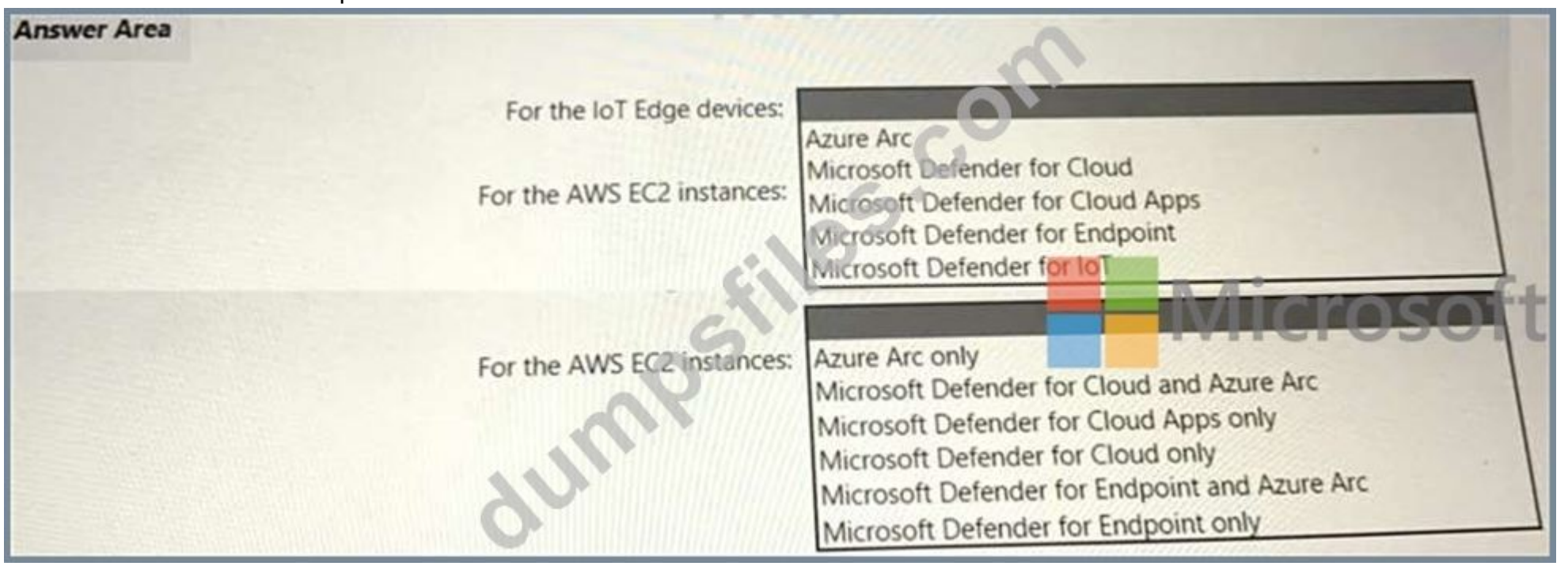
NEW QUESTION: 30
You need to design a strategy for securing the SharePoint Online and Exchange Online dat a. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.
A. Microsoft Defender for Endpoint
B. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. access reviews in Azure AD
E. Azure AD Conditional Access
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 31

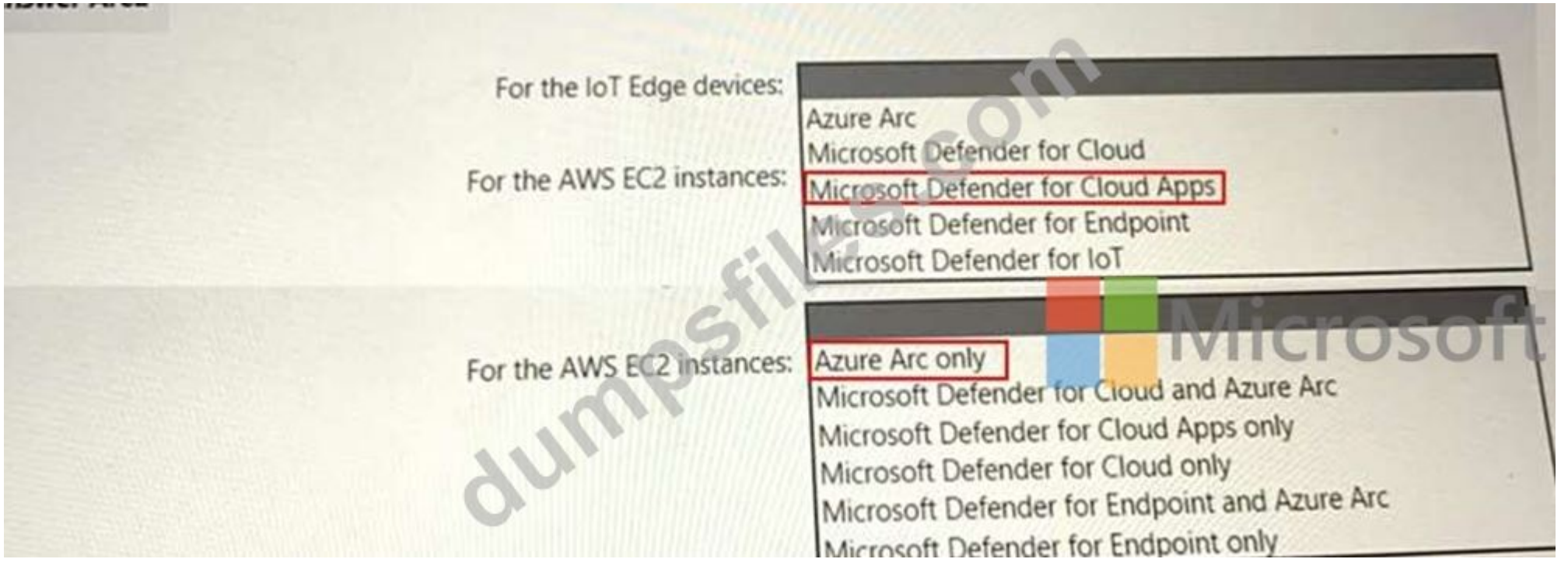
Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

* Azure IoT Edge devices
* AWS EC2 instances

Which services 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:



Topic 2, Fabrikam, Inc

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;

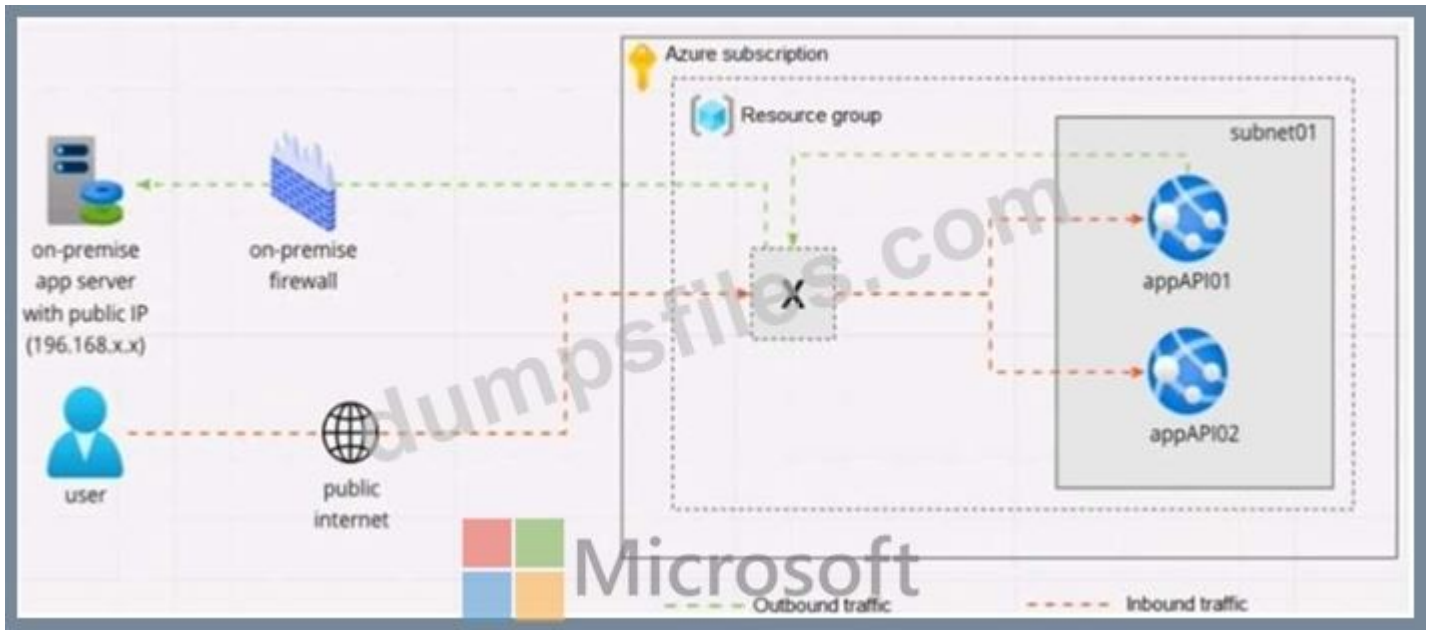
* Every month, the membership of the ContosoDevelopers group must be verified.
* The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
* The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the 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: 32

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Front Door with Azure Web Application Firewall (WAF)

B. Azure Application Gateway v2 with user-defined routes (UDRs).

C. Azure Firewall with policy rule sets

D. Azure Traffic Manager with priority traffic-routing methods

Answer: A (LEAVE A REPLY)

NEW QUESTION: 33

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. threat modeling by using the Microsoft Threat Modeling Tool

C. static application security testing (SAST) by using SonarQube

D. dynamic application security testing (DAST) by using Veracode

Answer: (SHOW ANSWER)

NEW QUESTION: 34

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: 35
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)
Explanation
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulat

NEW QUESTION: 36
You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?
A. Azure DevTest Labs
B. Azure Key Vault
C. Application Insights in Azure Monitor
D. GitHub Advanced Security
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
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: 38

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C.

The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies

B. access packages in Identity Governance

C. Azure AD workbooks to monitor risk detections

D. custom resource owner password credentials (ROPC) flows in Azure AD B2C

E. smart account lockout in Azure AD B2C

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 39

You have a Microsoft 365 E5 subscription.

You need to recommend a solution to add a watermark to email attachments that contain sensitive dat

a. What should you include in the recommendation?

A. insider risk management

B. Microsoft Defender for Cloud Apps

C. Microsoft Information Protection

D. Azure Purview

Answer: B (LEAVE A REPLY)

NEW QUESTION: 40

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

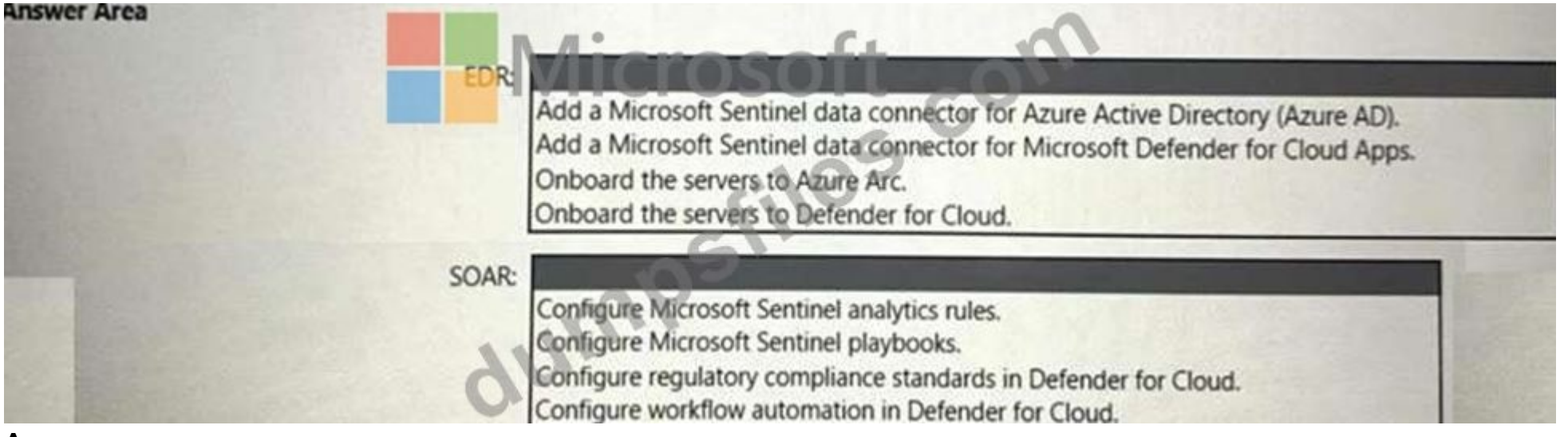
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

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

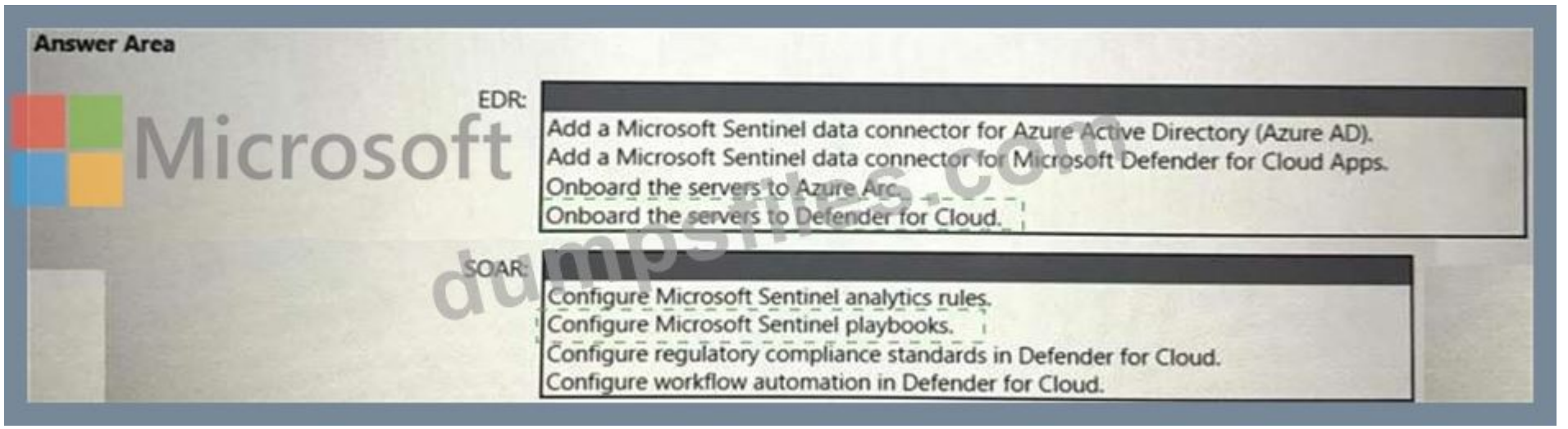
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

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

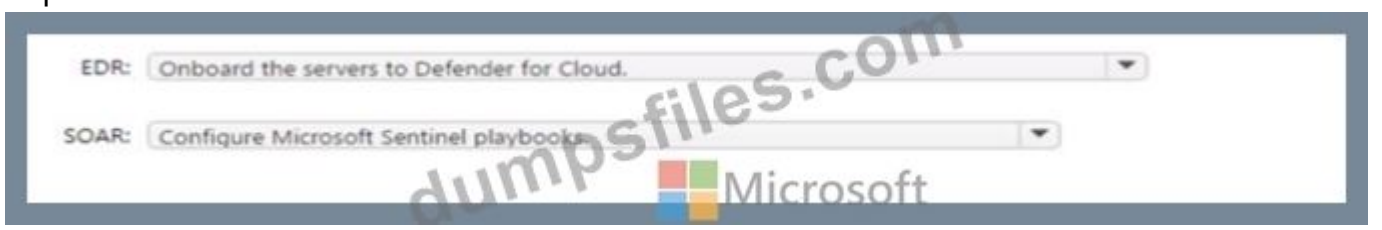
NOTE: Each correct selection is worth one point.



Answer:



Explanation



NEW QUESTION: 41

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: 42

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

Answer:

NEW QUESTION: 43

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: 44

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 Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

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

D. From Defender for Cloud, add a regulatory compliance standard.

Answer: D (LEAVE A REPLY)

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

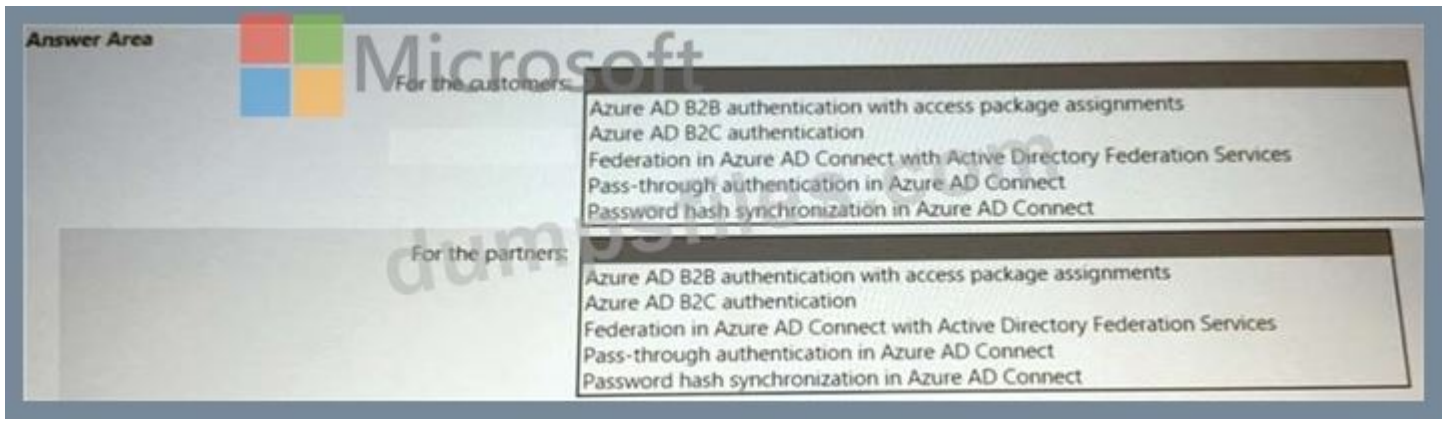
NEW QUESTION: 45

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:

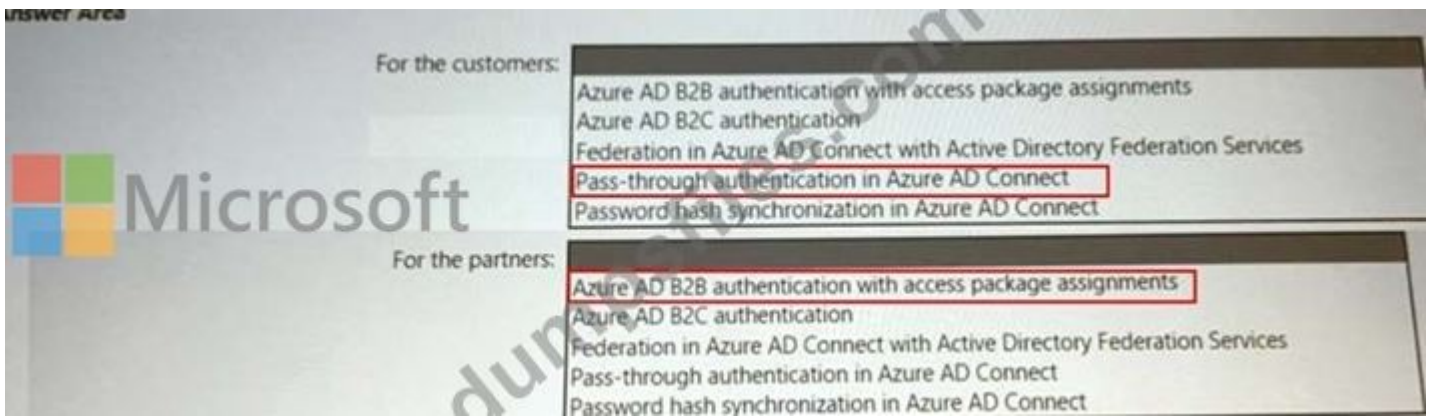
* Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

* 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.



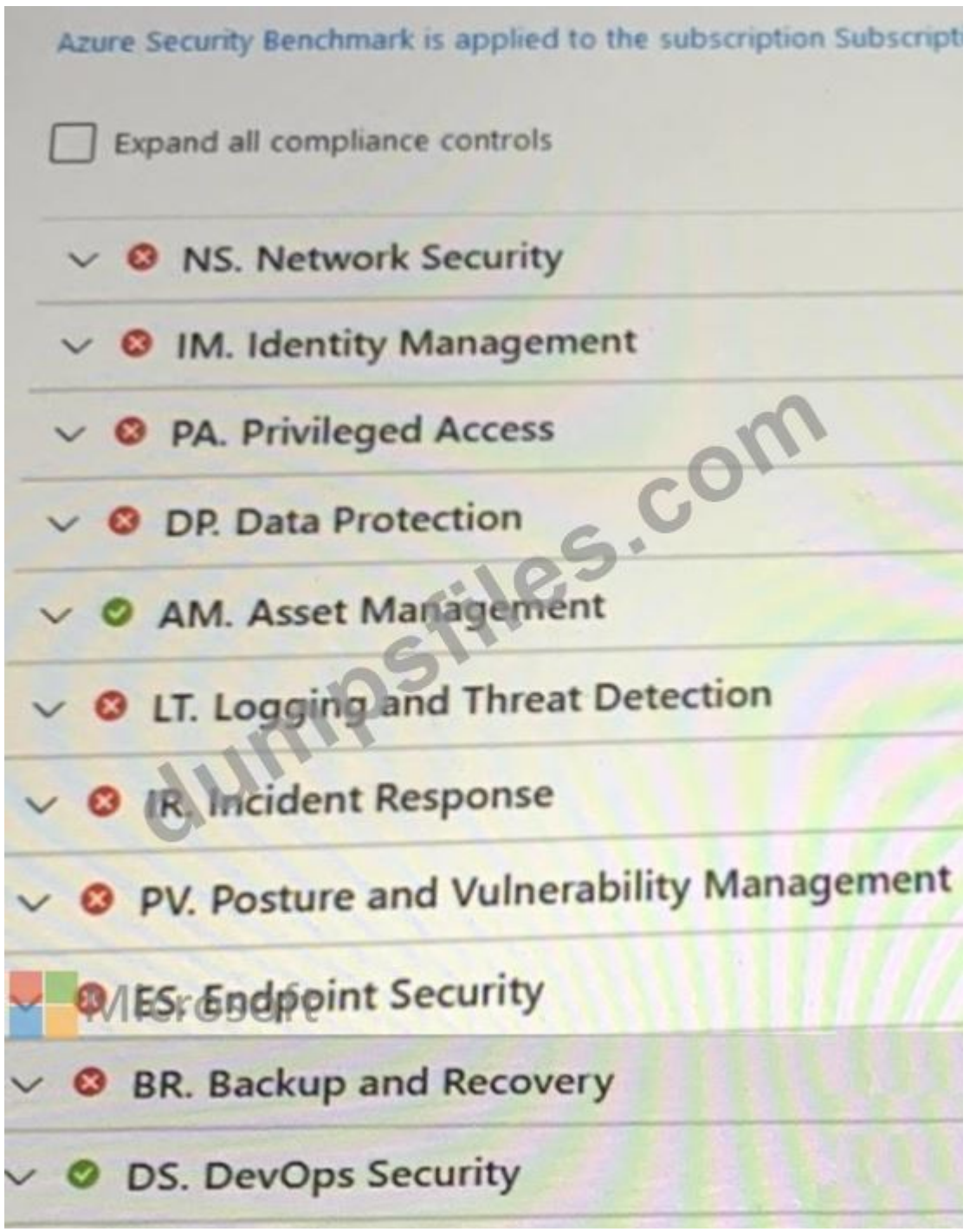
Answer:



NEW QUESTION: 46

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: E (LEAVE A REPLY)

Explanation

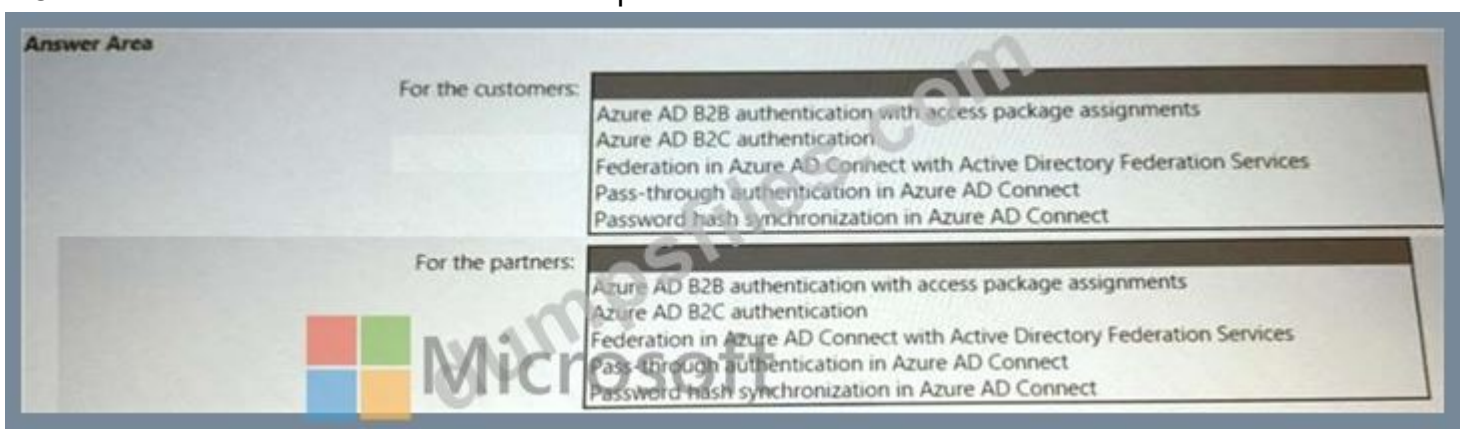
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

NEW QUESTION: 47
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.

