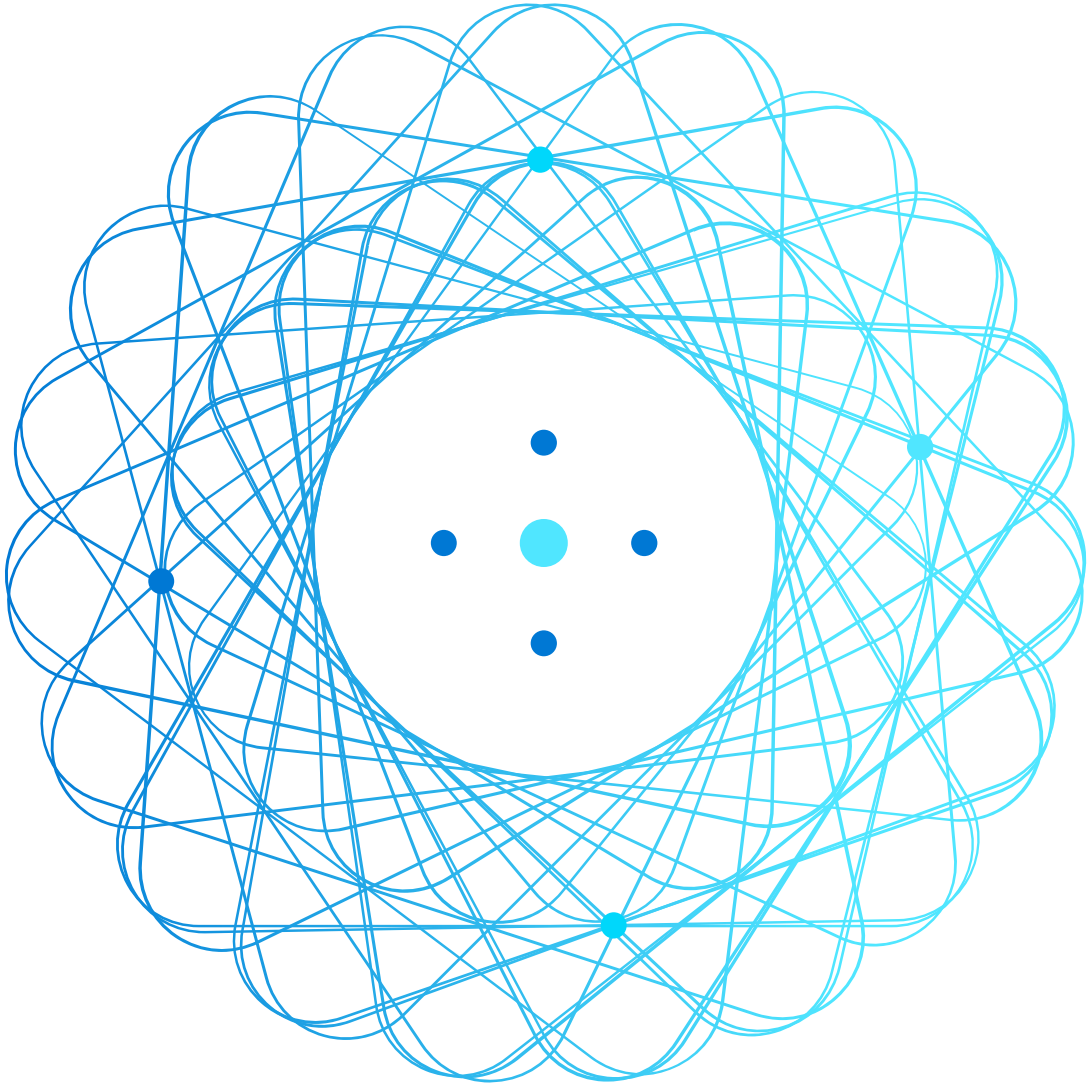
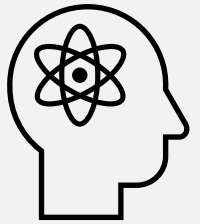
Microsoft Azure

AZ-900T0x Module 04: Security



Module outline



Module 04 – Outline

You will learn the following concepts:

