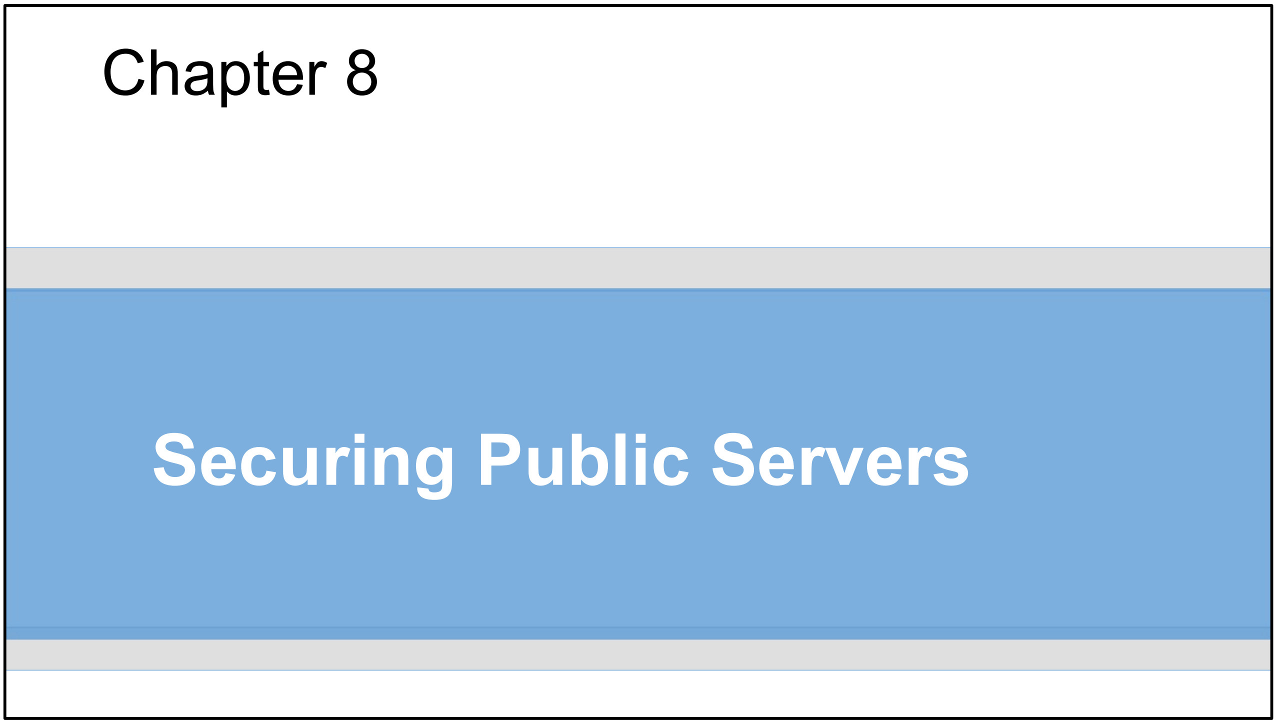
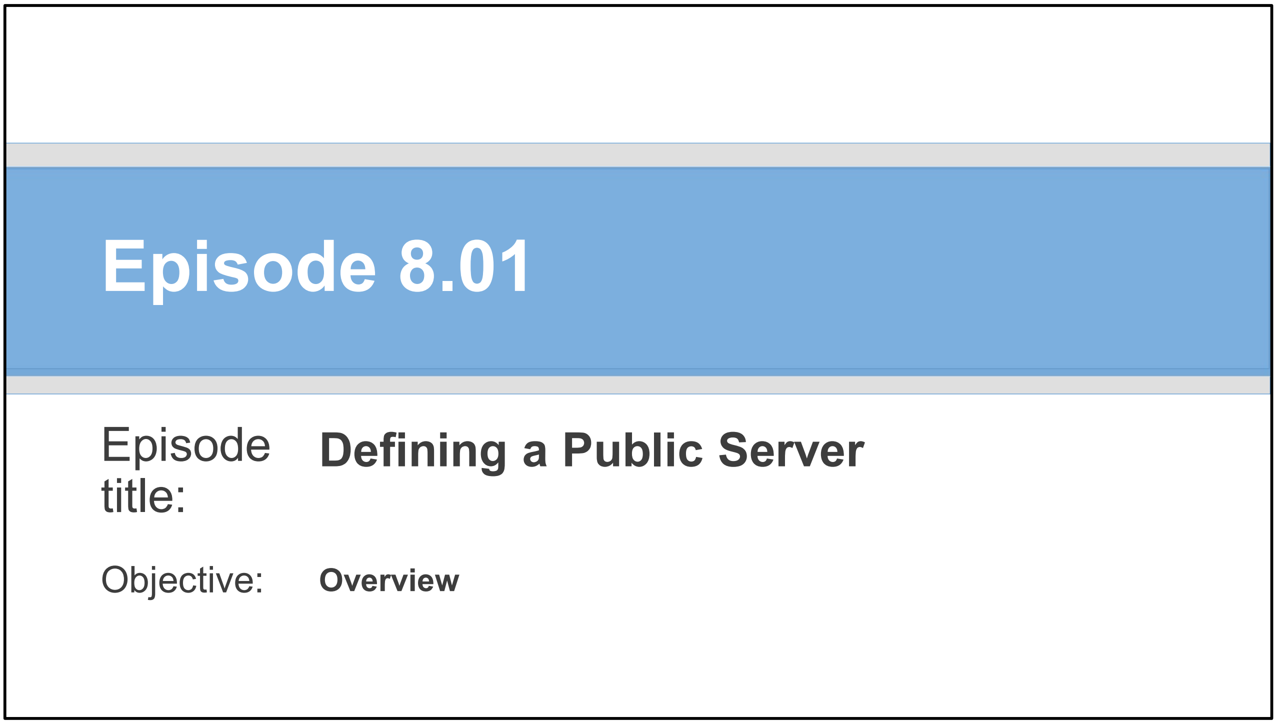


Chapter 8

Securing Public Servers



Episode 8.01

Episode title: **Defining a Public Server**

Objective: **Overview**

Episode 8.02

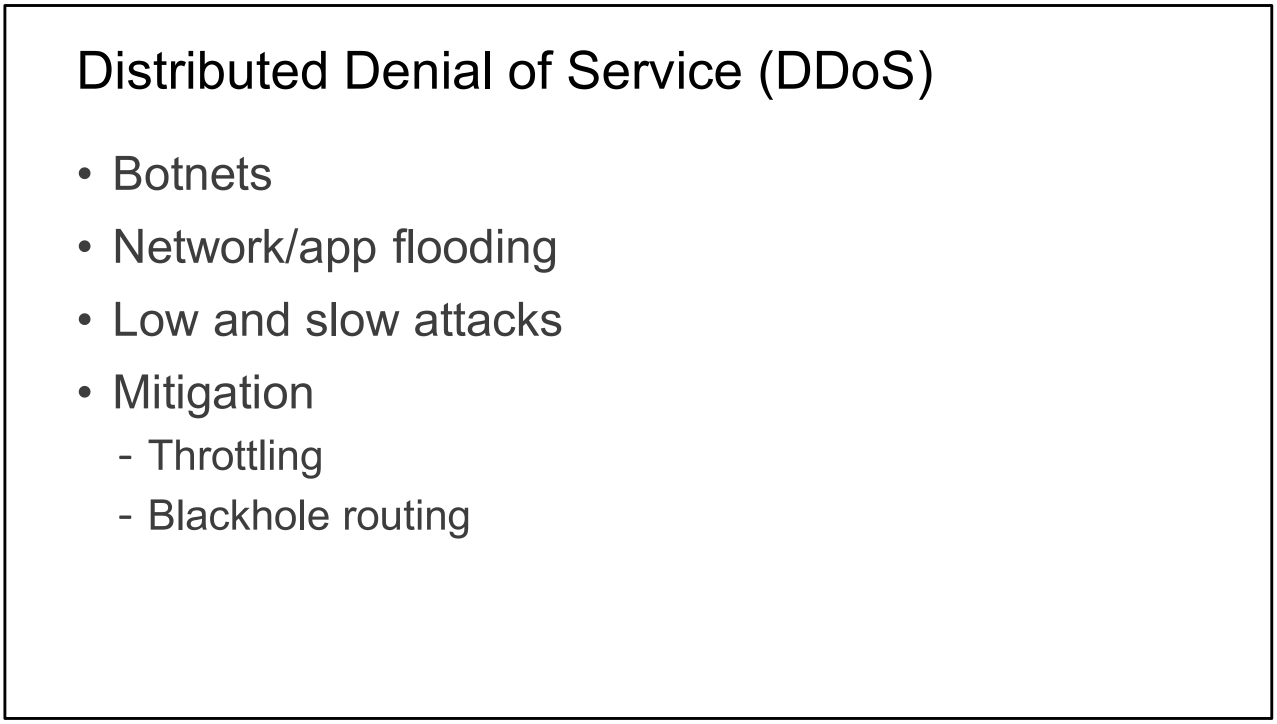
Episode title: **Common Attacks and Mitigations**

Objective:

1.3 Given a scenario, analyze potential indicators associated with application attacks.

1.4 Given a scenario, analyze potential indicators associated with network attacks.

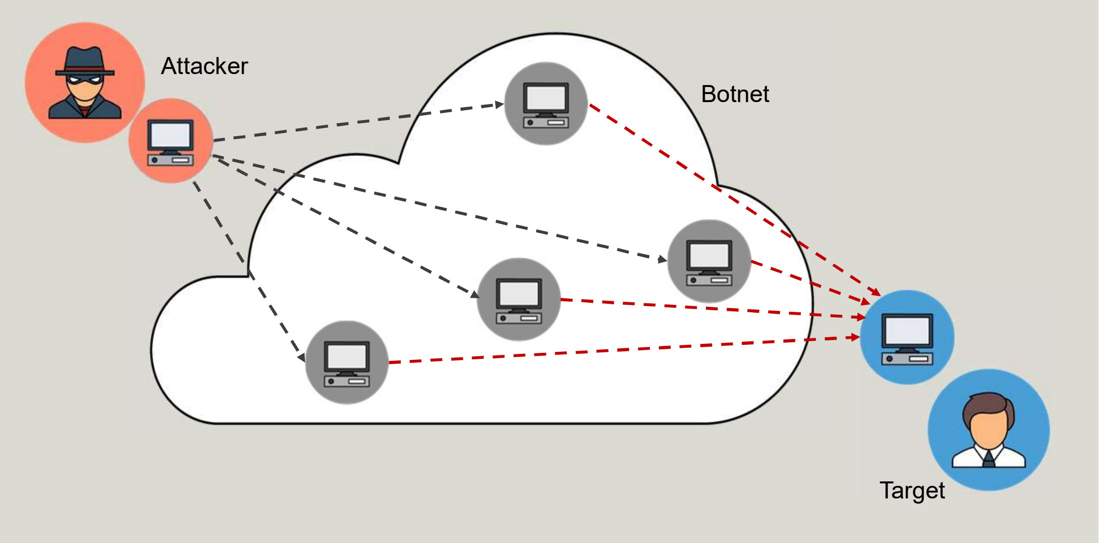
2.2 Summarize virtualization and cloud computing concepts.

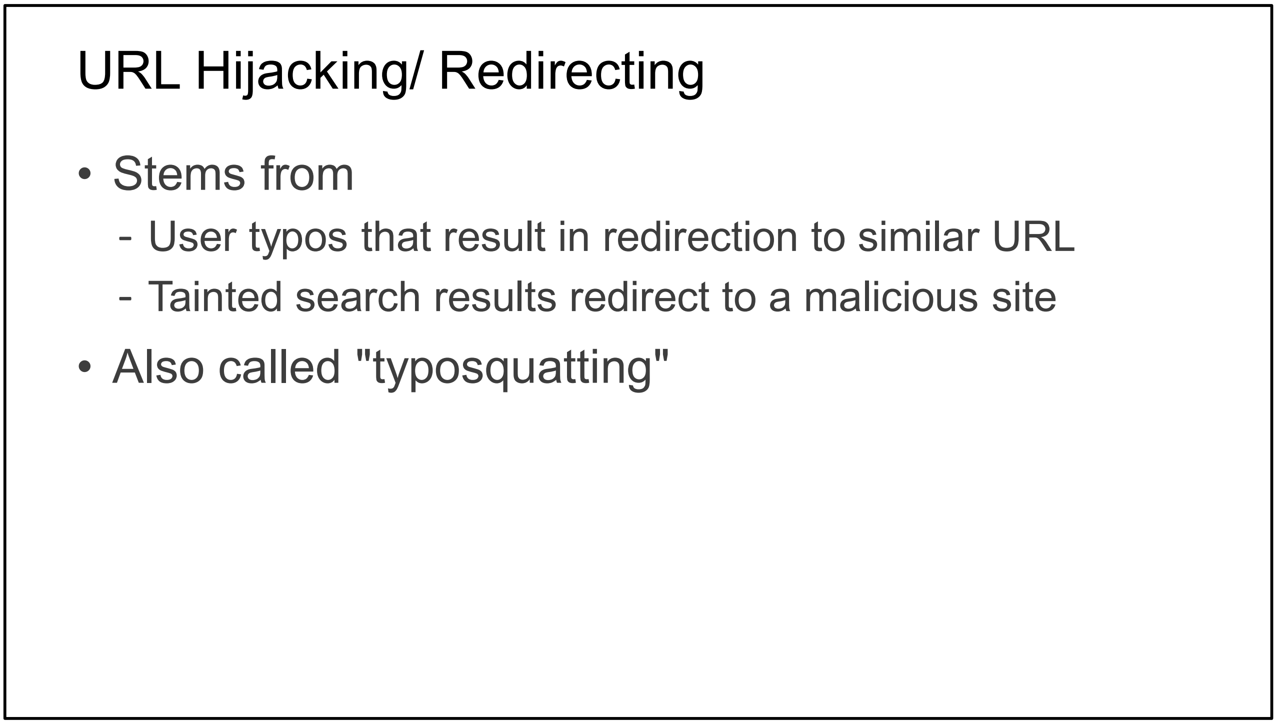


Distributed Denial of Service (DDoS)

- Botnets
- Network/app flooding
- Low and slow attacks
- Mitigation
  - Throttling
  - Blackhole routing

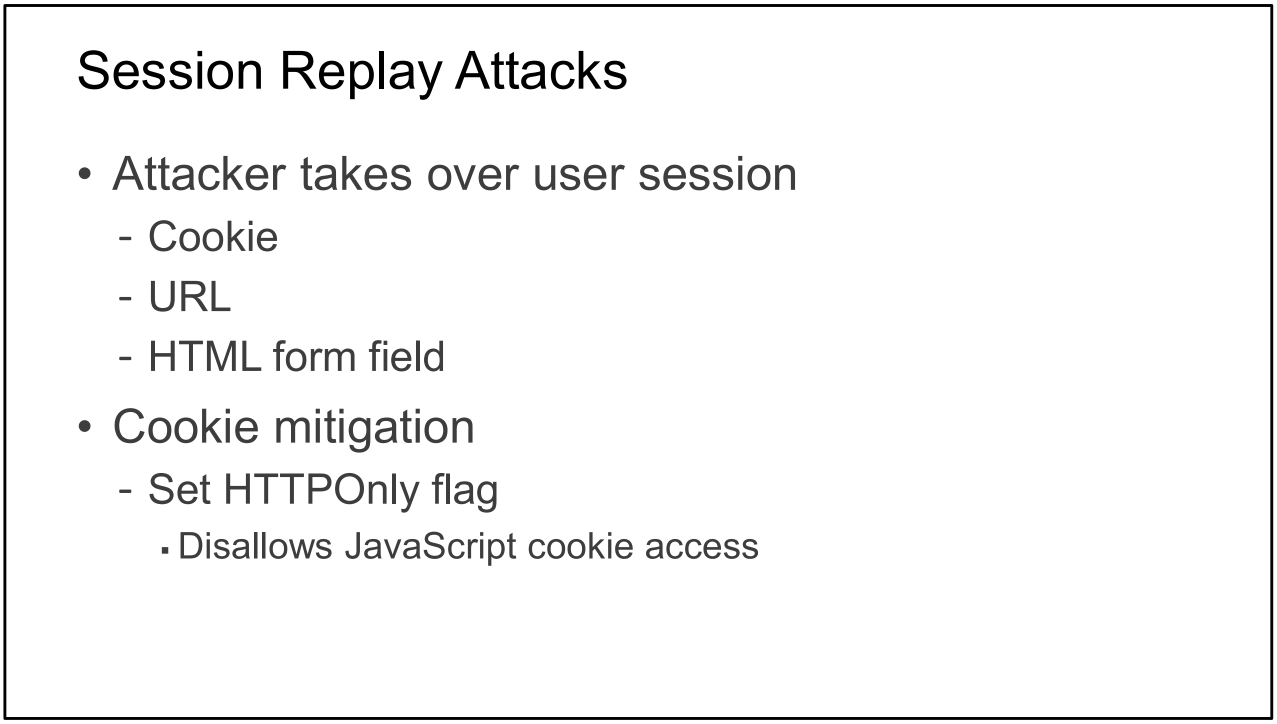
DDoS Attack





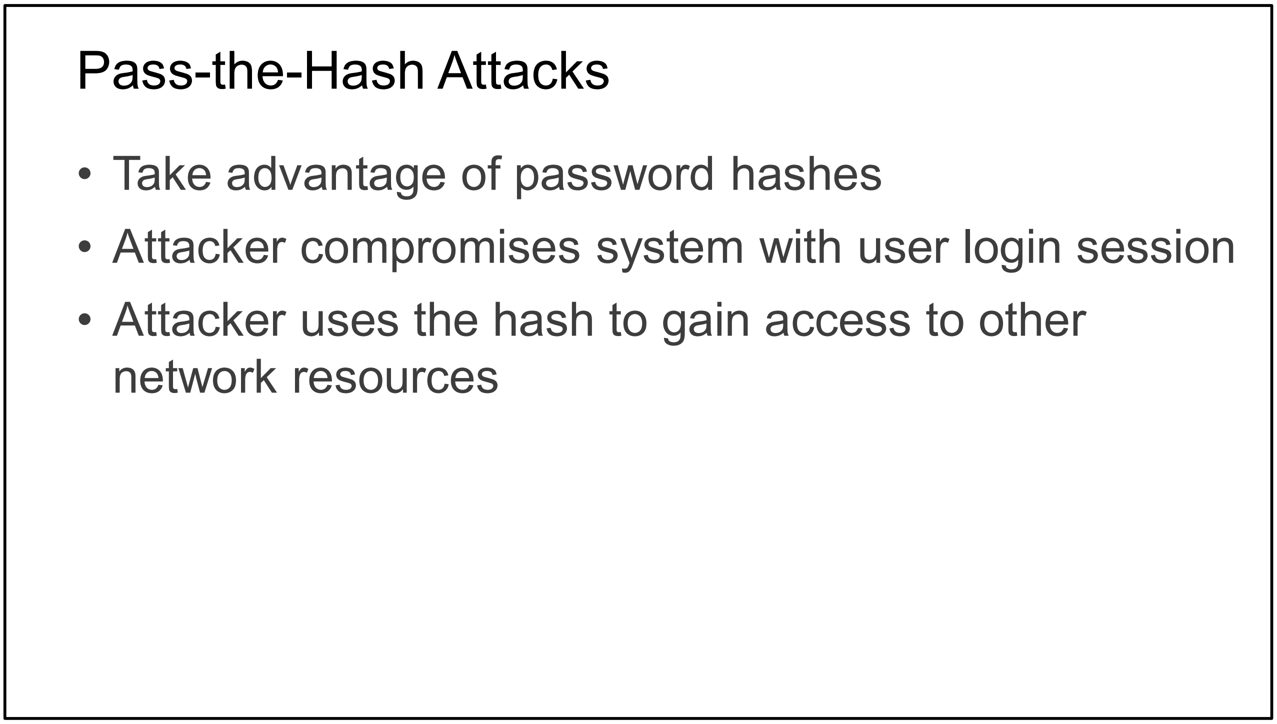
URL Hijacking/ Redirecting

- Stems from
  - User typos that result in redirection to similar URL
  - Tainted search results redirect to a malicious site
- Also called "typosquatting"



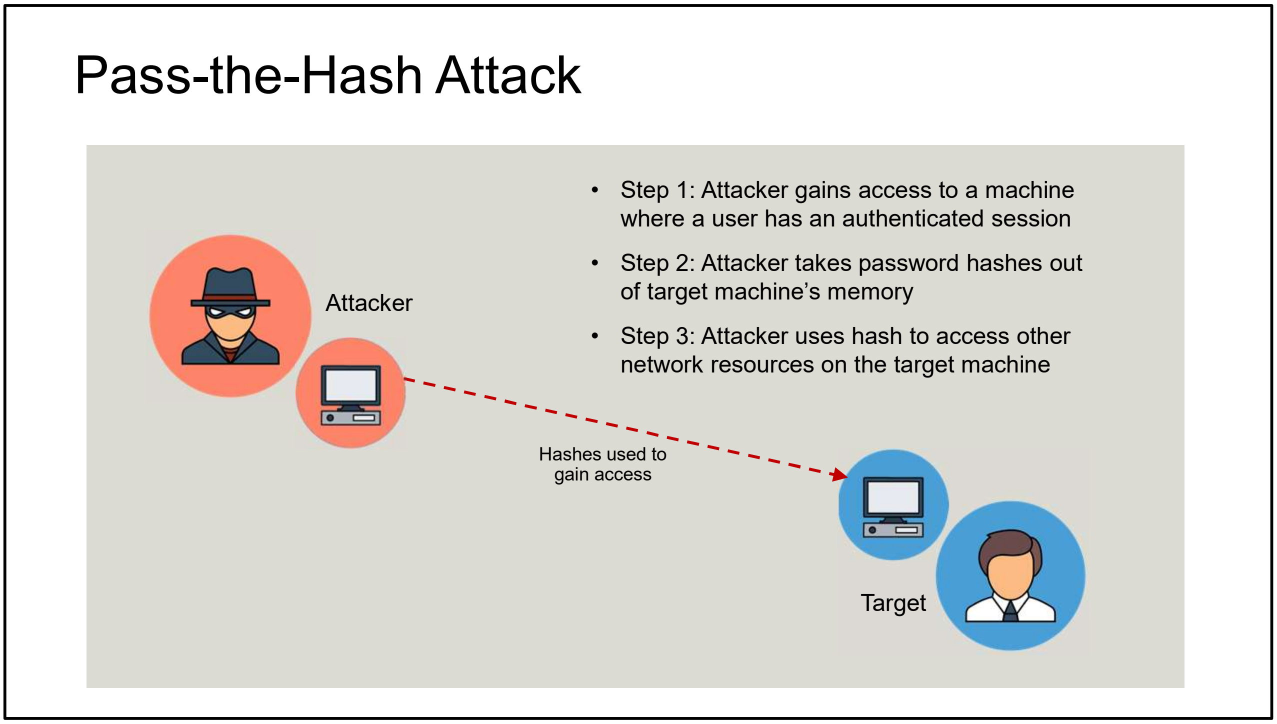
Session Replay Attacks

- Attacker takes over user session
  - Cookie
  - URL
  - HTML form field
- Cookie mitigation
  - Set HTTPOnly flag
    - Disallows JavaScript cookie access



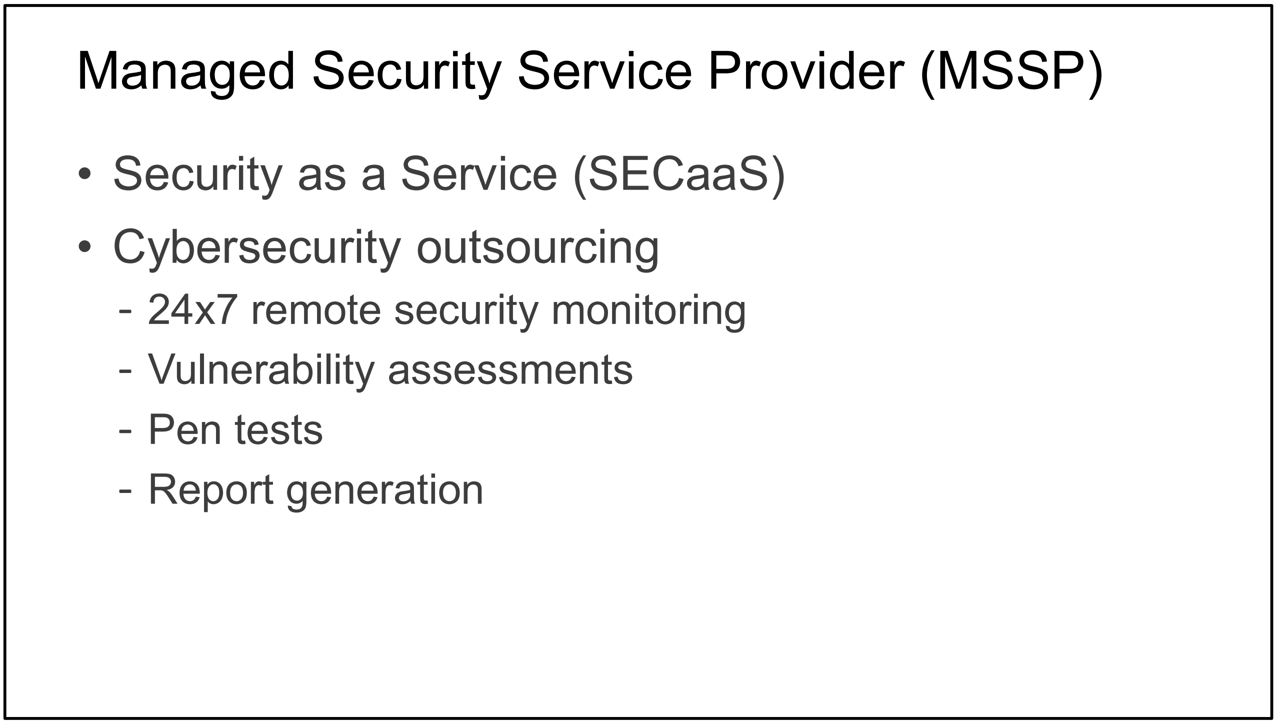
Pass-the-Hash Attacks

- Take advantage of password hashes
- Attacker compromises system with user login session
- Attacker uses the hash to gain access to other network resources



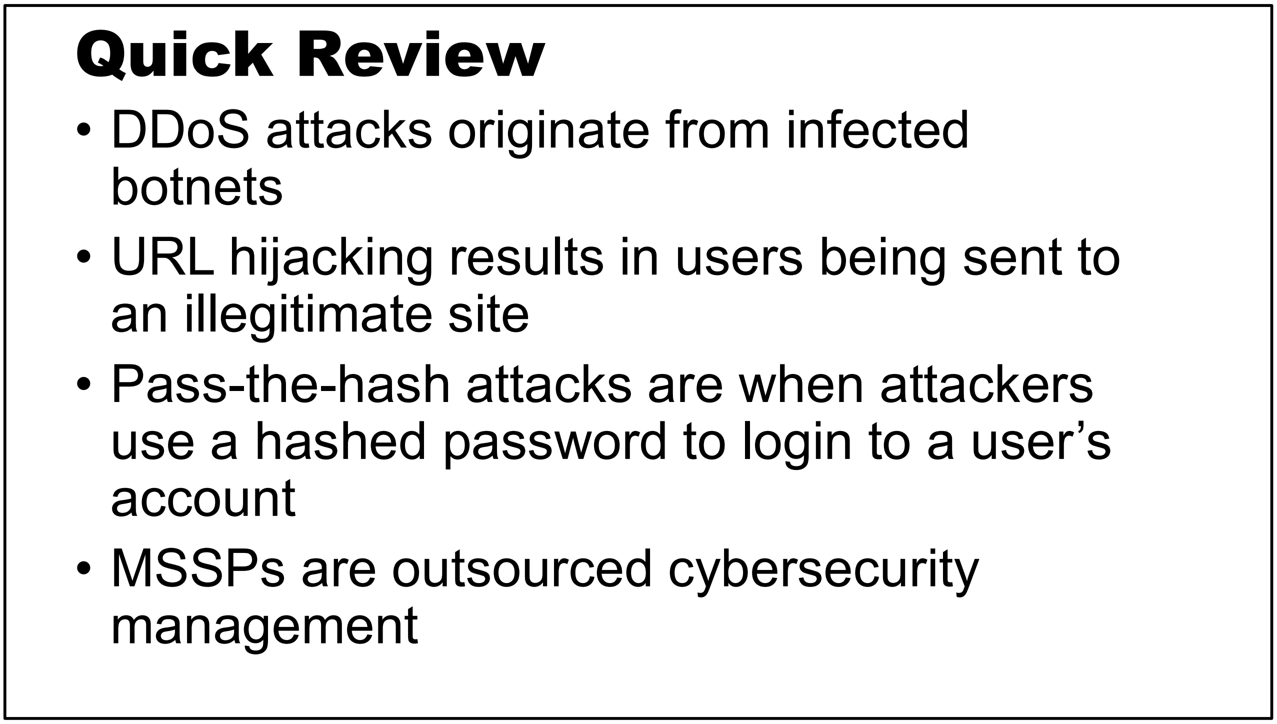
Pass-the-Hash Attack

- Step 1: Attacker gains access to a machine where a user has an authenticated session
- Step 2: Attacker takes password hashes out of target machine's memory
- Step 3: Attacker uses hash to access other network resources on the target machine



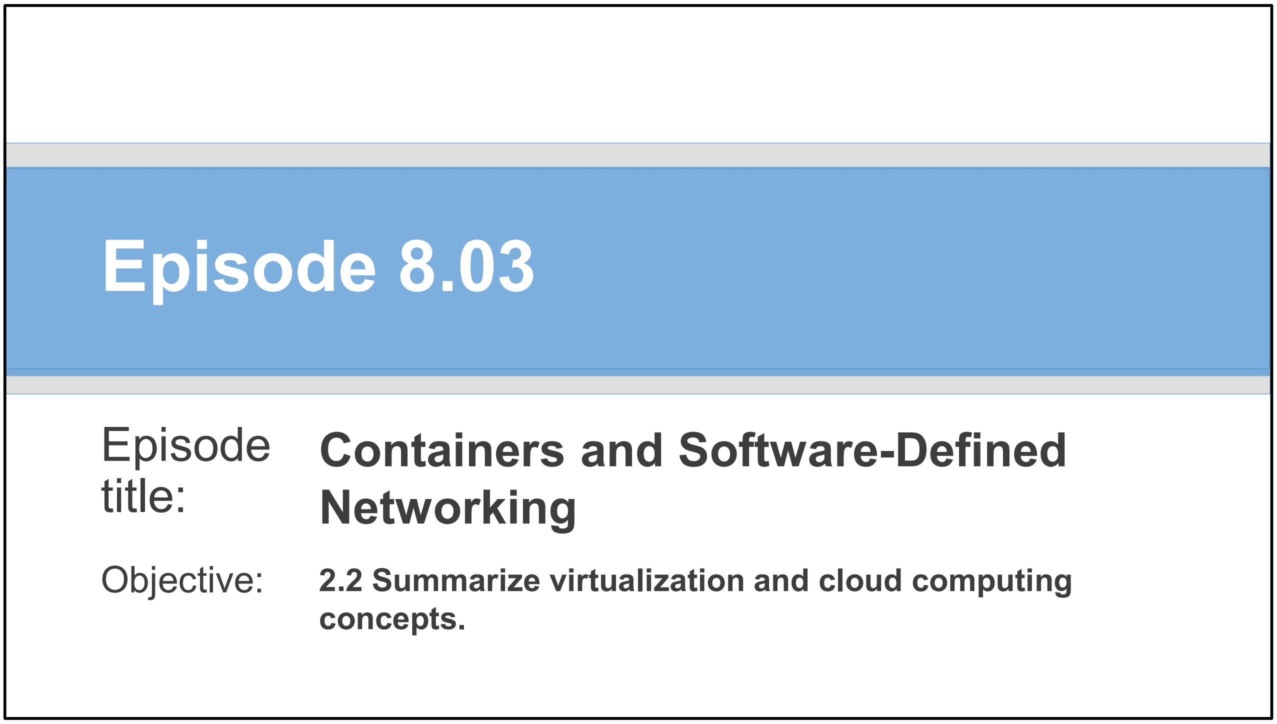
Managed Security Service Provider (MSSP)

- Security as a Service (SECaaS)
- Cybersecurity outsourcing
  - 24x7 remote security monitoring
  - Vulnerability assessments
  - Pen tests
  - Report generation



Quick Review

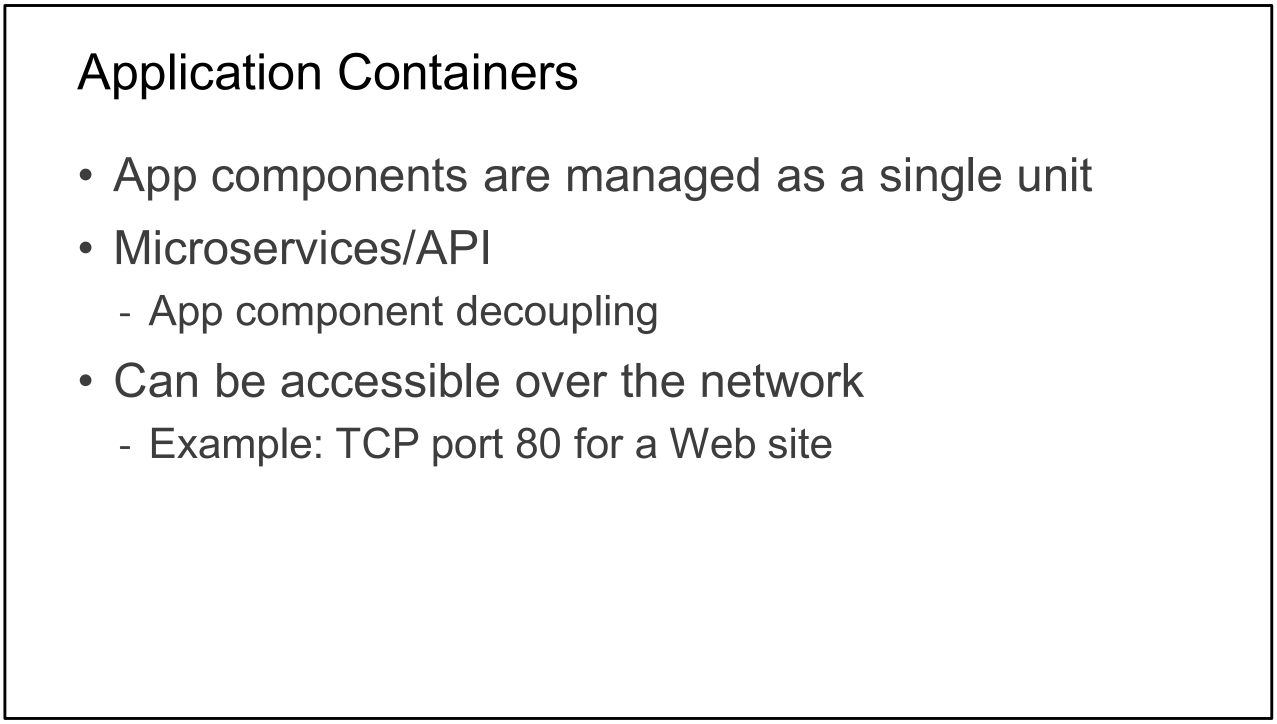
- DDoS attacks originate from infected botnets
- URL hijacking results in users being sent to an illegitimate site
- Pass-the-hash attacks are when attackers use a hashed password to login to a user's account
- MSSPs are outsourced cybersecurity management



Episode 8.03

Episode title: **Containers and Software-Defined Networking**

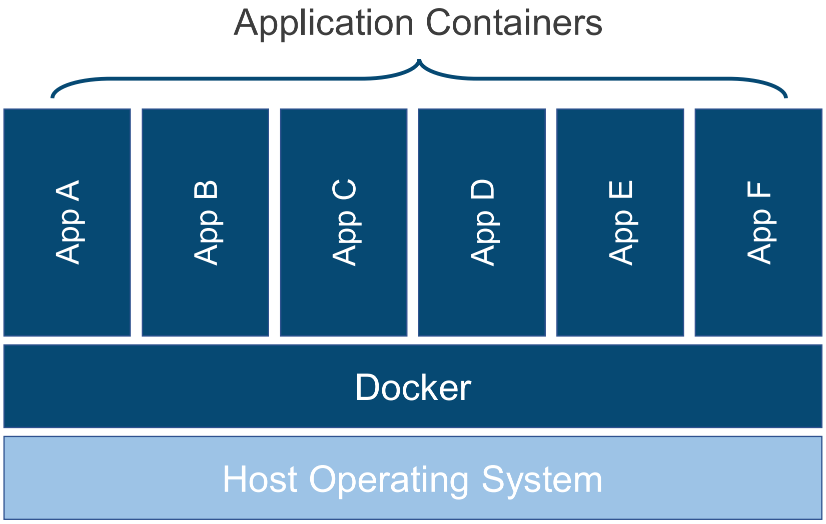
Objective: **2.2 Summarize virtualization and cloud computing concepts.**



Application Containers

- App components are managed as a single unit
- Microservices/API
  - App component decoupling
- Can be accessible over the network
  - Example: TCP port 80 for a Web site

Application Containers



Application Containers

App A

App B

App C

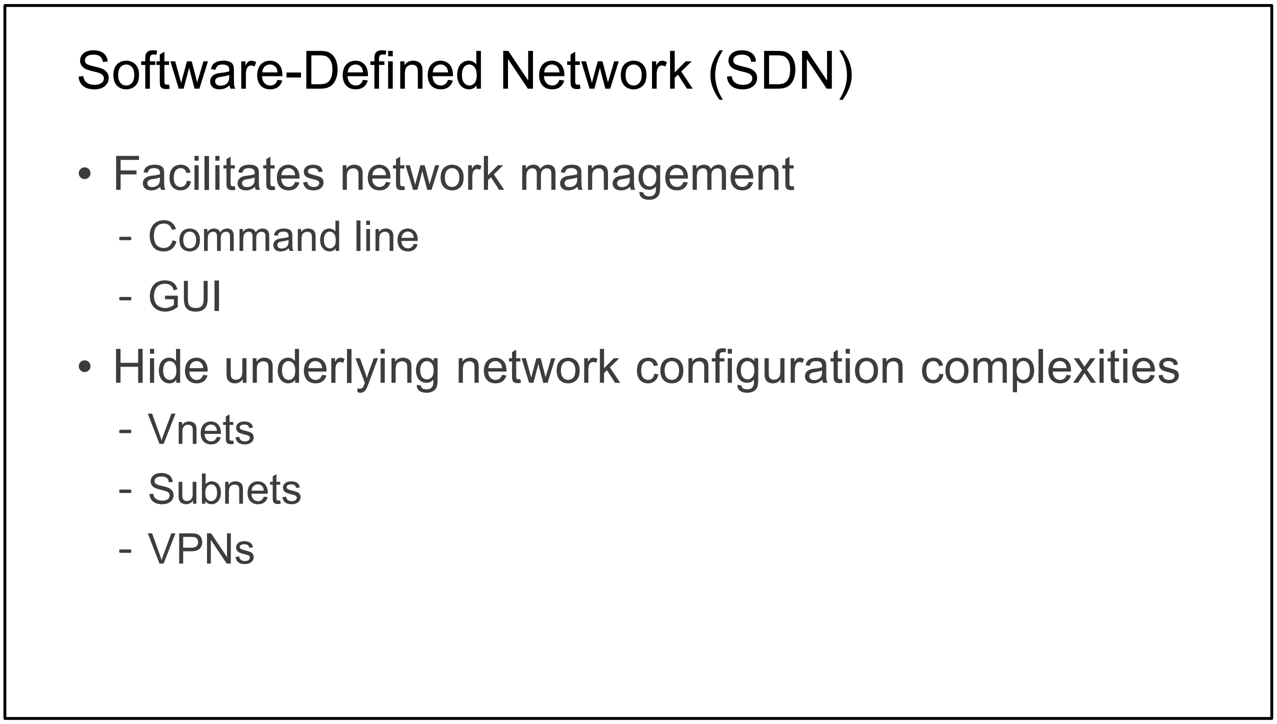
App D

App E

App F

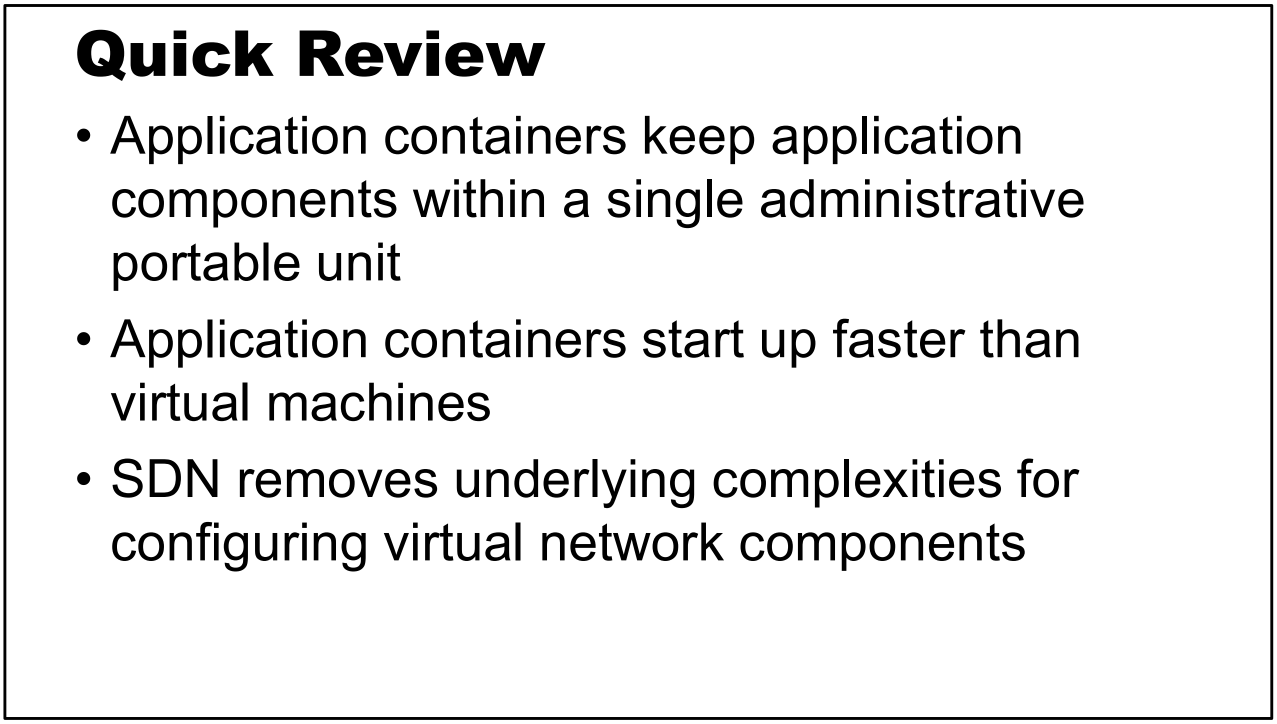
Docker

Host Operating System



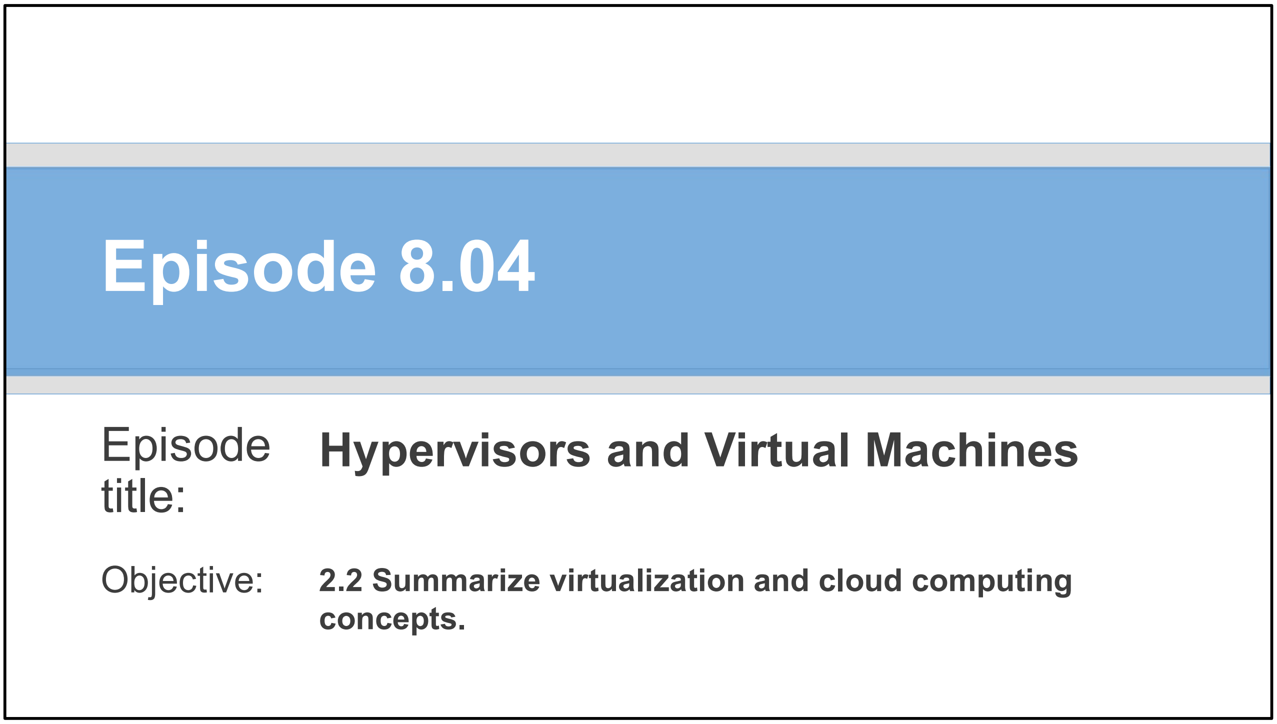
Software-Defined Network (SDN)

- Facilitates network management
  - Command line
  - GUI
- Hide underlying network configuration complexities
  - Vnets
  - Subnets
  - VPNs



Quick Review

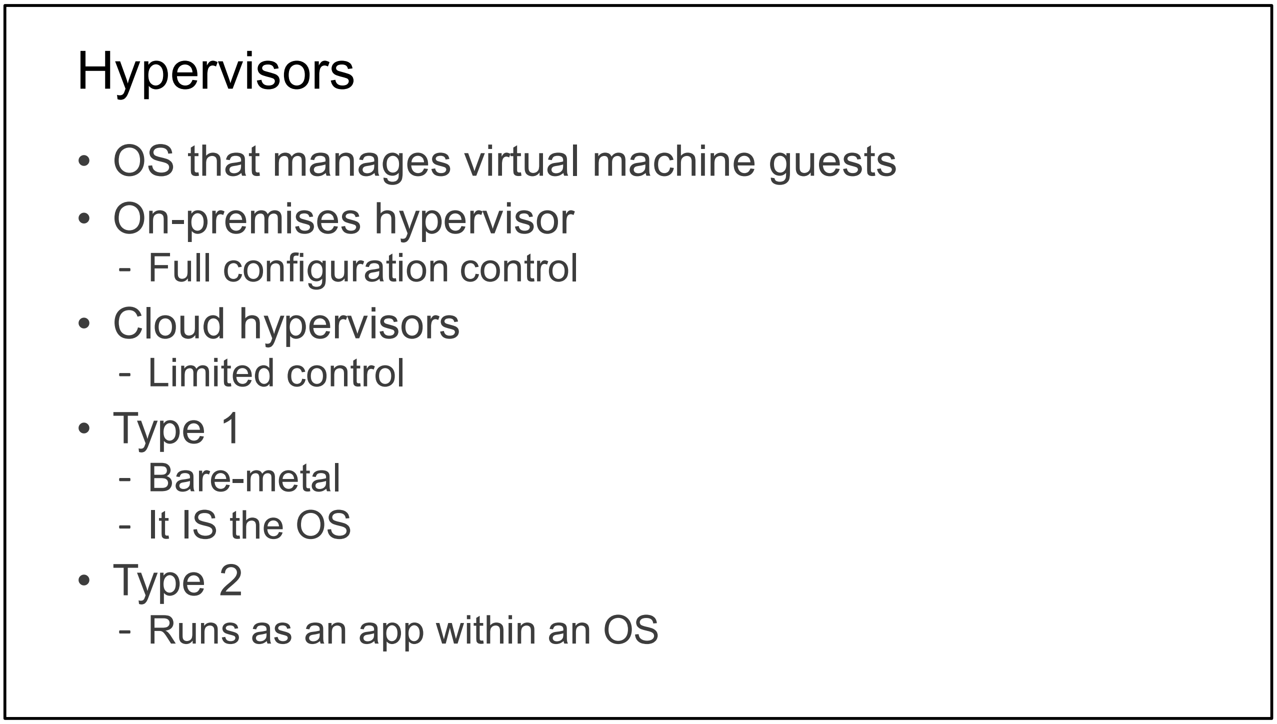
- Application containers keep application components within a single administrative portable unit
- Application containers start up faster than virtual machines
- SDN removes underlying complexities for configuring virtual network components



Episode 8.04

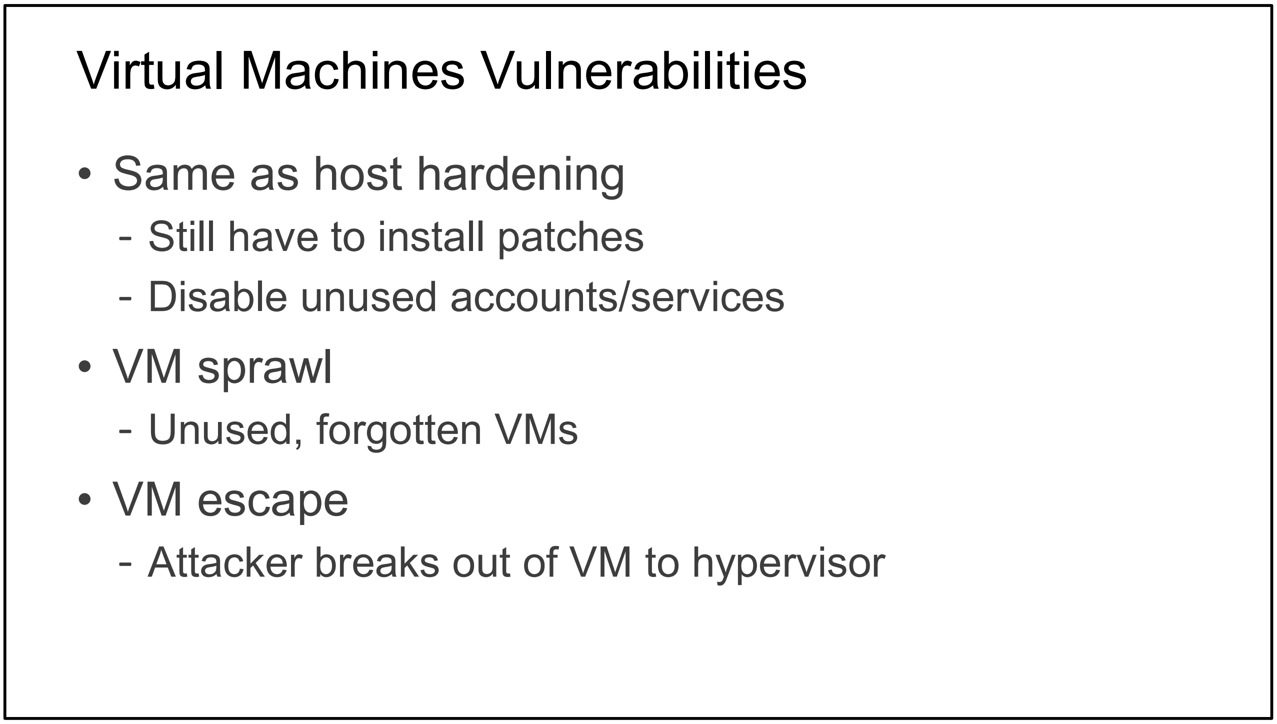
Episode title: **Hypervisors and Virtual Machines**

Objective: **2.2 Summarize virtualization and cloud computing concepts.**



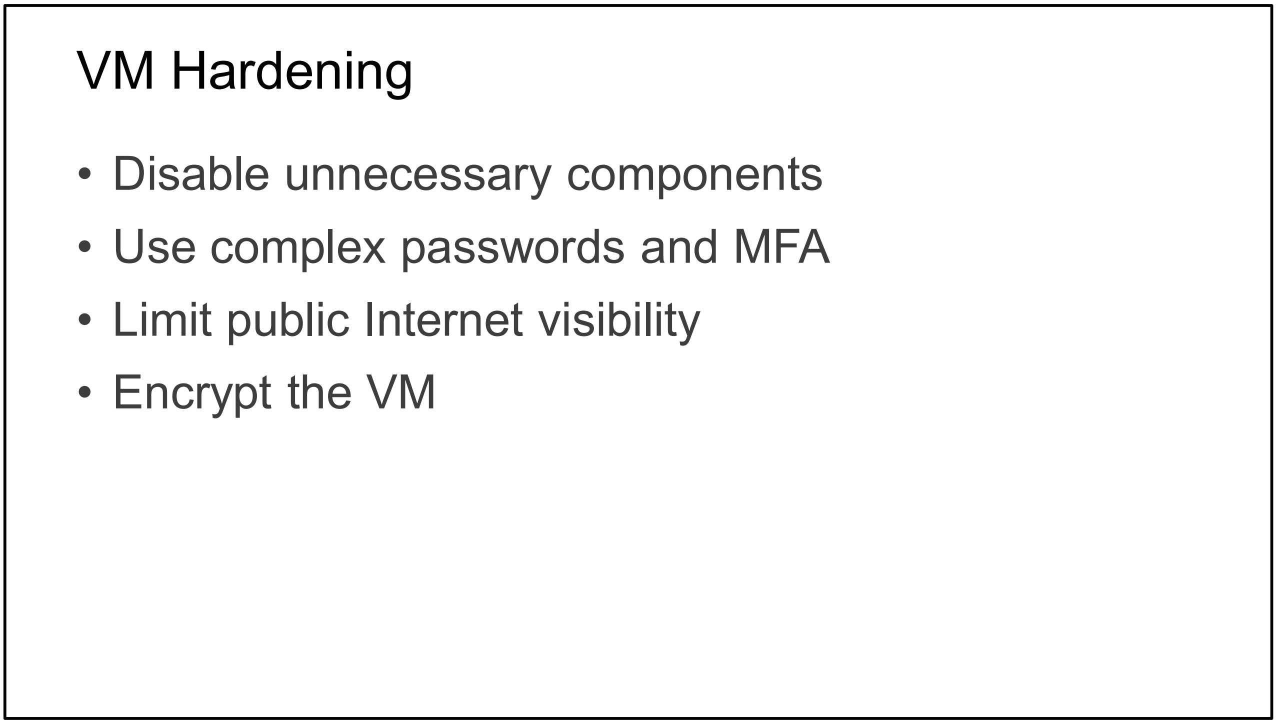
Hypervisors

- OS that manages virtual machine guests
- On-premises hypervisor
  - Full configuration control
- Cloud hypervisors
  - Limited control
- Type 1
  - Bare-metal
  - It IS the OS
- Type 2
  - Runs as an app within an OS



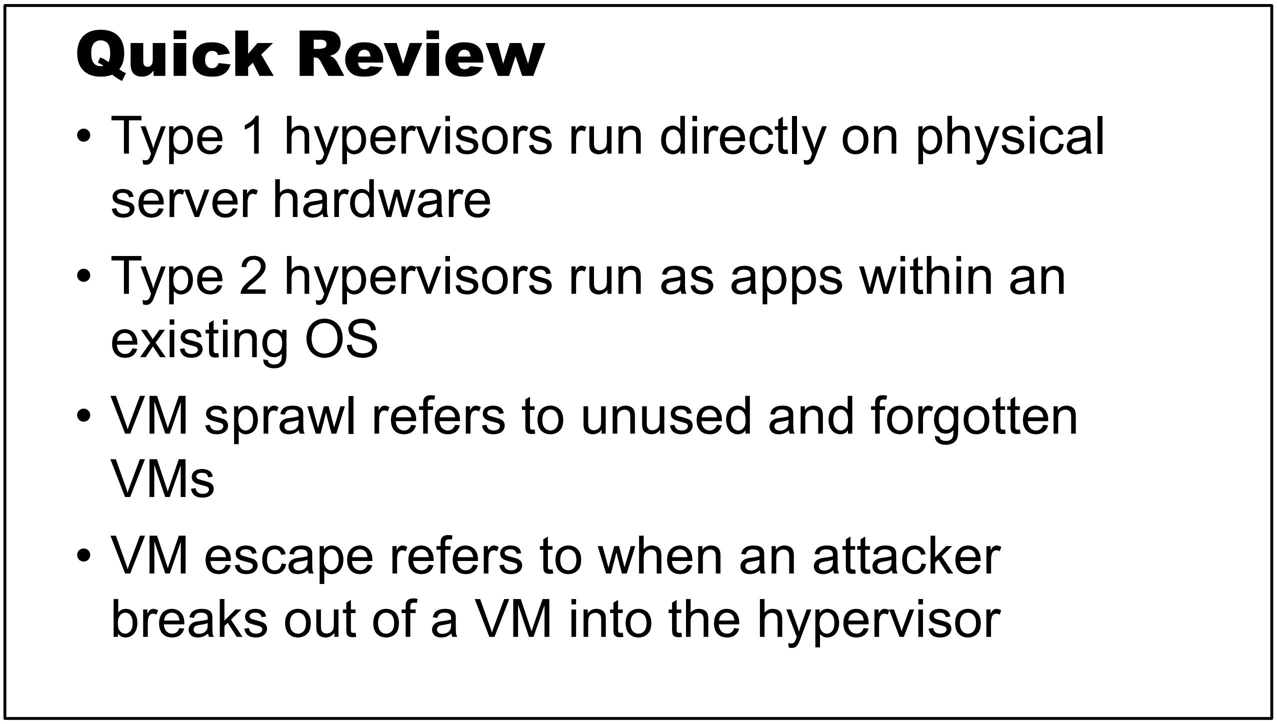
Virtual Machines Vulnerabilities

- Same as host hardening
  - Still have to install patches
  - Disable unused accounts/services
- VM sprawl
  - Unused, forgotten VMs
- VM escape
  - Attacker breaks out of VM to hypervisor



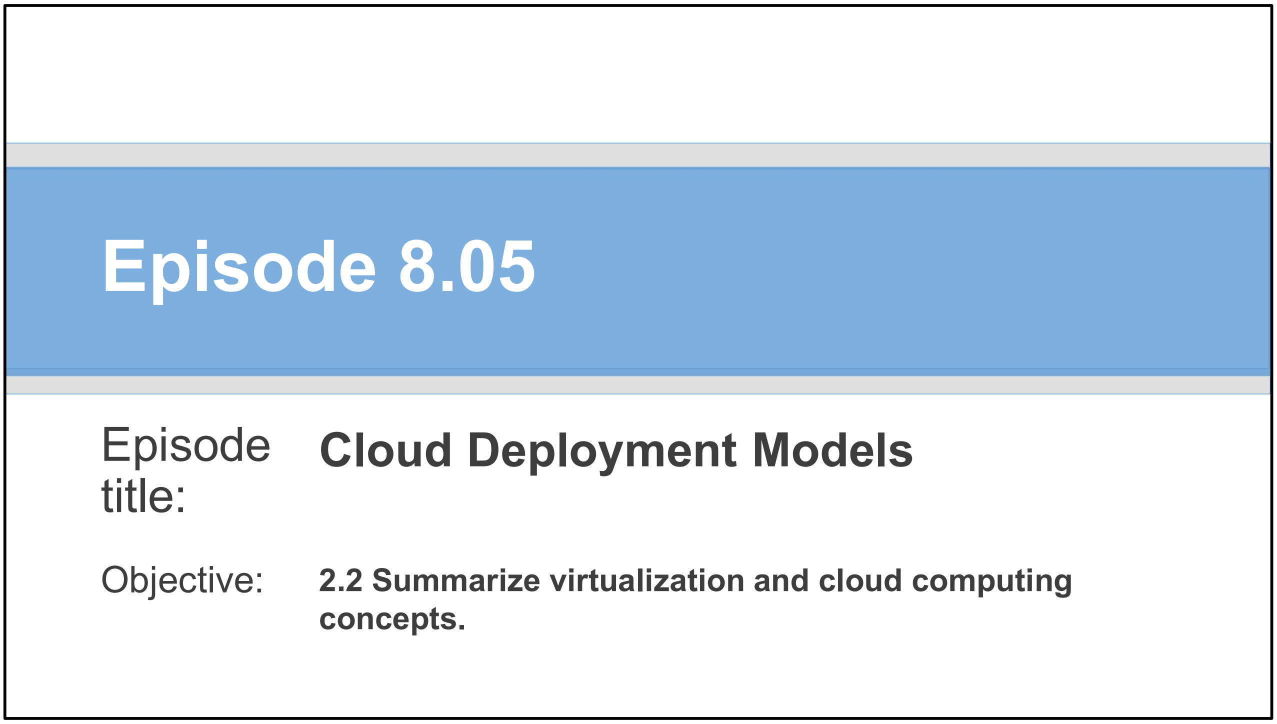
VM Hardening

- Disable unnecessary components
- Use complex passwords and MFA
- Limit public Internet visibility
- Encrypt the VM



Quick Review

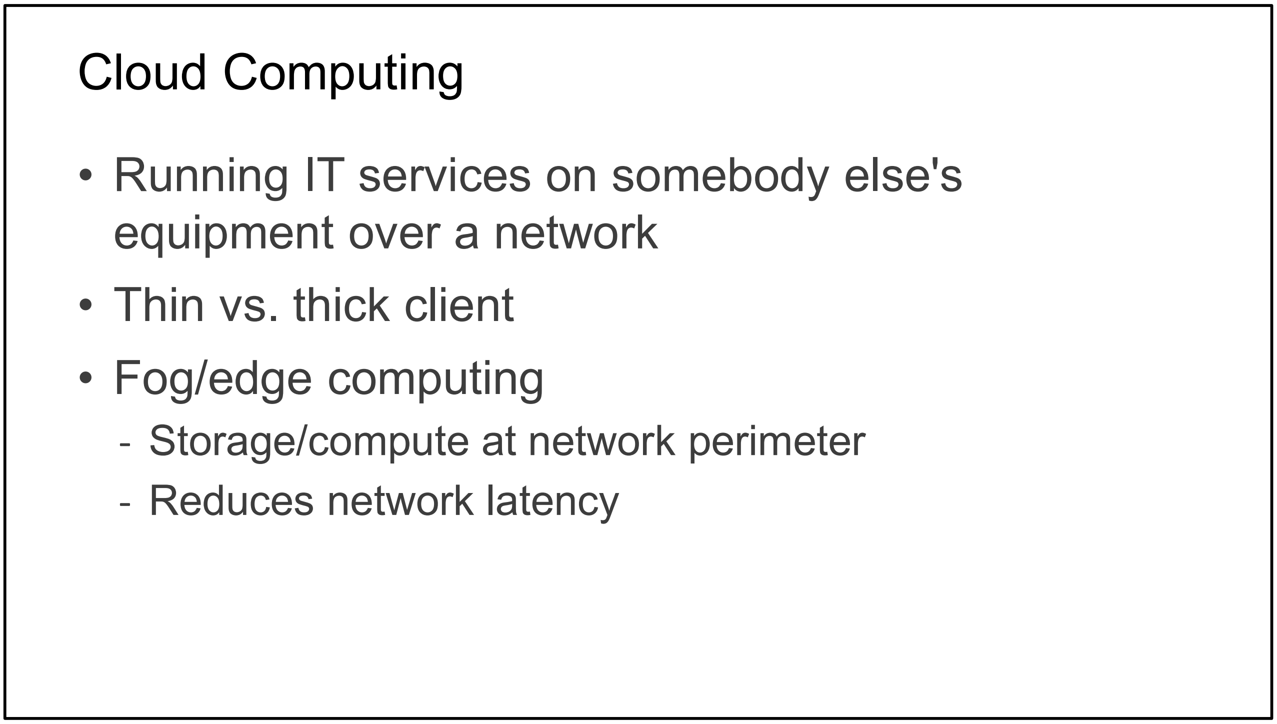
- Type 1 hypervisors run directly on physical server hardware
- Type 2 hypervisors run as apps within an existing OS
- VM sprawl refers to unused and forgotten VMs
- VM escape refers to when an attacker breaks out of a VM into the hypervisor



Episode 8.05

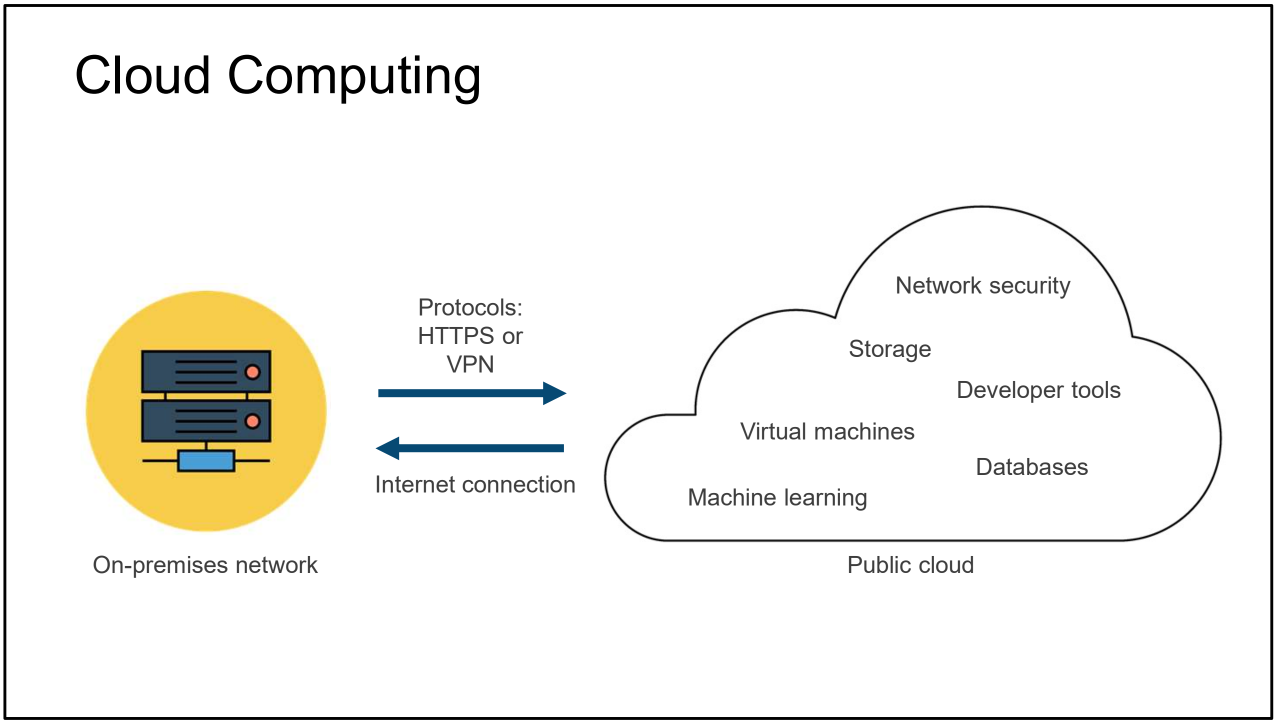
Episode title: **Cloud Deployment Models**

Objective: **2.2 Summarize virtualization and cloud computing concepts.**



Cloud Computing

- Running IT services on somebody else's equipment over a network
- Thin vs. thick client
- Fog/edge computing
  - Storage/compute at network perimeter
  - Reduces network latency



Cloud Computing

Protocols: HTTPS or VPN

Internet connection

On-premises network

Network security

Storage

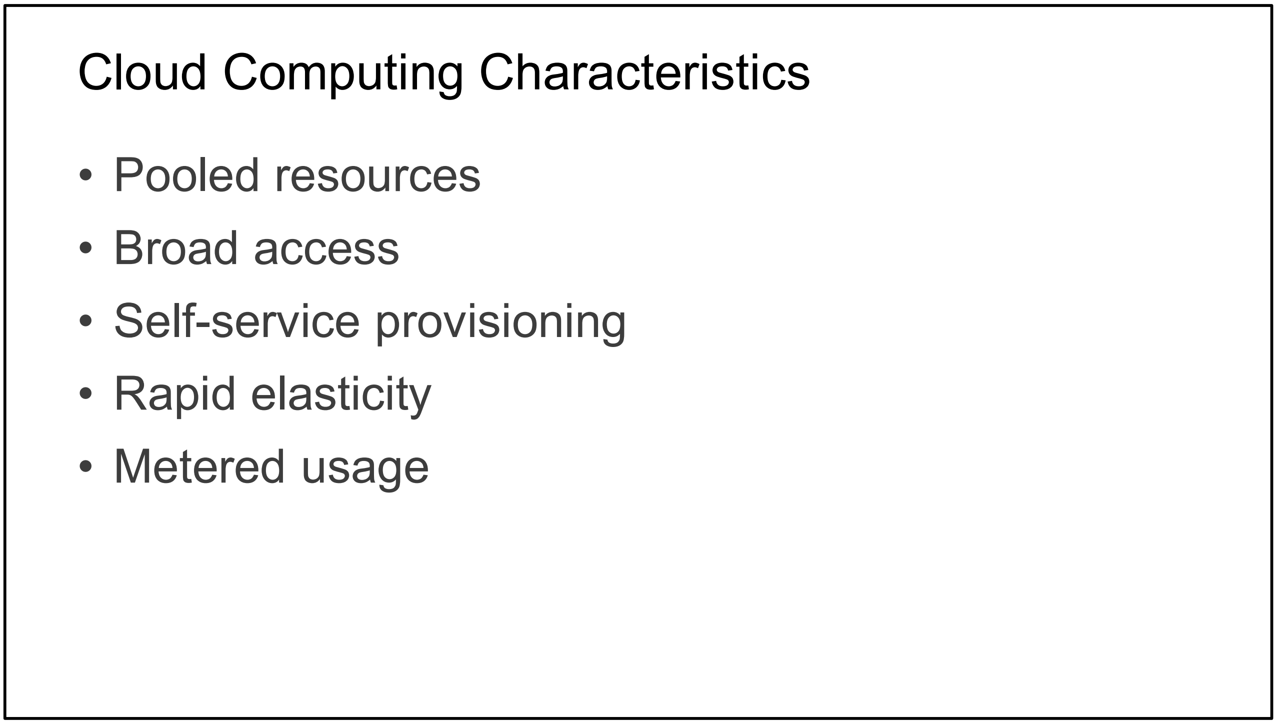
Developer tools

Virtual machines

Databases

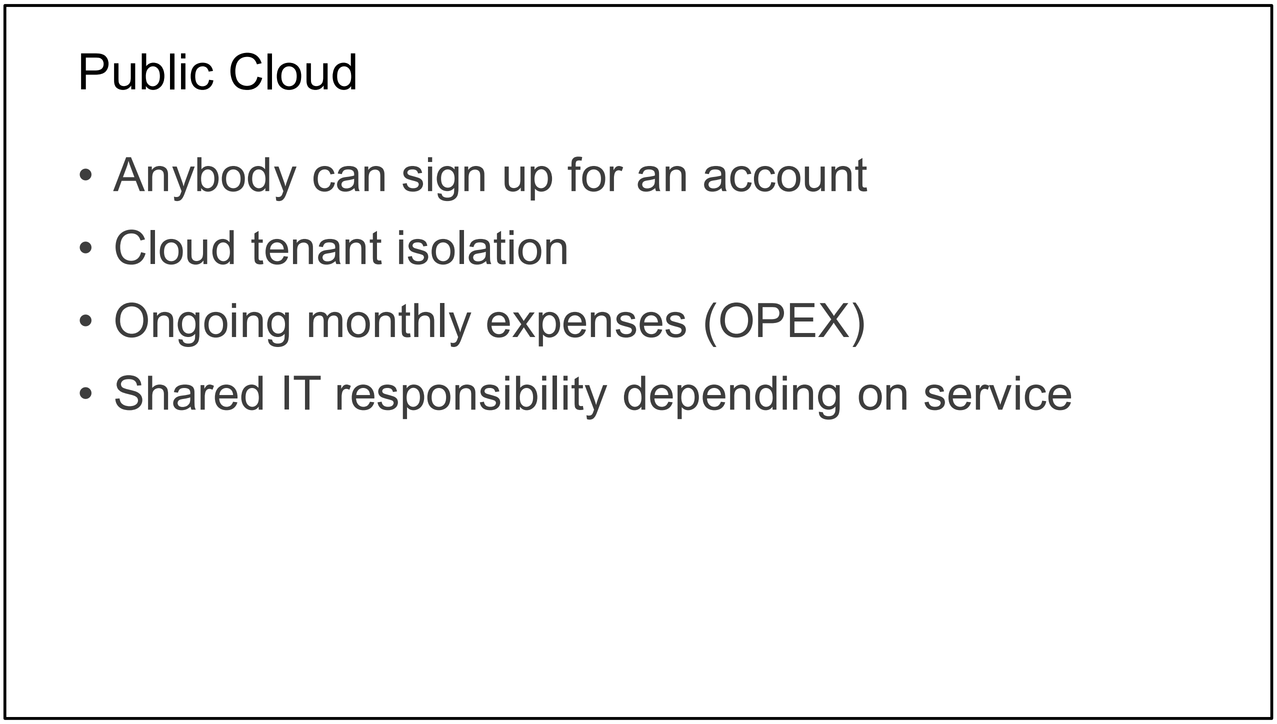
Machine learning

Public cloud



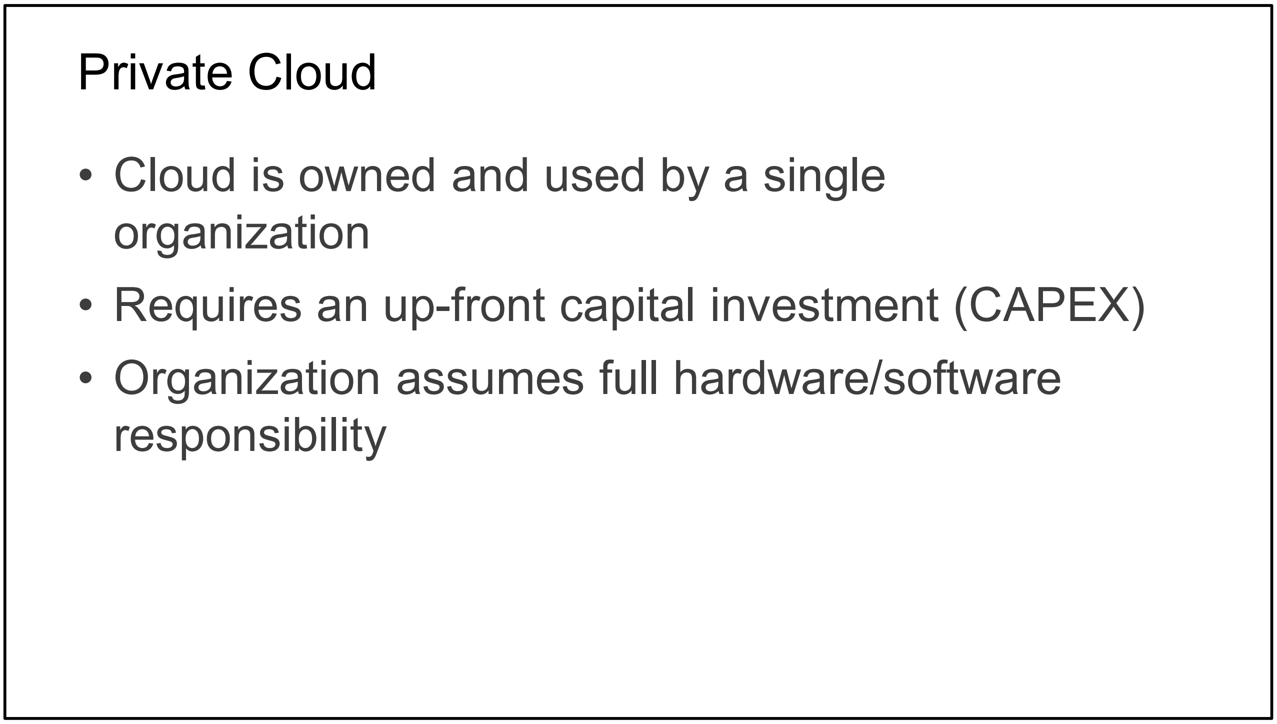
Cloud Computing Characteristics

- Pooled resources
- Broad access
- Self-service provisioning
- Rapid elasticity
- Metered usage



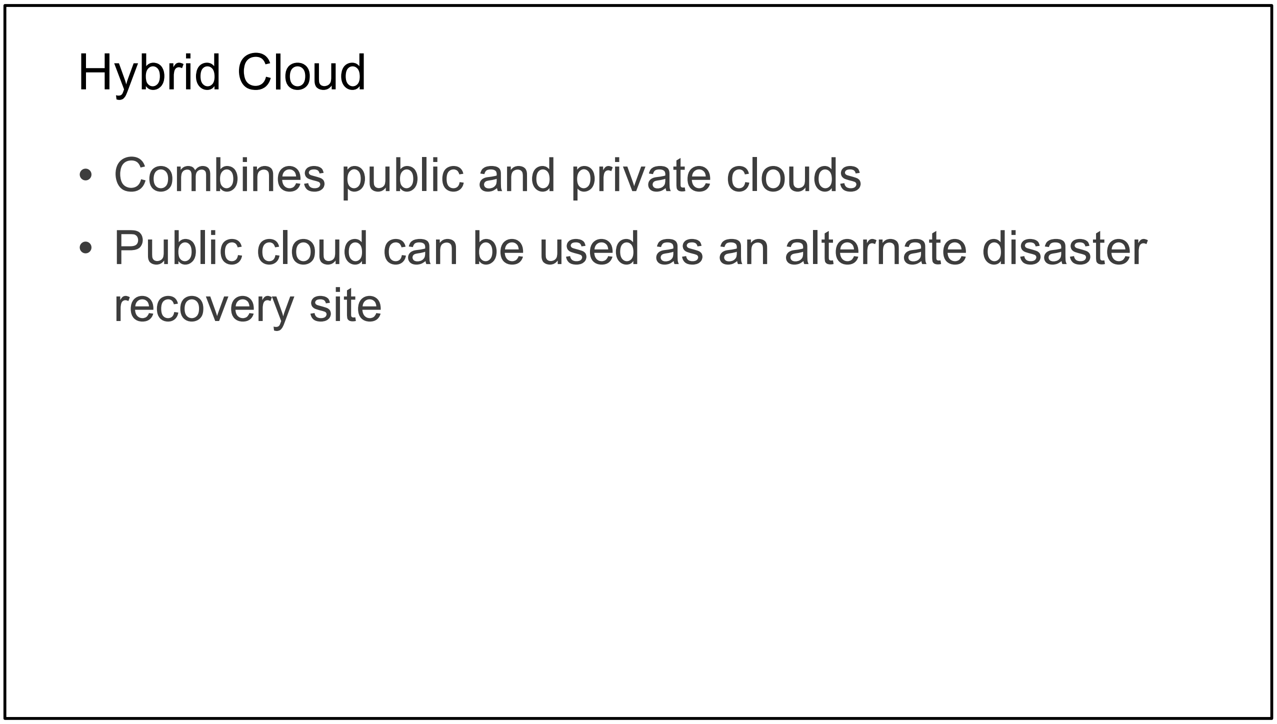
Public Cloud

- Anybody can sign up for an account
- Cloud tenant isolation
- Ongoing monthly expenses (OPEX)
- Shared IT responsibility depending on service



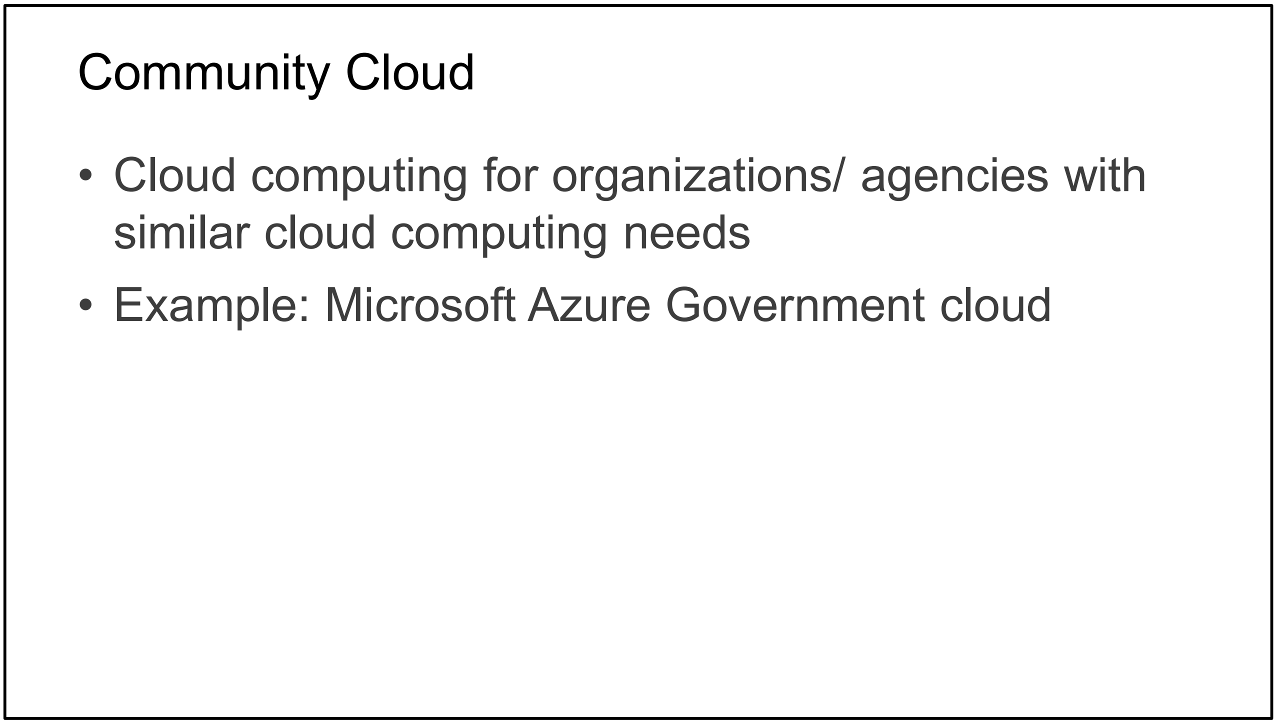
Private Cloud

- Cloud is owned and used by a single organization
- Requires an up-front capital investment (CAPEX)
- Organization assumes full hardware/software responsibility



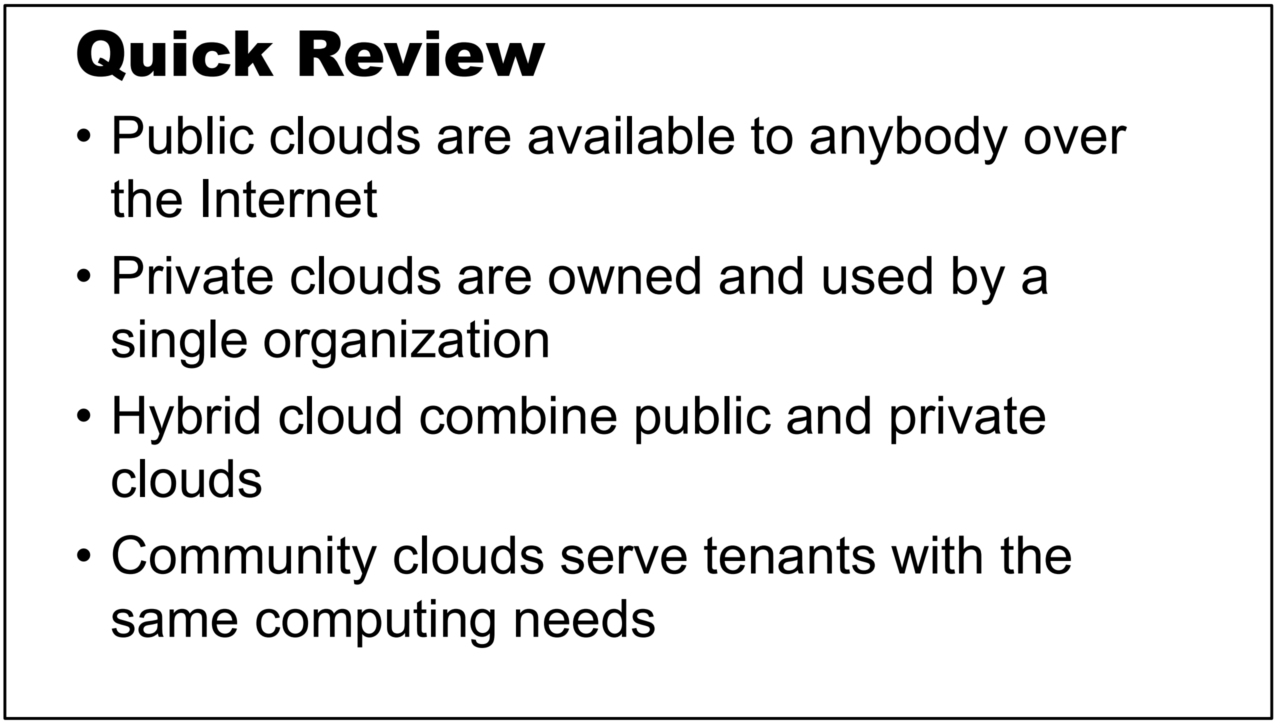
Hybrid Cloud

- Combines public and private clouds
- Public cloud can be used as an alternate disaster recovery site



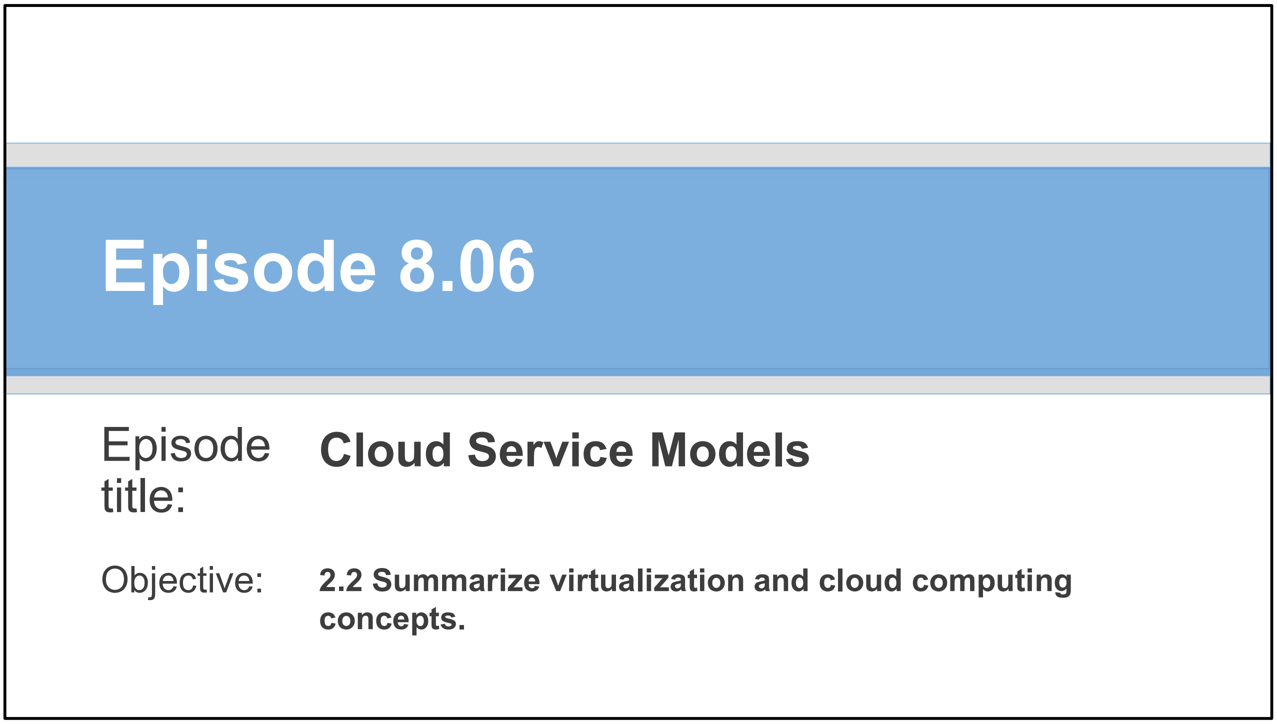
Community Cloud

- Cloud computing for organizations/ agencies with similar cloud computing needs
- Example: Microsoft Azure Government cloud



Quick Review

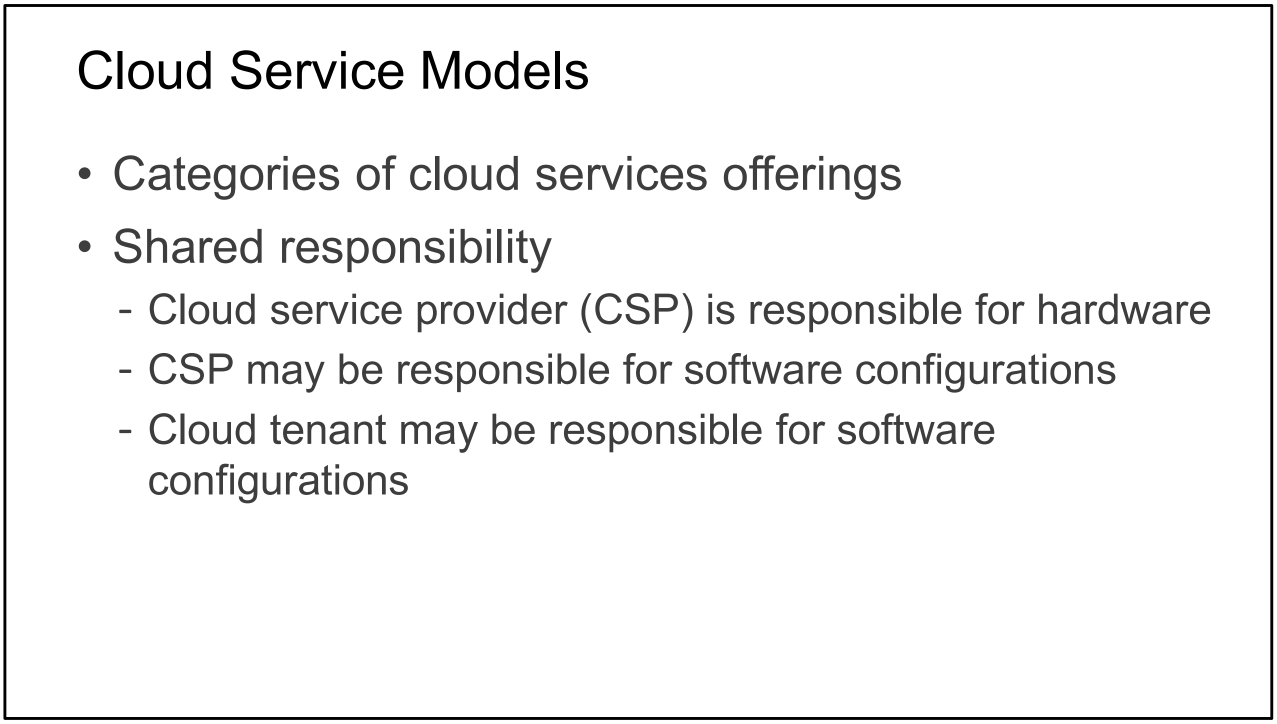
- Public clouds are available to anybody over the Internet
- Private clouds are owned and used by a single organization
- Hybrid cloud combine public and private clouds
- Community clouds serve tenants with the same computing needs



Episode 8.06

Episode title: **Cloud Service Models**

Objective: **2.2 Summarize virtualization and cloud computing concepts.**

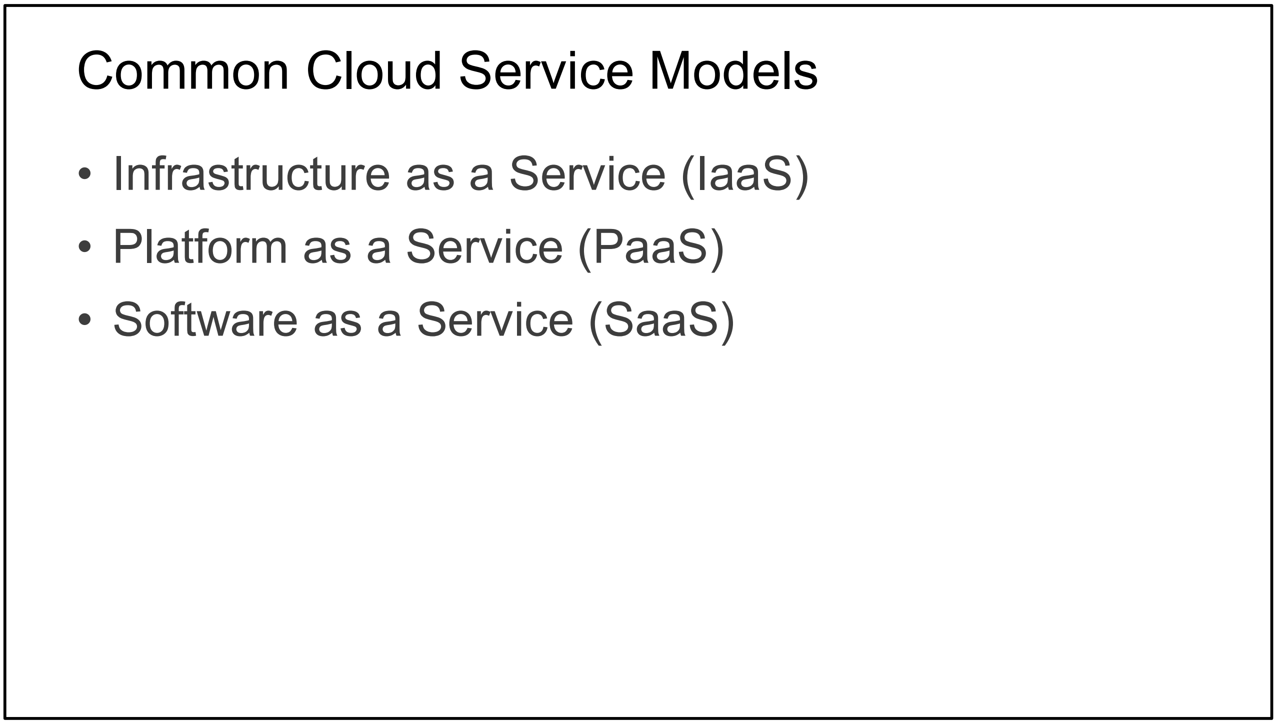


Cloud Service Models

- Categories of cloud services offerings
- Shared responsibility
  - Cloud service provider (CSP) is responsible for hardware
  - CSP may be responsible for software configurations
  - Cloud tenant may be responsible for software configurations

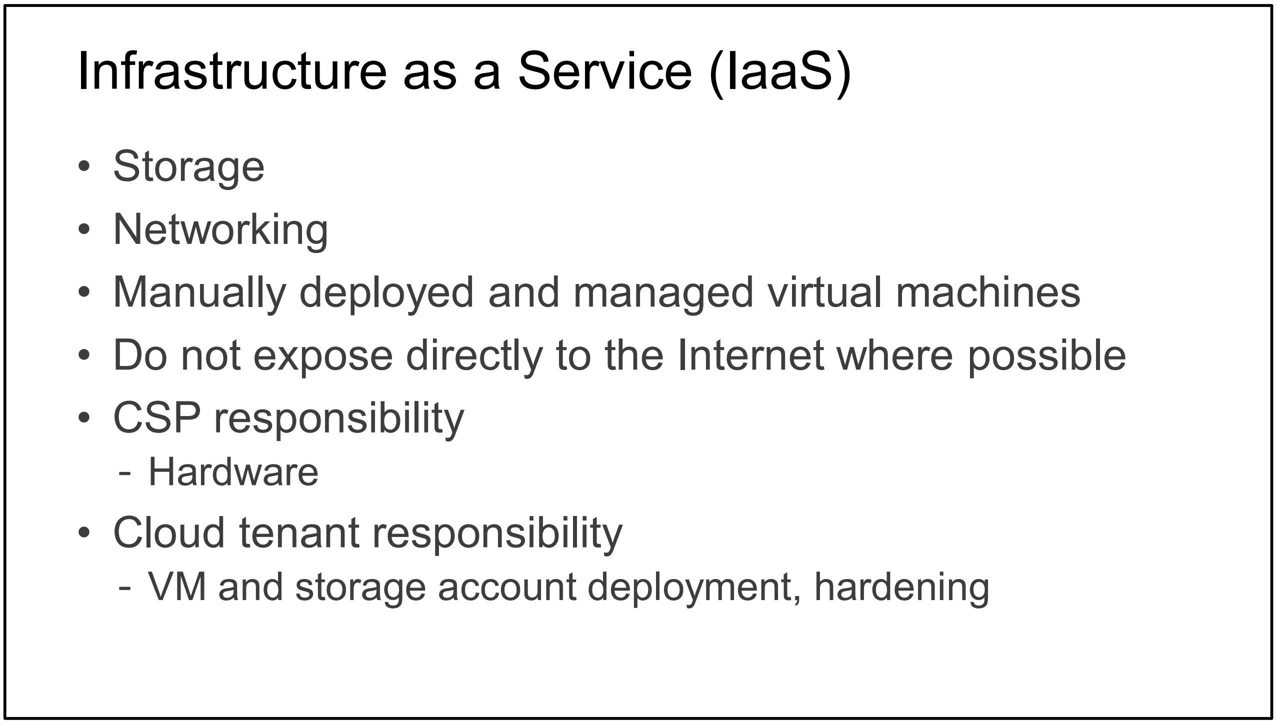
Anything as a Service (XaaS)