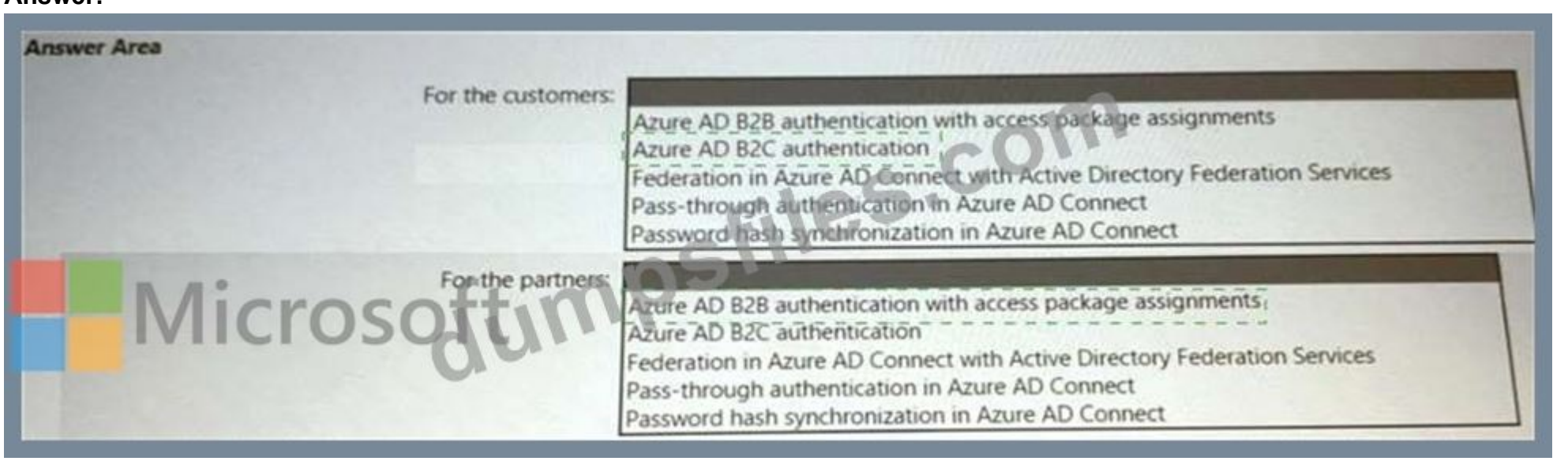
Answer:

NEW QUESTION: 48
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:



Explanation

Graphical user interface, application Description automatically generated

Box 1 --> https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview Box 2 -- > https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers

NEW QUESTION: 49

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

* Prevent the need to enable ports 3389 and 22 from the internet.
* Only provide permission to connect the virtual machines when required.
* Ensure that administrators use the Azure portal to connect to the virtual machines.

Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
B. Configure Azure VPN Gateway.
C. Enable Just Enough Administration (JEA).
D. Enable just-in-time (JIT) VM access.
E. Configure Azure Bastion.
Answer: C,E (LEAVE A REPLY)
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: 50
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.

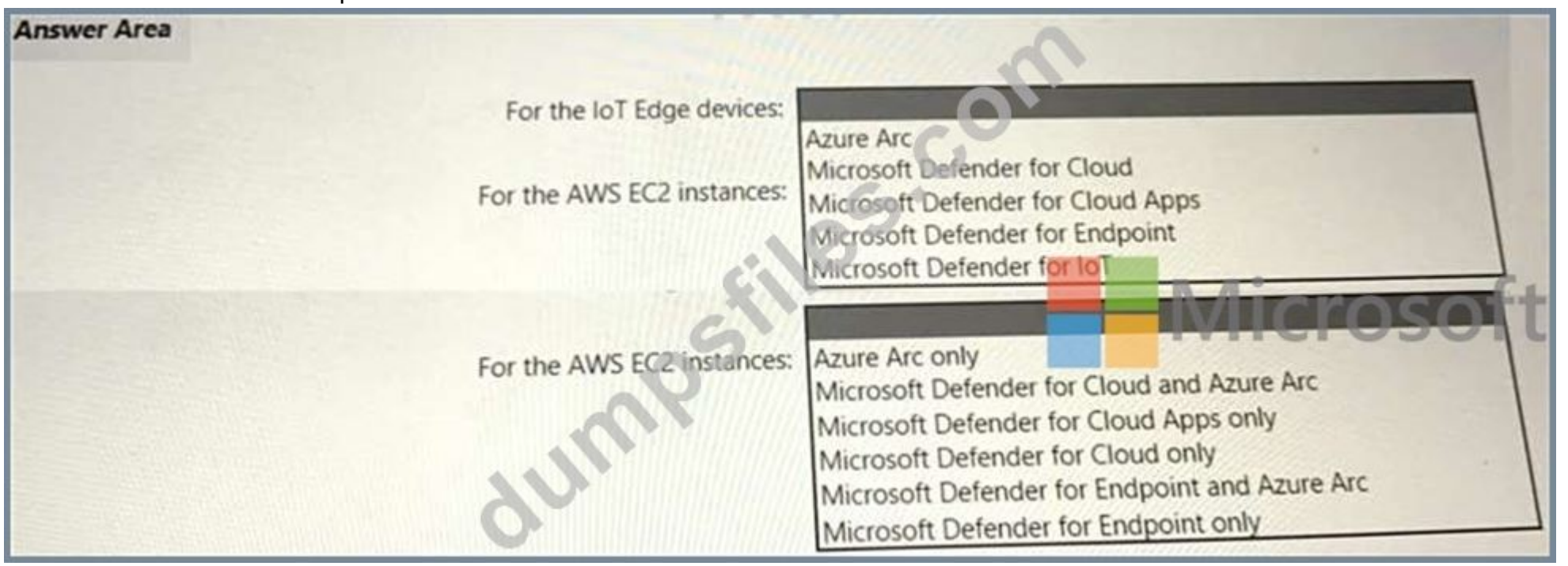
You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF). Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

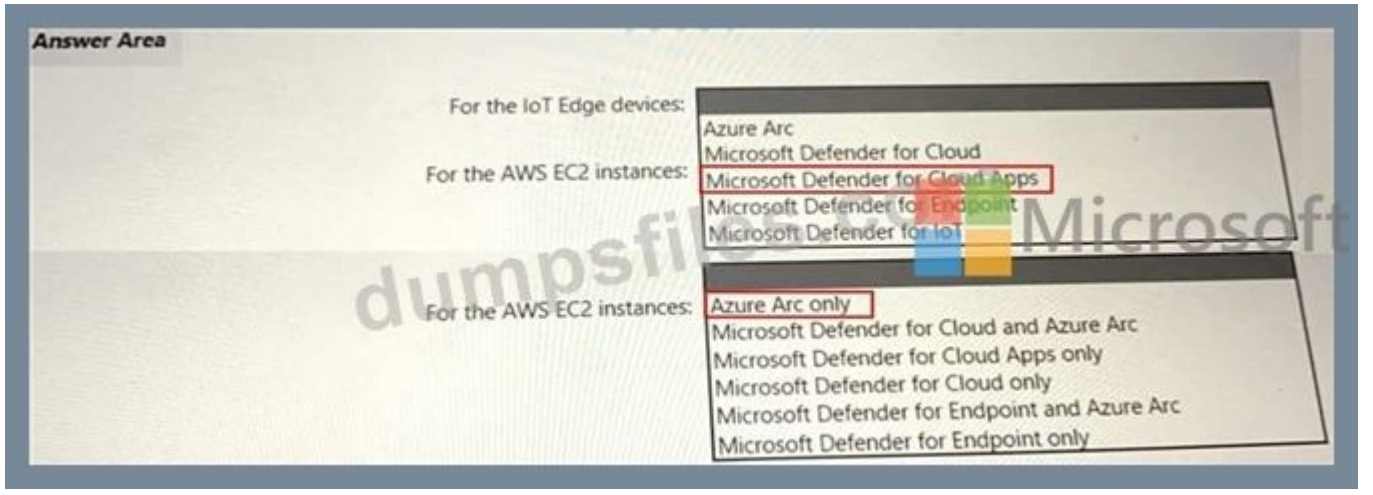
Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

* Azure IoT Edge devices
* AWS EC2 instances

Which services 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: 52

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 Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

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

D. From Defender for Cloud, add a regulatory compliance standard.

Answer: D (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 53

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

* Access to storage accounts with firewall and virtual network configurations should be restricted,
* Storage accounts should restrict network access using virtual network rules.
* Storage account should use a private link connection.
* Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations. What should you recommend?

A. Azure Storage Analytics

B. Azure Network Watcher

C. Microsoft Sentinel

D. Azure Policy

Answer: D (LEAVE A REPLY)

Explanation

https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept

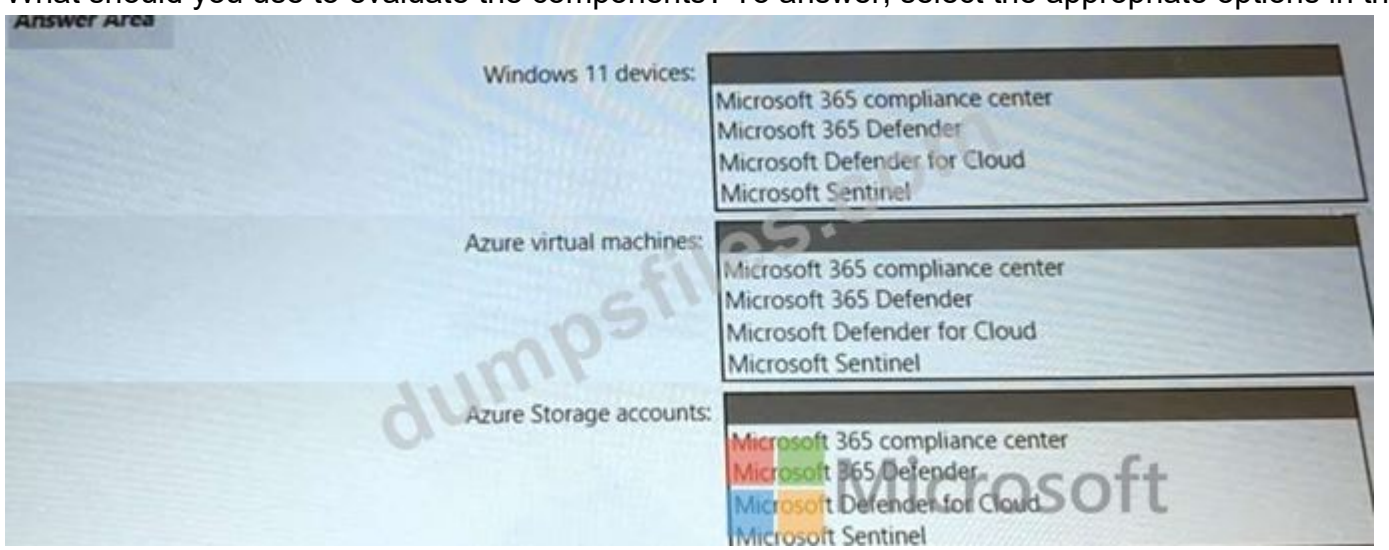
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

NEW QUESTION: 54

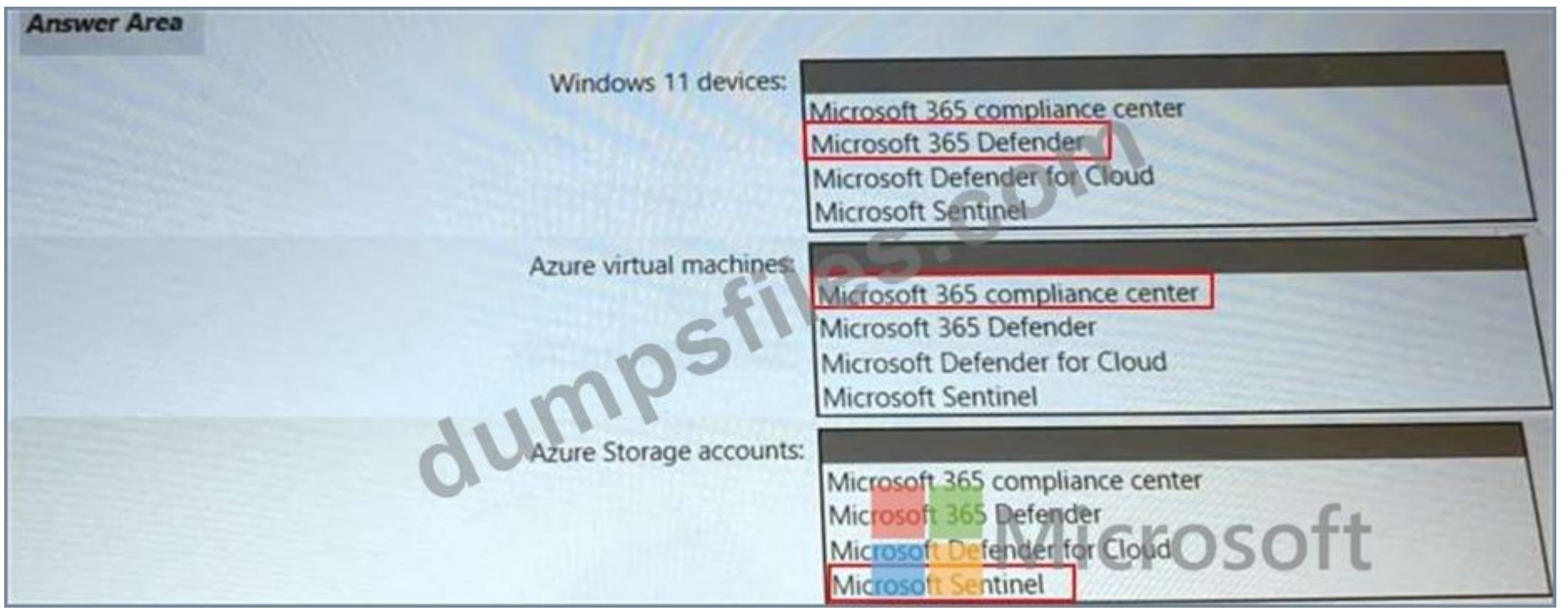
You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:

* 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: 55

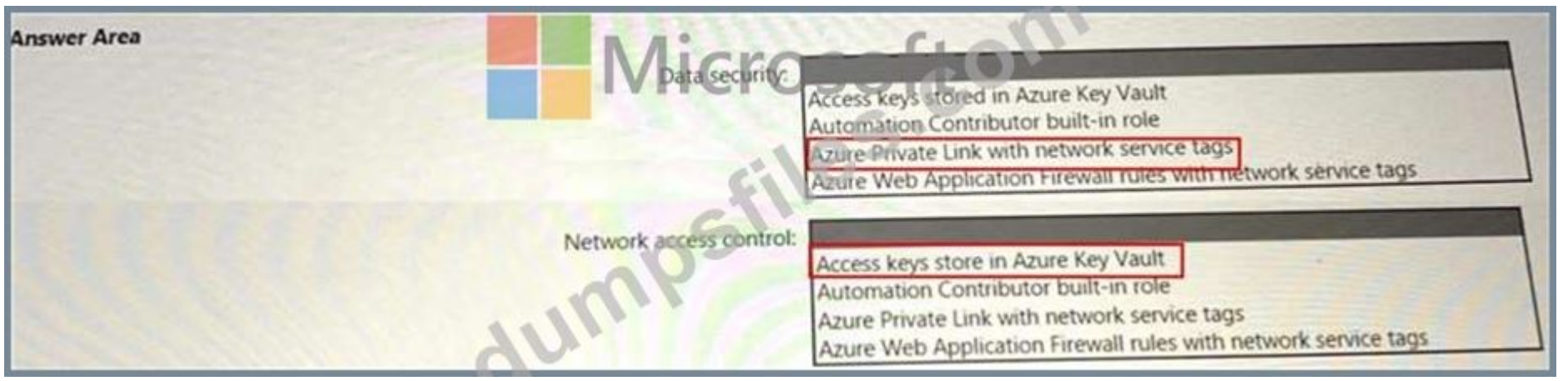
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

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.

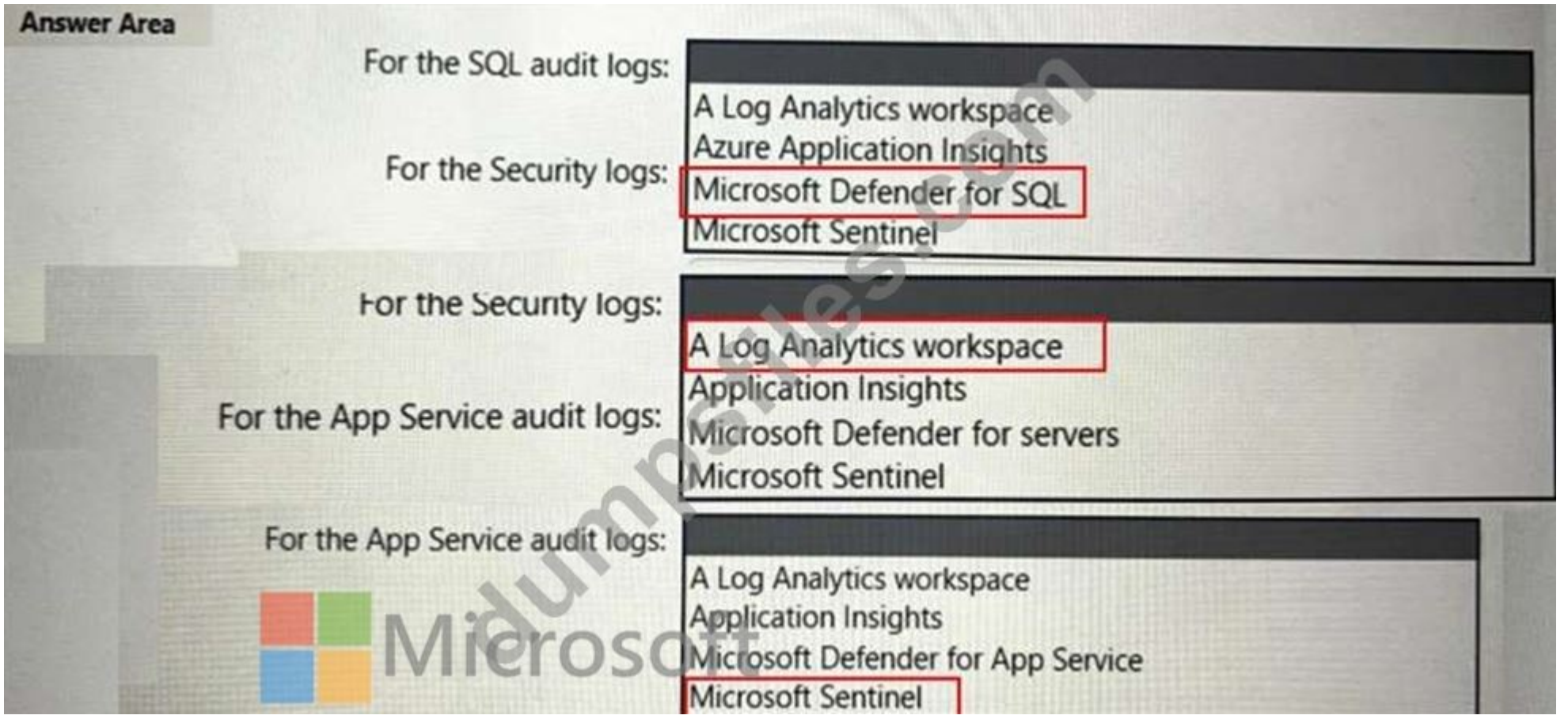
Answer:



NEW QUESTION: 56

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: 57

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. service chaining

B. local network gateways

C. forced tunneling

D. a VNet-to-VNet connection

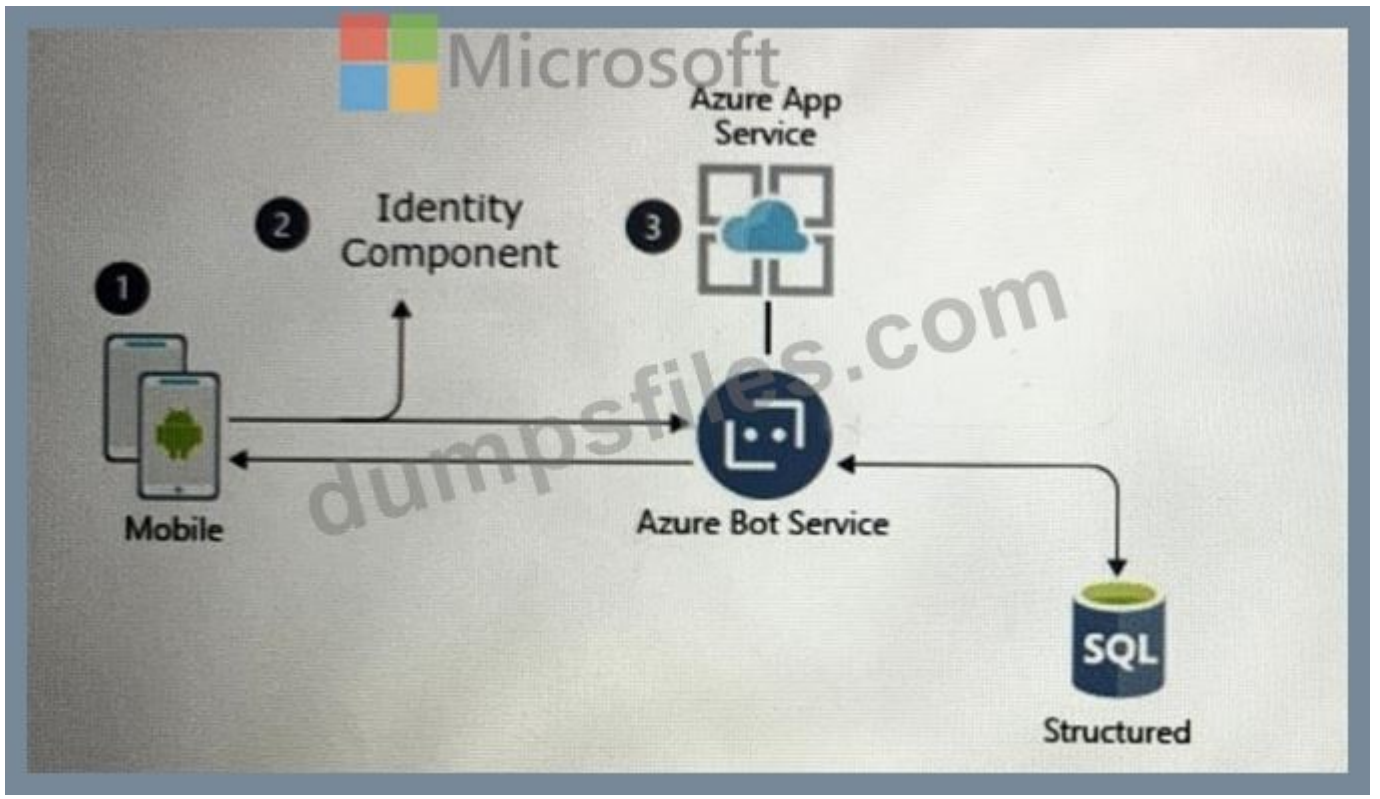
Answer: A (LEAVE A REPLY)

Explanation

https://docs.microsoft.com/en-us/learn/modules/configure-vnet-peering/5-determine-service-chaining-uses

NEW QUESTION: 58

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

* Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
* Be managed separately from the identity store of the customer.
* Support fully customizable branding for each app.

Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2C

B. Azure AD Connect

C. Azure Active Directory (Azure AD) B2B

D. Azure Active Directory Domain Services (Azure AD DS)

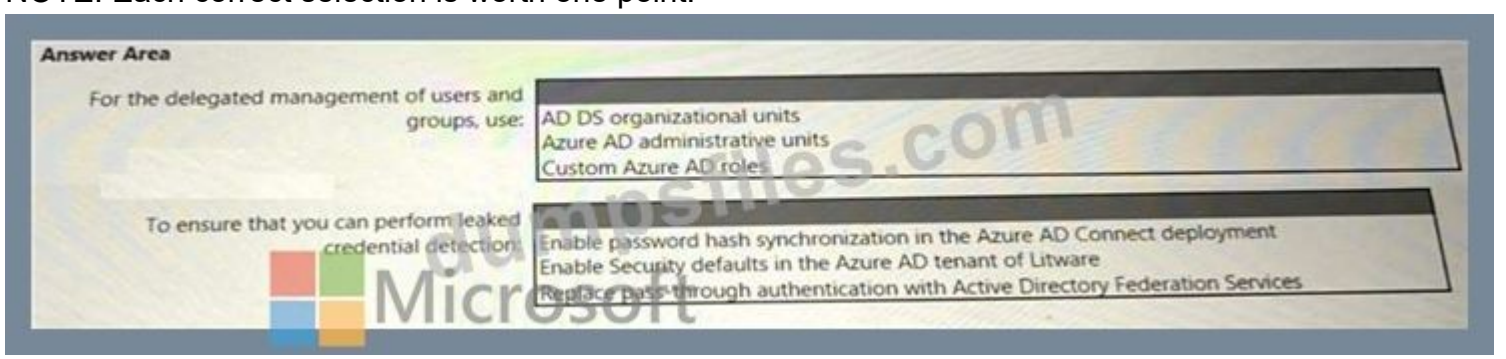
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59

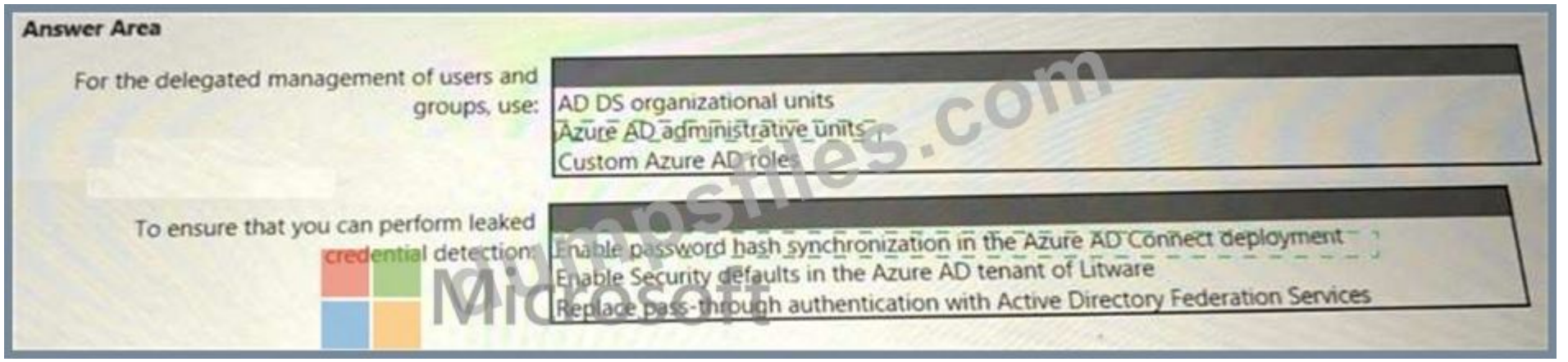
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.

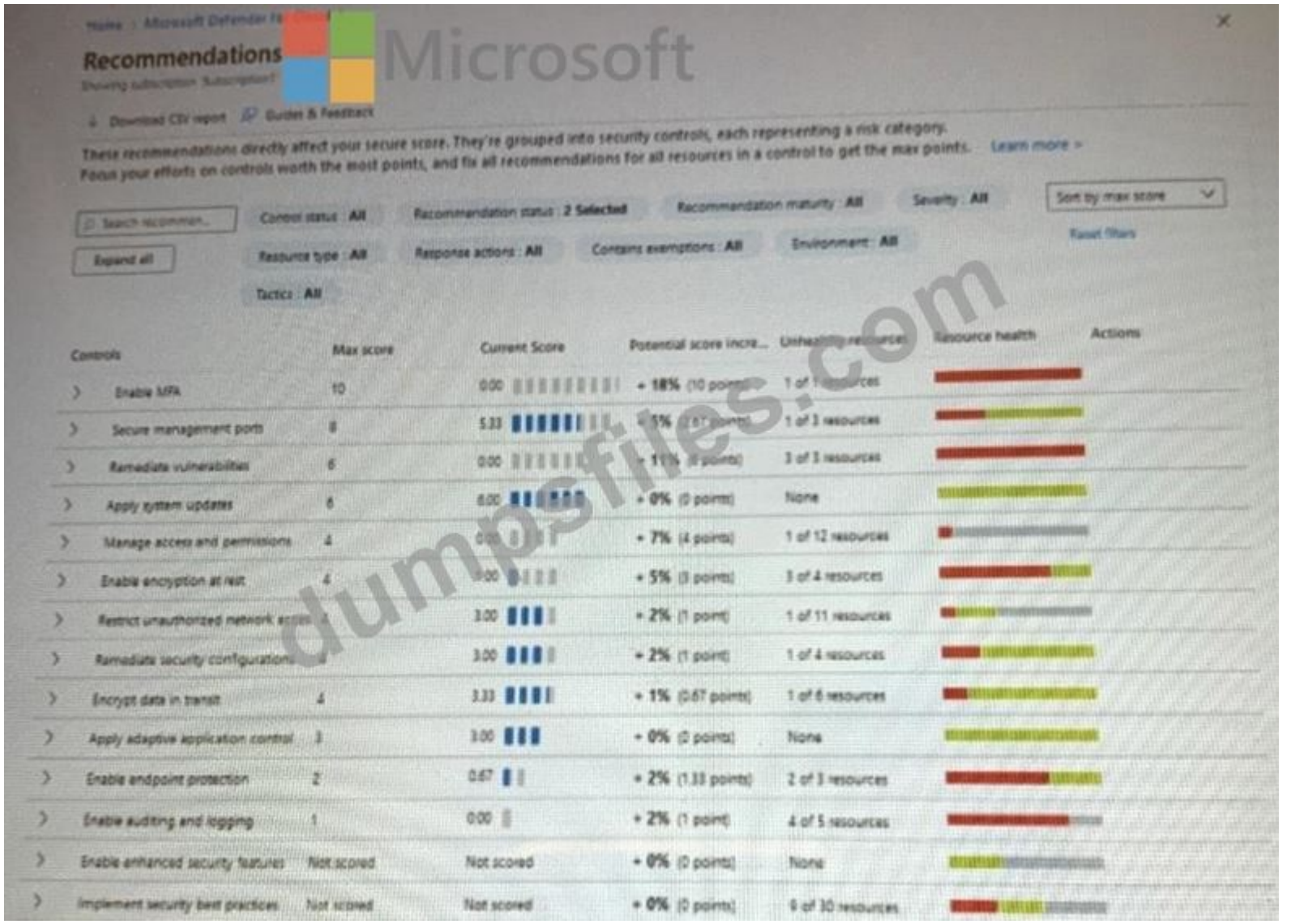


Answer:



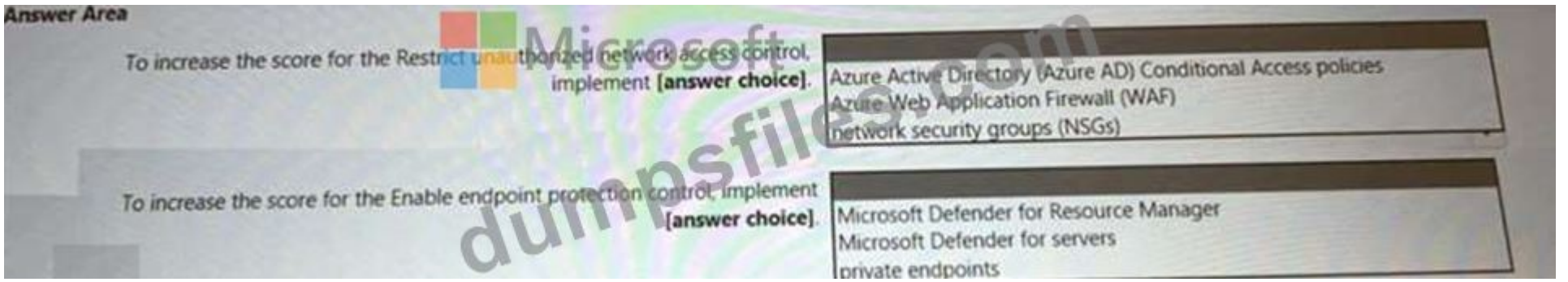
NEW QUESTION: 60

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

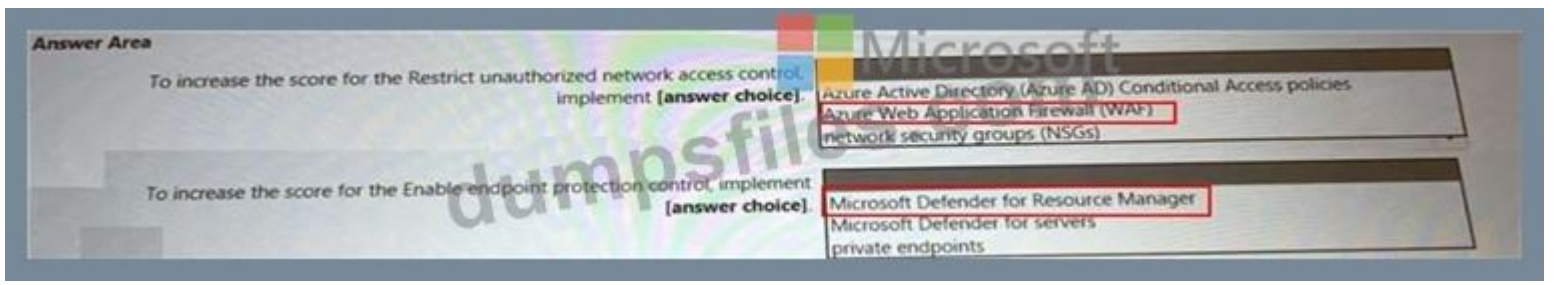


Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 61

Your company has a Microsoft 365 E5 subscription.

The company plans to deploy 45 mobile self-service kiosks that will run Windows 10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:

* Ensure that only authorized applications can run on the kiosks.
* Regularly harden the kiosks against new threats.

Which two actions should you include in the recommendations? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard the kiosks to Azure Monitor.

B. Implement Privileged Access Workstation (PAW) for the kiosks.

C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.

D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Answer: (SHOW ANSWER)

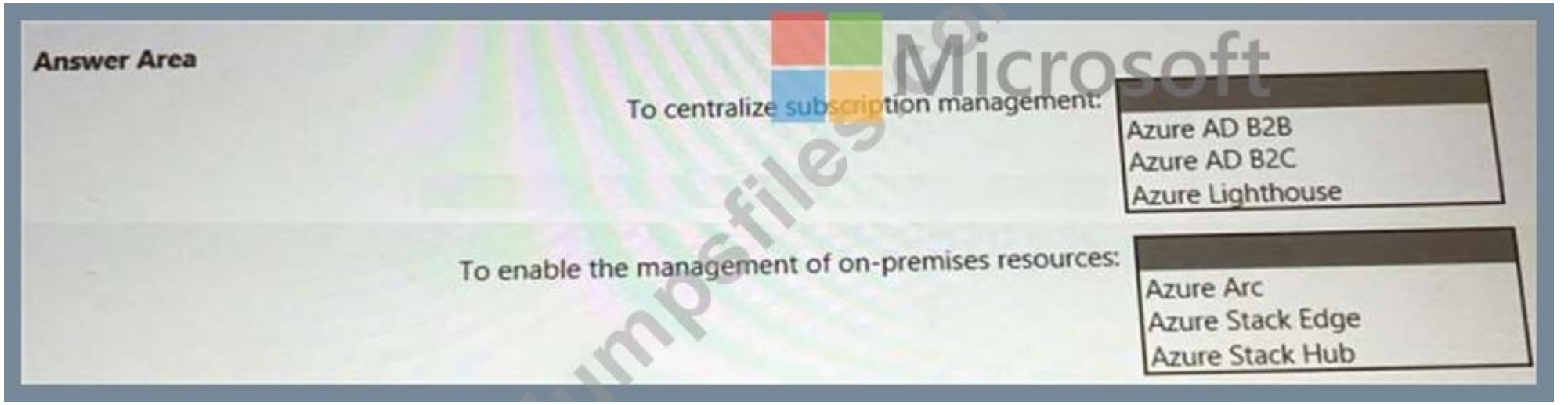
Explanation

(https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerab

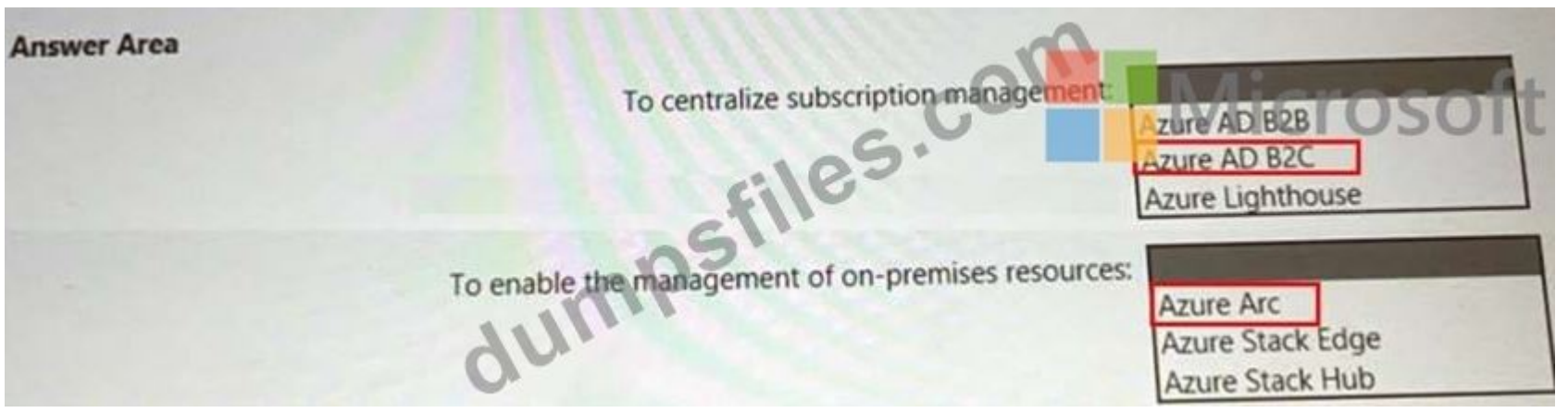
NEW QUESTION: 62

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities.
You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?
A. standalone sensors
B. honeytoken entity tags
C. sensitivity labels
D. custom user tags
Answer: B (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

NEW QUESTION: 63
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.

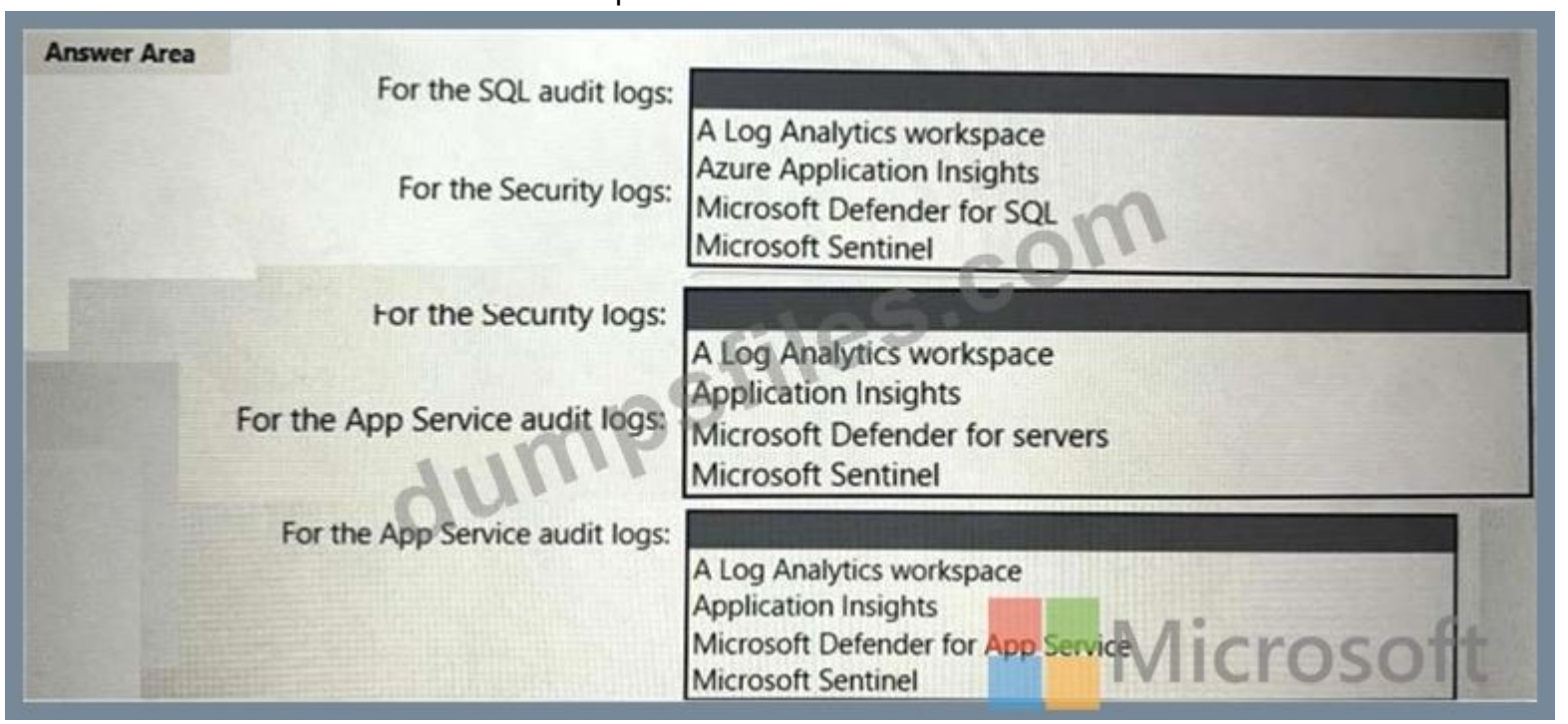


Answer:

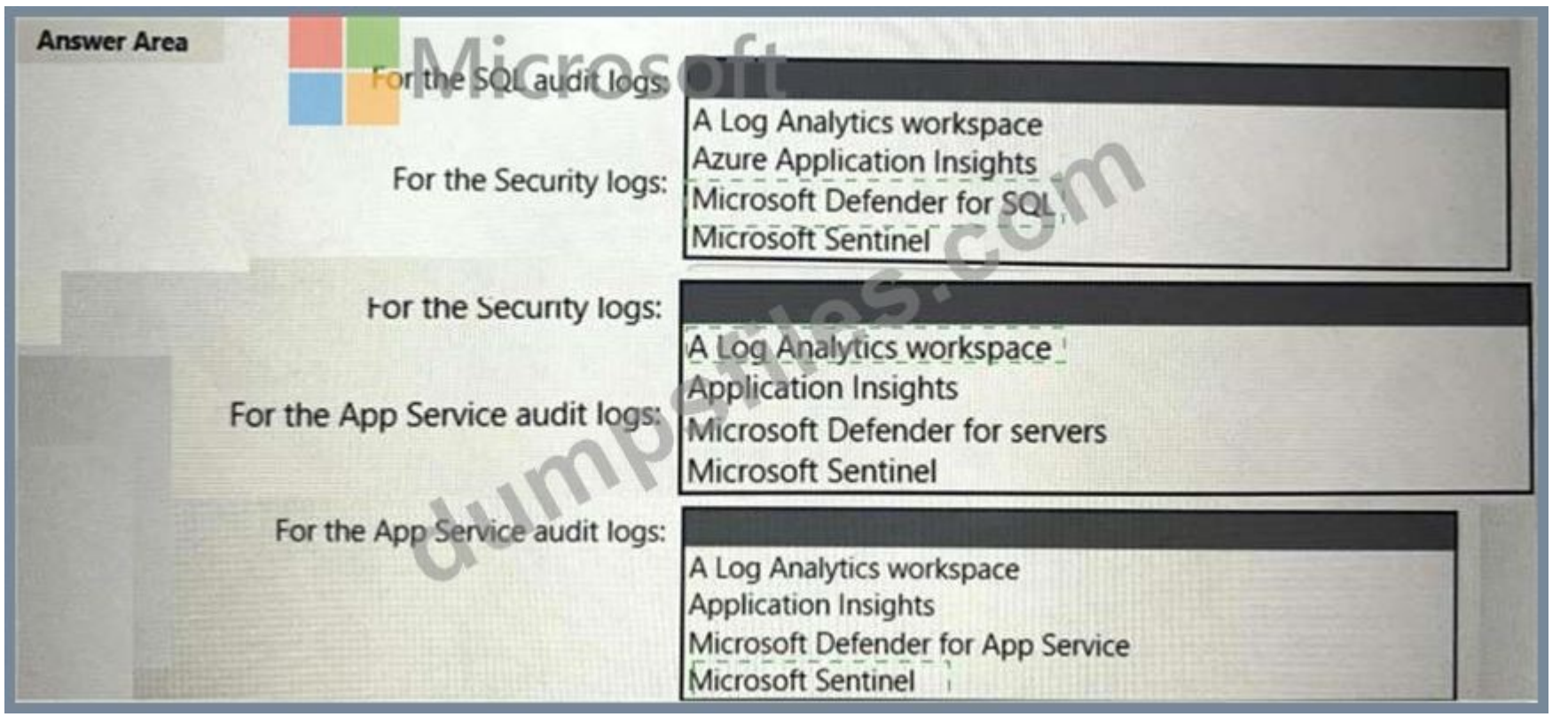


NEW QUESTION: 64
Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.
You receive the following recommendations in Defender for Cloud
* Access to storage accounts with firewall and virtual network configurations should be restricted,
* Storage accounts should restrict network access using virtual network rules.
* Storage account should use a private link connection.
* Storage account public access should be disallowed.
You need to recommend a service to mitigate identified risks that relate to the recommendations. What should you recommend?
A. Azure Storage Analytics
B. Microsoft Sentinel
C. Azure Policy
D. Azure Network Watcher
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
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 area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 66