- **Azure Security features**
  - Security Center and resource hygiene
  - Key Vault, Sentinel, and Dedicated Hosts
- **Azure network security**
  - Defense in depth
  - Network Security Groups and Firewalls
  - DDoS protection

Security tools and features

Security tools and features - Objective Domain

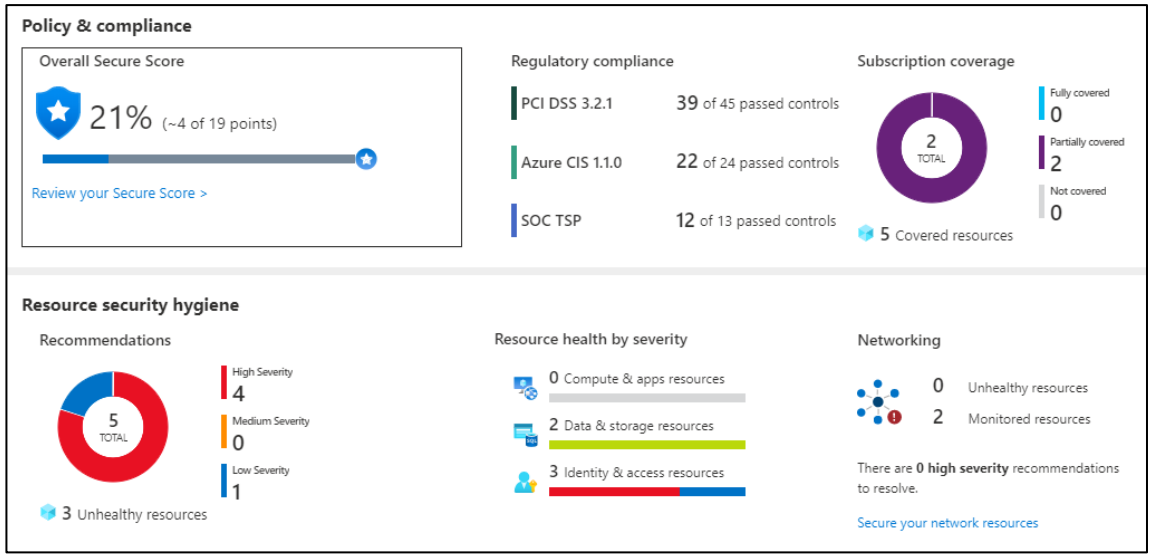
Describe the features and the functionality of:

- Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
- Azure Sentinel
- Key Vault
- Azure Dedicated Hosts

Azure Security Center

Azure Security Center is a monitoring service that provides threat protection across both Azure and on-premises datacenters.

- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports



Azure Security Center - capabilities

Policy Compliance

Run policies across management groups, subscriptions, or tenants.

Continuous Assessments

Assess new and deployed resources to ensure that they are configure properly.

Tailored Recommendations

Recommendations based on existing workload with instructions on how to implement them.

