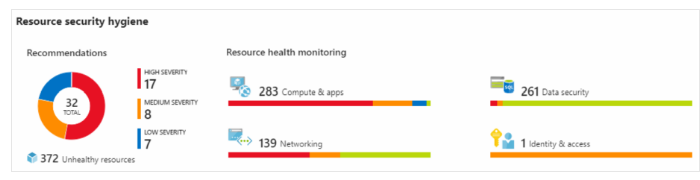
**[Azure Fundamentals part 4: Describe general security and network security features](https://docs.microsoft.com/en-us/learn/paths/az-900-describe-general-security-network-security-features/)**

# **Protect against security threats by using Azure Security Center**

1. **What's Azure Security Center?**
   1. **Monitoring** service that provides visibility of your **security** **posture**
   2. **Security** **posture** refers to **cybersecurity** **policies** and **controls**
   3. Security Center can:
      1. Monitor security settings
      2. Automatically apply required security settings
      3. Provide security recommendation
      4. Continuously monitor your resources and perform automatic security assessments
      5. Use machine learning to detect and block malware
      6. Detect and analyze potential inbound attack
      7. Provide just-in-time access control for network ports

## **Understand your security posture**

1. In the **Resource security hygiene** section, you can see the health of its resources from a security perspective. To help prioritize remediation actions, recommendations are categorized as low, medium, and high. Here's an example
2. 

### What's secure score?

1. Is a measurement of an organization's security posture
2. Your score is based on the percentage of security controls that you satisfy
3. The more security controls you satisfy, the higher the score you receive.
4. Secure score helps you:
   1. Report on the current state of your organization's security posture
   2. Improve your security posture
   3. Compare with benchmarks

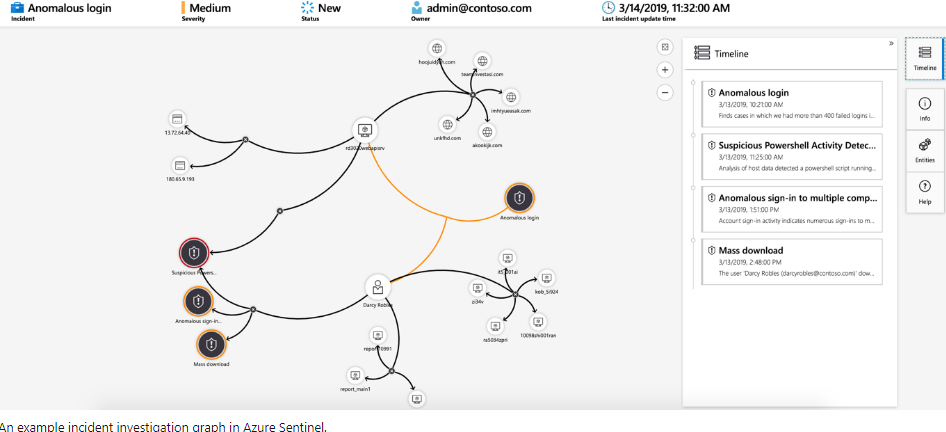
## **Protect against threats**

1. **Just-in-time VM access:** Configure just-in-time access to VMs
2. **Adaptive application controls:** Control which applications are allowed to run on its VMs
3. **Adaptive network hardening:** Monitor the internet traffic patterns of the VMs
4. **File integrity monitoring:** monitoring of changes to important files on both Windows and Linux

## **Respond to security alerts**

1. **Security** **Center** to get a **centralized** **view** of all of its **security** **alerts**
2. Company can **dismiss** false **alerts**, **investigate** them further, **remediate** alerts manually, or use an **automated** **response** with a **workflow** **automation**
3. **Workflow** **automation** uses **Azure** **Logic** **Apps** and **Security** **Center** **connectors**

# **Detect and respond to security threats by using Azure Sentinel**

1. Security information and event management (**SIEM**)
2. **Azure Sentinel capabilities**:
   1. Azure Sentinel enables you to:
      1. **Collect cloud data at scale:** Collect data across all users, devices, applications, and infrastructure, both on-premises and from Azure.
      2. **Detect previously undetected threats:** Minimize false positives
      3. **Investigate threats with artificial intelligence:** Examine suspicious activities at scale
      4. **Respond to incidents rapidly:** Use built-in orchestration
3. **Connect your data sources:**
   1. Azure Sentinel supports a number of data sources, which it can analyze for security events
   2. Data sources include:
      1. **Connect Microsoft solutions:**  services like Microsoft 365
      2. **Connect other services and solutions:** For common non-Microsoft services
      3. **Connect industry-standard data sources: Other sources such as** Common Event Format (CEF) messaging standard, Syslog, or REST API
4. **Detect threats:**
   1. Can used Built in analytics and Custom analytics
   2. **Built in analytics: Templates designed by Microsoft.** Templates can be **customized** and can use **machine** **learning**.
   3. **Custom analytics:**  **Rules** that you create to search for specific criteria within your **environment**. You can also set an **alert** **threshold**.
5. **Investigate and respond:**
   1. With the **investigation** **graph**, the company can review information from entities directly
   2. 
   3. The company will also use [Azure Monitor Playbooks](https://docs.microsoft.com/en-us/learn/modules/threat-response-sentinel-playbooks/) to automate responses to threats with these steps:
      1. When the alert is triggered, open a ticket
      2. Send a message to the security operations channel
      3. Message can be **Block** or **Ignore**
   4. When an admin chooses **Block**, the IP address is blocked in the firewall
   5. When an admin chooses **Ignore**, the alert is closed in Azure Sentinel