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. Microsoft Tunnel

B. web content filtering in Microsoft Defender for Endpoint

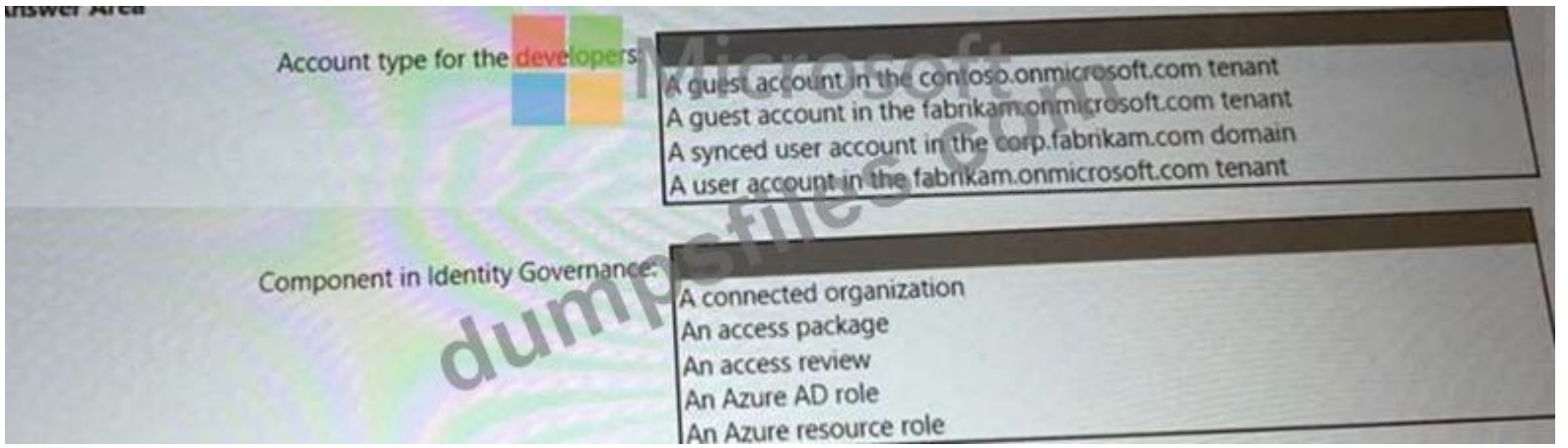
C. Azure AD Application Proxy

D. Azure Virtual WAN

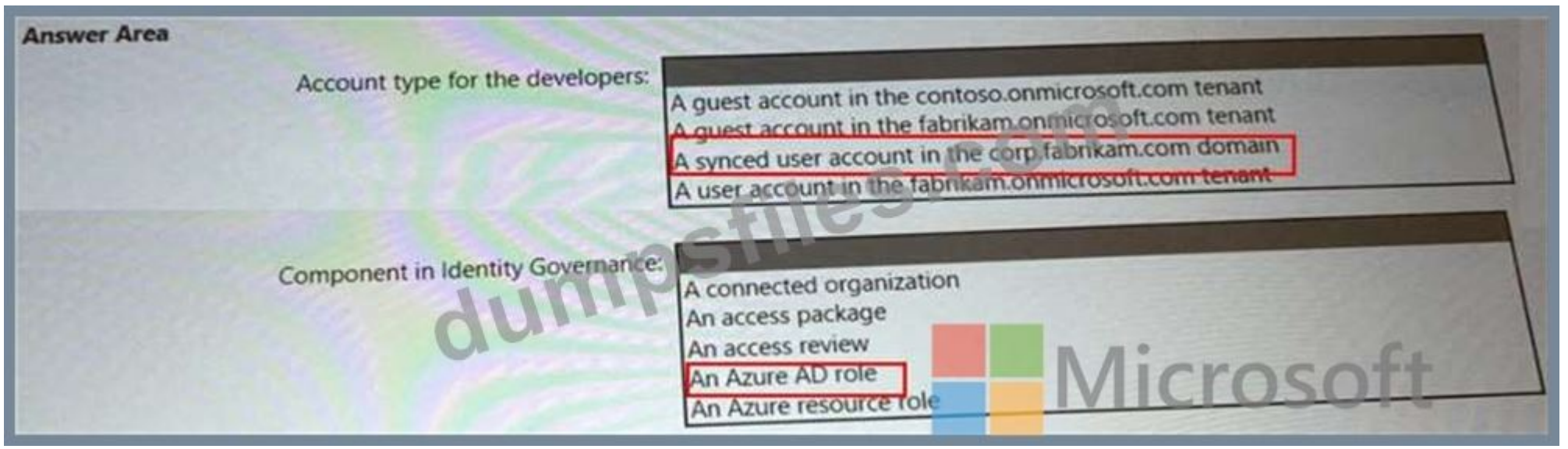
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67

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



Answer:



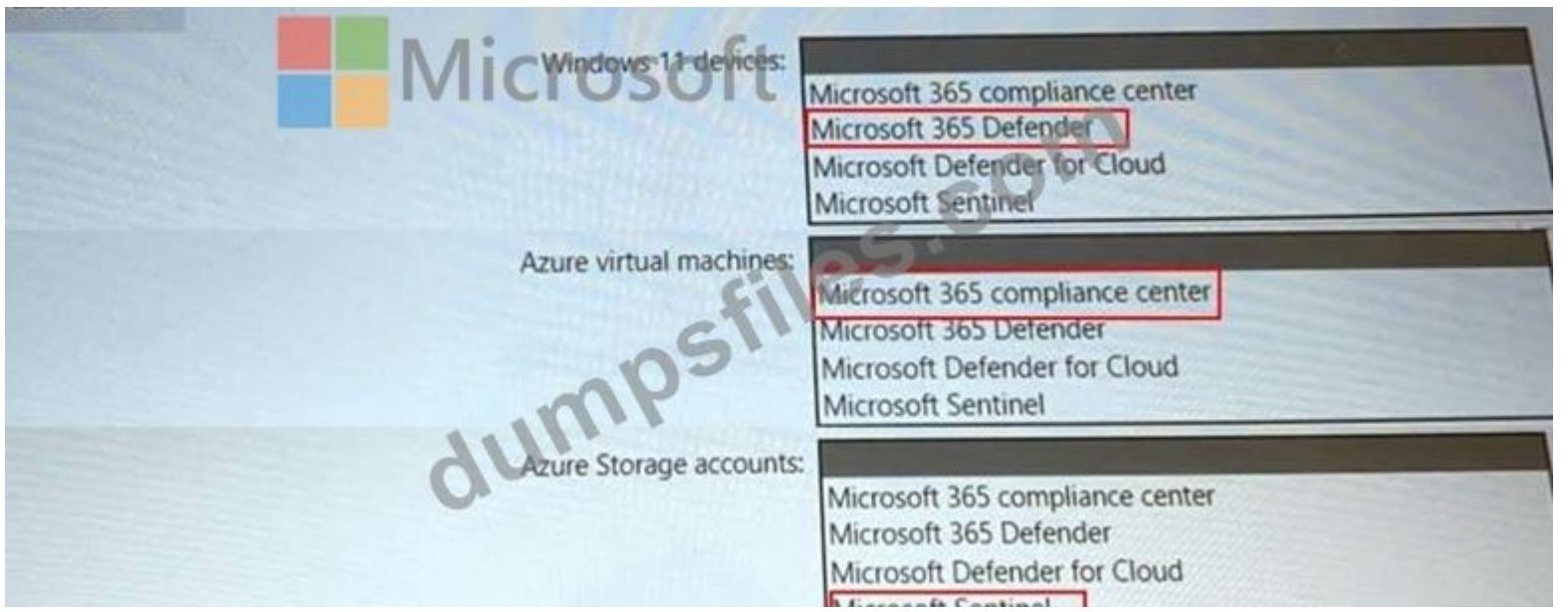
NEW QUESTION: 68

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: 69

Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app. You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection. What should you include in the recommendation?

A. interactive application security testing (IAST)

B. static application security testing (SAST)

C. runtime application se/f-protection (RASP)

D. dynamic application security testing (DAST)

Answer: D (LEAVE A REPLY)

Explanation

https://docs.microsoft.com/en-us/azure/security/develop/secure-develop#test-your-application-in-an-operating-st

NEW QUESTION: 70

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)

Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Application Gateway v2 with user-defined routes (UDRs).

C. Azure Front Door with Azure Web Application Firewall (WAF)

D. Azure Firewall with policy rule sets

Answer: (SHOW ANSWER)

Explanation

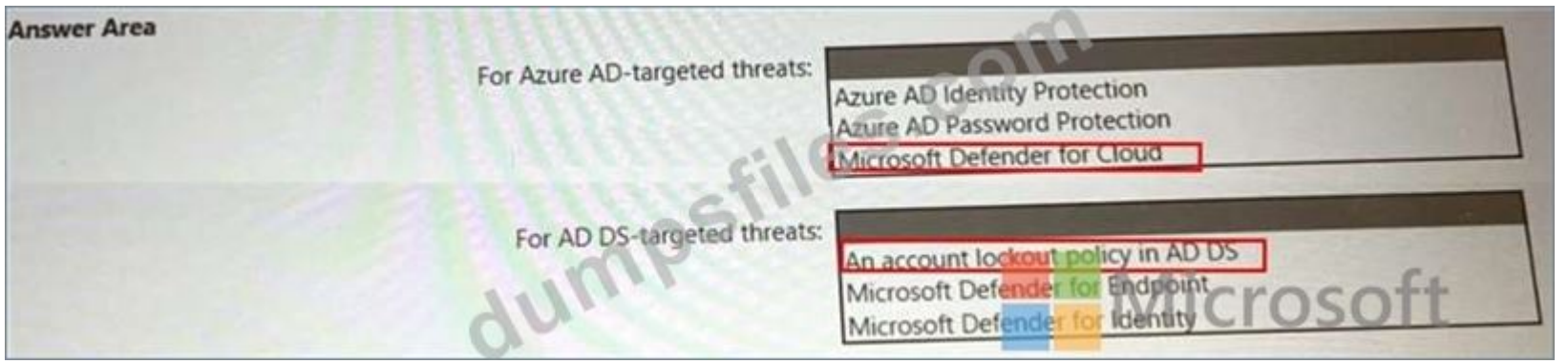
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

NEW QUESTION: 71

You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. 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:



Topic 2, Fabrikam, Inc

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 VnetI 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: 72
Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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 creating private endpoints for the web app and the database layer. Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

NEW QUESTION: 73

Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool.

Which type of diagram should you create?

A. process flow

B. dataflow

C. system flow

D. network flow

Answer: (SHOW ANSWER)

NEW QUESTION: 74

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: 75
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. adaptive application controls in Defender for Cloud
B. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. Azure Security Benchmark compliance controls m Defender for Cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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. retention label policies
C. eDiscovery cases
D. sensitivity label policies
Answer: A,C (LEAVE A REPLY)

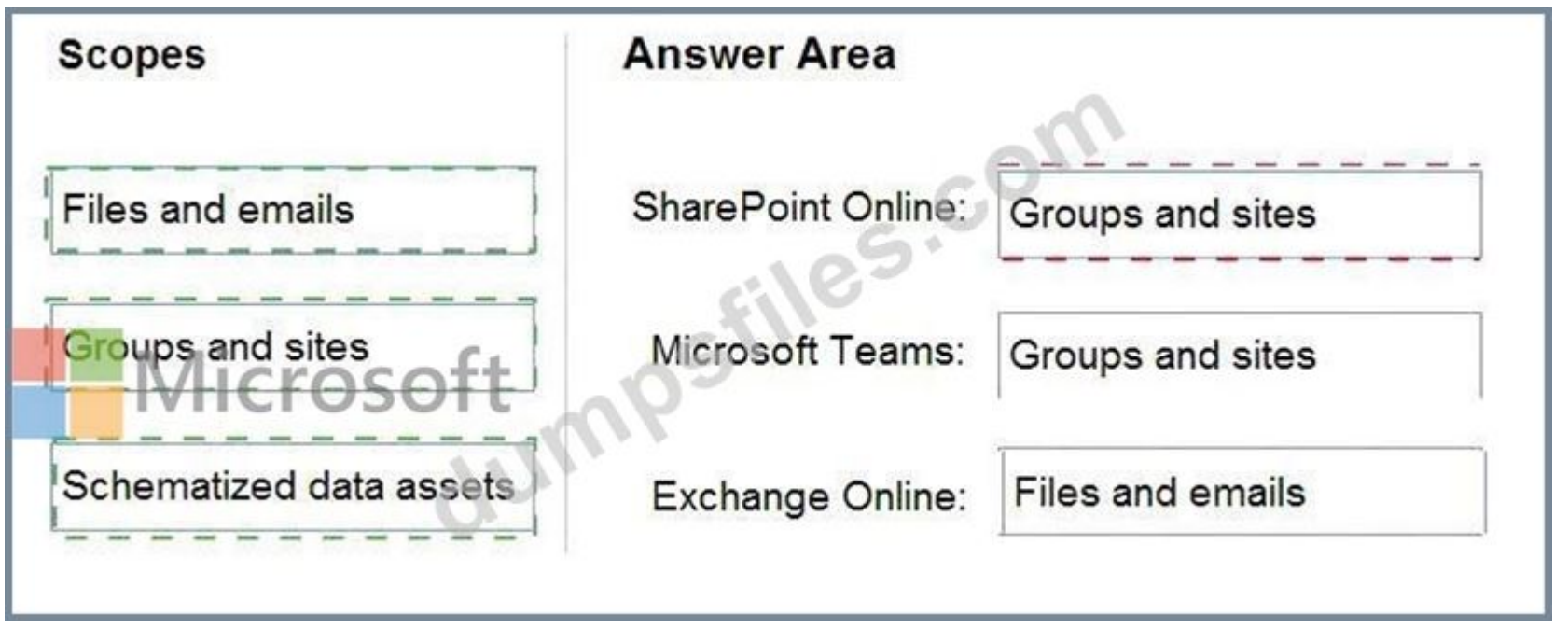
NEW QUESTION: 77
You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD)
The customer plans to obtain an Azure subscription and provision several Azure resources.
You need to evaluate the customer's security environment.

What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?
A. Azure AD Multi-Factor Authentication
B. Azure AD Privileged Identity Management (PIM)
C. resource-based authorization
D. role-based authorization
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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: A (LEAVE A REPLY)

NEW QUESTION: 79
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:



Explanation

Box 1: Groups and sites

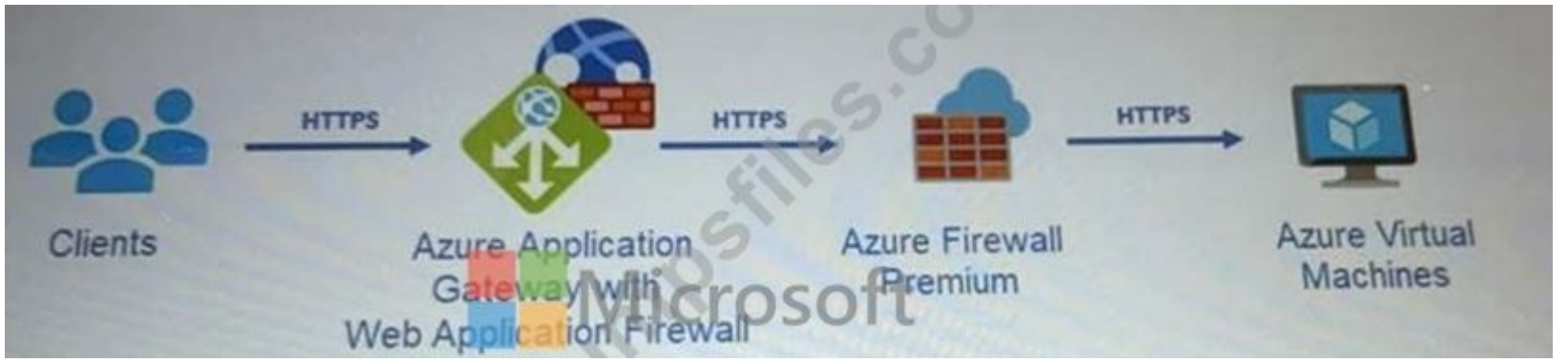
Box 2: Groups and sites

Box 3: Files and emails -

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

NEW QUESTION: 80

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.



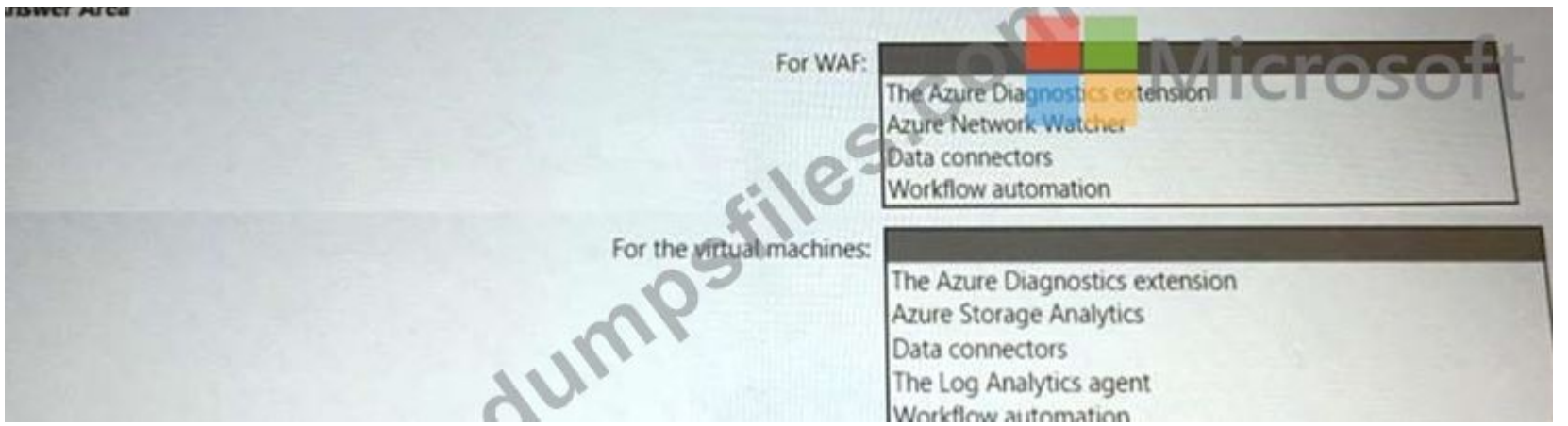
You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

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

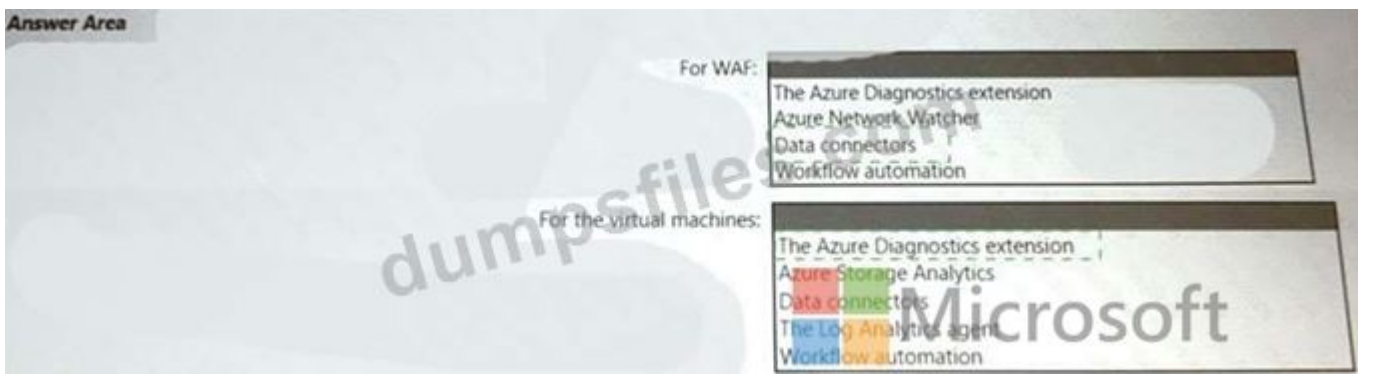
* Use Defender for Cloud to review alerts from the virtual machines.

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: 81

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Azure AD workbooks to monitor risk detections

B. smart account lockout in Azure AD B2C

C. Azure AD Conditional Access integration with user flows and custom policies

D. custom resource owner password credentials (ROPC) flows in Azure AD B2C

E. access packages in Identity Governance

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 82

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. Microsoft Sentinel notebooks

C. threat intelligence reports in Defender for Cloud

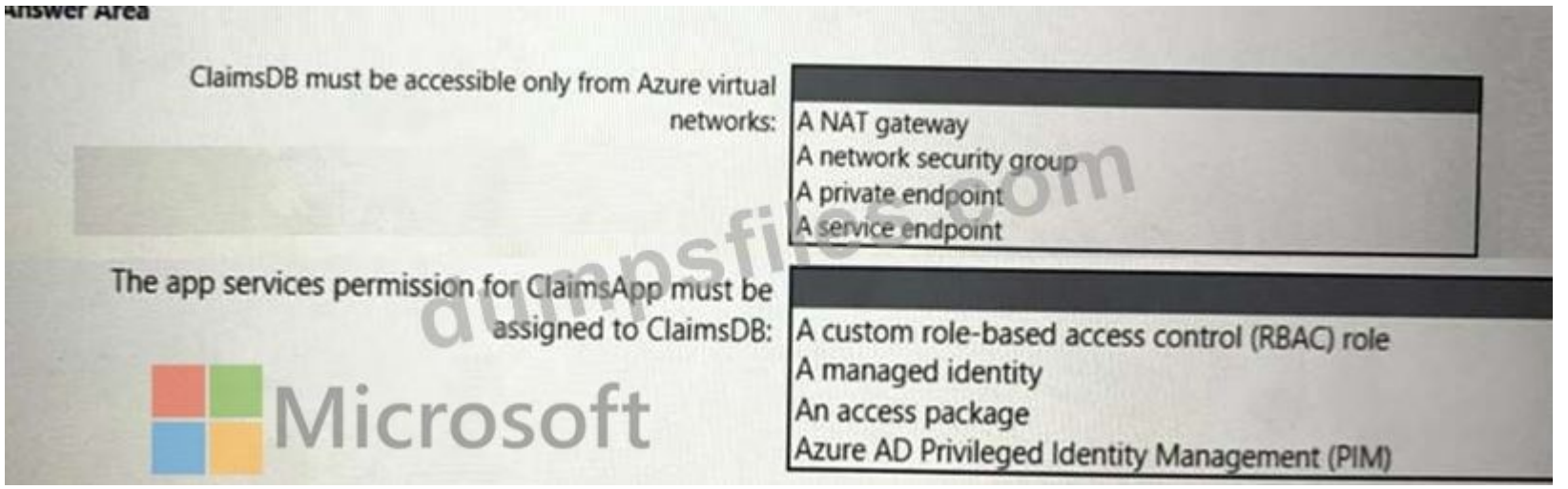
D. Microsoft Sentinel threat intelligence workbooks

Answer: A,D (LEAVE A REPLY)

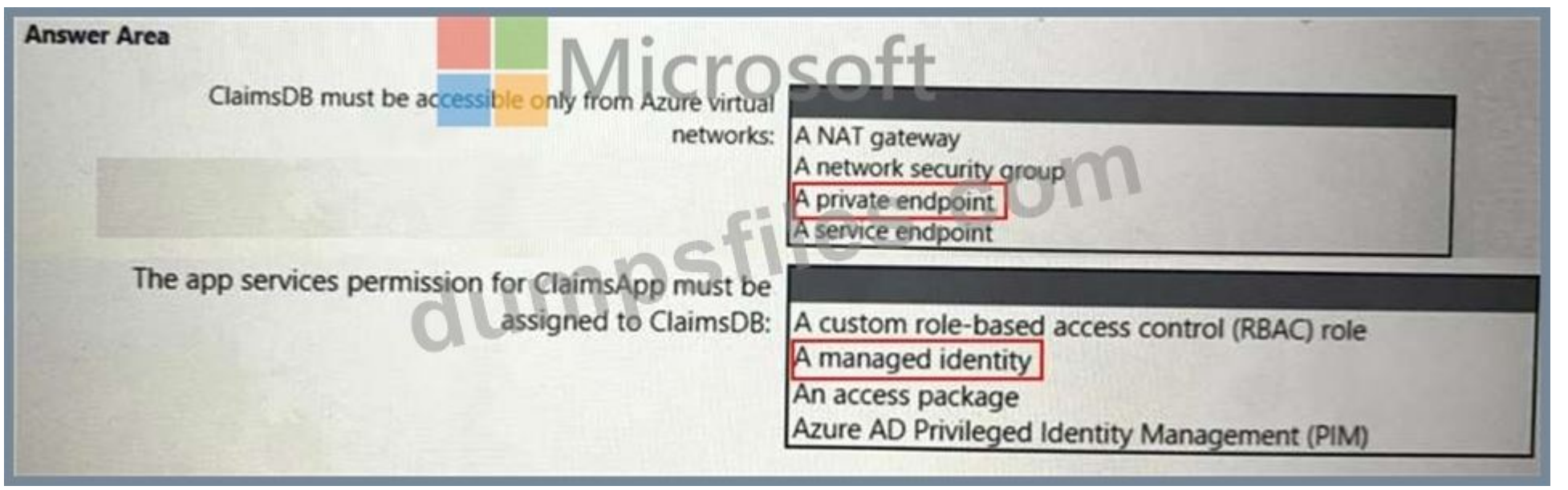
NEW QUESTION: 83
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation. You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) Conditional Access
C. Microsoft Defender for servers
D. Azure Policy
E. Microsoft Defender for Containers
Answer: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-contai

NEW QUESTION: 84
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: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION: 85
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: 86

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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 Key Vault to store credentials.