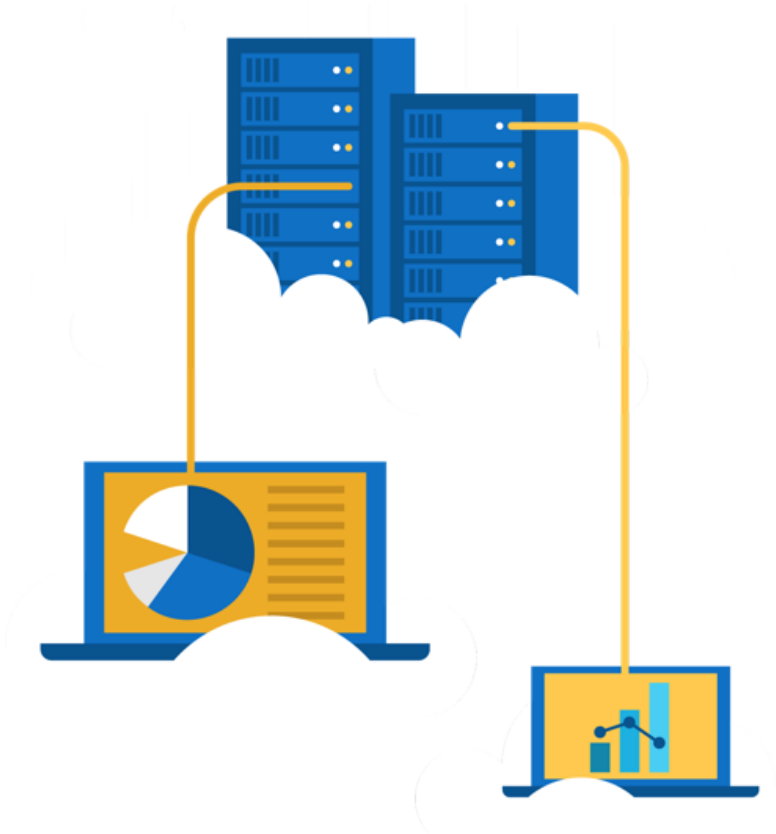
Threat Protection

Analyze attempted threats through alerts and impacted resource reports.

Walkthrough - Azure Security Center

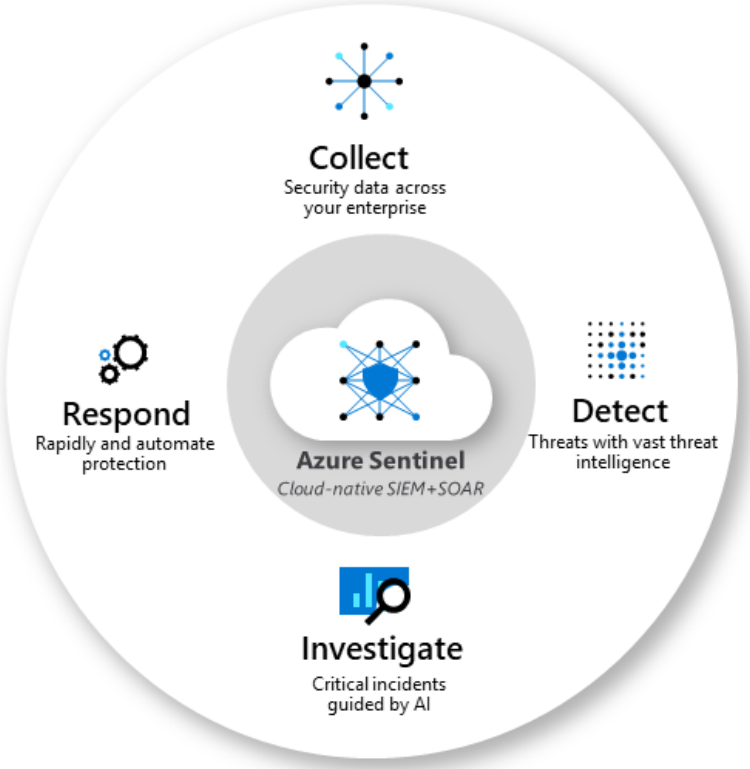
Open Azure Security Center and view some of the common features and configuration options.

1. Launch Azure Security Center.
2. View Policy compliance options.
3. Review your Secure Score.
4. Set a Security Alert.
5. Explore Resource Hygiene.



Azure Sentinel

Azure Sentinel is a security information management (SIEM) and security automated response (SOAR) solution that provides security analytics and threat intelligence across an enterprise.



Connector and Integrations:

- Office 365
- Azure Active Directory
- Azure Advanced Threat Protection
- Microsoft Cloud App Security

Azure Key Vault

Azure Key Vault stores application secrets in a centralized cloud location in order to securely control access permissions and access logging.

- Secrets management.
- Key management.
- Certificate management.
- Storing secrets backed by hardware security modules (HSMs).

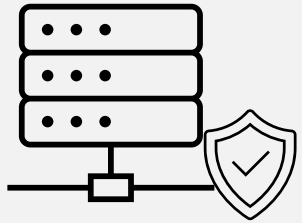
Azure Dedicated Host

Azure Dedicated Host provides physical servers that host one or more Azure virtual machines that is dedicated to a single organization's workload.