# **Store and manage secrets by using Azure Key Vault**

1. [Azure Key Vault](https://azure.microsoft.com/services/key-vault) is a centralized cloud service for storing an application's secrets in a single, central location
2. It provides secure access to sensitive information by providing access control and logging capabilities

## **What can Azure Key Vault do?**

1. **Manage secrets**
2. **Manage encryption keys**
3. **Manage SSL/TLS certificates**
4. **Store secrets backed by hardware security modules (HSMs)**

## **What are the benefits of Azure Key Vault?**

1. **Centralized application secrets:**  Reduces the chances that secrets are accidentally leaked
2. **Securely stored secrets and keys:** Access to Key Vault requires proper authentication and authorization
3. **Access monitoring and access control:** You can monitor and control access to your application secrets
4. **Simplified administration of application secrets:** Key Vault makes it easier to enroll and renew certificates
5. **Integration with other Azure services:** Integrate Key Vault Azure services

## **AZURE KEY VAULT EXERCISE**

1. In practice, there are several ways to add secrets to and read secrets from Key Vault. You can use the Azure portal, the Azure CLI, or Azure PowerShell
2. I had an error first time attempting this

# **Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host**

1. On **Azure**, **virtual** **machines** (**VMs**) run on **shared** **hardware** that Microsoft manages
2. Some organizations must follow **regulatory** **compliance** that requires them to be the **only** **customer** using the **physical** **machine** that hosts their virtual machine

## **What are the benefits of Azure Dedicated Host?**

1. Gives you visibility into, and control over, the server infrastructure
2. Helps address compliance requirements
3. Let’s you choose the number of processors, server capabilities

## **Availability considerations for Dedicated Host**

1. For **high** **availability**, you can provision multiple hosts in a **host** **group**, and **deploy** your VMs across this group
2. This feature enables you to control when **regular** **maintenance** updates occur, within a **35-day** rolling window

## **Pricing considerations**

1. You're charged per dedicated host
2. Software licensing, storage, and network usage are billed separately from the host and VMs

## **Knowledge Check**

<https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/7-knowledge-check>

**[Secure network connectivity on Azure](https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.az-900-describe-general-security-network-security-features)**

# **What is defense in depth?**

1. The **objective** of **defense** **in** **depth** is to **protect** **information** and **prevent** it from being **stolen** by those who **aren't** **authorized** to access it

## **Layers of defense in depth**

1. Visualize defense in depth as a set of layers: ***PIPNCAD***
   1. **The physical security layer:** First line of defense to protect computing hardware
   2. **The identity and access layer:** Controls access to infrastructure a
   3. **The perimeter layer:** Distributed denial of service (DDoS) protection
   4. **The network layer:** Limits communication
   5. **The compute layer:**  Secures access to virtual machines
   6. **The application layer:** Ensure that applications are secure
   7. **The data layer:**  Controls access to business and customer data
2. Azure provides security tools and features at every level:
   1. **Physical security: Microsoft uses various physical security mechanisms in its cloud datacentres.**
   2. **Identity and access:** 1) Control access to infrastructure, 2) Use single sign-on (SSO) and multifactor authentication, 3) Audit events and changes
   3. **Perimeter:** 1) Use DDoS protection, 2) Use perimeter firewalls
   4. **Network: 1)** Limit communication between resources, 2) Deny by default, 3) **Restrict** **inbound** internet access and **limit** **outbound** access, 4) Implement secure connectivity to on-premises networks
   5. **Compute:** 1) Secure access to virtual machines, 2) Implement endpoint protection on devices and keep systems patched
   6. **Application:** 1) Ensure applications are secure with no vulnerabilities, 2) Store sensitive application secrets in a secure storage medium, 3) Make security a design requirement
   7. **Data:** Protect data stored in: 1) Databases, 2) VM disks, 3) SaaS eg. Office 65, 4) Cloud storage

## **Security posture**

1. Security posture is your organization's ability to protect from and respond to security threats
2. Collectively as CIA
   1. **Confidentiality:** The **principle** of **least** **privilege** - **level** that **they** **need** to perform their **work**
   2. **Integrity:** Prevent unauthorized changes to information using hash algorithms
   3. **Availability:** Ensure that services are functioning and can be accessed only by authorized users

# **Protect virtual networks by using Azure Firewall**

1. A firewall is a network security device that monitors incoming and outgoing network traffic
2. It decides to allow or block traffic

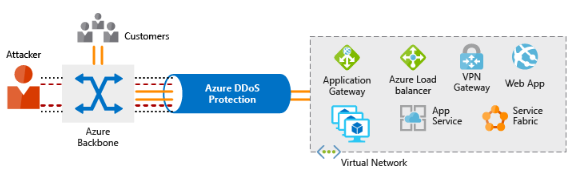
## **What's Azure Firewall?**

1. Is a **managed**, **cloud**-**based** network **security** **service** that helps protect resources in your **Azure** virtual networks
2. Azure Firewall is a stateful firewall - analyzes the complete context of a network connection, not just an individual packet.
3. Azure Firewall provides many features, including:
   1. Built-in high availability
   2. Unrestricted cloud scalability
   3. Inbound and outbound filtering rules
   4. Inbound Destination Network Address Translation (DNAT) support
   5. Azure Monitor logging

## **What can I configure with Azure Firewall?**

1. Application rules that define fully qualified domain names (FQDNs)
2. Network rules
3. Network Address Translation (NAT) rules, which define destination IP addresses and inbound requests
4. [Azure Application Gateway](https://azure.microsoft.com/services/application-gateway) also provides a firewall that's called the web application firewall (WAF)
5. [Azure Front Door](https://azure.microsoft.com/services/frontdoor/) and [Azure Content Delivery Network](https://azure.microsoft.com/services/cdn/) also provide WAF services.

# **Protect from DDoS attacks by using Azure DDoS Protection**

1. What are DDoS attacks?
   1. Attempts to overwhelm and exhaust an application's resources
   2. Making the application slow
2. What is Azure DDoS Protection?
   1. Combine DDoS Protection with recommended application design practices
   2. DDoS Protection uses the scale and elasticity of Microsoft's global network
   3. Helps protect your Azure applications by analyzing and discarding DDoS traffic
   4. **DDoS** **Protection** **identifies** the **attacker's** attempt to overwhelm the network and blocks further traffic from them, **ensuring** that **traffic** **never** reaches **Azure** **resources**
   5. **Elastic** **computing** means that you can **automatically** **scale** **out** your **deployment** to meet demand
   6. A **cleverly** **designed** **DDoS** **attack** can cause you to **increase** your resource allocation, which incurs unneeded **expense**

## **What service tiers are available to DDoS Protection?**

1. DDoS Protection provides these service tiers:
   1. **Basic** **service:**
      1. Is **automatically** enabled for **free** as part of your Azure subscription.
      2. **Azure** **global** **network** is used to **distribute** and **mitigate** **attack** traffic across Azure regions
   2. **Standard:**
      1. Standard service tier provides additional mitigation capabilities
      2. Provides always-on traffic monitoring and real-time mitigation
      3. Protection policies are tuned through **dedicated** **traffic** **monitoring** and **machine** **learning** **algorithms**

## **What kinds of attacks can DDoS Protection help prevent?**

1. The Standard service tier can help prevent:
   1. **Volumetric attacks:** Goal of this attack is to flood the network
   2. **Protocol attacks:** These attacks render a target inaccessible
   3. **Resource-layer (application-layer) attacks (only with web application firewall):** These attacks target web application packets

# **Filter network traffic by using network security groups**

1. A company may want to understand how to protect its internal networks on Azure
2. What are network security groups?
   1. You can think of NSGs like an internal firewall
   2. When you create a network security group, Azure creates a series
   3. You can't remove the default rules, but you can override them

Exercise is not working

# **Combine Azure services to create a complete network security solution**

1. Secure the perimeter layer:
   1. The **perimeter** **layer** is about **protecting** your **organization's** **resources** from **network**-**based** **attacks**
   2. Use Azure DDoS Protection
   3. Use perimeter firewalls with Azure Firewall
2. Secure the network layer
   1. Focus is on limiting network connectivity
   2. Segment your resources and use network-level controls
   3. Here are some recommended practices:
      1. Limit communication between resources by segmenting your network
      2. Deny by default
      3. Restrict inbound internet access
      4. Implement secure connectivity to on-premises networks
3. Combine services:
   1. You can combine Azure networking and security services to manage your network security:
      1. **Network security groups and Azure Firewall: 1)** Azure Firewall complements the functionality of network security groups.
      2. **Azure Application Gateway web application firewall and Azure Firewall: 1)** Web application firewall (WAF) is a feature of Azure Application Gateway. Azure Firewall provides:
         1. **Inbound Protection**
         2. **Outbound Protection**
         3. **Application-Level Protection**

Knowledge Check:

https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/8-knowledge-check