A. Yes

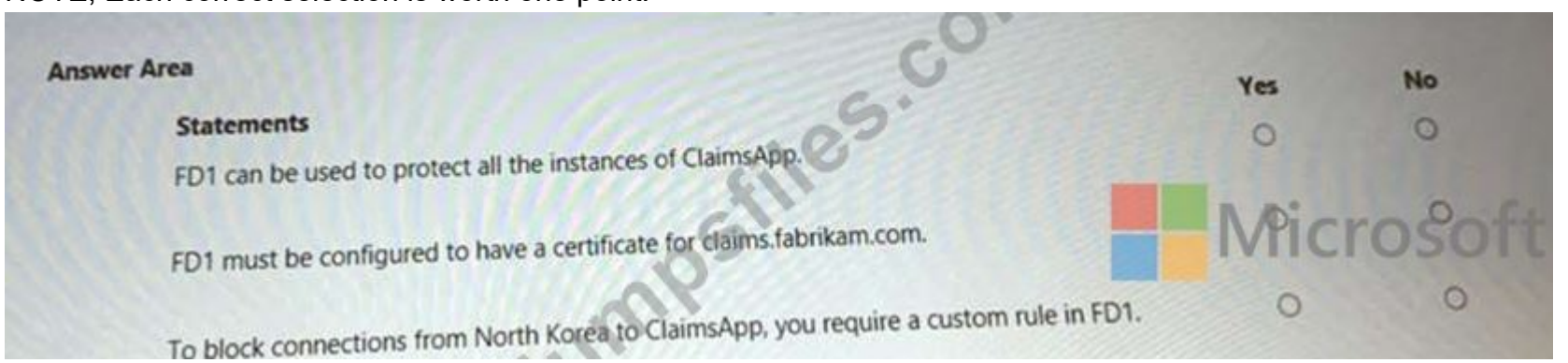
B. No

Answer: (SHOW ANSWER)

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: 87
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: 88
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: 89

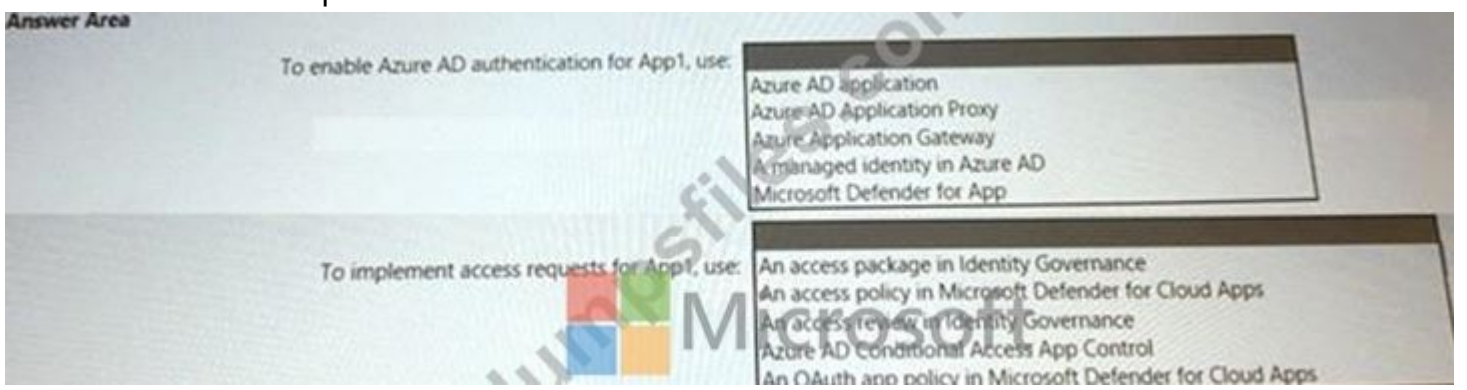
You are creating the security recommendations for an Azure App Service web app named App1.

App1 has the following specifications:

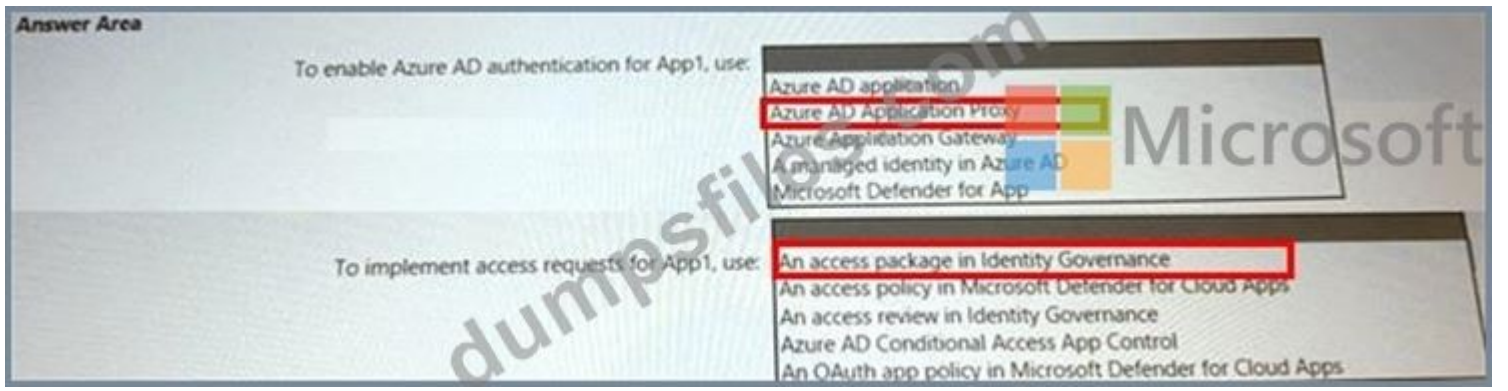
* Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
* Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

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



Answer:



NEW QUESTION: 90

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.

All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.

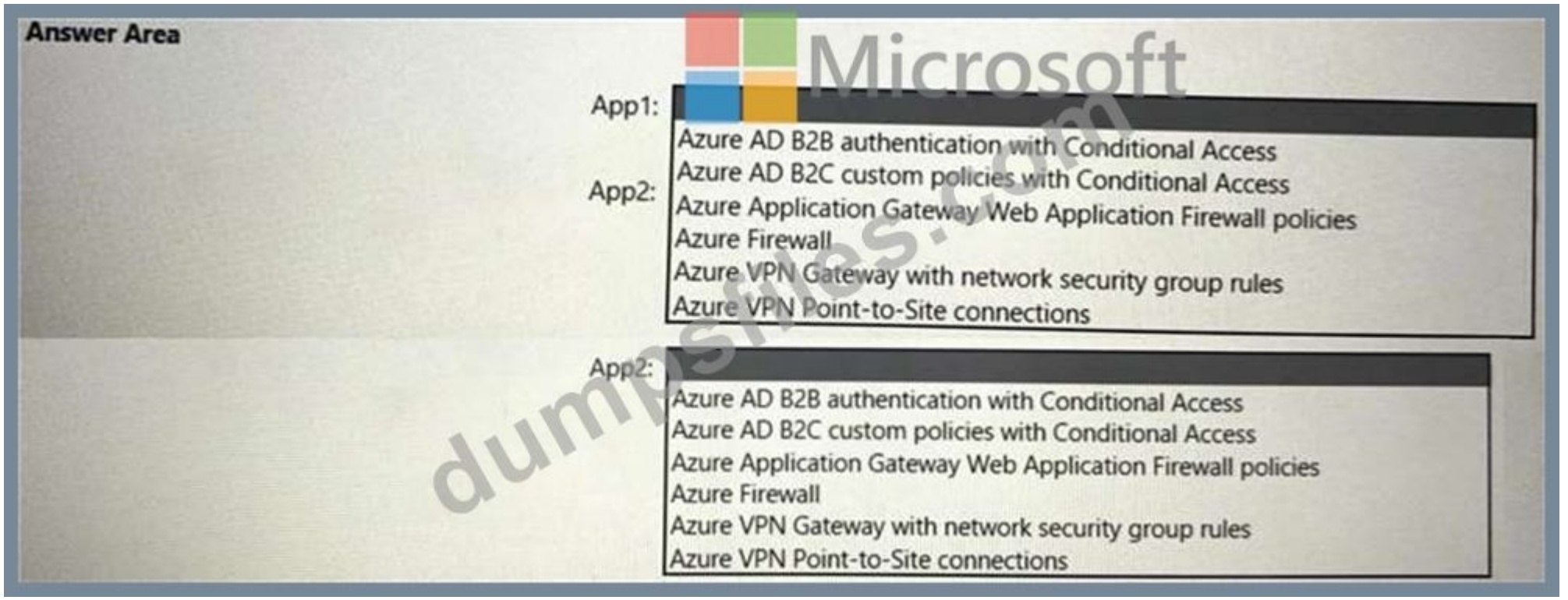
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successtu\ ransonvwaTe attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. Use Azure Monitor notifications when backup configurations change.
B. Enable soft delete for backups.
C. Require PINs for critical operations.
D. Encrypt backups by using customer-managed keys (CMKs).
E. Perform offline backups to Azure Data Box.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 91
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.
A. Assign an initiative to a management group.
B. Assign a policy to each subscription.
C. Assign a policy to a management group.
D. Assign an initiative to each subscription.
E. Assign a blueprint to each subscription.
F. Assign a blueprint to a management group.
Answer: A,F (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview
https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001
https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

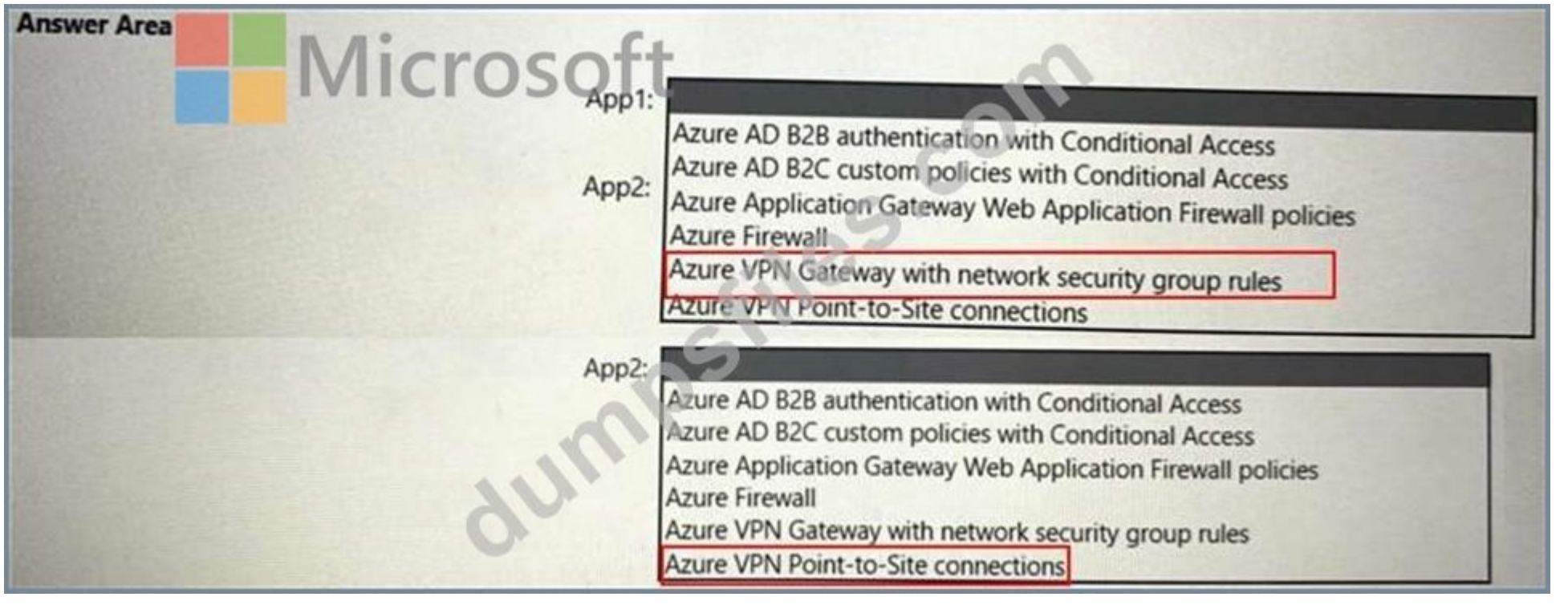
NEW QUESTION: 92
You have a hybrid cloud infrastructure.
You plan to deploy the Azure applications shown in the following table.

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.

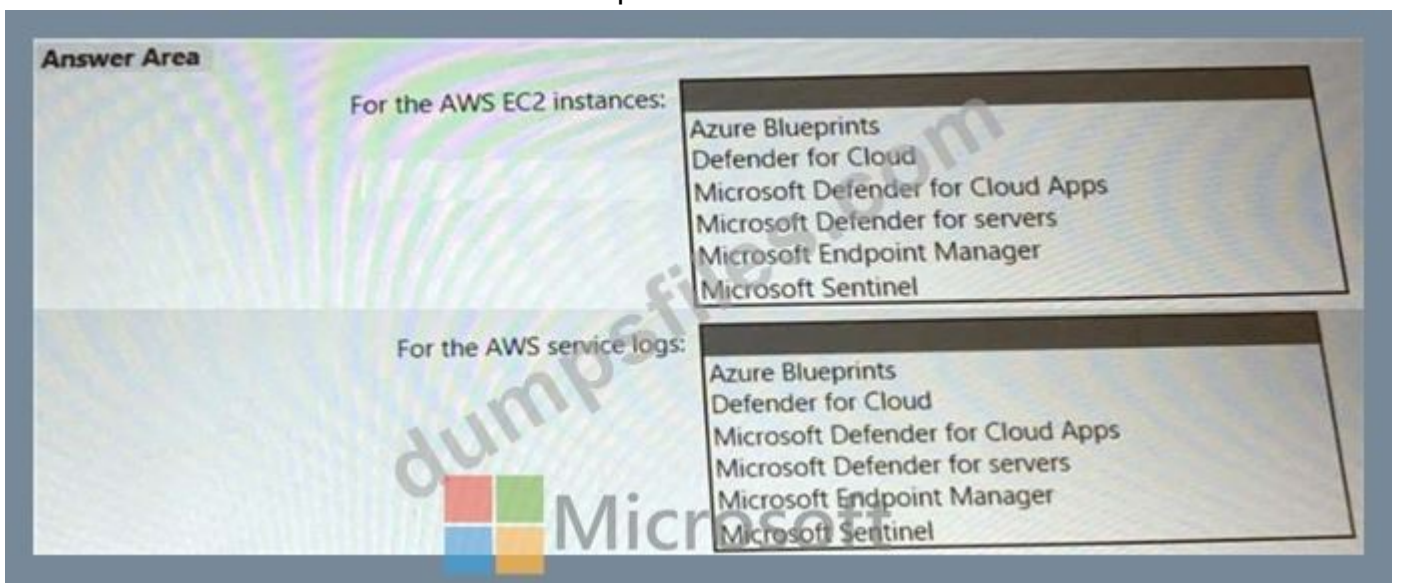


Answer:

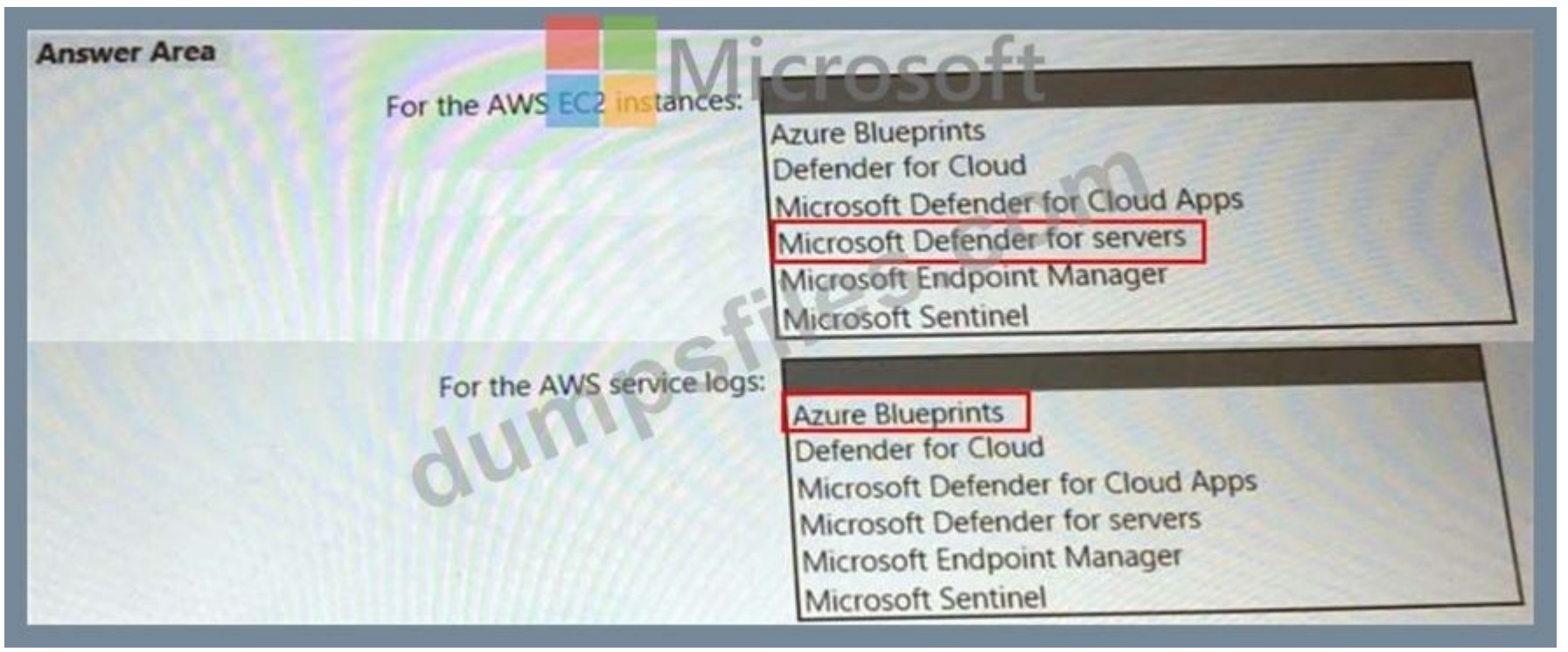


NEW QUESTION: 93

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.

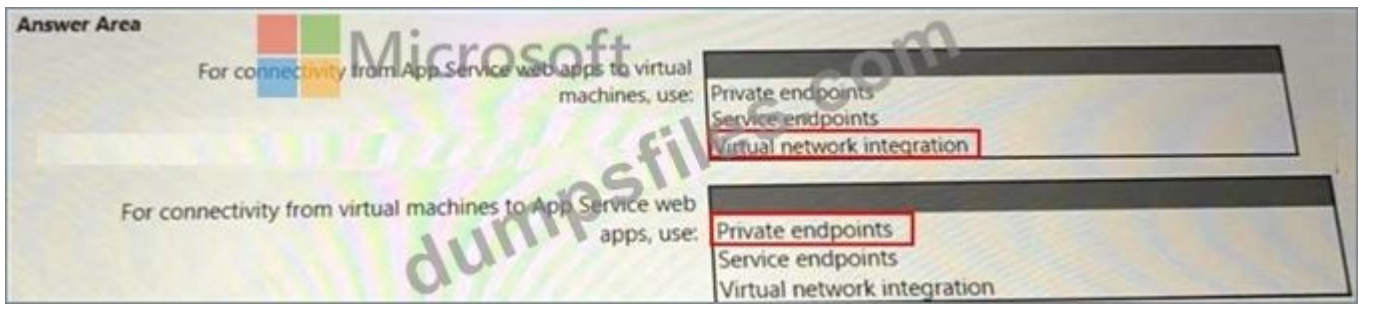


Answer:



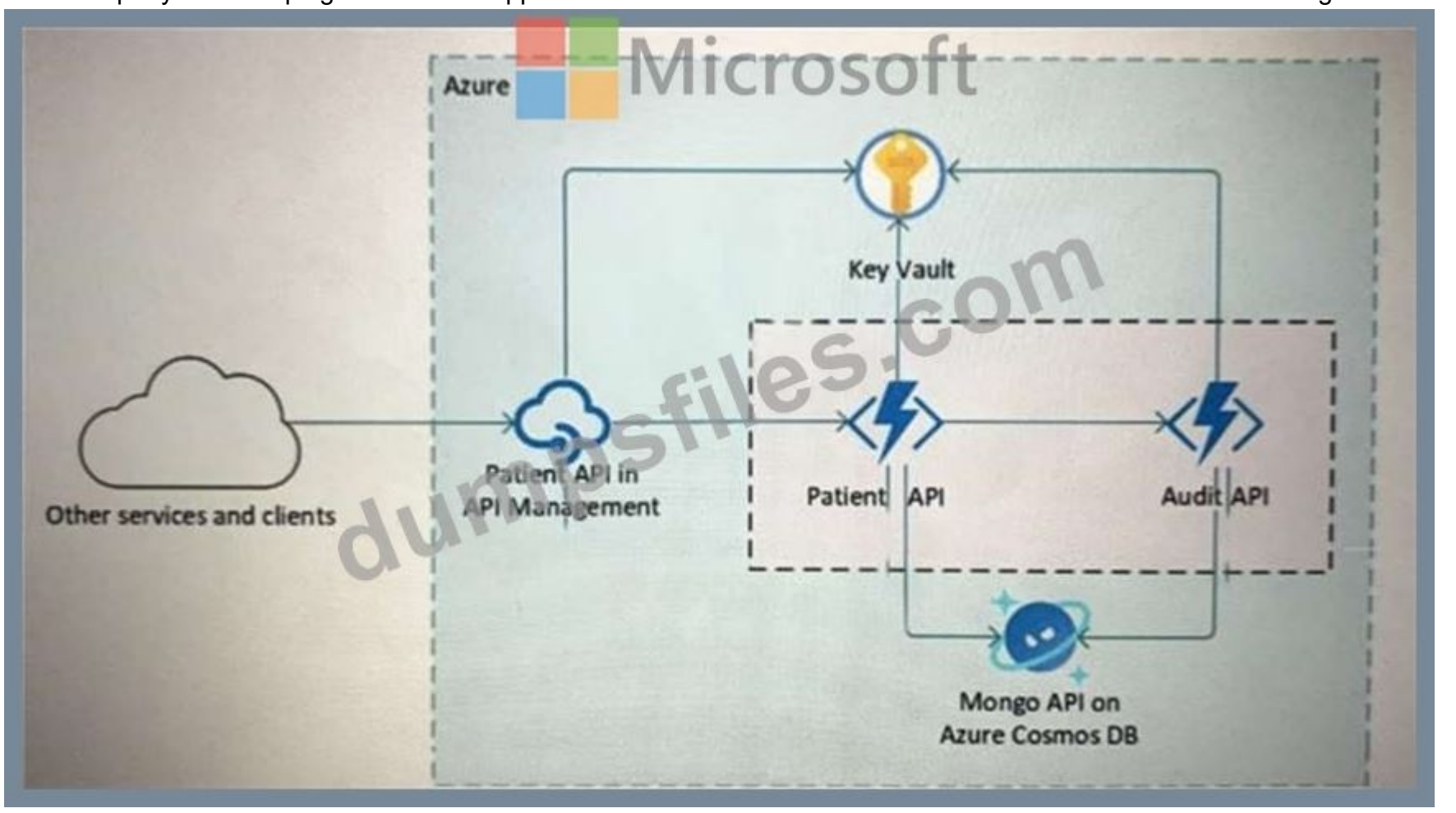
NEW QUESTION: 94
You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer are
a. NOTE Each correct selection is worth one point.