Benefits

- Hardware isolation at the server level
- Control over maintenance event timing
- Aligned with Azure Hybrid Use Benefits

Secure network connectivity



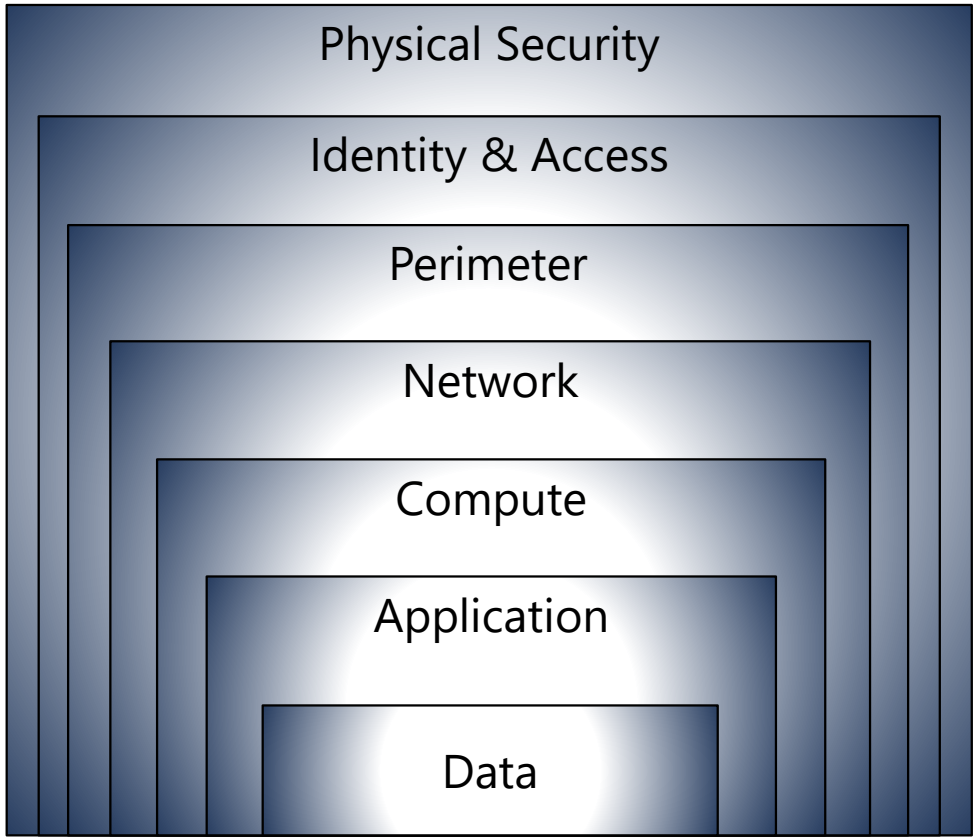
Secure Network Connectivity - Objective Domain

Describe the concept and functionality of:

- Defense in depth
- Network Security Groups (NSG)
- Azure Firewall
- Azure DDoS protection

Defense in depth

- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Shared Security

- Migrating from customer-controlled to cloud-based datacenters shifts the responsibility for security.
- Security becomes a shared concern between cloud providers and customers.

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Network Security Groups (NSGs)

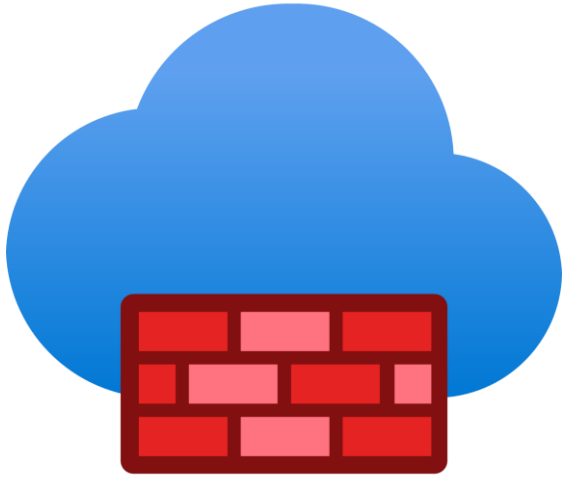
Network Security Groups (NSGs) filter network traffic to and from Azure resources on Azure Virtual Networks.

- Set inbound and outbound rules to filter by source and destination IP address, port, and protocol.
- Add multiple rules, as needed, within subscription limits.
- Azure applies default, baseline security rules to new NSGs.
- Override default rules with new, higher priority rules.