- An IT service that is accessible remotely over a network
- IT services run on provider infrastructure
- Adheres to cloud computing characteristics



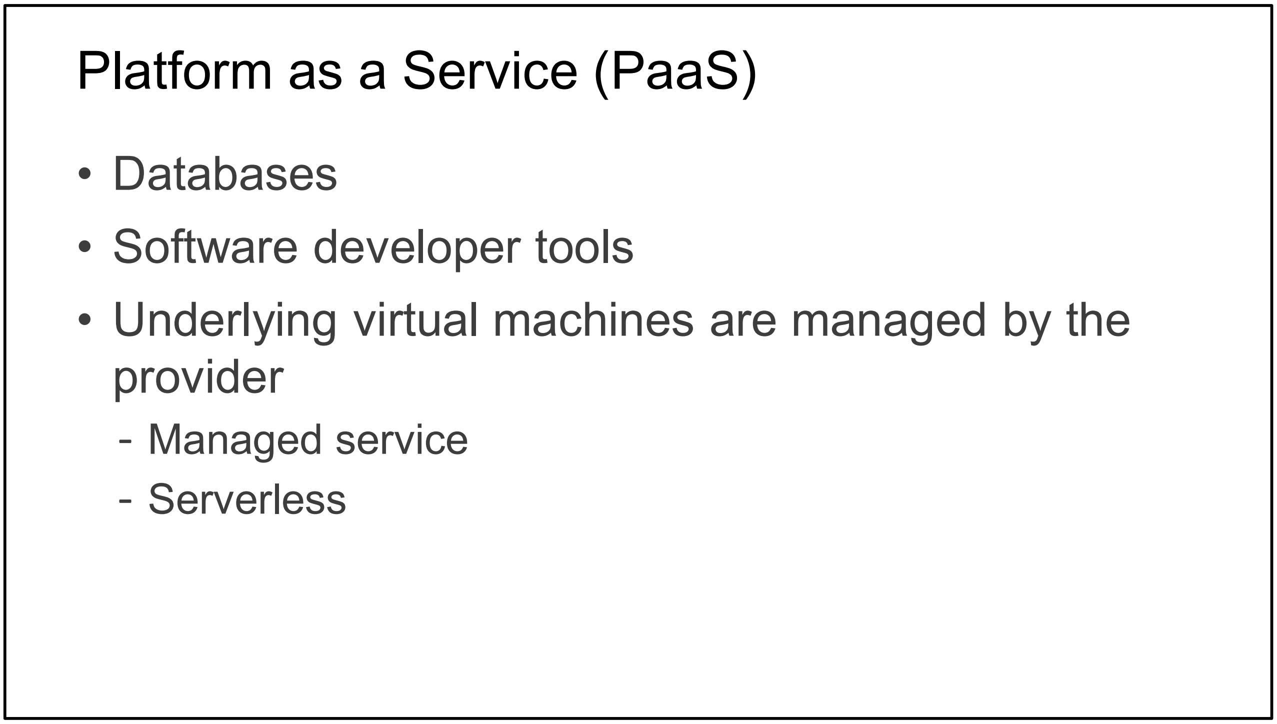
Common Cloud Service Models

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)



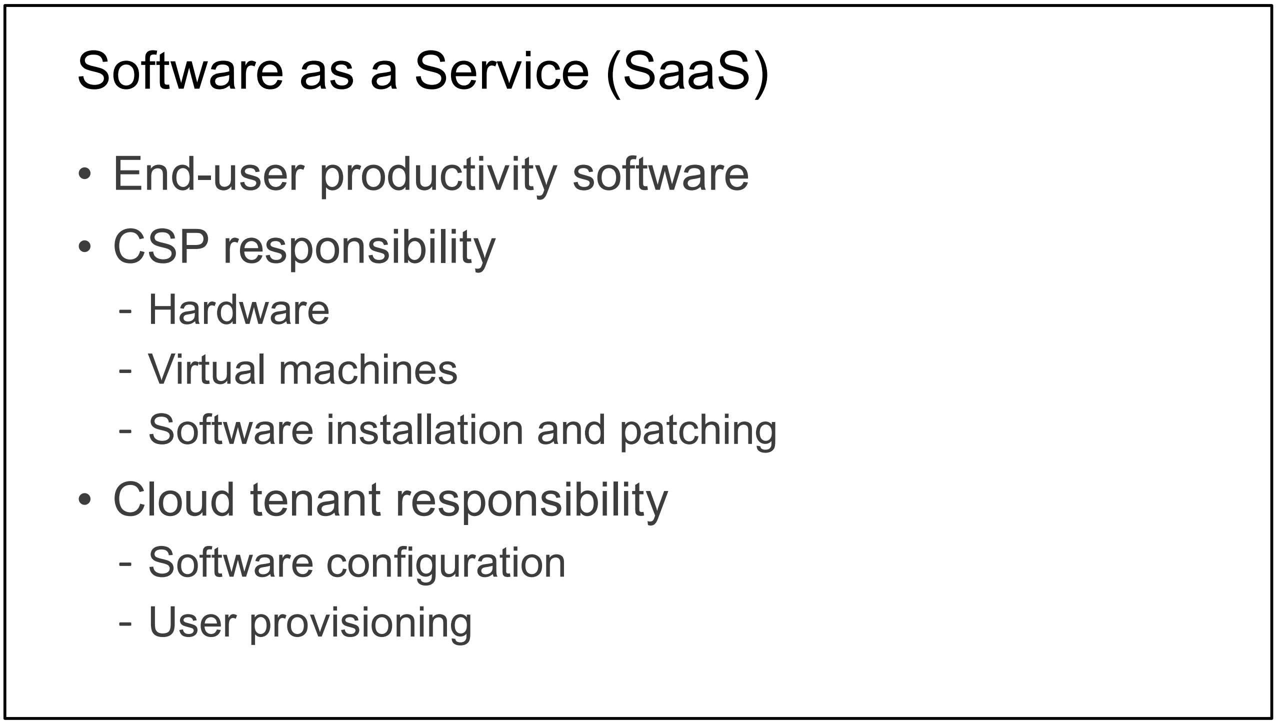
Infrastructure as a Service (IaaS)

- Storage
- Networking
- Manually deployed and managed virtual machines
- Do not expose directly to the Internet where possible
- CSP responsibility
  - Hardware
- Cloud tenant responsibility
  - VM and storage account deployment, hardening



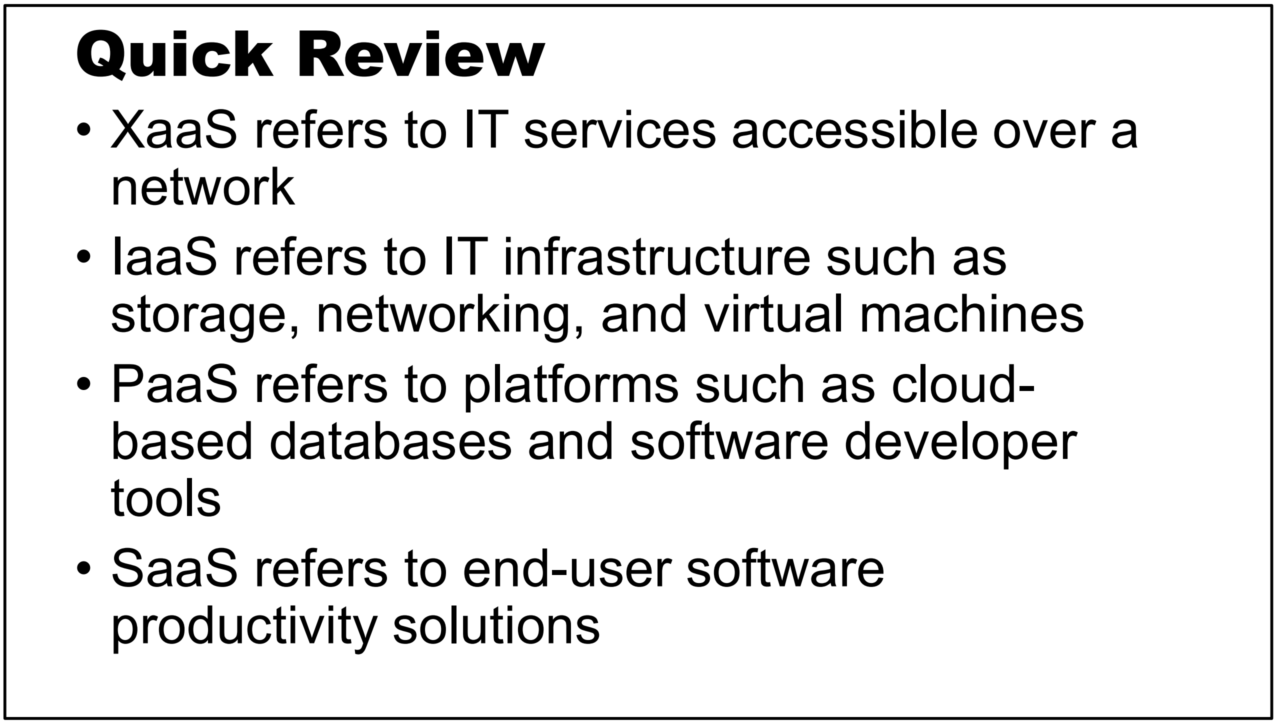
Platform as a Service (PaaS)

- Databases
- Software developer tools
- Underlying virtual machines are managed by the provider
  - Managed service
  - Serverless



Software as a Service (SaaS)

- End-user productivity software
- CSP responsibility
  - Hardware
  - Virtual machines
  - Software installation and patching
- Cloud tenant responsibility
  - Software configuration
  - User provisioning



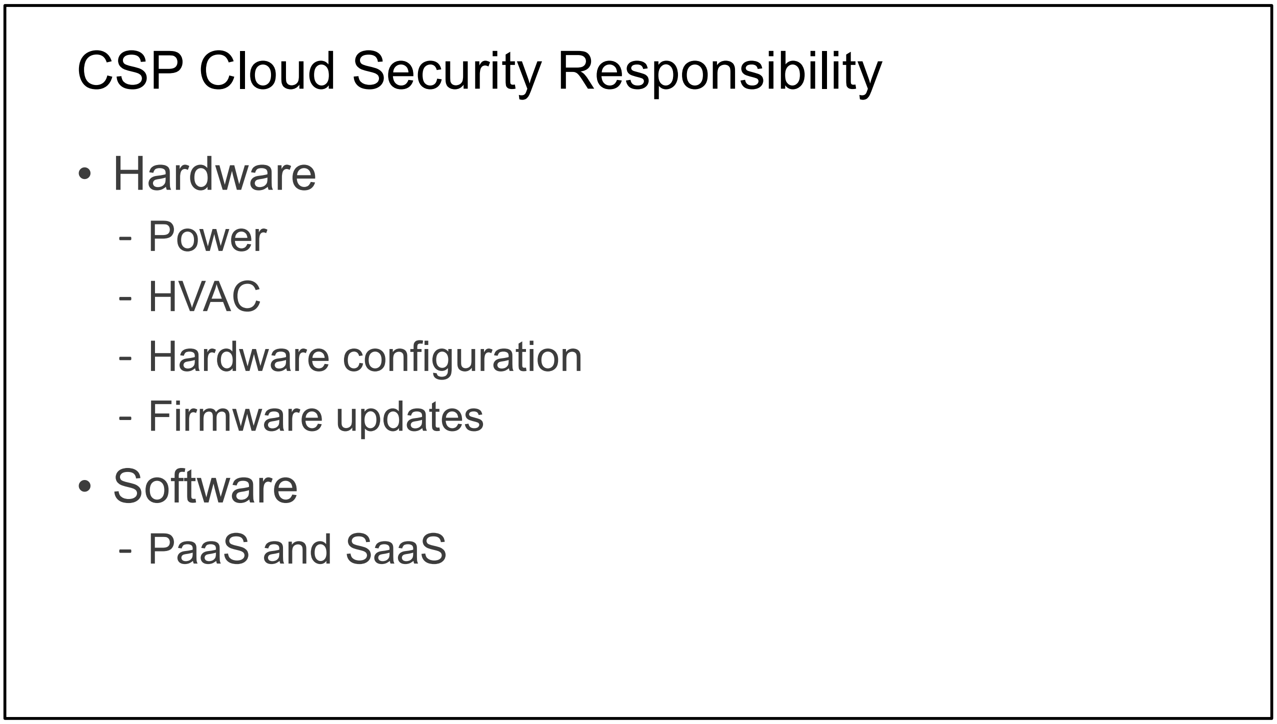
Quick Review

- XaaS refers to IT services accessible over a network
- IaaS refers to IT infrastructure such as storage, networking, and virtual machines
- PaaS refers to platforms such as cloud-based databases and software developer tools
- SaaS refers to end-user software productivity solutions

Episode 8.07

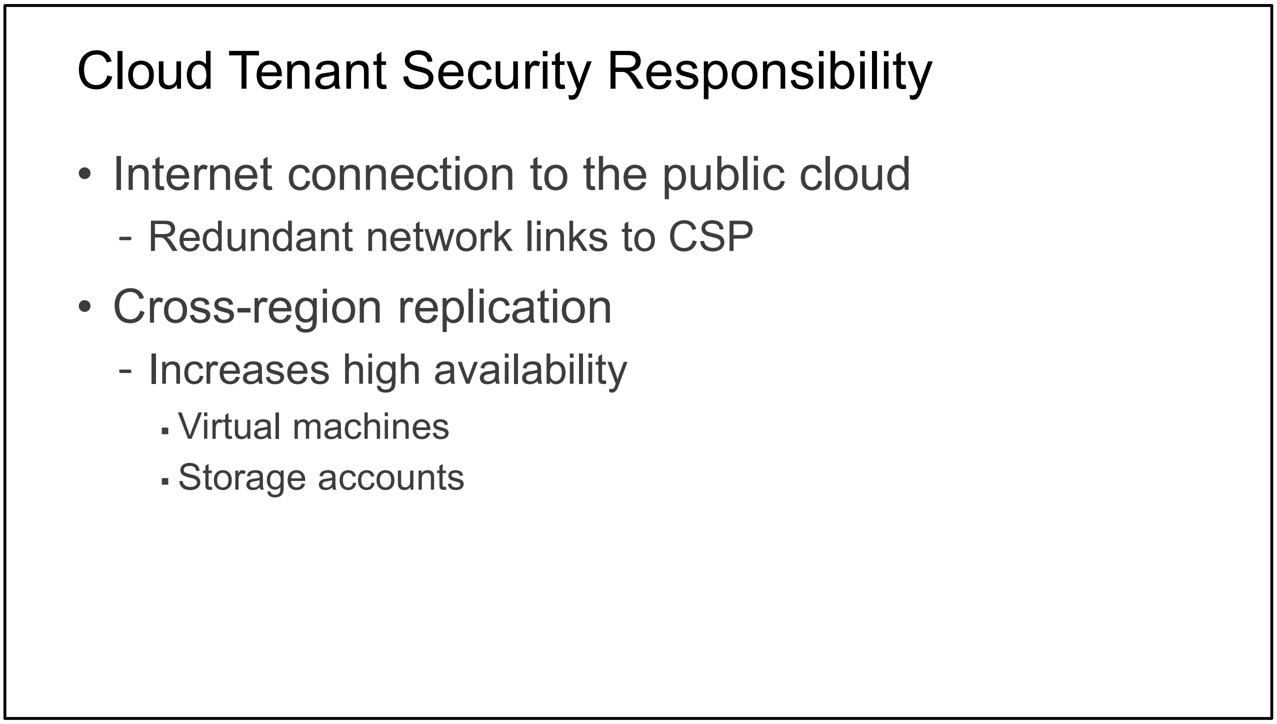
Episode title: **Securing the Cloud**

Objective: **3.6 Given a scenario, apply cybersecurity solutions to the cloud.**



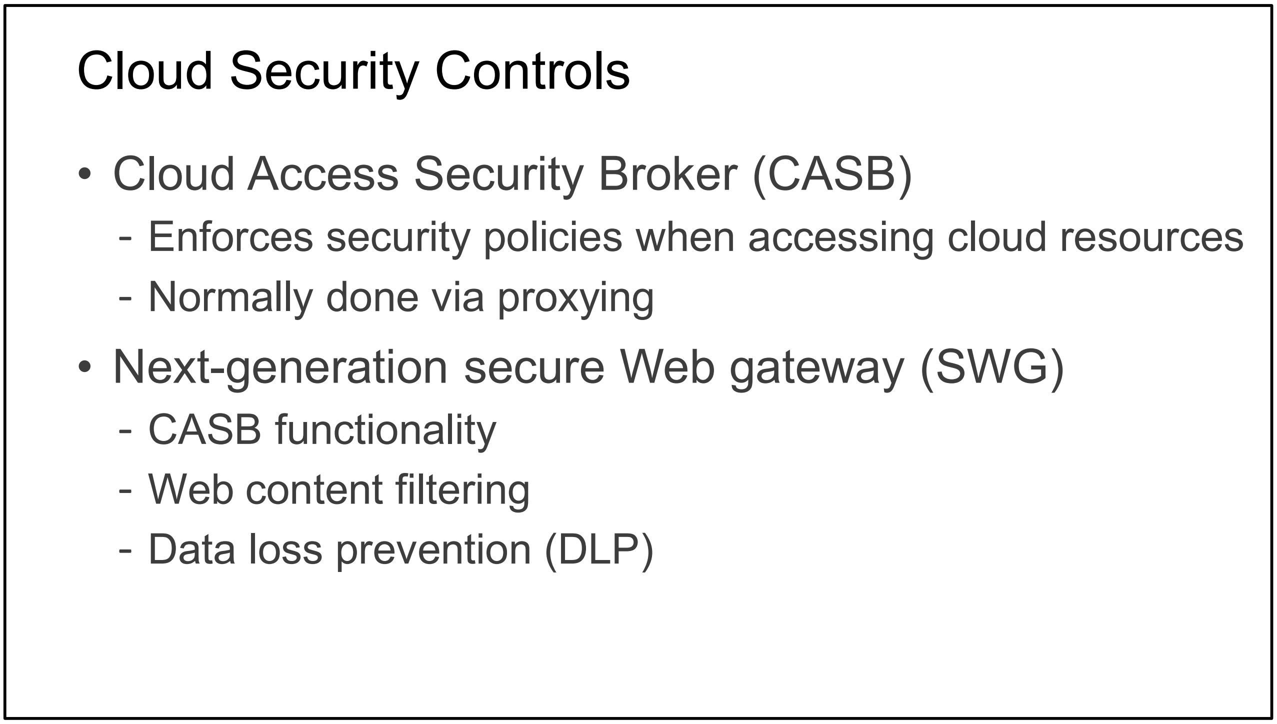
CSP Cloud Security Responsibility

- Hardware
  - Power
  - HVAC
  - Hardware configuration
  - Firmware updates
- Software
  - PaaS and SaaS



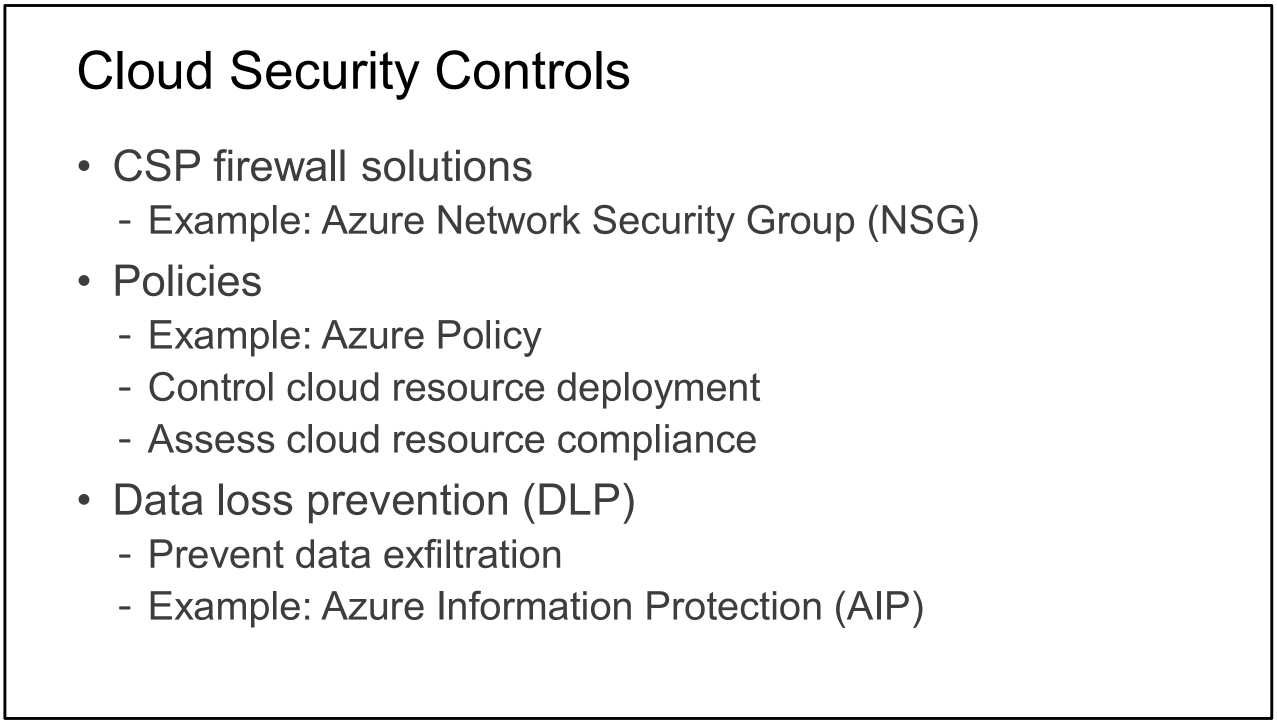
Cloud Tenant Security Responsibility

- Internet connection to the public cloud
  - Redundant network links to CSP
- Cross-region replication
  - Increases high availability
    - Virtual machines
    - Storage accounts



Cloud Security Controls

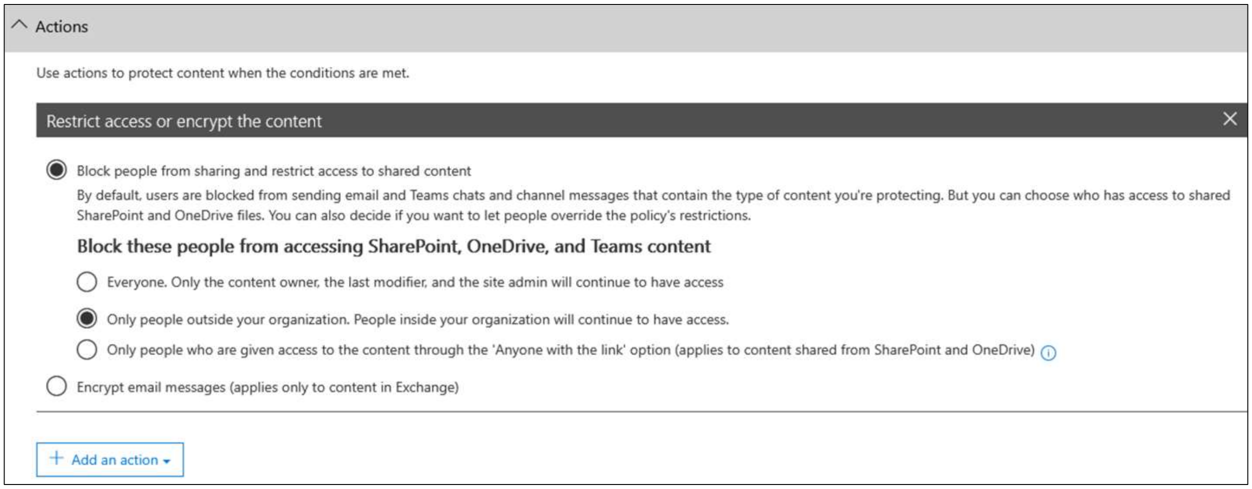
- Cloud Access Security Broker (CASB)
  - Enforces security policies when accessing cloud resources
  - Normally done via proxying
- Next-generation secure Web gateway (SWG)
  - CASB functionality
  - Web content filtering
  - Data loss prevention (DLP)



Cloud Security Controls

- CSP firewall solutions
  - Example: Azure Network Security Group (NSG)
- Policies
  - Example: Azure Policy
  - Control cloud resource deployment
  - Assess cloud resource compliance
- Data loss prevention (DLP)
  - Prevent data exfiltration
  - Example: Azure Information Protection (AIP)

Azure Policy Compliance



Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

● Block people from sharing and restrict access to shared content

By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

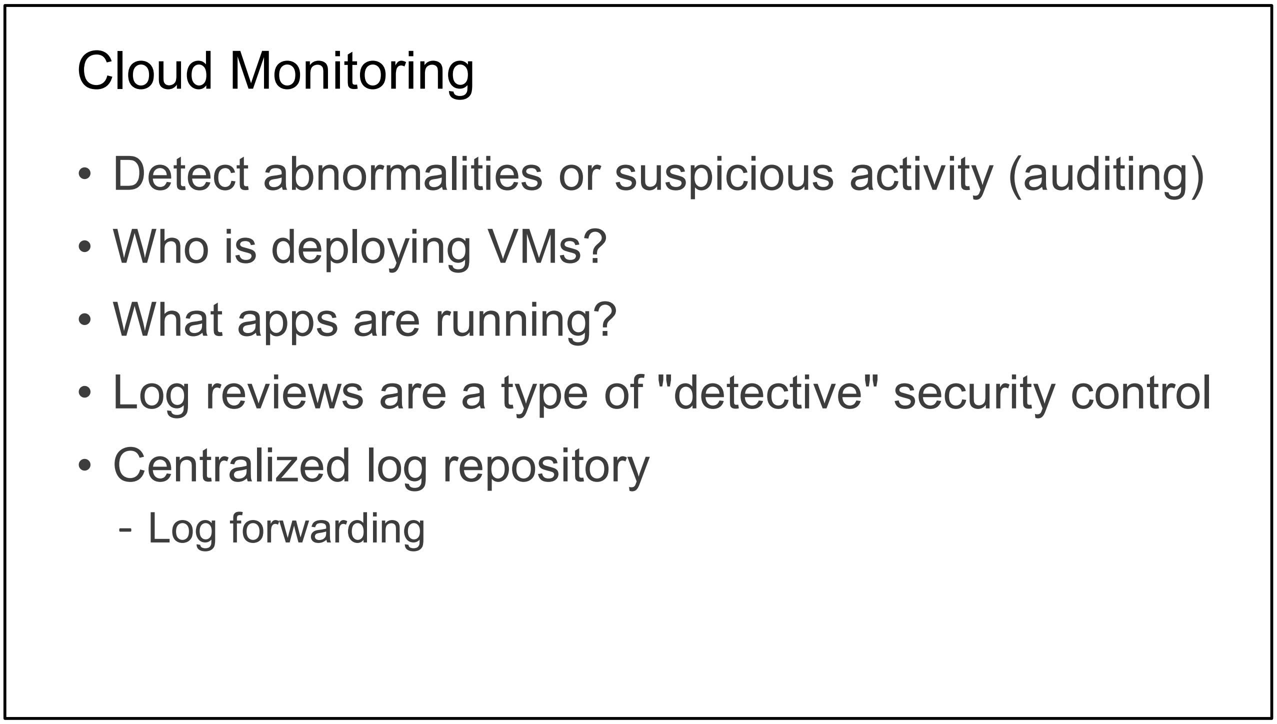
Block these people from accessing SharePoint, OneDrive, and Teams content

○ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access

● Only people outside your organization. People inside your organization will continue to have access.

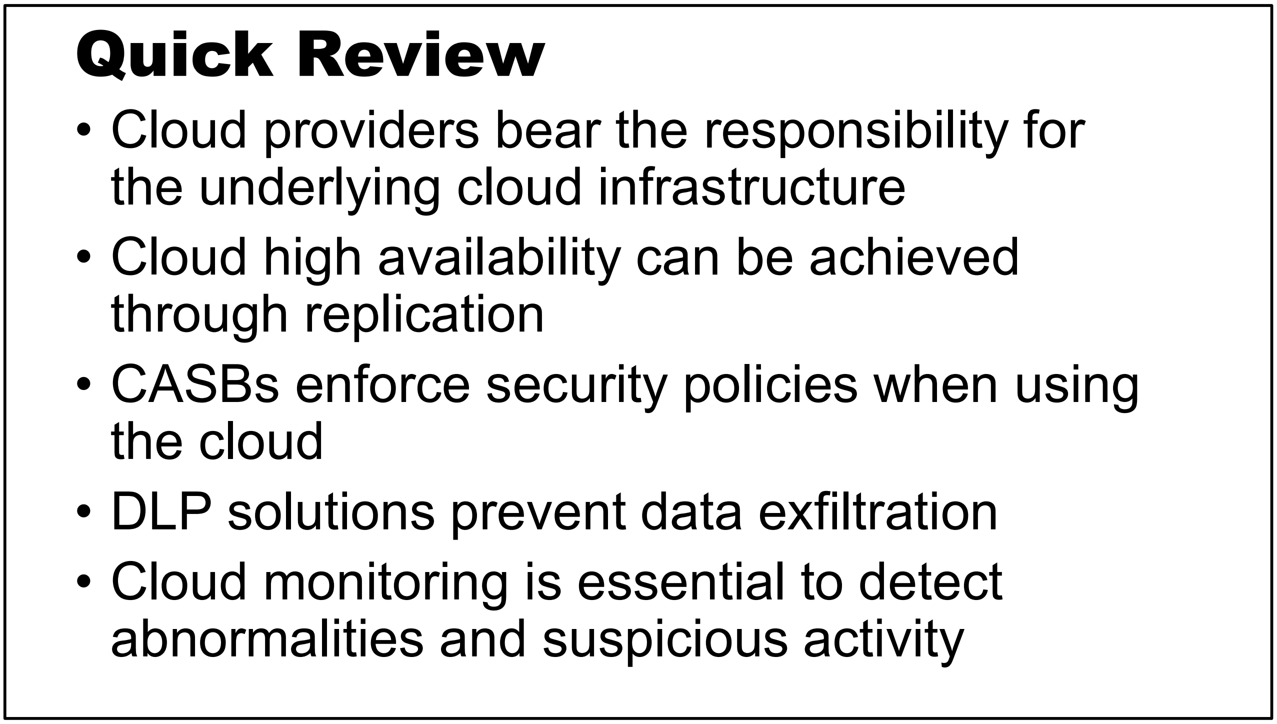
○ Only people who are given access to the content through the 'Anyone with the link' option (applies to content shared from SharePoint and OneDrive)

○ Encrypt email messages (applies only to content in Exchange)



Cloud Monitoring

- Detect abnormalities or suspicious activity (auditing)
- Who is deploying VMs?
- What apps are running?
- Log reviews are a type of "detective" security control
- Centralized log repository
  - Log forwarding



Quick Review

- Cloud providers bear the responsibility for the underlying cloud infrastructure
- Cloud high availability can be achieved through replication
- CASBs enforce security policies when using the cloud
- DLP solutions prevent data exfiltration
- Cloud monitoring is essential to detect abnormalities and suspicious activity