Answer:



NEW QUESTION: 95

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

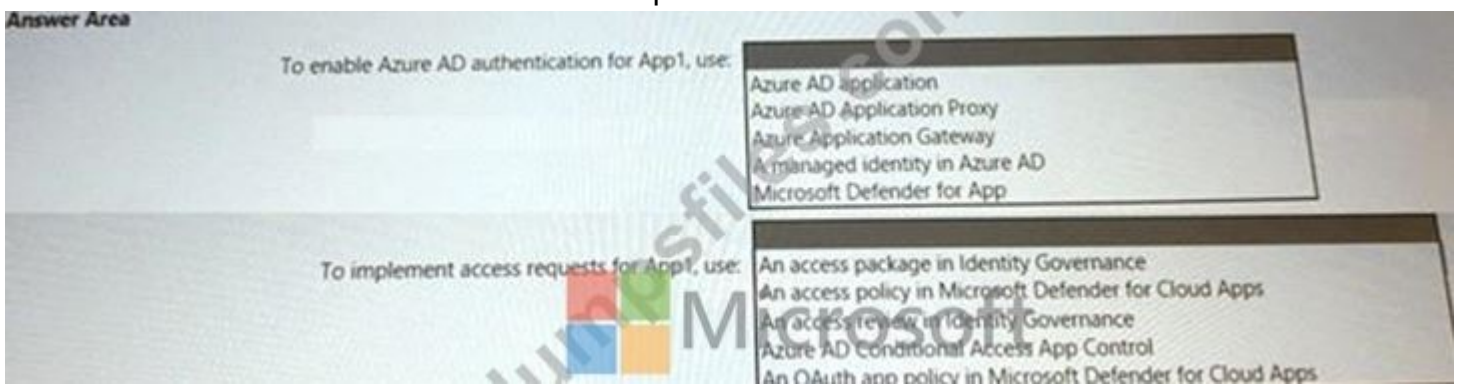


You need to recommend a solution to isolate the compute components on an Azure virtual network. What should you include in the recommendation?

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)
Explanation
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: 96
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 are
a. NOTE: Each correct selection is worth one point.



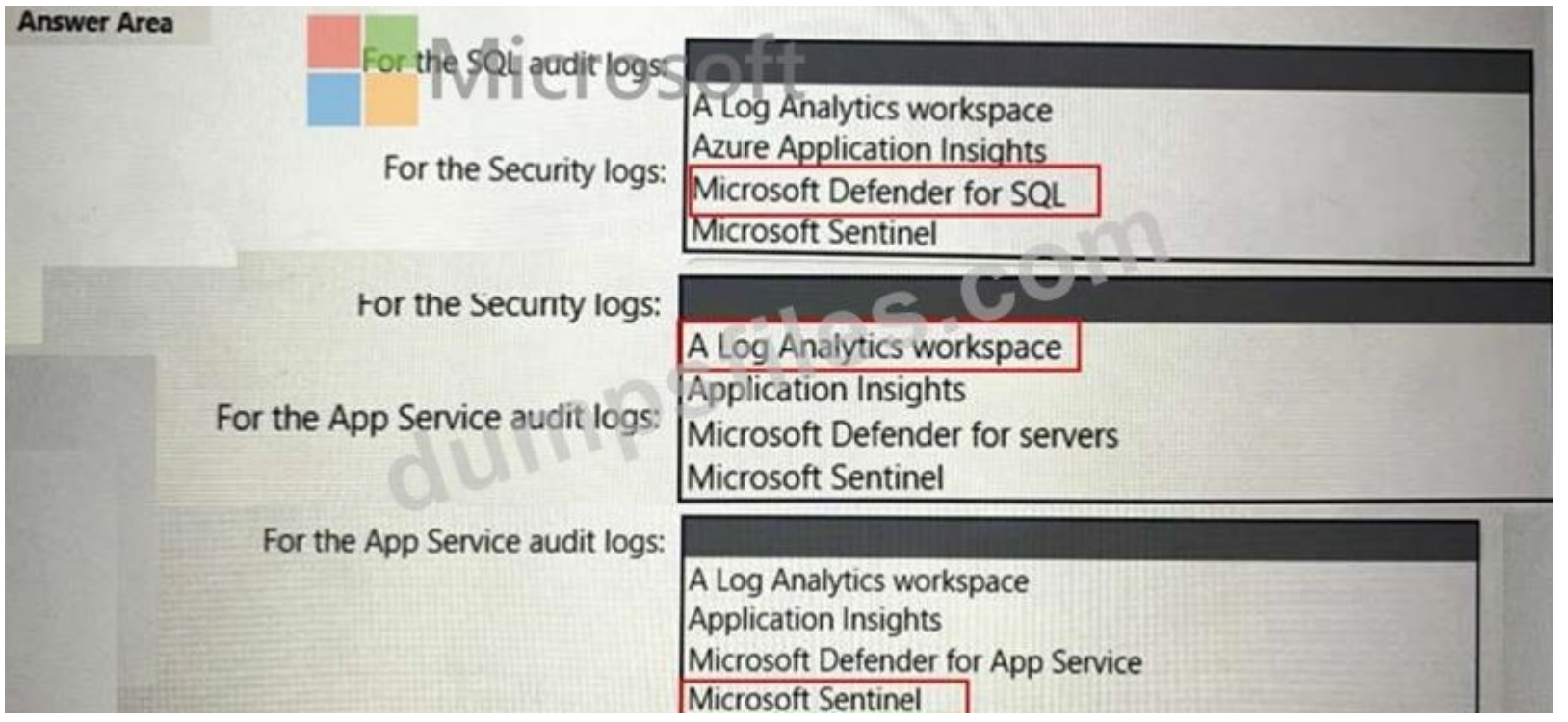
Answer:

NEW QUESTION: 97
Your company has a Microsoft 365 E5 subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
* Identify unused personal data and empower users to make smart data handling decisions.
* Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.

* Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?
A. Microsoft Viva Insights
B. Advanced eDiscovery
C. Privacy Risk Management in Microsoft Priva
D. communication compliance in insider risk management
Answer: C (LEAVE A REPLY)
Explanation
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:Detect overexposed personal data so that users can secure it.Spot and limit transfers of personal data across departments or regional borders.Help users identify and reduce the amount of unused personal data that you store.
https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management

NEW QUESTION: 98
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:

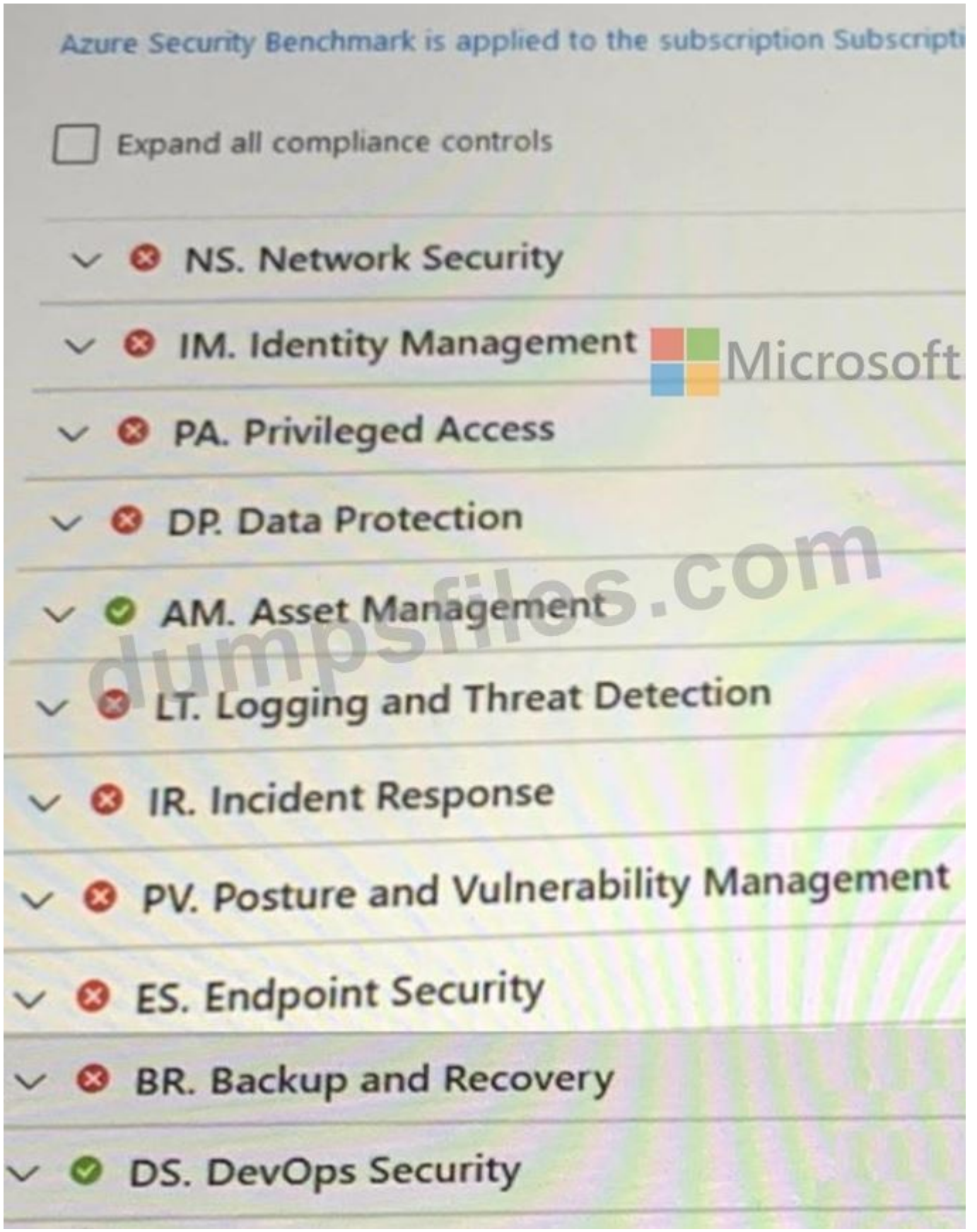


NEW QUESTION: 99

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.


Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud
Showing subscription 'Subscription1'
Microsoft
Download report
Manage compliance policies
Open query
Audit reports
You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.
Azure Security Benchmark V3
ISO 27001
PCI DSS 3.2.1
SOC TSP
HIPAA HITRUST
Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.
Azure Security Benchmark is applied to the subscription Subscription1



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?

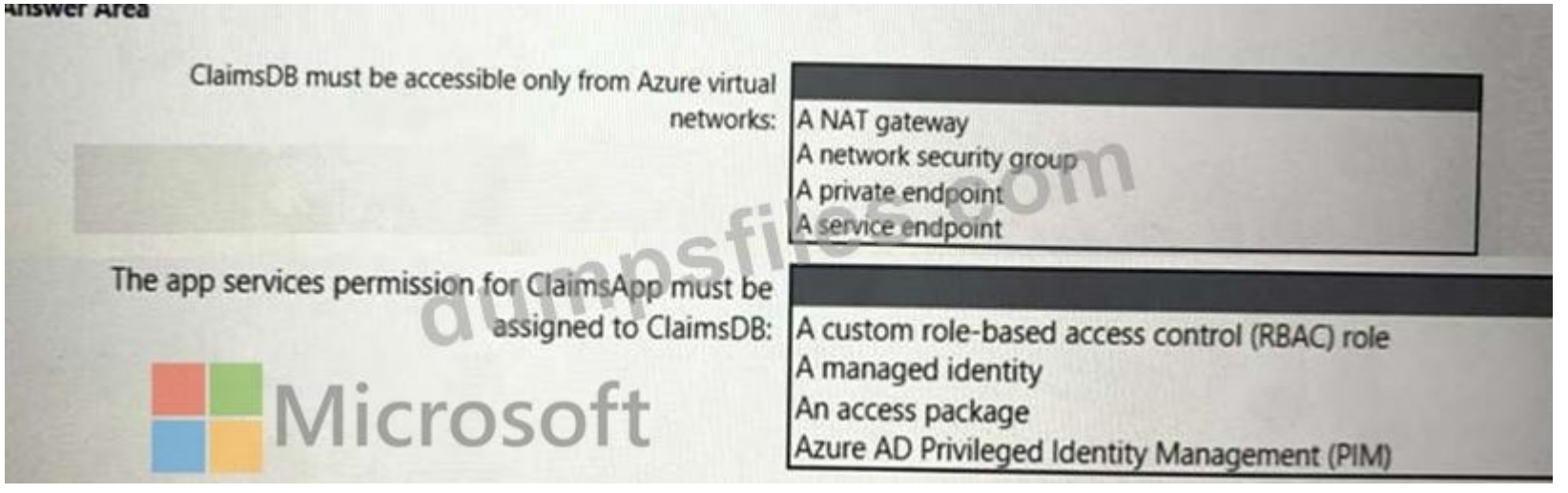
A. Incident Response

B. Asset Management

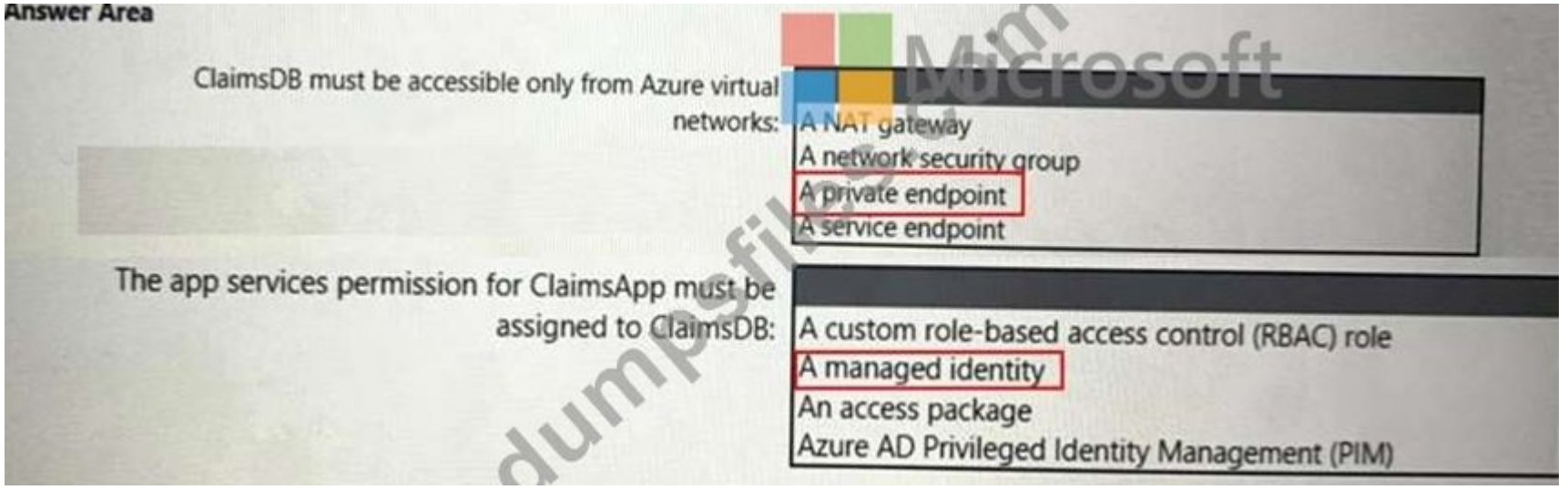
C. Data Protection

D. Endpoint Security
E. Posture and Vulnerability Management
Answer: D (LEAVE A REPLY)

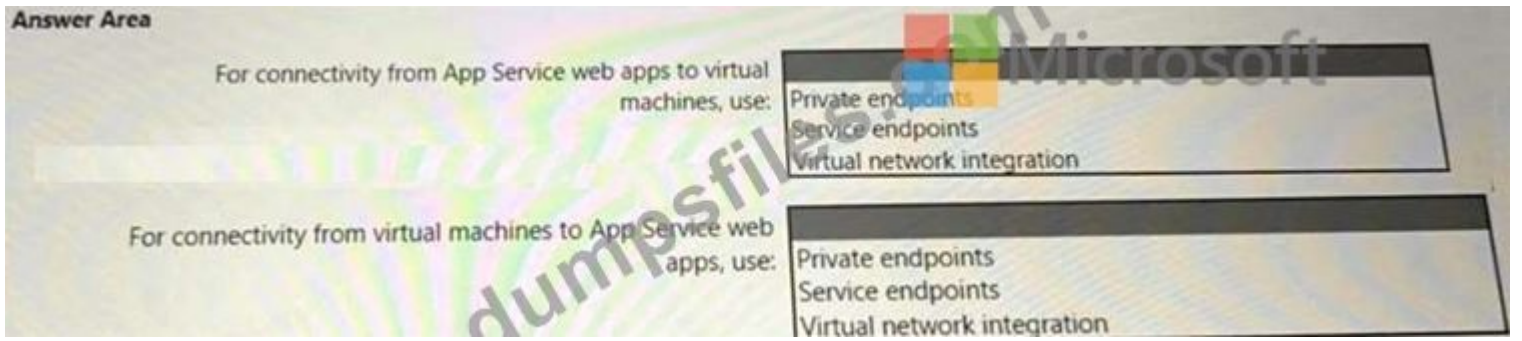
NEW QUESTION: 100
You need to recommend a solution to meet the requirements for connections to ClaimsDB.
What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 101
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: 102

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)

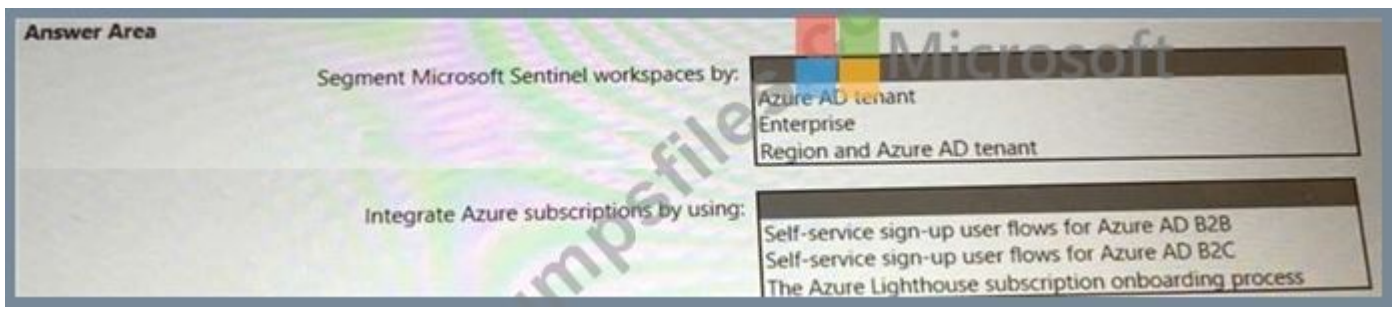
https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing?rtc=1

NEW QUESTION: 103

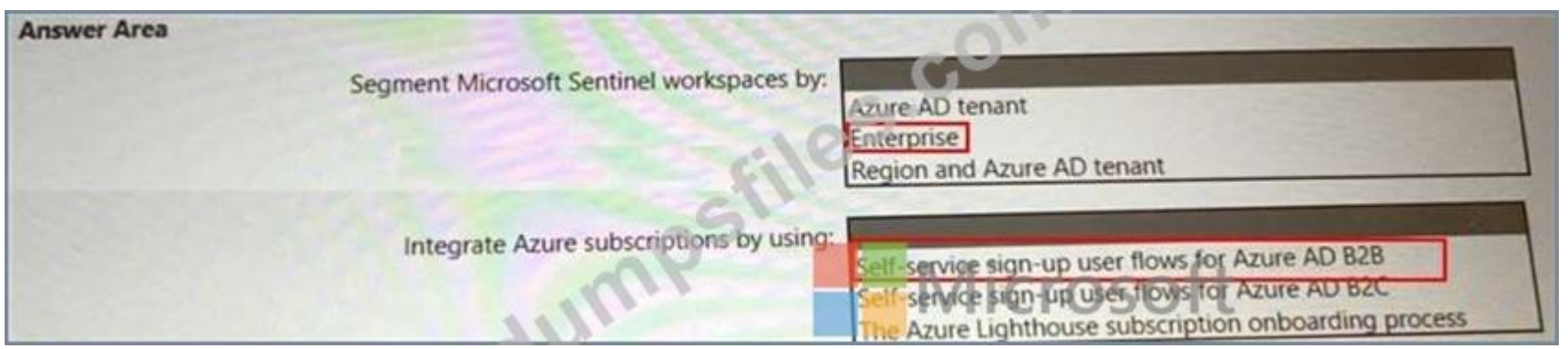
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.



Answer:



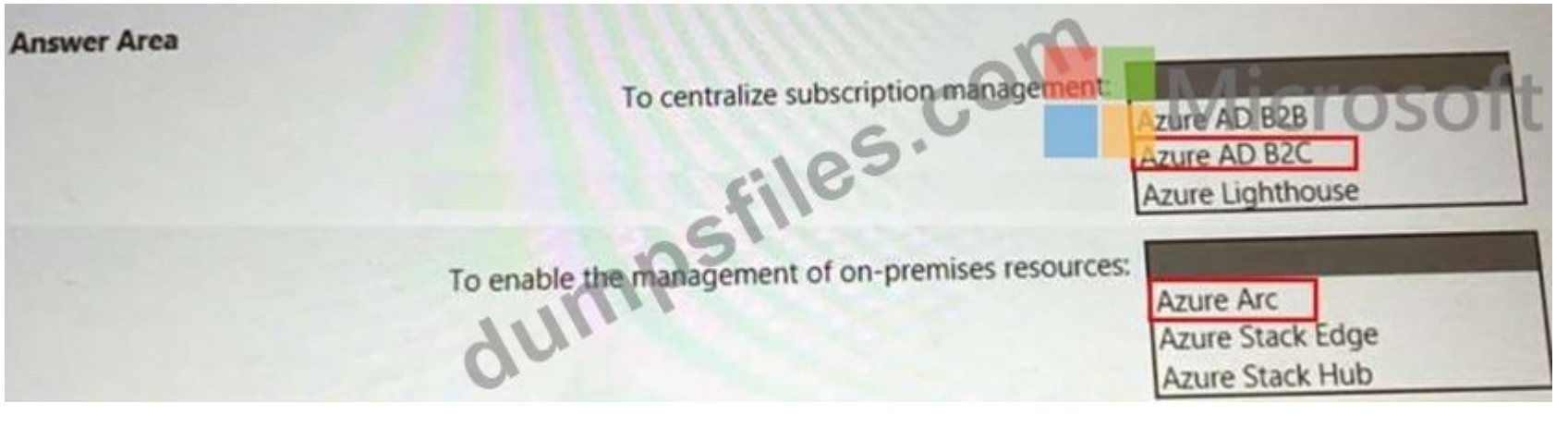
NEW QUESTION: 104

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: 105

Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.

You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.

What should you include in the recommendation?