Azure Firewall

A stateful, managed Firewall as a Service (FaaS) that grants/denies server access based on originating IP address, in order to protect network resources.

- Applies inbound and outbound traffic filtering rules
- Built-in high availability
- Unrestricted cloud scalability
- Uses Azure Monitor logging



Azure Application Gateway also provides a firewall, Web Application Firewall (WAF). WAF provides centralized, inbound protection for your web applications.

Azure Distributed Denial of Service (DDoS) protection

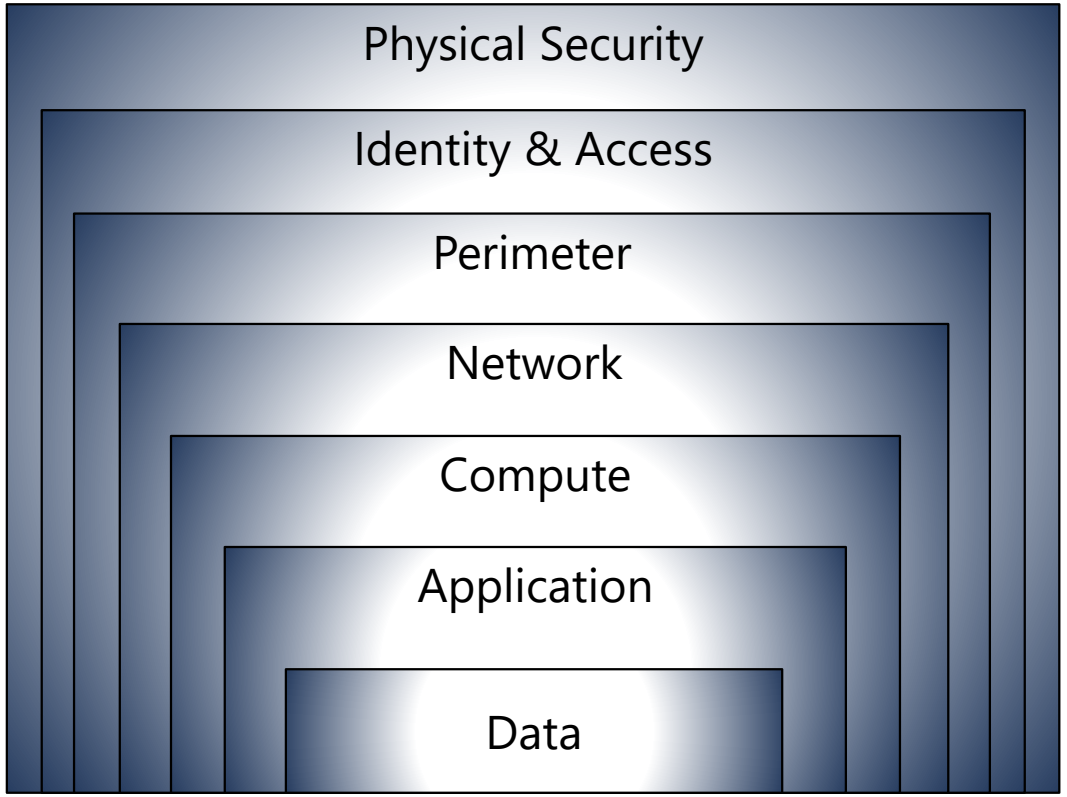
DDoS attacks overwhelm and exhaust network resources, making apps slow or unresponsive.

- Sanitizes unwanted network traffic before it impacts service availability.
- Basic service tier is automatically enabled in Azure.
- Standard service tier adds mitigation capabilities that are tuned to protect Azure Virtual Network resources.

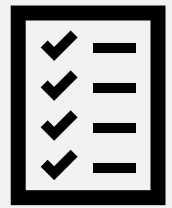
Defense in Depth Reviewed

Combining network security solutions

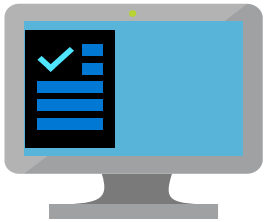
- **NSGs** with **Azure Firewall** to achieve defense in depth.
- **Perimeter layer** protects your network boundaries with Azure DDoS Protection and Azure Firewall.
- **Networking layer** only permits traffic to pass between networked resources with Network Security Group (NSG) inbound and outbound rules.



Knowledge Checks (5 min)



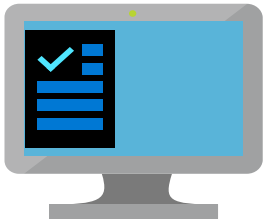
Knowledge Check



1. What type of data is actively moving from one location to another, such as across the internet or through a private network?

a) Immutable
b) In transit
c) At rest
d) In the cloud

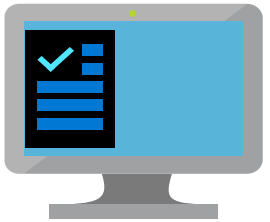
Knowledge Check



1. What type of data is actively moving from one location to another, such as across the internet or through a private network?

a) Immutable
b) In transit
c) At rest
d) In the cloud

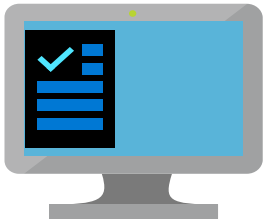
Knowledge Check



2. What Azure service would you for use to run your virtual machines in an environment that ensures they are isolated from other virtual machines?

a) Availability Zone
b) Availability Set
c) Azure Dedicated Hosts
d) Azure Reserved VM Instances

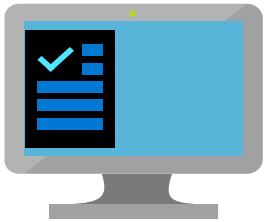
Knowledge Check



2. What Azure service would you for use to run your virtual machines in an environment that ensures they are isolated from other virtual machines?

a) Availability Zone
b) Availability Set
c) Azure Dedicated Hosts
d) Azure Reserved VM Instances

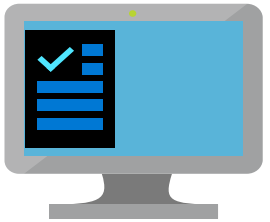
Knowledge Check



3. What strategy employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to data?

a) Ciphertext
b) Blob security
c) Network security layers
d) Defense-in-depth

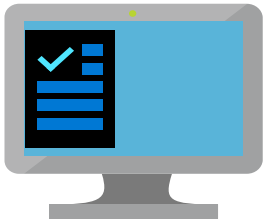
Knowledge Check



3. What strategy employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to data?

a) Ciphertext
b) Blob security
c) Network security layers
d) Defense-in-depth

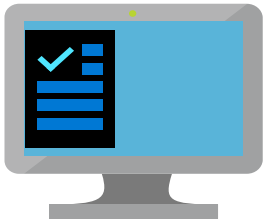
Knowledge Check



4. What type of attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users?

a) Distributed Denial of Service (DDoS)
b) Resource request attack (RRA)
c) Man in the Middle Attack
d) Firewall Bypass

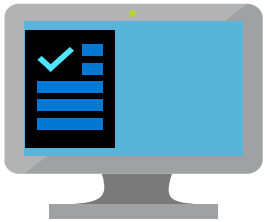
Knowledge Check



4. What type of attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users?

a) Distributed Denial of Service (DDoS)
b) Resource request attack (RRA)
c) Man in the Middle Attack
d) Firewall Bypass

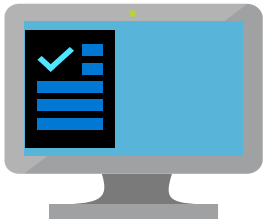
Knowledge Check



5. Which layer of Defense-in-depth is focused on preventing network-based attacks?

a) Data layer
b) Identity and Access layer
c) Perimeter layer
d) Compute layer

Knowledge Check



5. Which layer of Defense-in-depth is focused on preventing network-based attacks?

a) Data layer
b) Identity and Access layer
c) Perimeter layer
d) Compute layer

Module 4 Review

Microsoft Learn Modules
(docs.microsoft.com/Learn)

- Azure Security Center and resource hygiene
- Key Vault, Sentinel, and Dedicated Hosts
- Defense in depth
- DDoS protection