A. Require PINs to disable backups.

B. Use geo-redundant storage (GRS).

C. Use customer-managed keys (CMKs) for encryption.

D. Implement Azure Site Recovery replication.

Answer: (SHOW ANSWER)

NEW QUESTION: 106

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

Answer:

Explanation

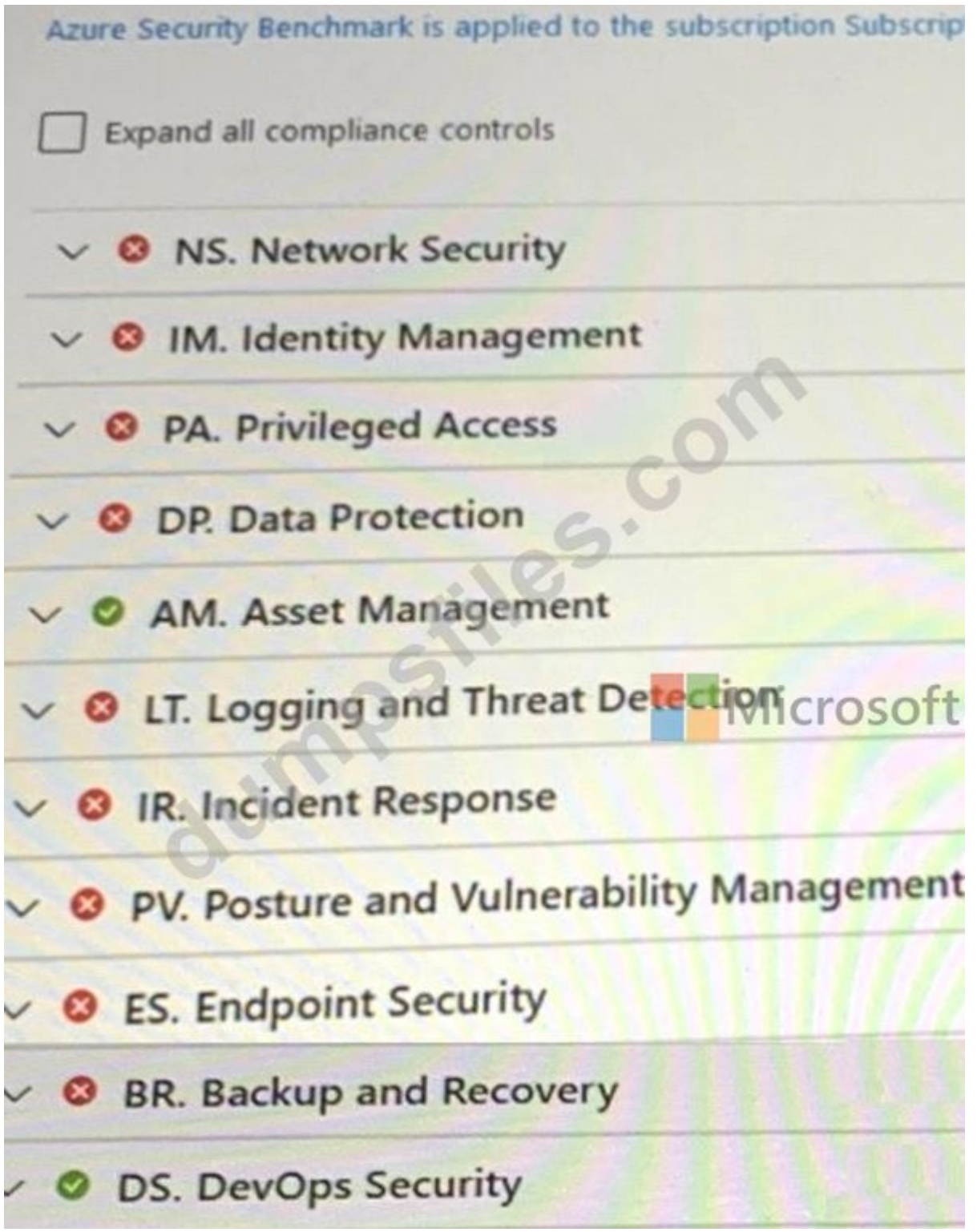
Graphical user interface, text, application Description automatically generated

NEW QUESTION: 107

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.


Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud
Showing subscription 'Subscription1'
Download report
Manage compliance policies
Open query
Audit reports
You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.
Azure Security Benchmark V3
ISO 27001
PCI DSS 3.2.1
SOC TSP
HIPAA HITRUST
Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.
Azure Security Benchmark is applied to the subscription Subscription1
Microsoft

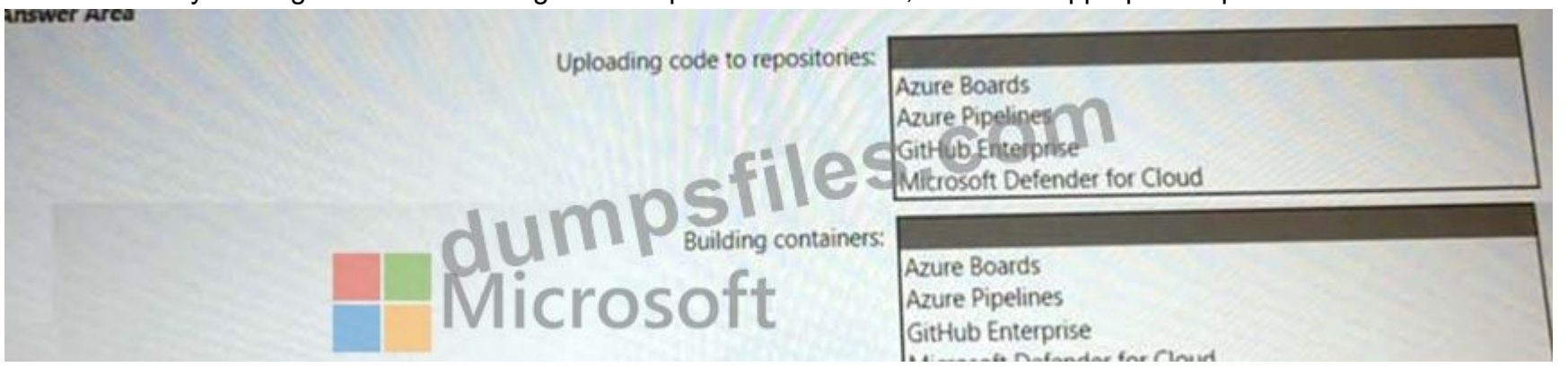


You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

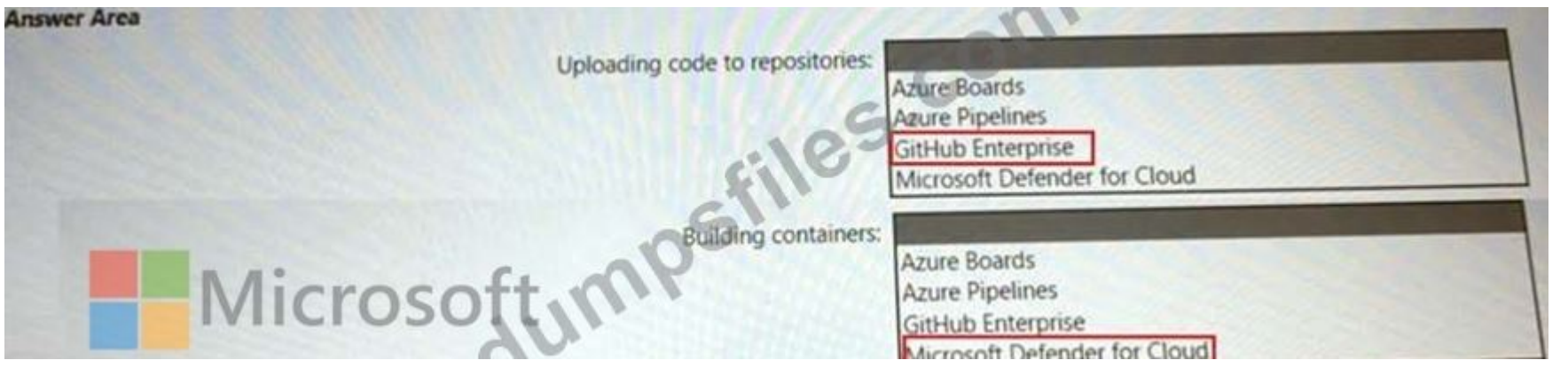
A. Posture and Vulnerability Management
B. Asset Management
C. Incident Response
D. Endpoint Security
E. Data Protection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
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 Monitor webhooks
C. Azure Functions apps
D. Azure Event Hubs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
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:

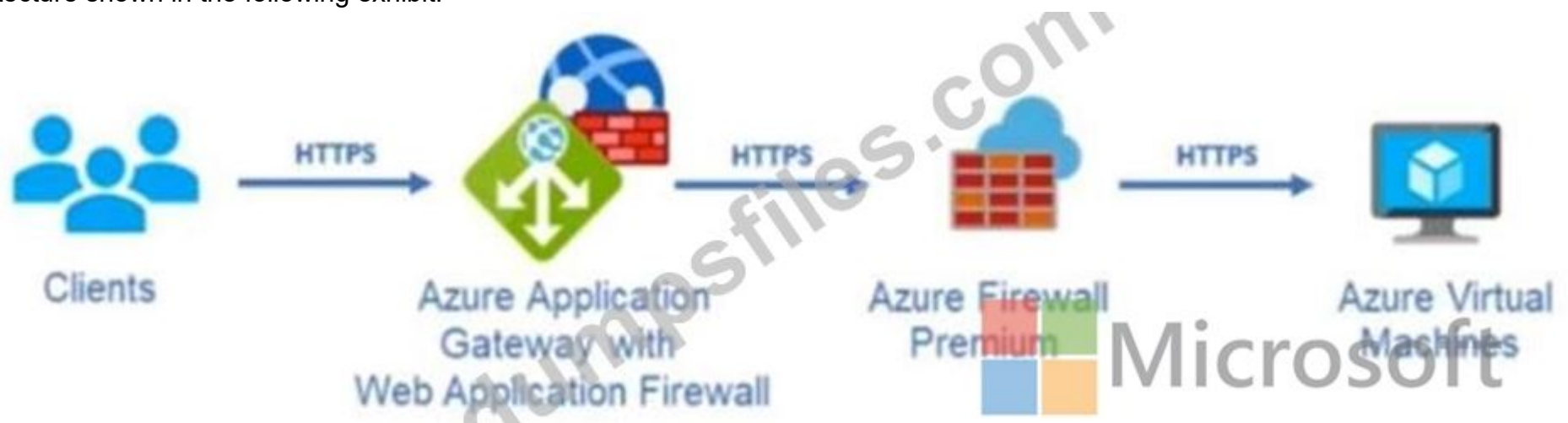


NEW QUESTION: 110
Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD). You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications. What should you include in the recommendation?
A. activity policies in Microsoft Defender for Cloud Apps

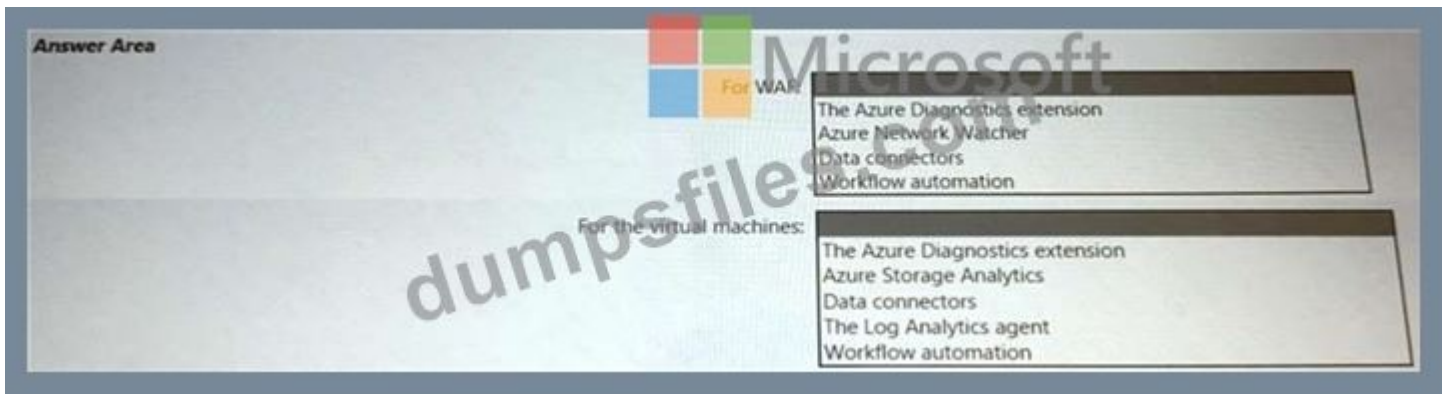
B. sign-in risk policies in Azure AD Identity Protection
C. device compliance policies in Microsoft Endpoint Manager
D. Azure AD Conditional Access policies
E. user risk policies in Azure AD Identity Protection
Answer: D (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-loca
https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules

NEW QUESTION: 111
You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:
* Encrypt cardholder data by using encryption keys managed by the company.
* Encrypt insurance claim files by using encryption keys hosted on-premises.
Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.
Answer: (SHOW ANSWER)
Explanation
https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service-encryption/

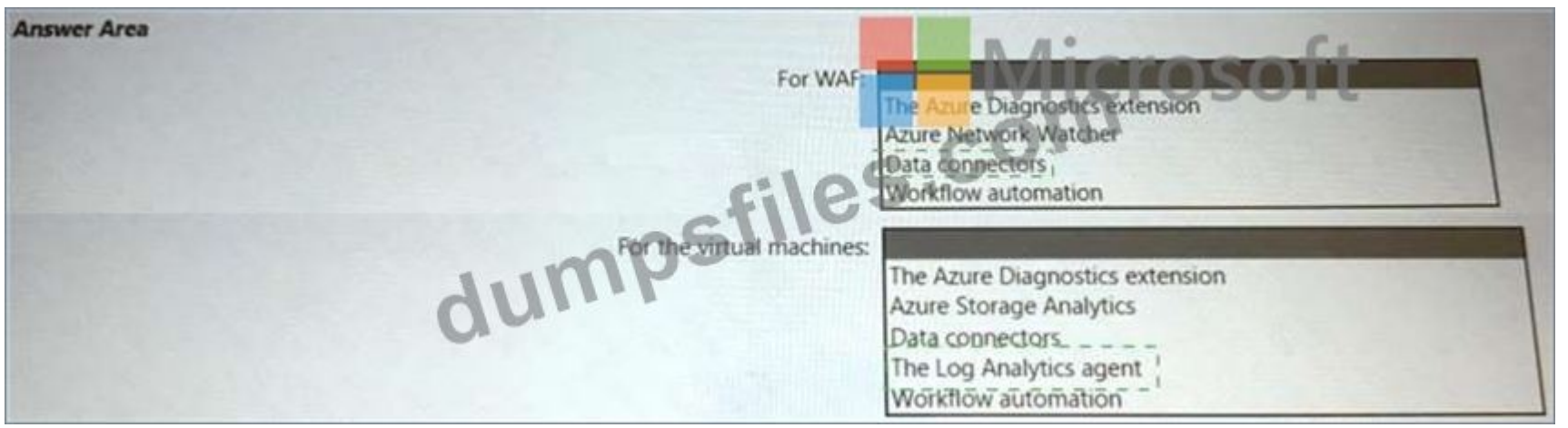
NEW QUESTION: 112
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



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.

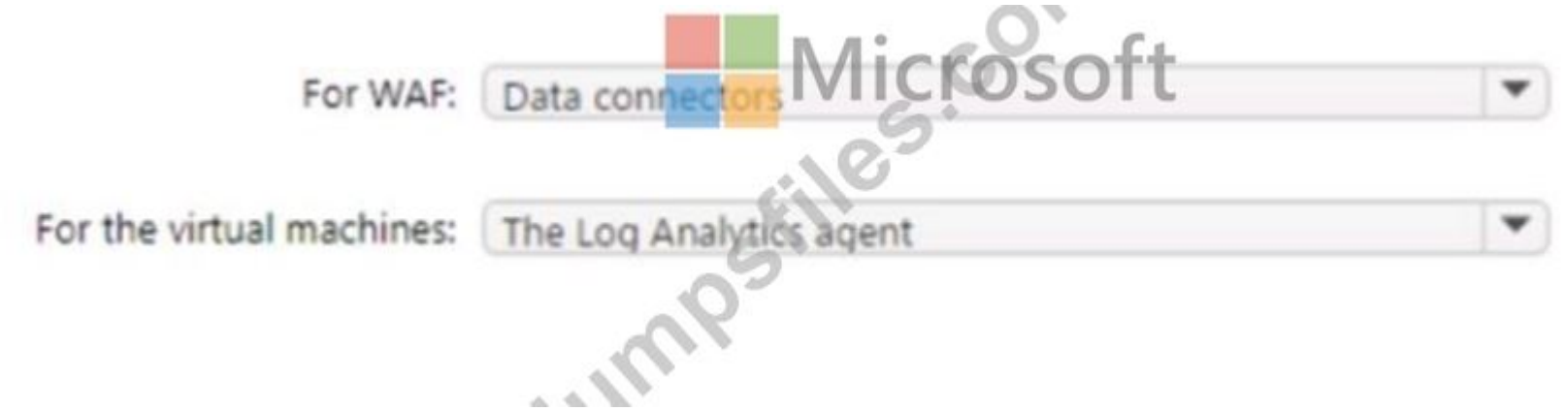


Answer:



Explanation

Graphical user interface Description automatically generated



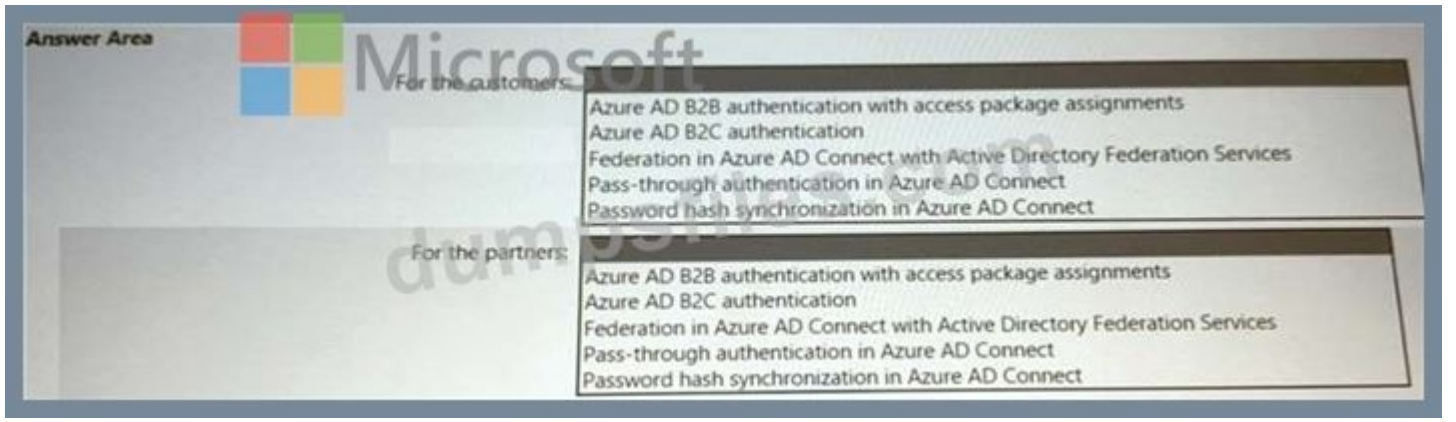
NEW QUESTION: 113

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:

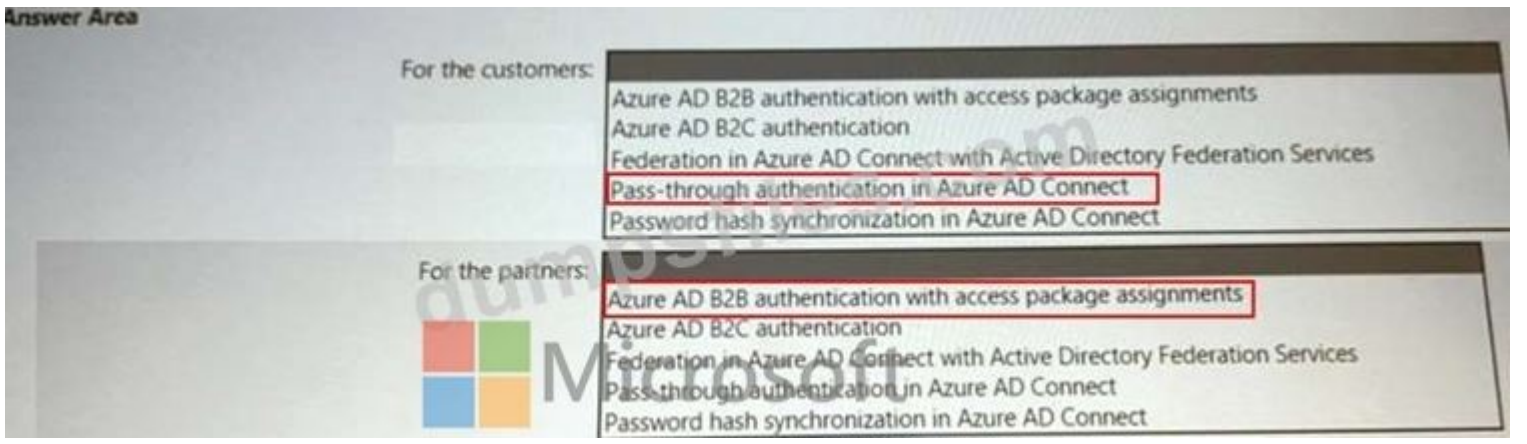
* Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

* 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:



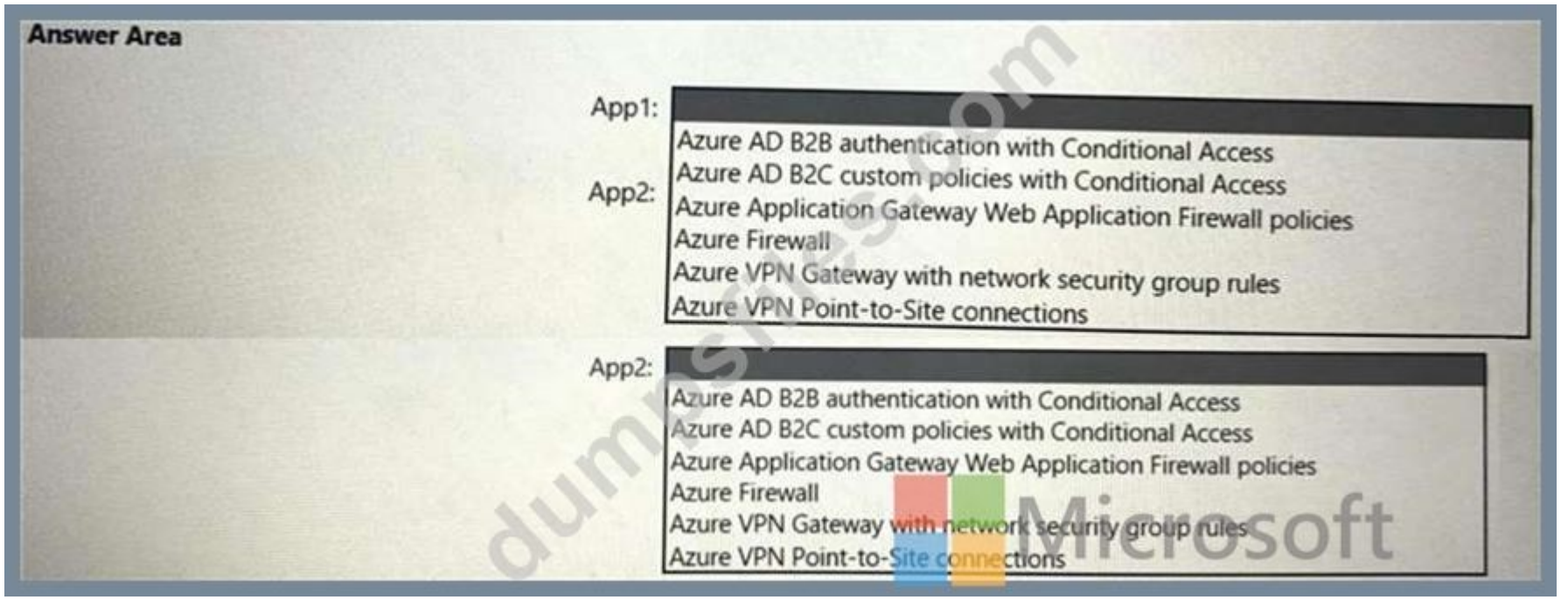
NEW QUESTION: 114

You have a hybrid cloud infrastructure.

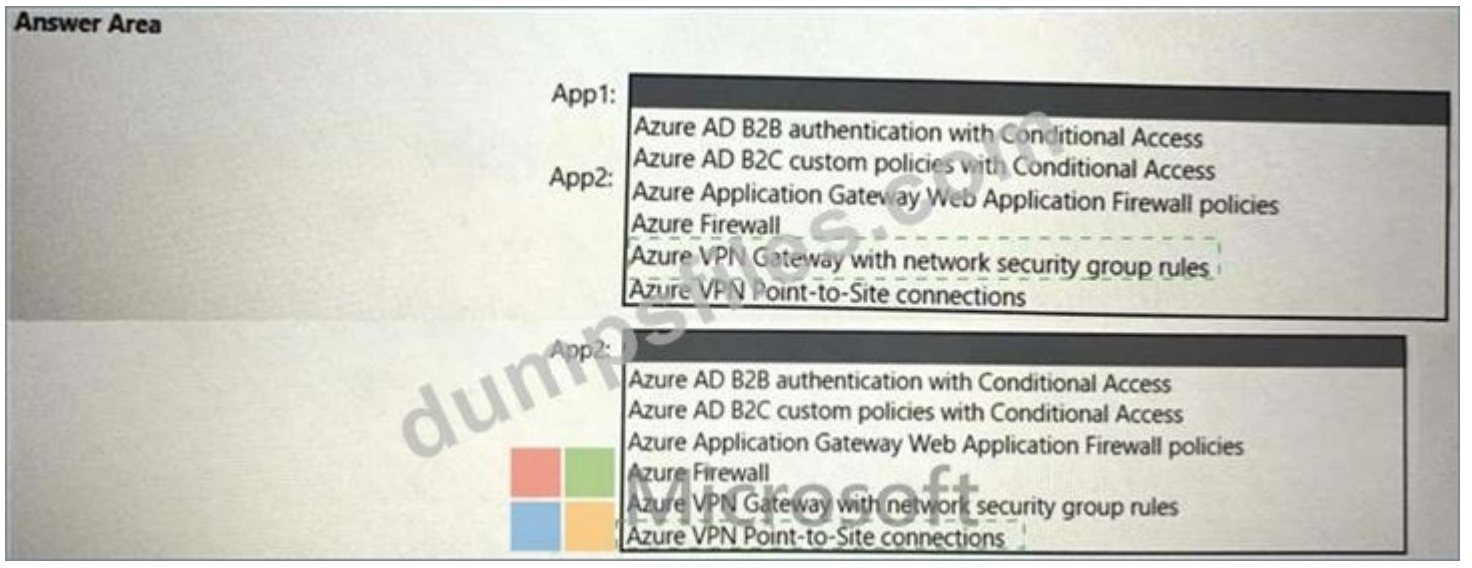
You plan to deploy the Azure applications shown in the following table.

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: 115

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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 Key Vault to store credentials.

A. No

B. Yes

Answer: A (LEAVE A REPLY)

NEW QUESTION: 116

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: 117

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

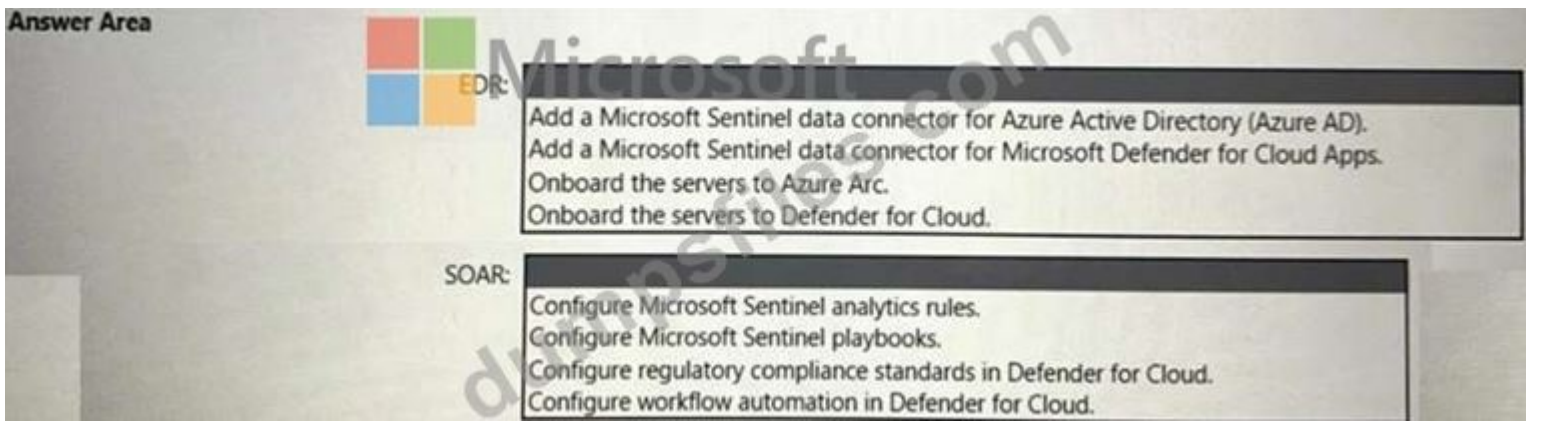
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

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

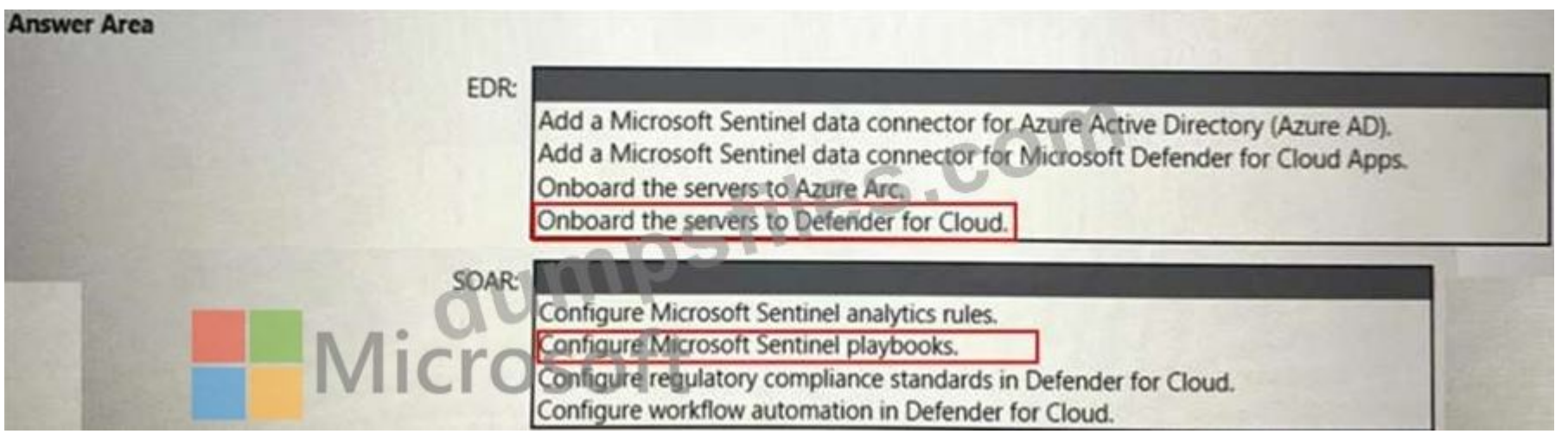
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

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: 118

You have a Microsoft 365 subscription

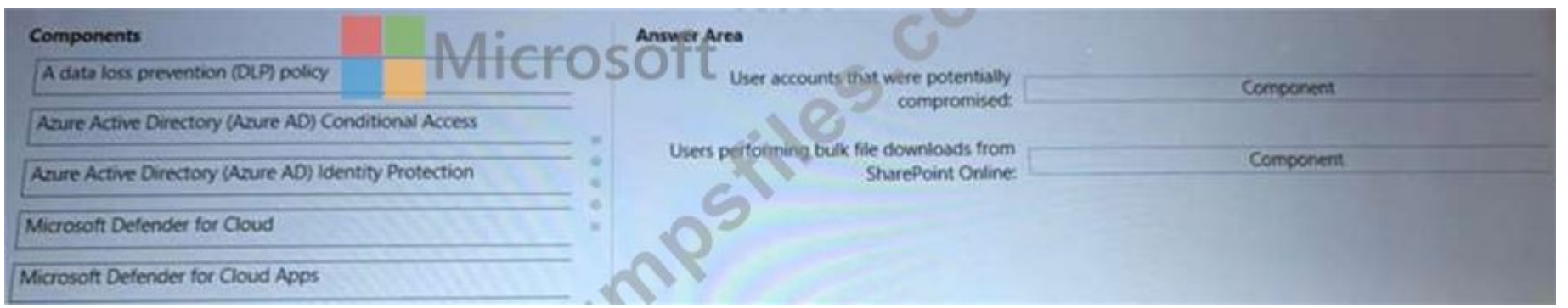
You need to recommend a security solution to monitor the following activities:

* User accounts that were potentially compromised

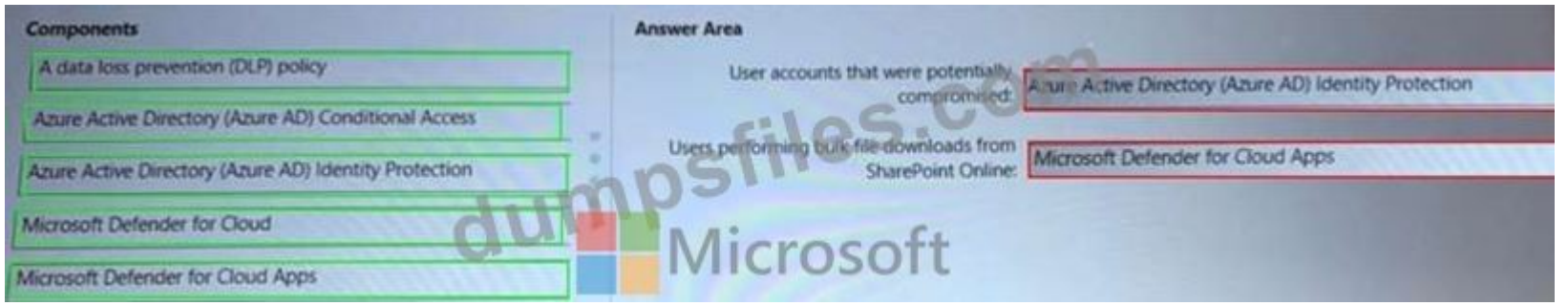
* Users performing bulk file downloads from Microsoft SharePoint Online What should you include in the recommendation for each activity?

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:



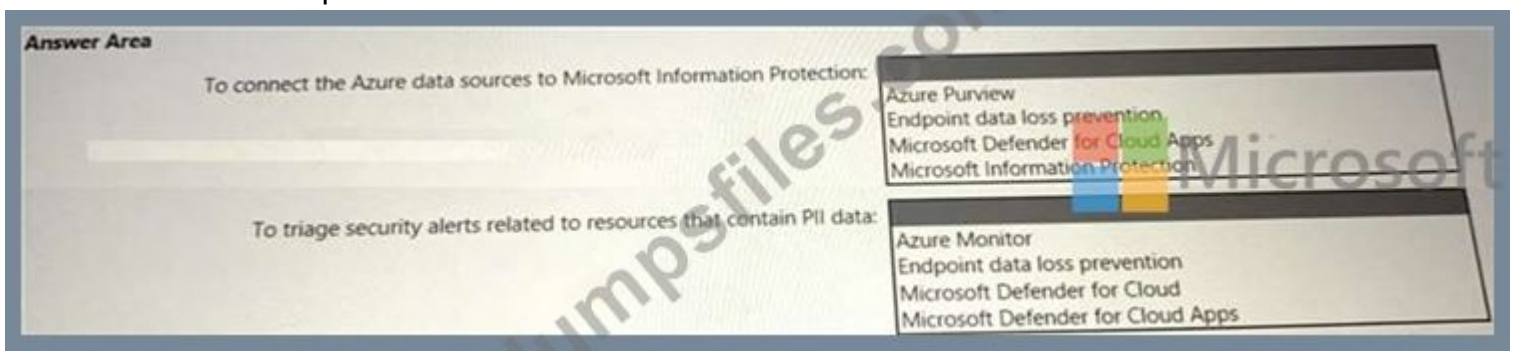
NEW QUESTION: 119
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions 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: 120
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 that allow traffic from the Front Door service tags.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
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: 122
Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C.
The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. custom resource owner password credentials (ROPC) flows in Azure AD B2C
B. access packages in Identity Governance
C. Azure AD Conditional Access integration with user flows and custom policies
D. Azure AD workbooks to monitor risk detections
E. smart account lockout in Azure AD B2C
Answer: C,E (LEAVE A REPLY)

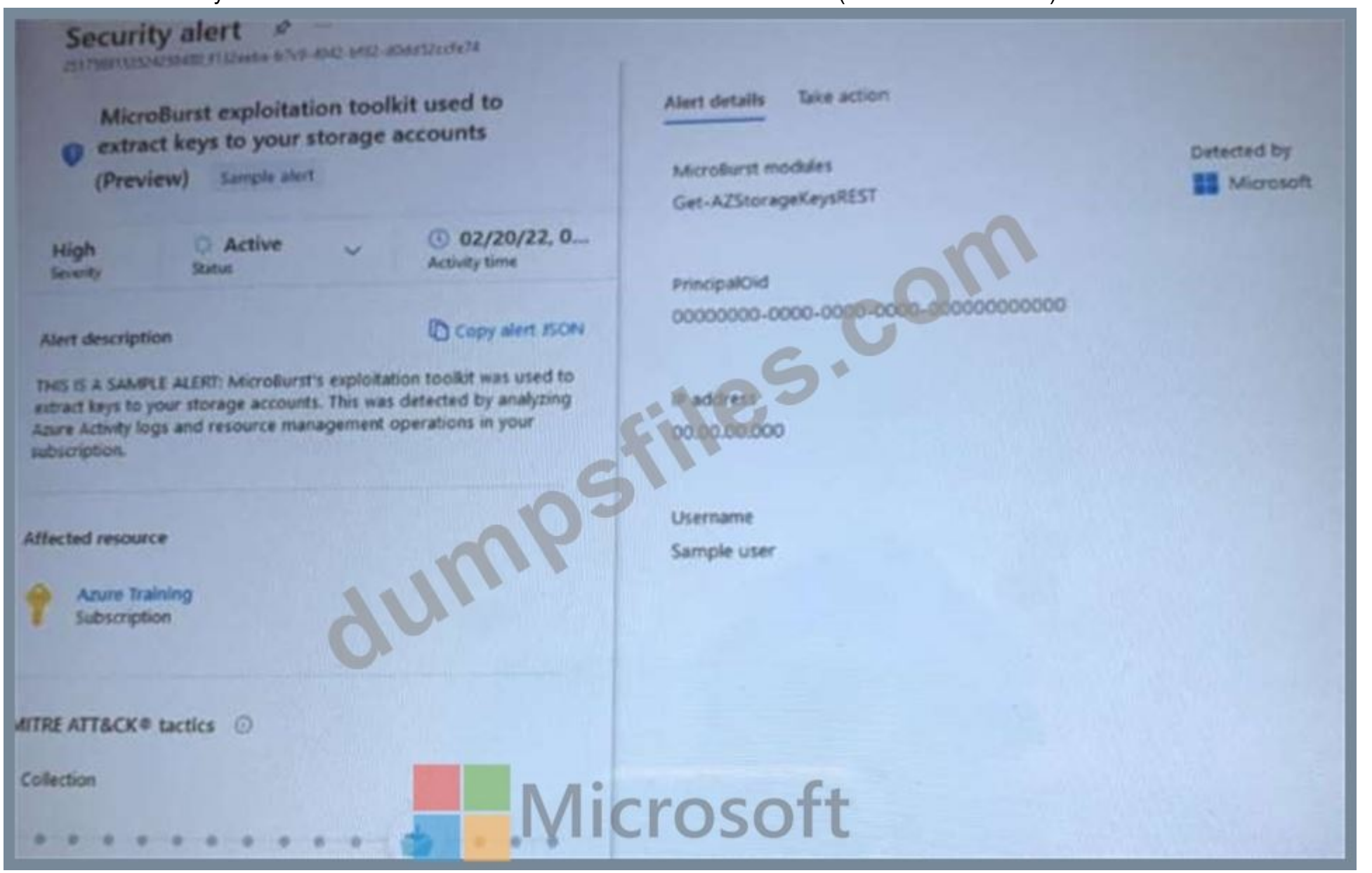
NEW QUESTION: 123
Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The company plans to use Microsoft Information Protection for the PII data store in Azure. You need to recommend a solution to discover PII data at risk in the Azure resources. What 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: 124

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 keys should not be expired

B. Storage accounts should prevent shared key access

C. Storage account public access should be disallowed

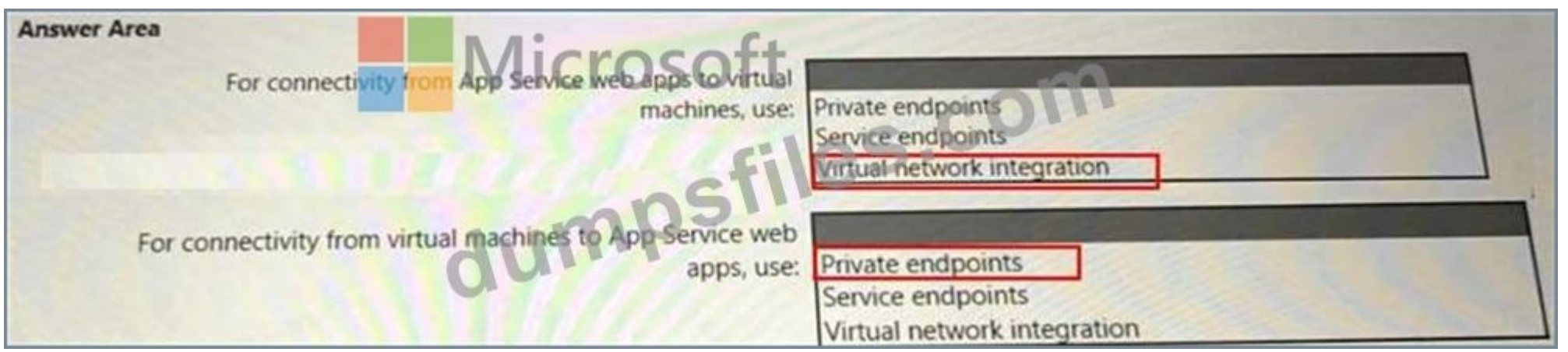
D. Azure Key Vault Managed HSM should have purge protection enabled

Answer: C (LEAVE A REPLY)

NEW QUESTION: 125

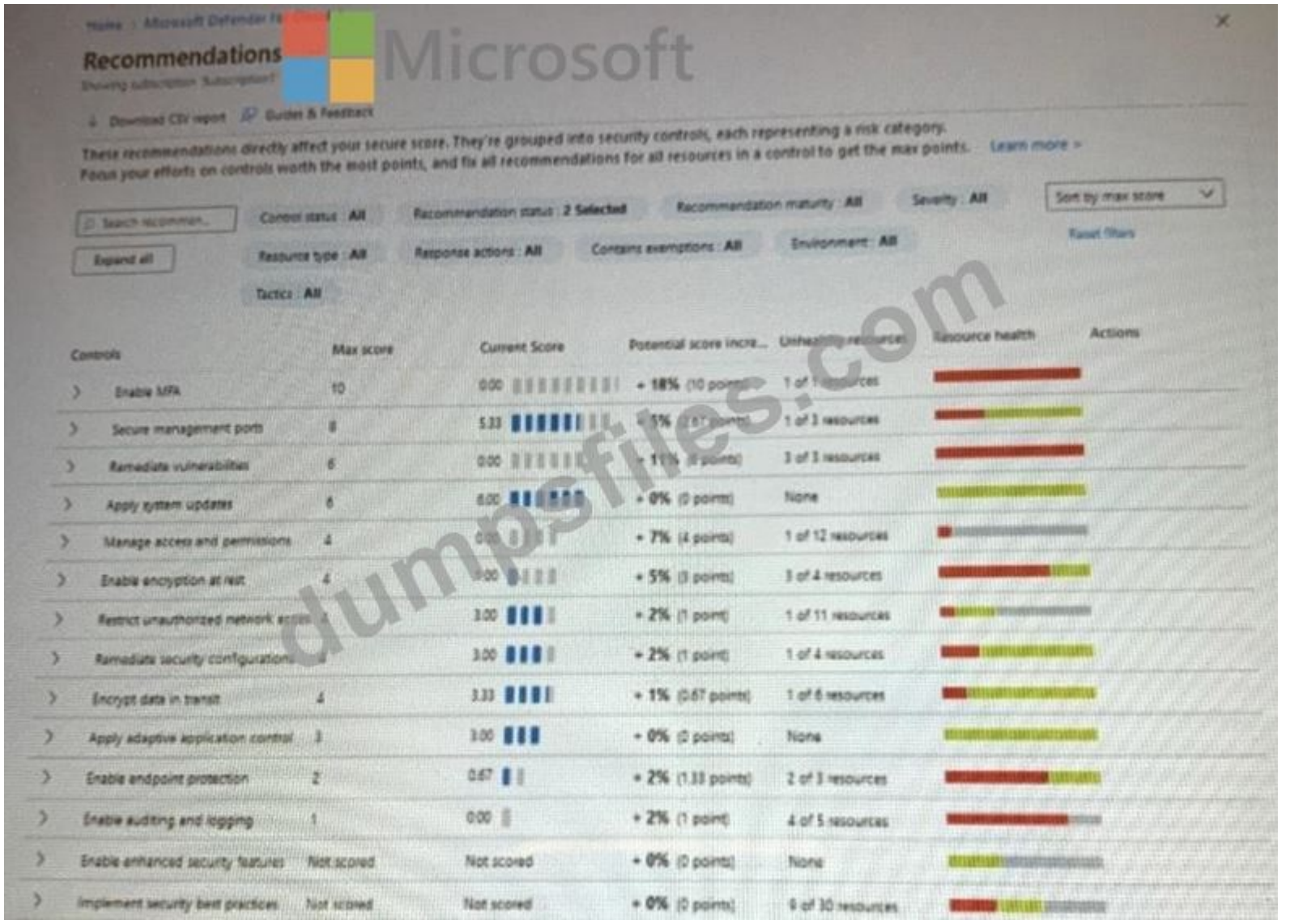
You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer are a. NOTE Each correct selection is worth one point.

Answer:



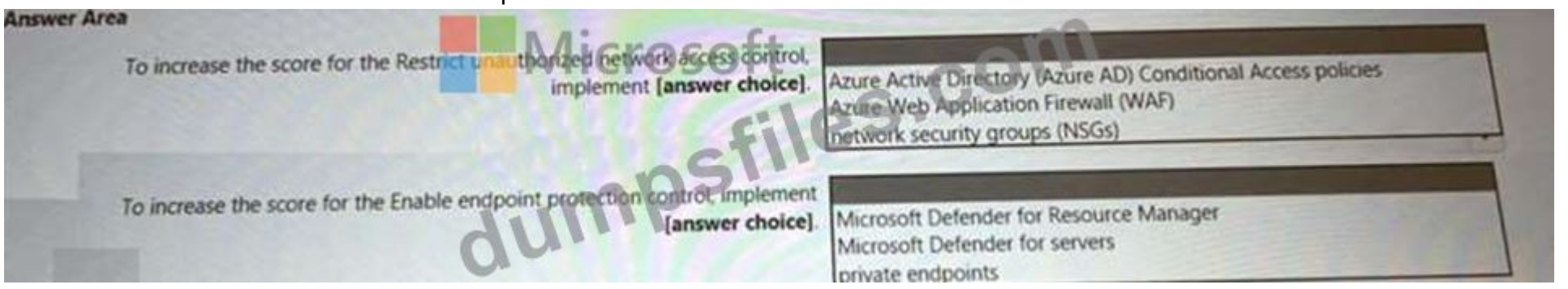
NEW QUESTION: 126

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: