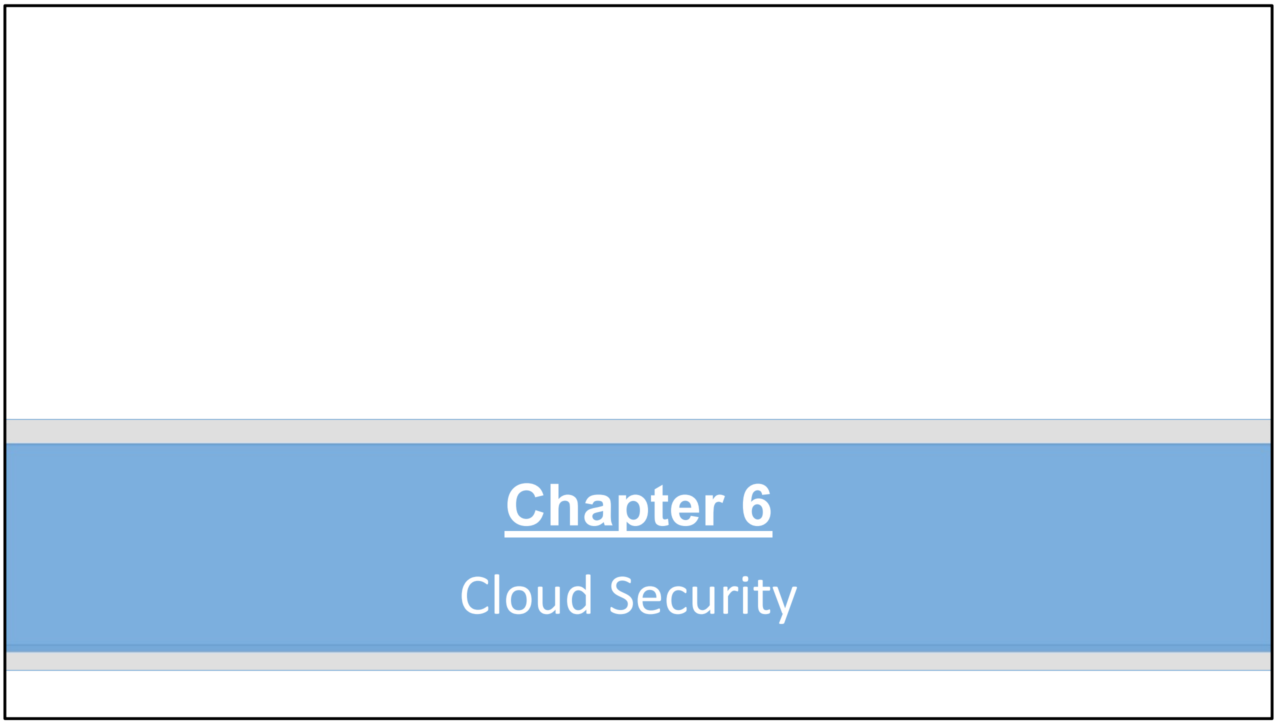
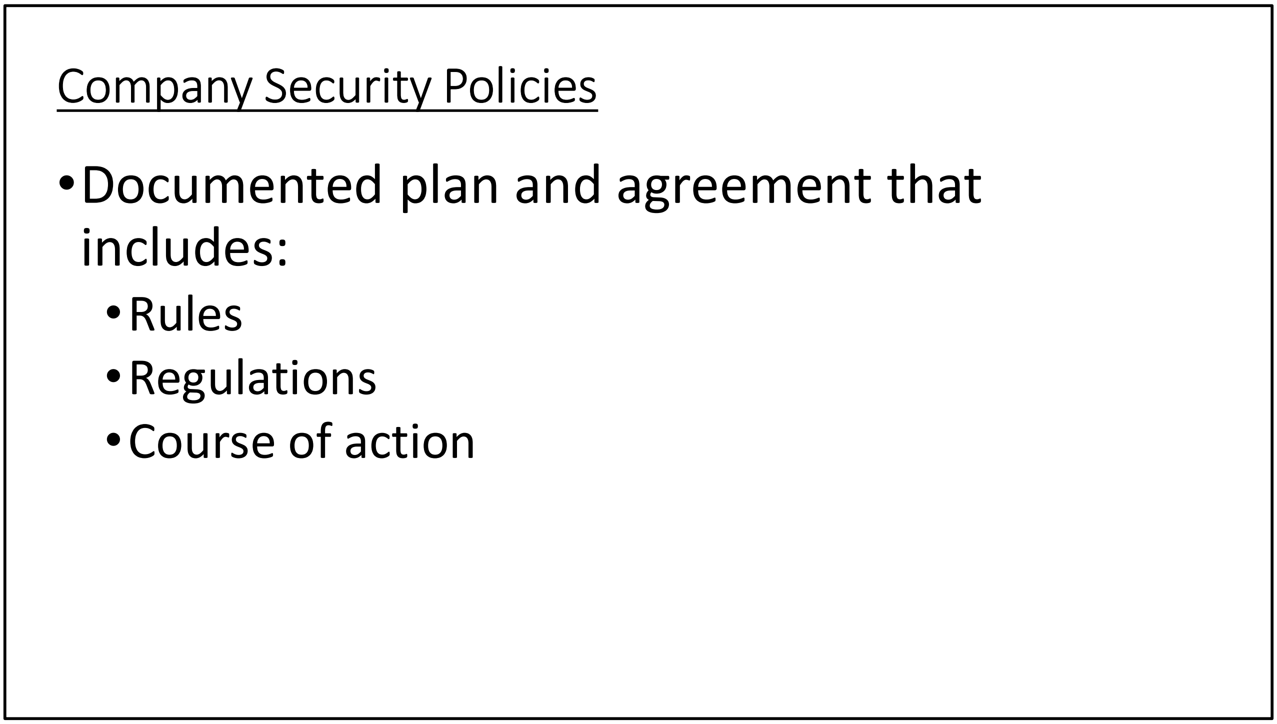


# Chapter 6

## Cloud Security

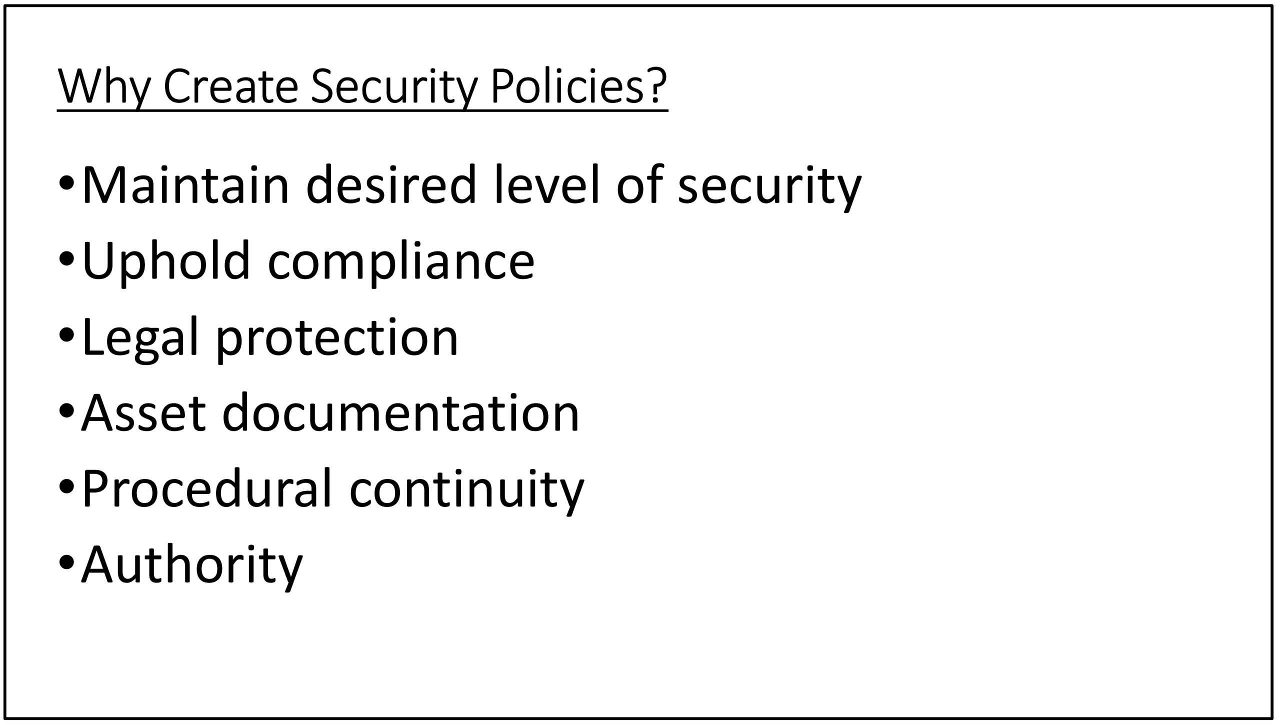
# 6.01 Security Policies

CH06: Cloud Security



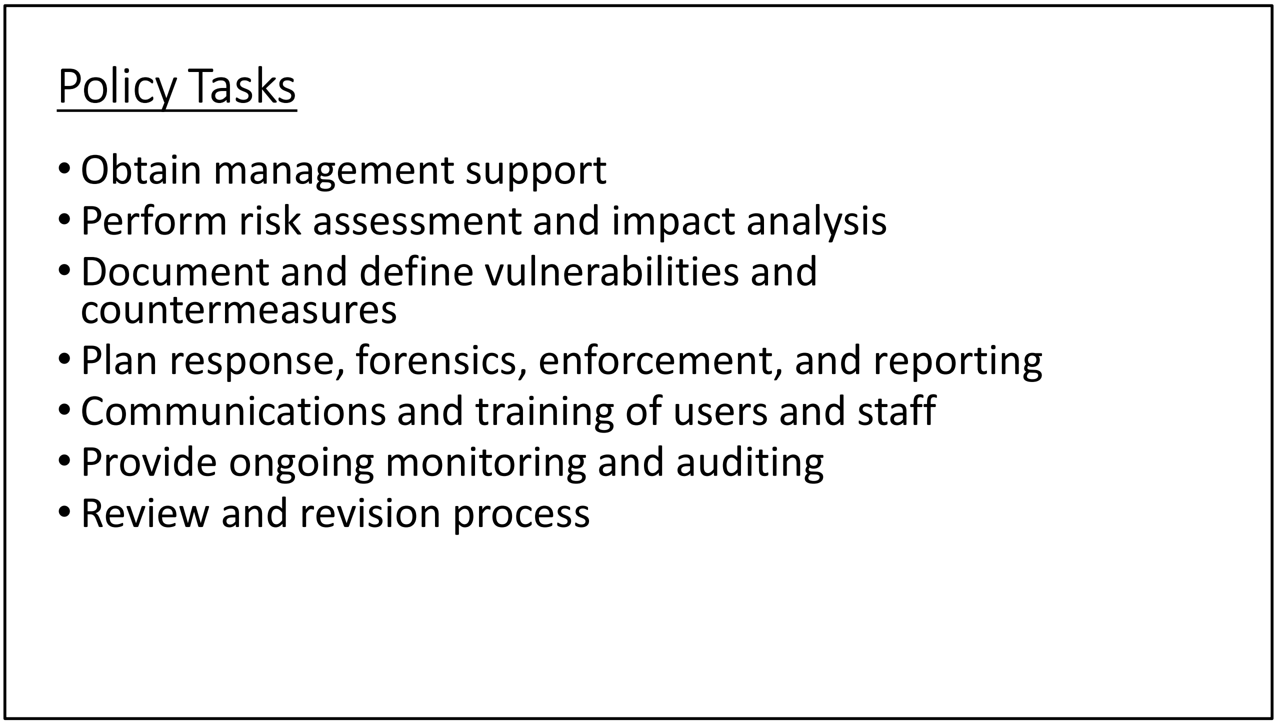
Company Security Policies

- Documented plan and agreement that includes:
  - Rules
  - Regulations
  - Course of action



Why Create Security Policies?

- Maintain desired level of security
- Uphold compliance
- Legal protection
- Asset documentation
- Procedural continuity
- Authority

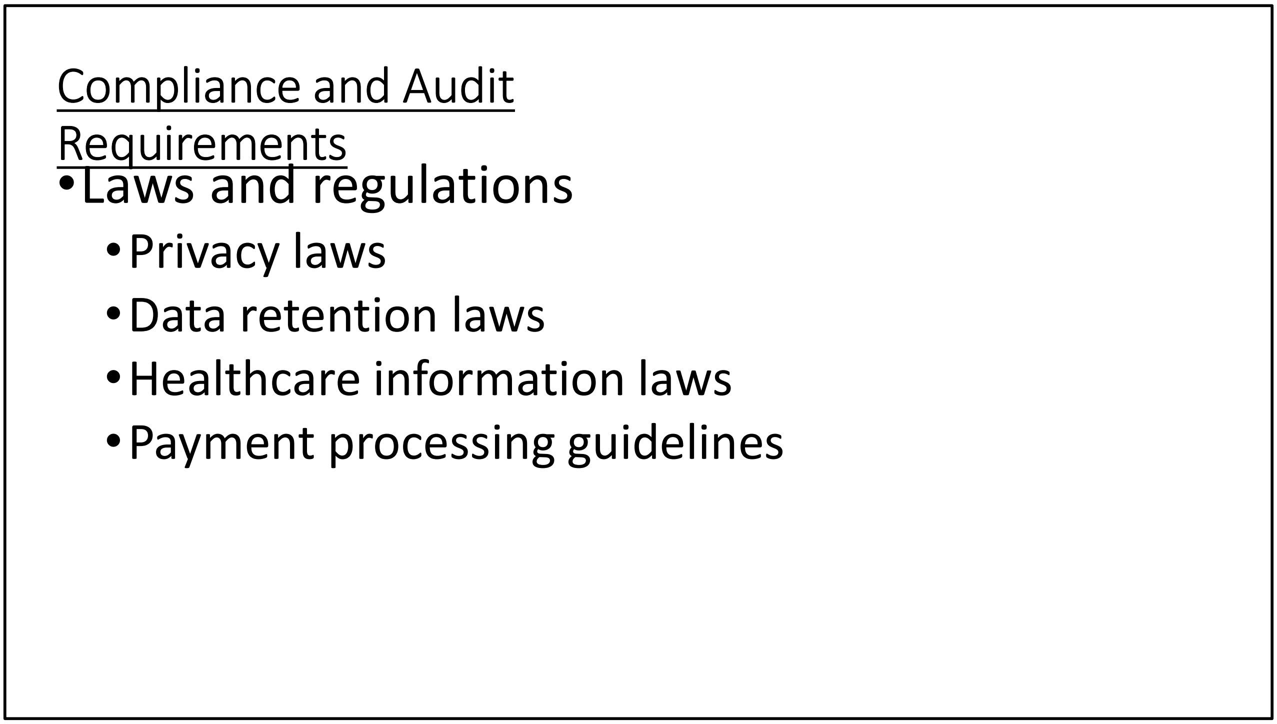


## Policy Tasks

- Obtain management support
- Perform risk assessment and impact analysis
- Document and define vulnerabilities and countermeasures
- Plan response, forensics, enforcement, and reporting
- Communications and training of users and staff
- Provide ongoing monitoring and auditing
- Review and revision process

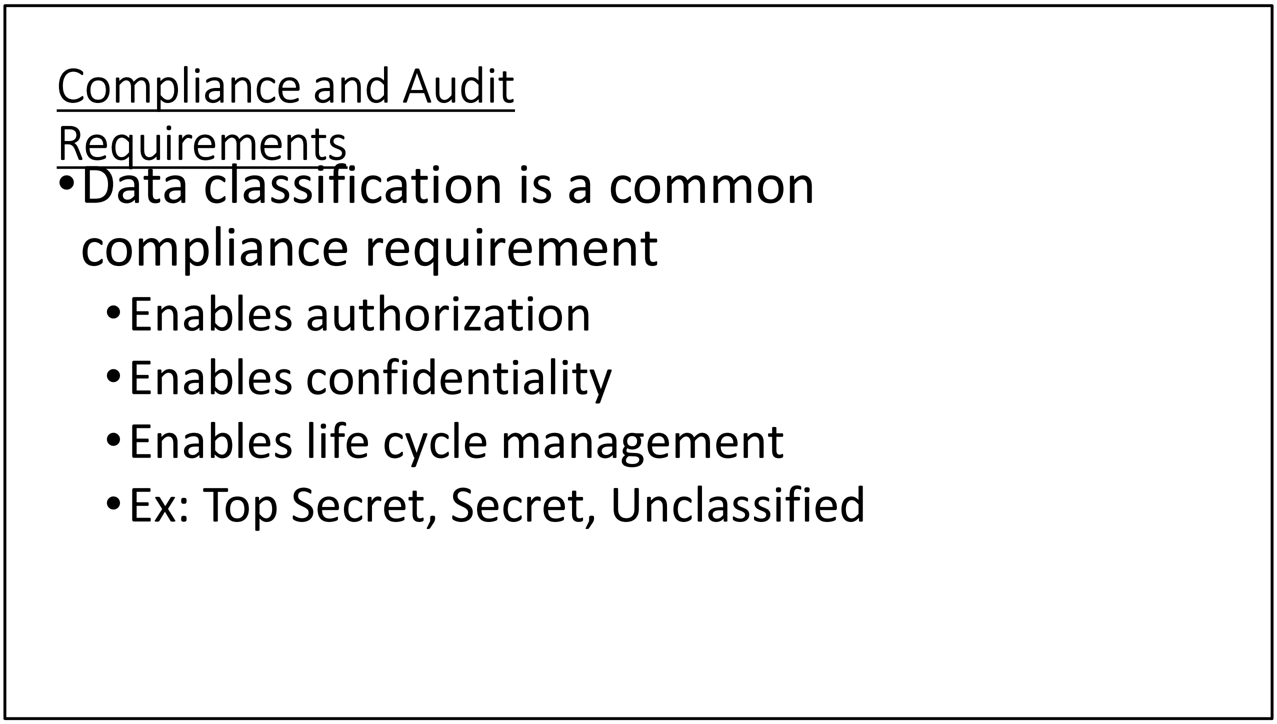
## 6.02 Standards and Compliance (Demo)

CH06: Cloud Security



## Compliance and Audit Requirements

- Laws and regulations
  - Privacy laws
  - Data retention laws
  - Healthcare information laws
  - Payment processing guidelines

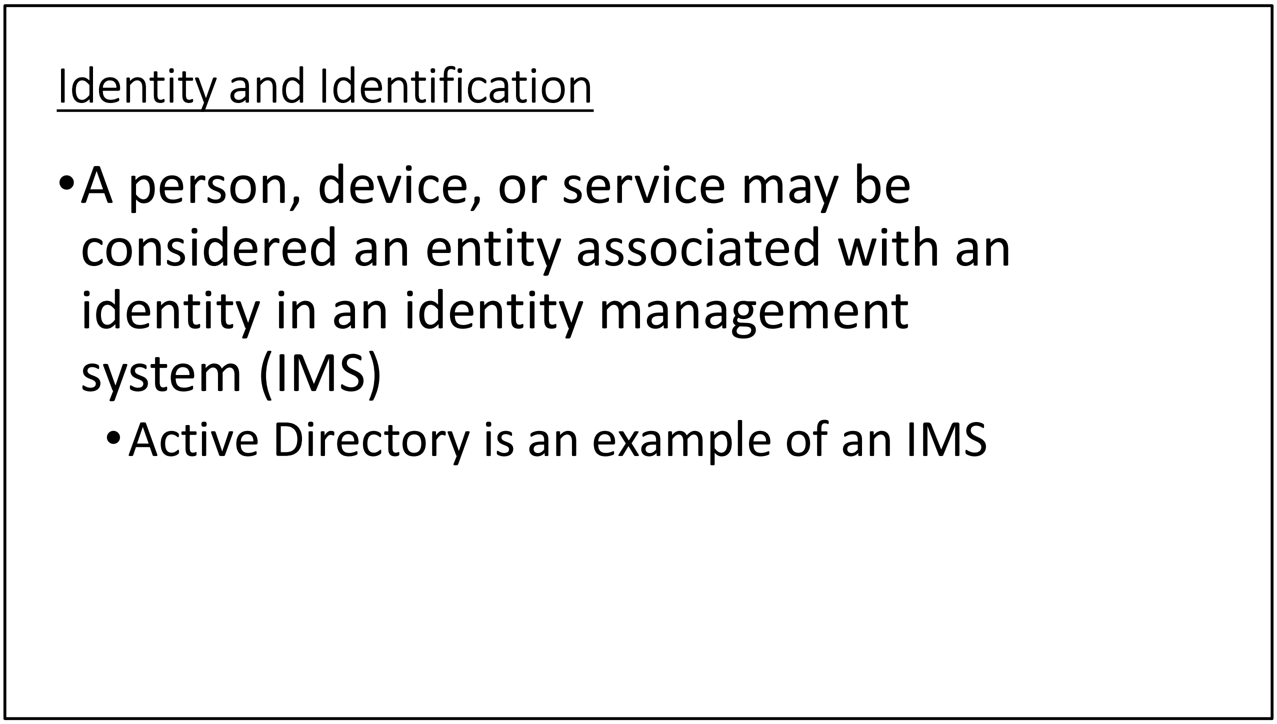


## Compliance and Audit Requirements

- Data classification is a common compliance requirement
  - Enables authorization
  - Enables confidentiality
  - Enables life cycle management
  - Ex: Top Secret, Secret, Unclassified

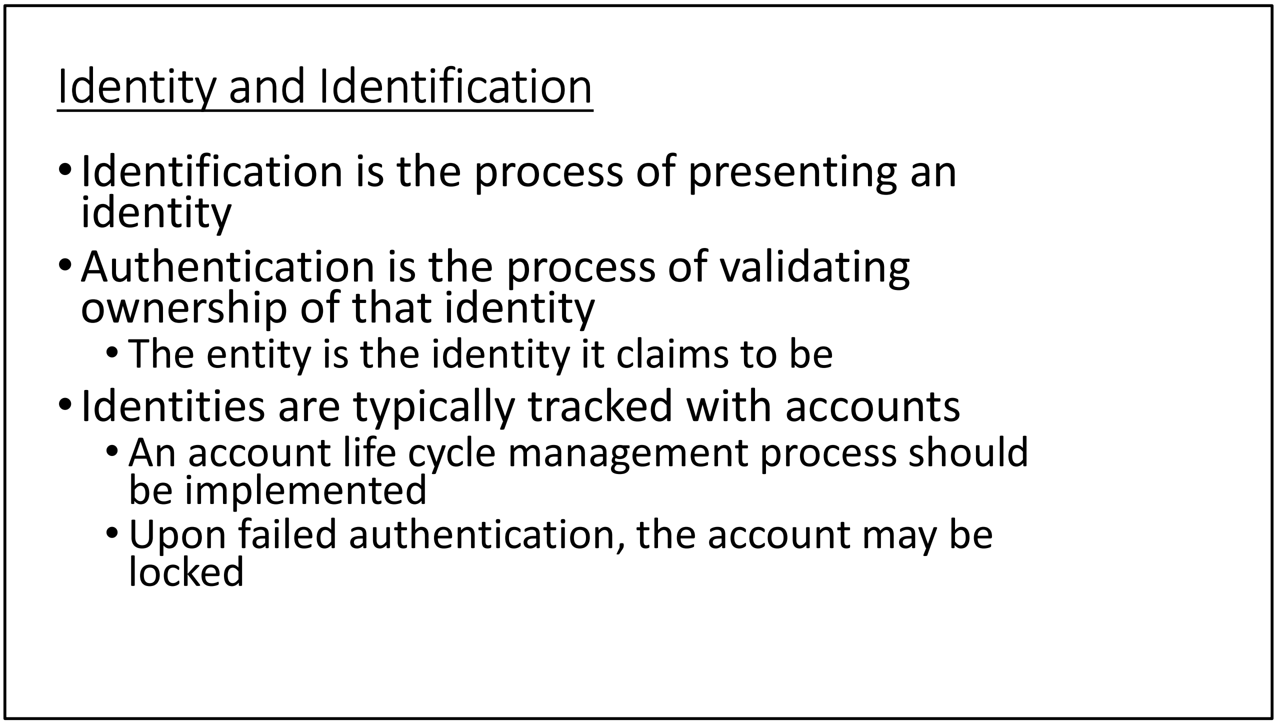
## 6.03 Identity, Authentication, and Authorization

CH06: Cloud Security



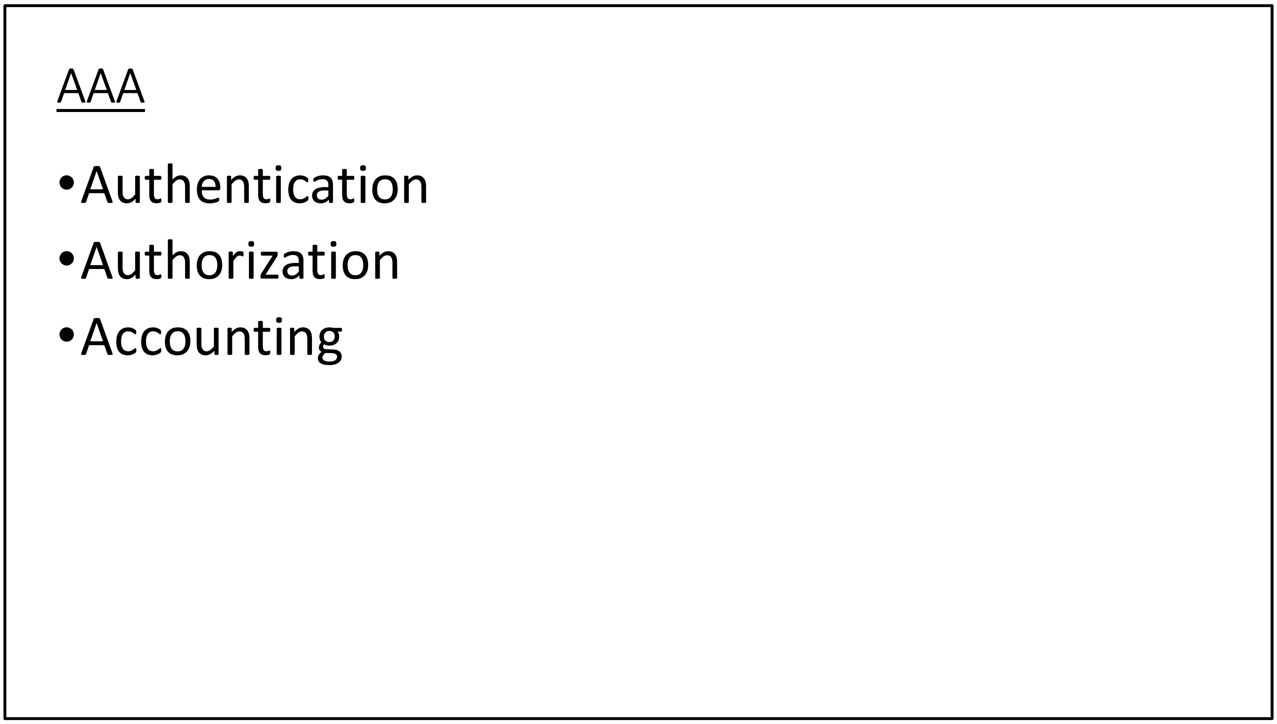
Identity and Identification

- A person, device, or service may be considered an entity associated with an identity in an identity management system (IMS)
  - Active Directory is an example of an IMS



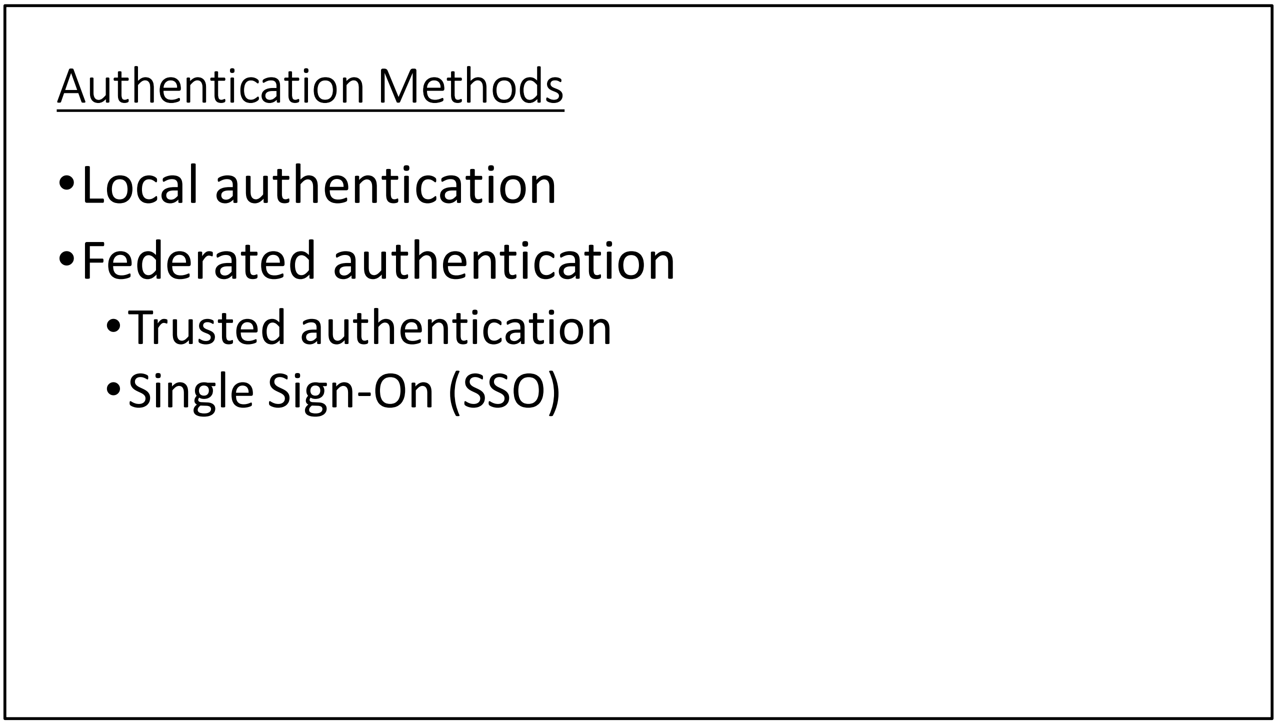
## Identity and Identification

- Identification is the process of presenting an identity
- Authentication is the process of validating ownership of that identity
  - The entity is the identity it claims to be
- Identities are typically tracked with accounts
  - An account life cycle management process should be implemented
  - Upon failed authentication, the account may be locked



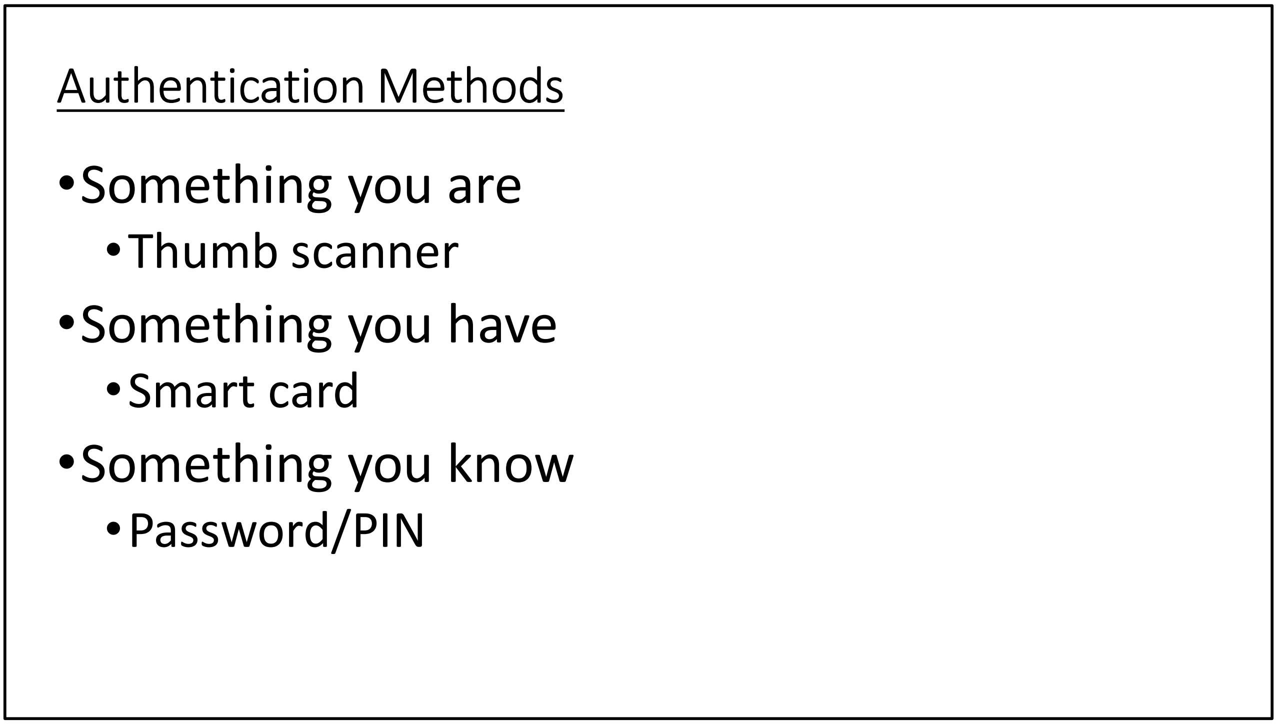
## AAA

- Authentication
- Authorization
- Accounting



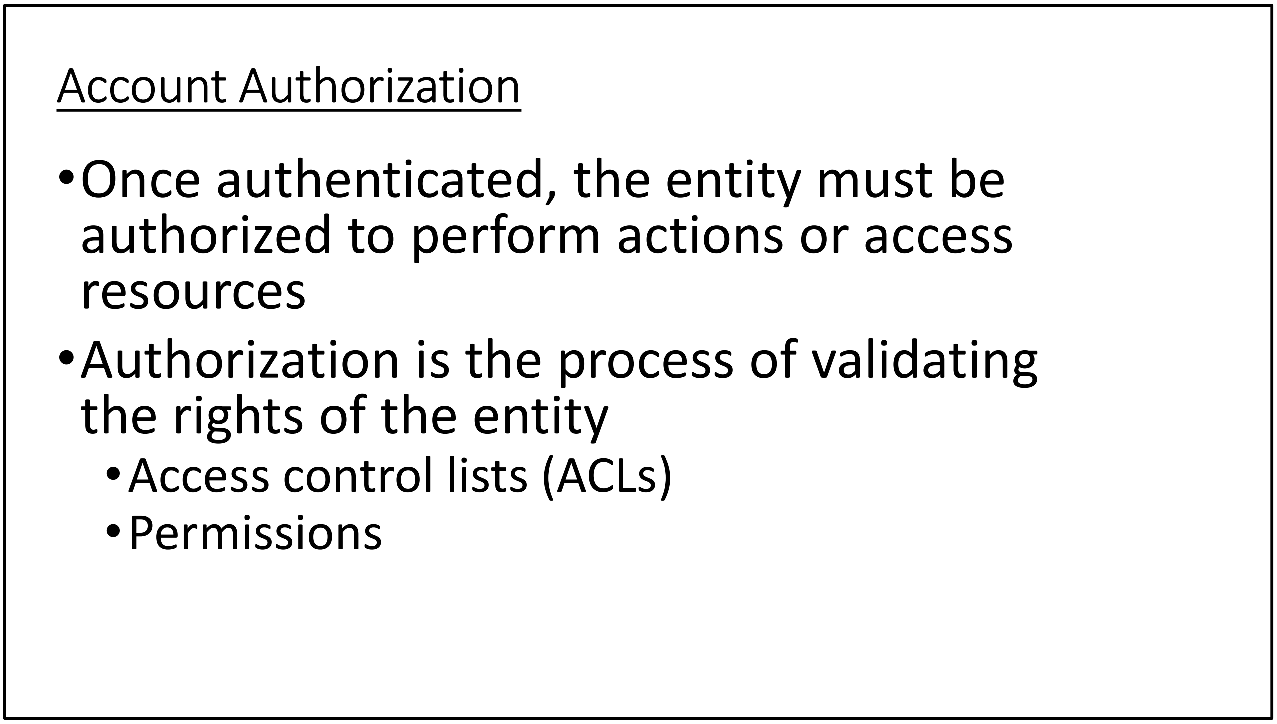
## Authentication Methods

- Local authentication
- Federated authentication
  - Trusted authentication
  - Single Sign-On (SSO)



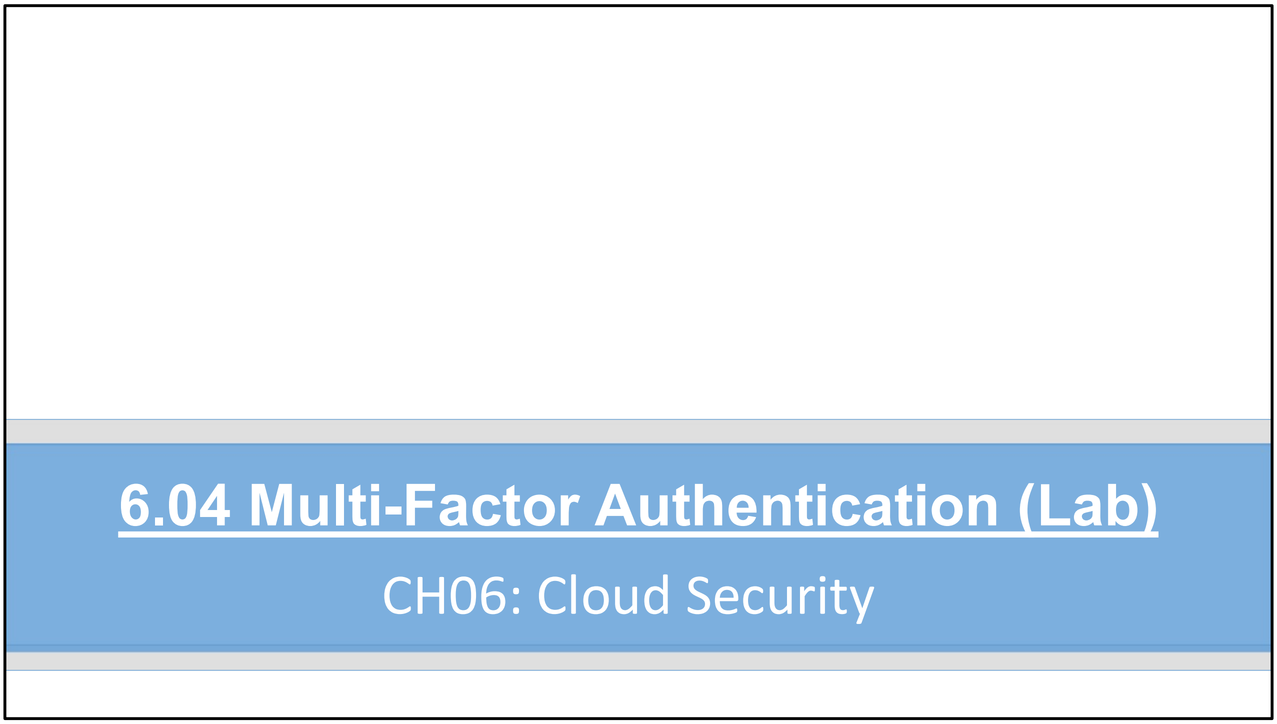
## Authentication Methods

- Something you are
  - Thumb scanner
- Something you have
  - Smart card
- Something you know
  - Password/PIN



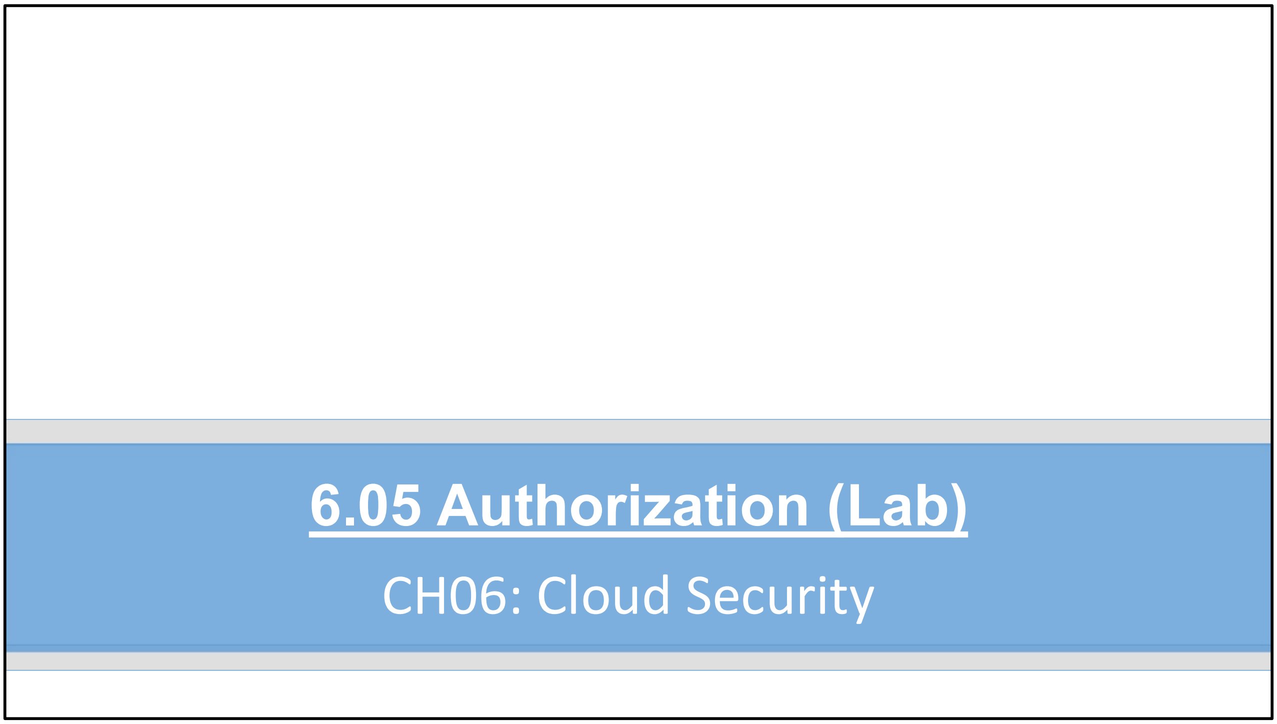
Account Authorization

- Once authenticated, the entity must be authorized to perform actions or access resources
- Authorization is the process of validating the rights of the entity
  - Access control lists (ACLs)
  - Permissions



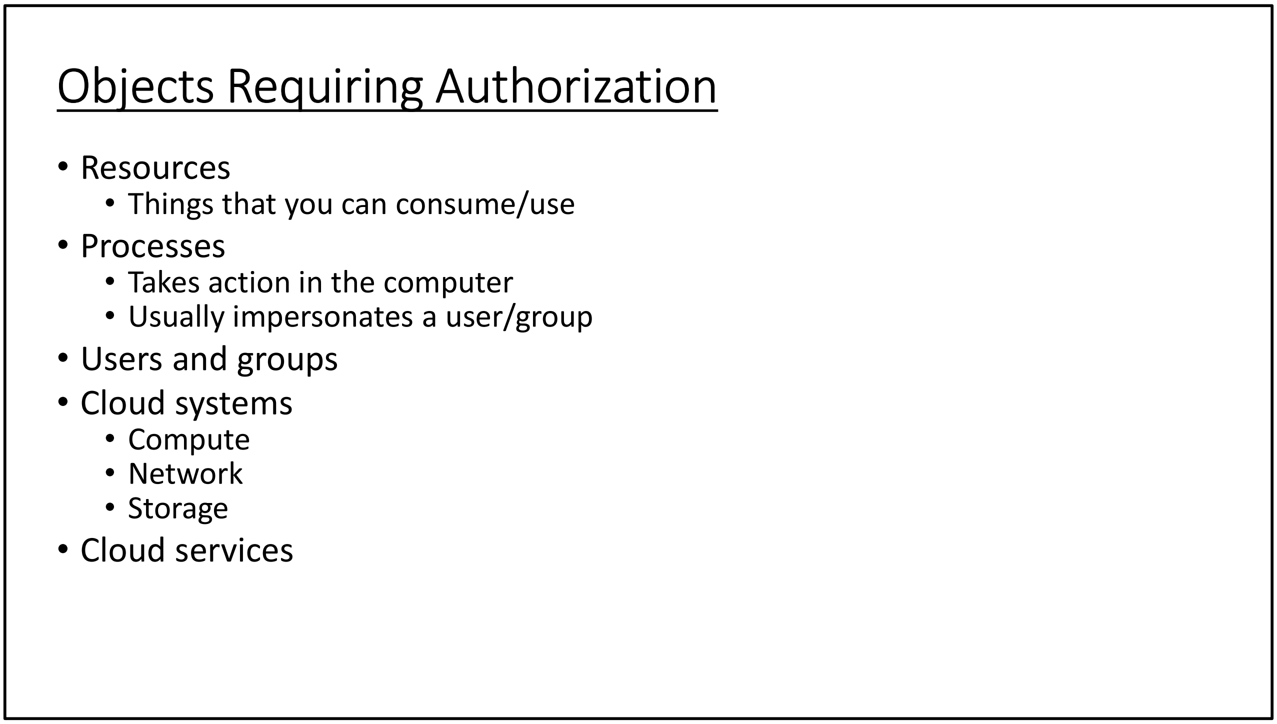
# 6.04 Multi-Factor Authentication (Lab)

CH06: Cloud Security



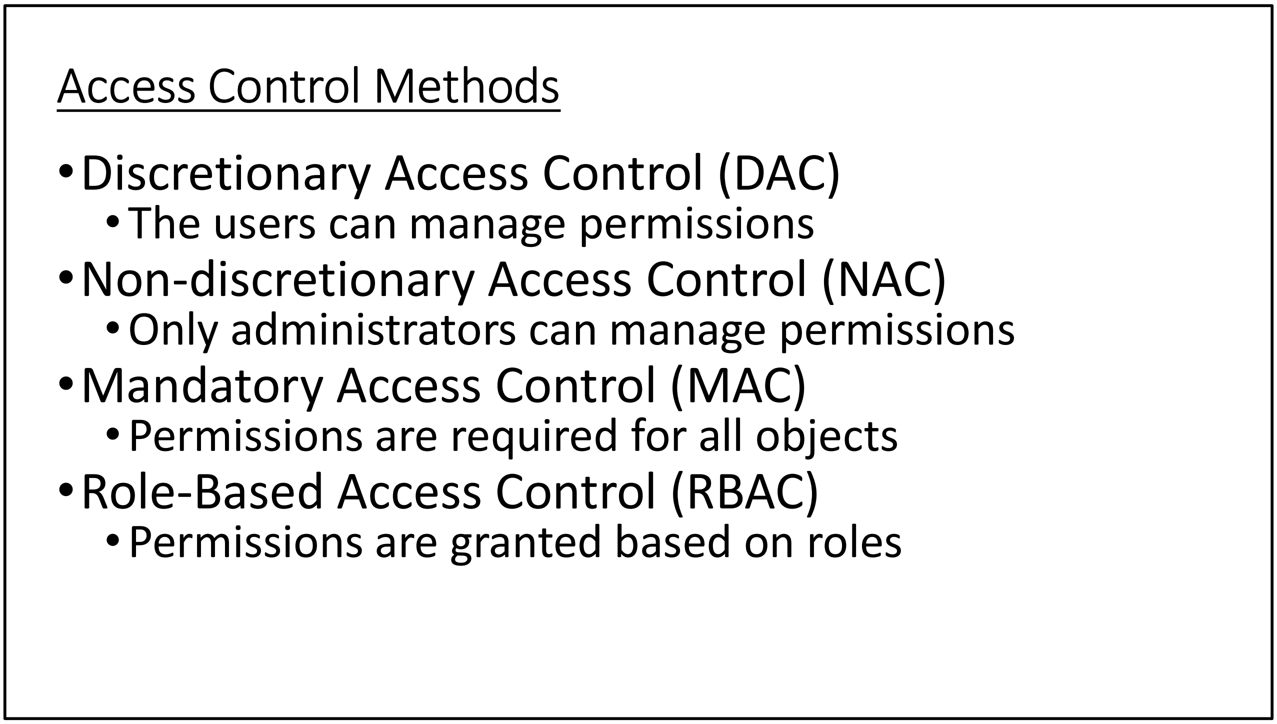
## 6.05 Authorization (Lab)

CH06: Cloud Security



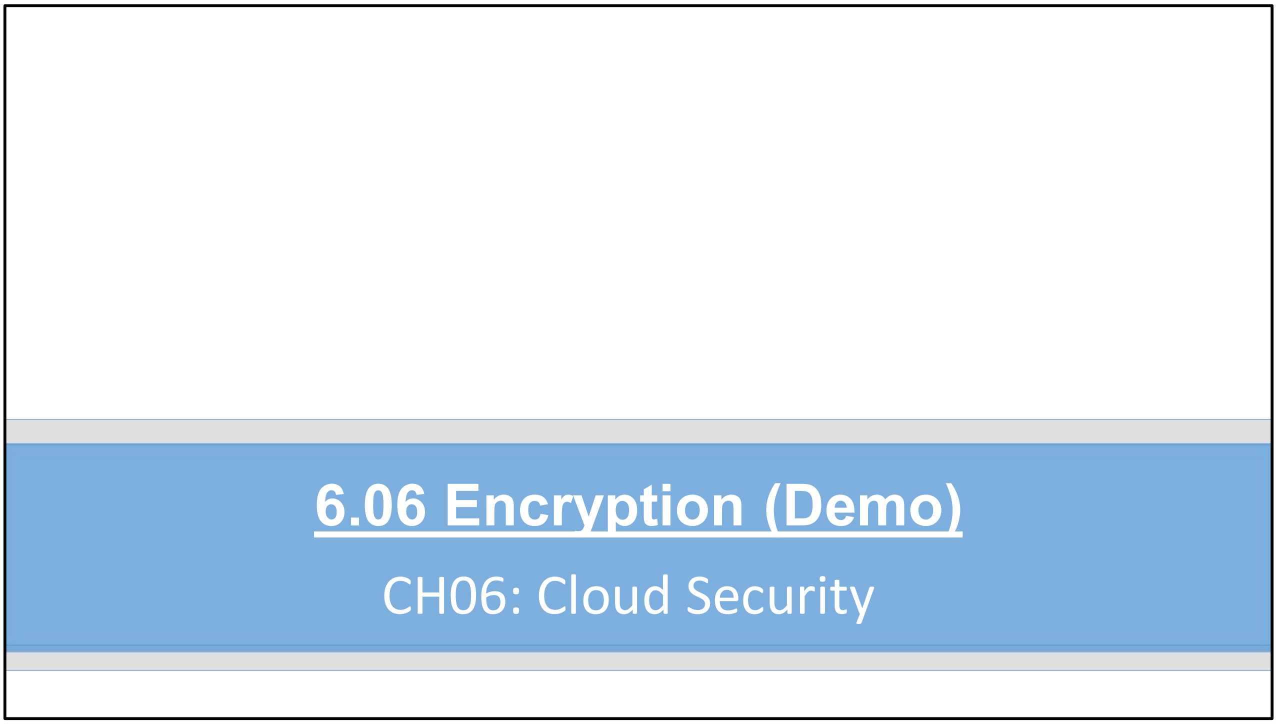
## Objects Requiring Authorization

- Resources
  - Things that you can consume/use
- Processes
  - Takes action in the computer
  - Usually impersonates a user/group
- Users and groups
- Cloud systems
  - Compute
  - Network
  - Storage
- Cloud services



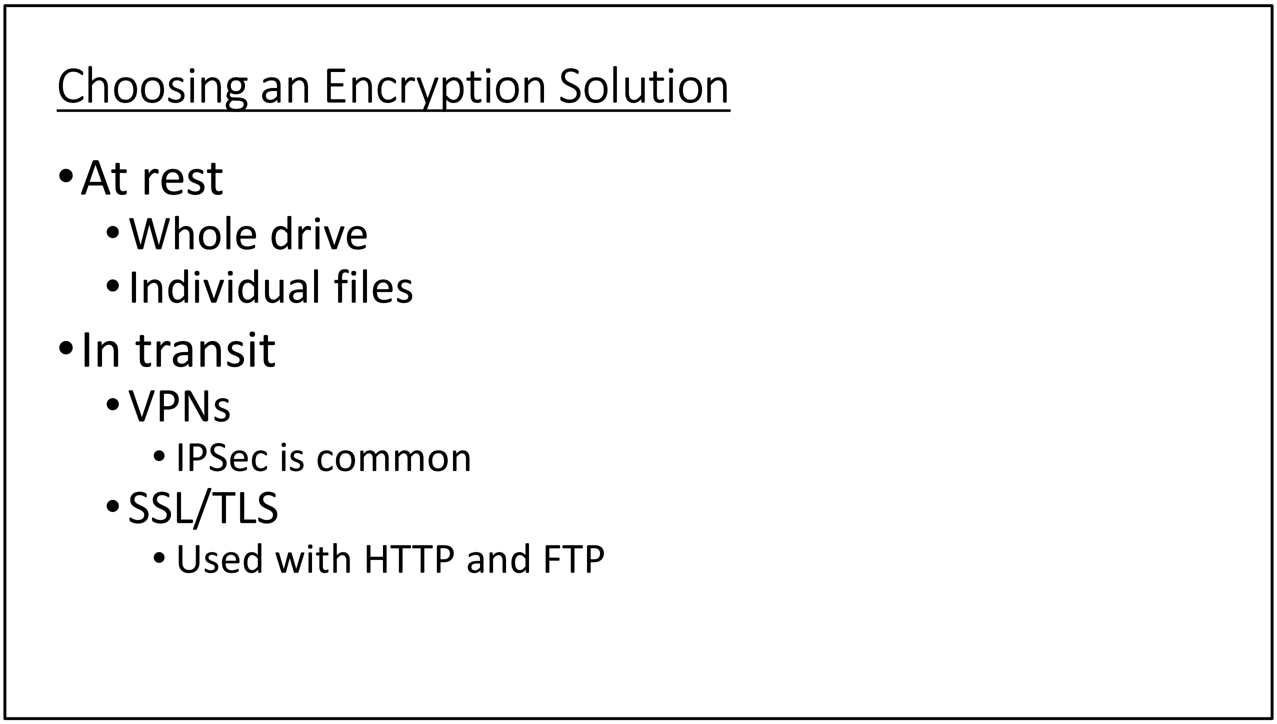
## Access Control Methods

- Discretionary Access Control (DAC)
  - The users can manage permissions
- Non-discretionary Access Control (NAC)
  - Only administrators can manage permissions
- Mandatory Access Control (MAC)
  - Permissions are required for all objects
- Role-Based Access Control (RBAC)
  - Permissions are granted based on roles



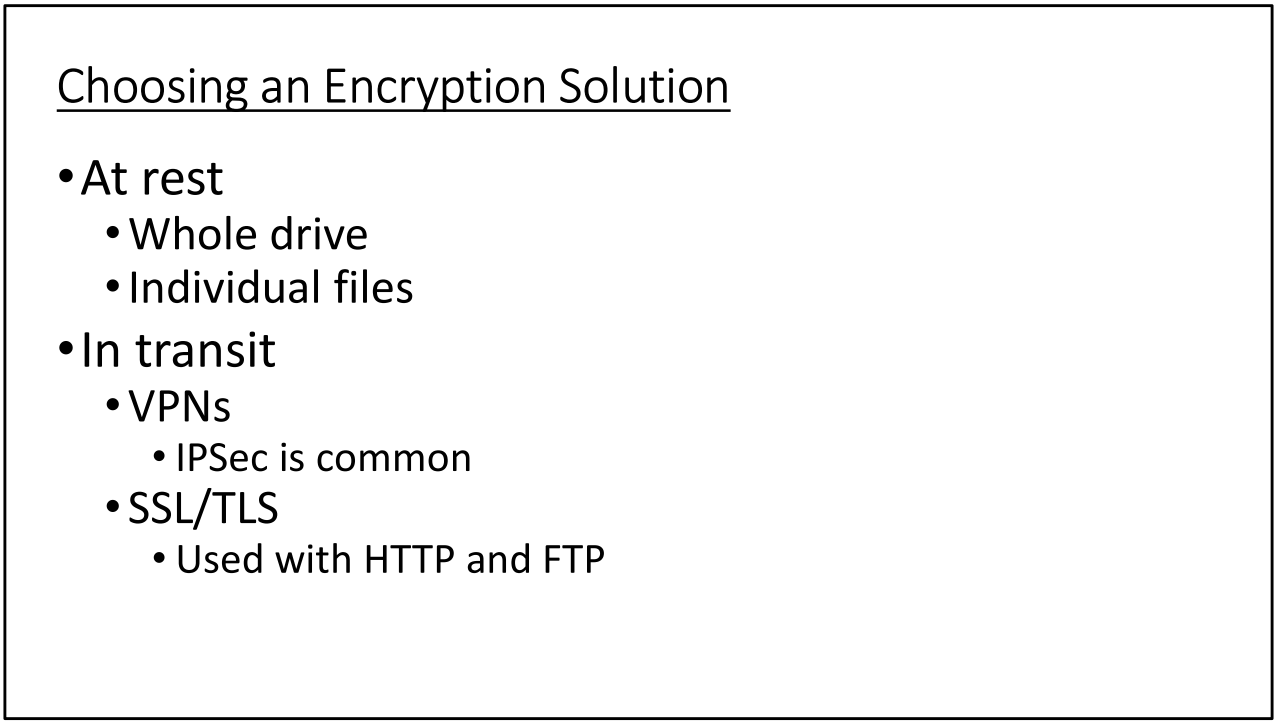
## 6.06 Encryption (Demo)

CH06: Cloud Security



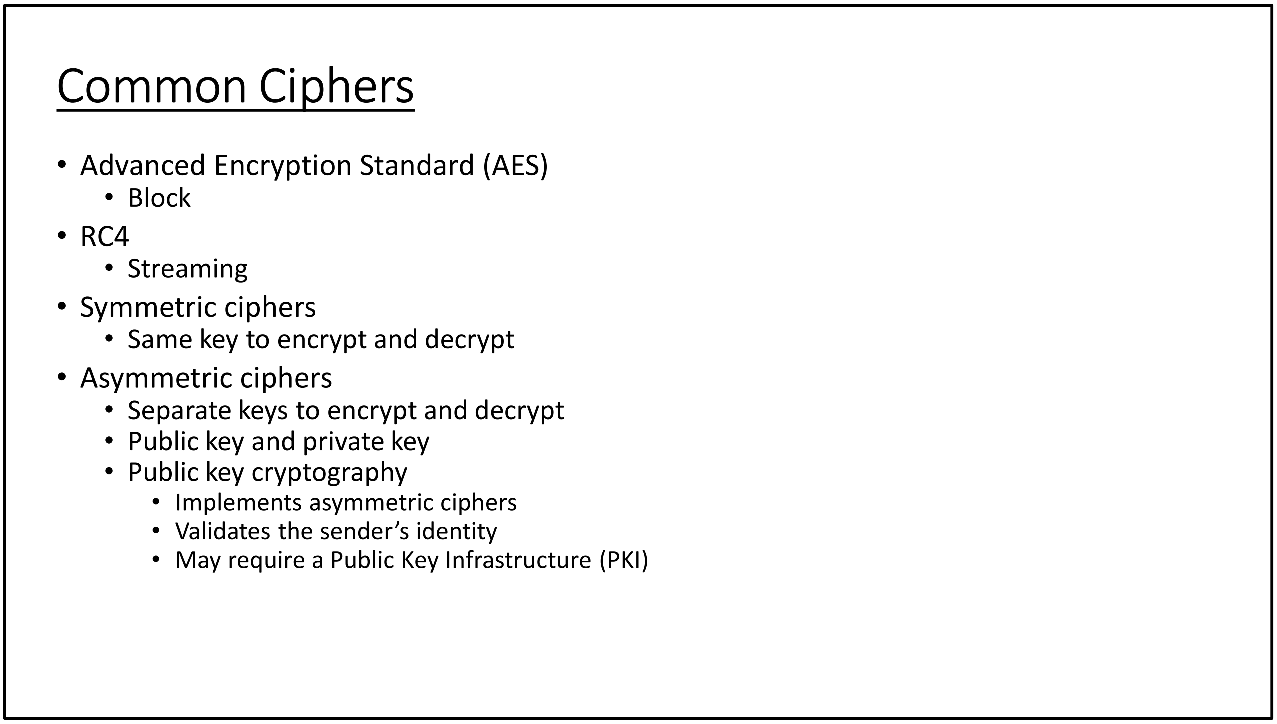
## Choosing an Encryption Solution

- At rest
  - Whole drive
  - Individual files
- In transit
  - VPNs
    - IPSec is common
  - SSL/TLS
    - Used with HTTP and FTP



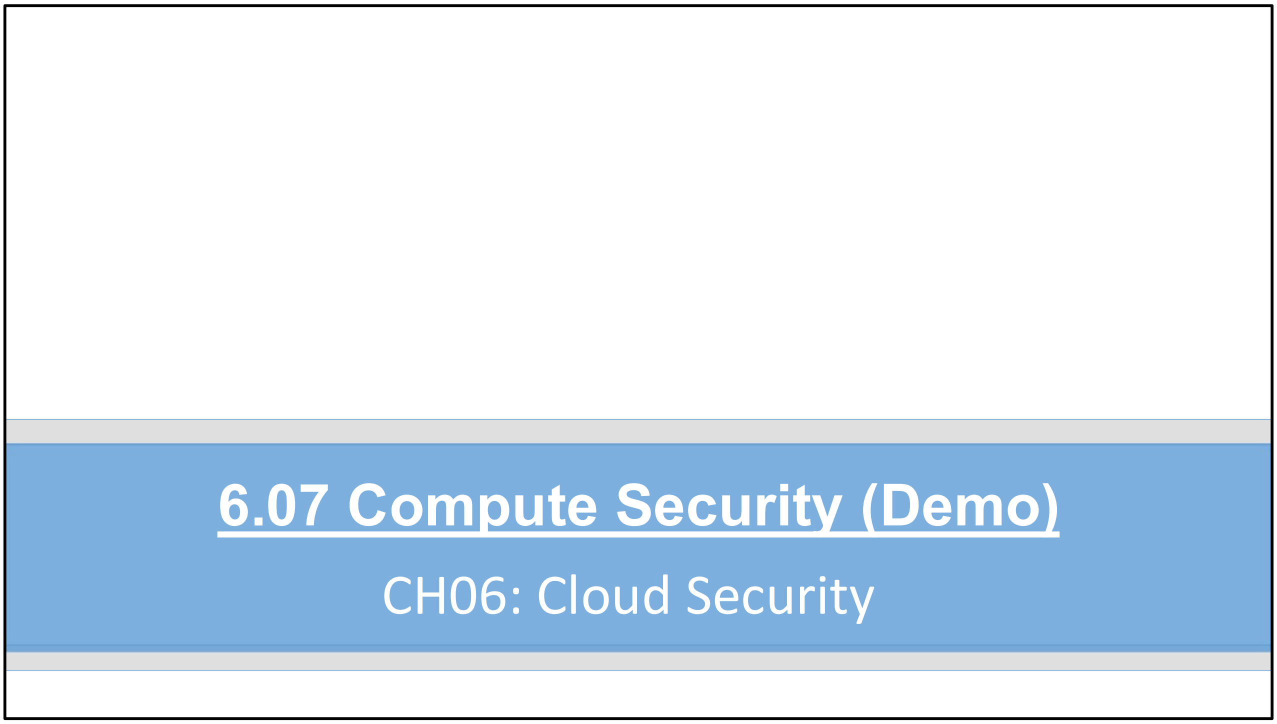
## Choosing an Encryption Solution

- At rest
  - Whole drive
  - Individual files
- In transit
  - VPNs
    - IPSec is common
  - SSL/TLS
    - Used with HTTP and FTP



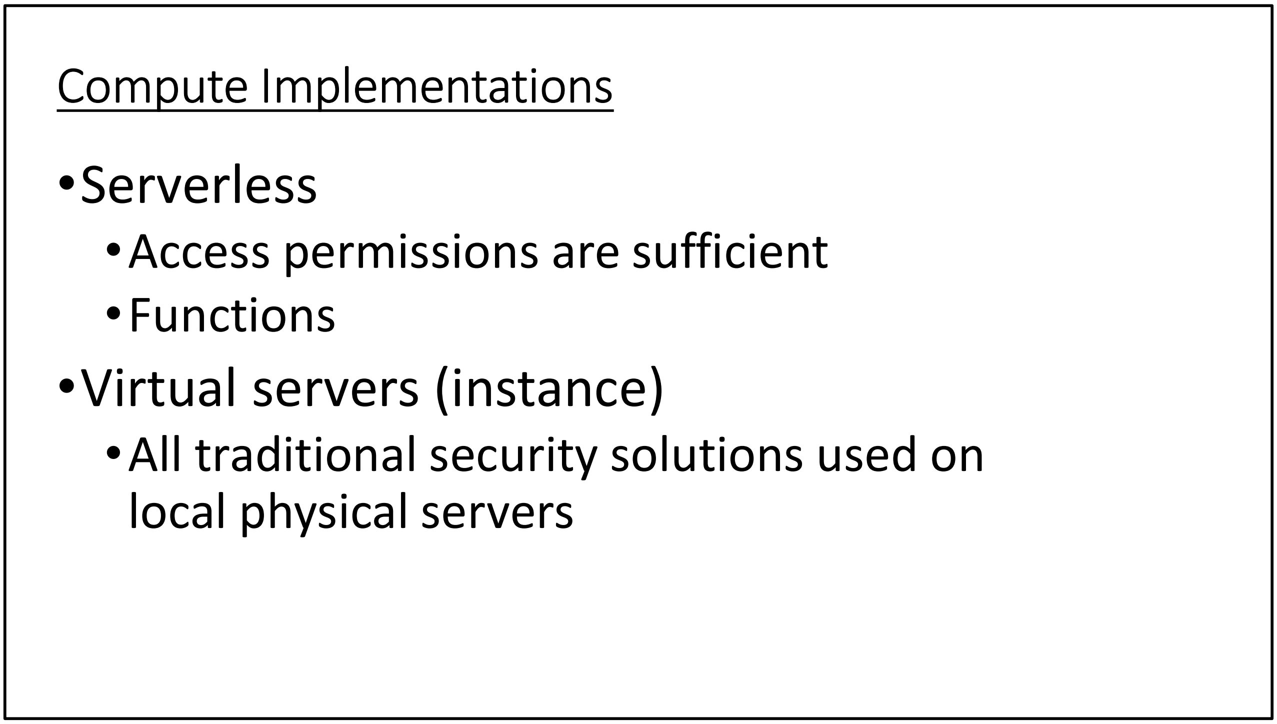
## Common Ciphers

- Advanced Encryption Standard (AES)
  - Block
- RC4
  - Streaming
- Symmetric ciphers
  - Same key to encrypt and decrypt
- Asymmetric ciphers
  - Separate keys to encrypt and decrypt
  - Public key and private key
  - Public key cryptography
    - Implements asymmetric ciphers
    - Validates the sender’s identity
    - May require a Public Key Infrastructure (PKI)



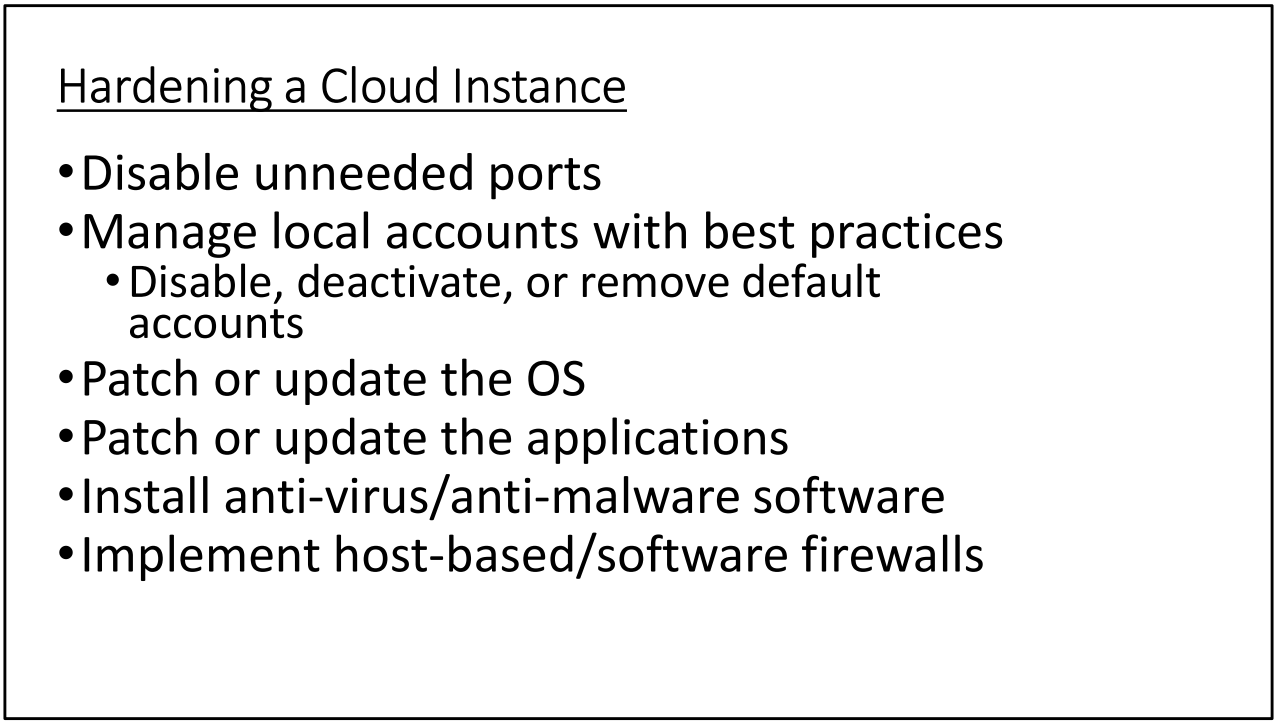
## 6.07 Compute Security (Demo)

CH06: Cloud Security



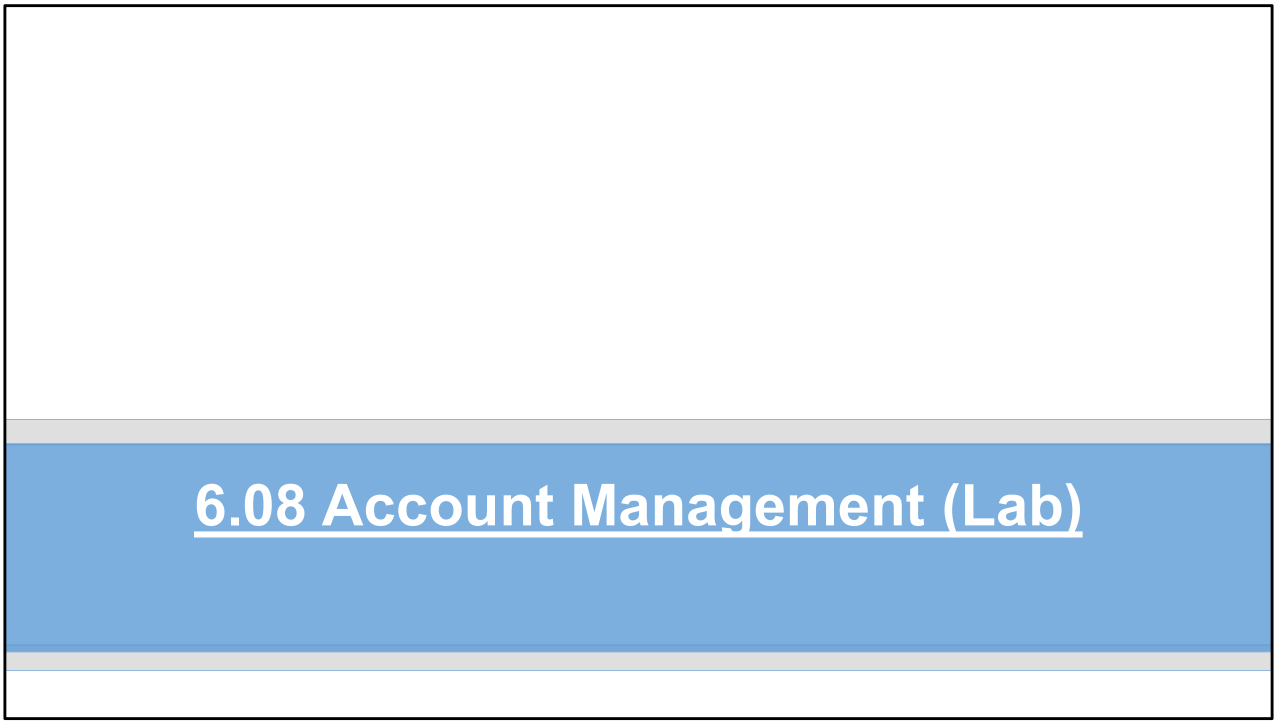
Compute Implementations

- Serverless
  - Access permissions are sufficient
  - Functions
- Virtual servers (instance)
  - All traditional security solutions used on local physical servers

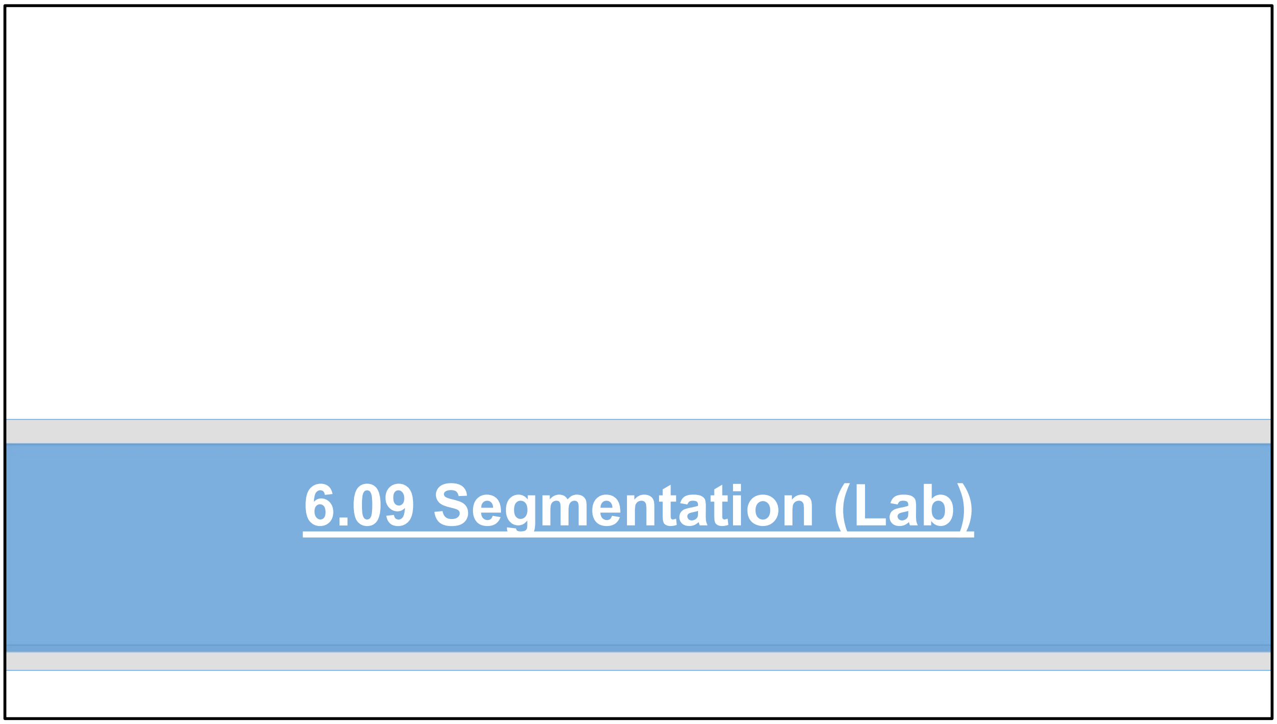


## Hardening a Cloud Instance

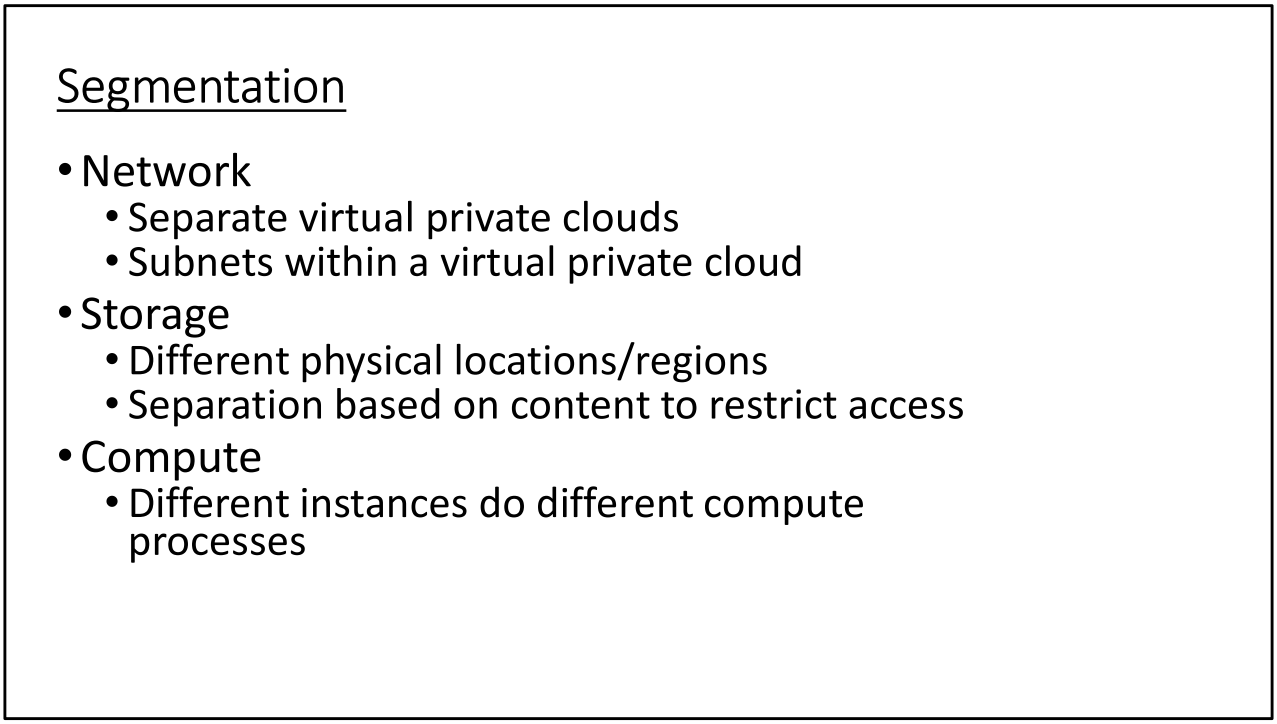
- Disable unneeded ports
- Manage local accounts with best practices
  - Disable, deactivate, or remove default accounts
- Patch or update the OS
- Patch or update the applications
- Install anti-virus/anti-malware software
- Implement host-based/software firewalls



# 6.08 Account Management (Lab)



## 6.09 Segmentation (Lab)

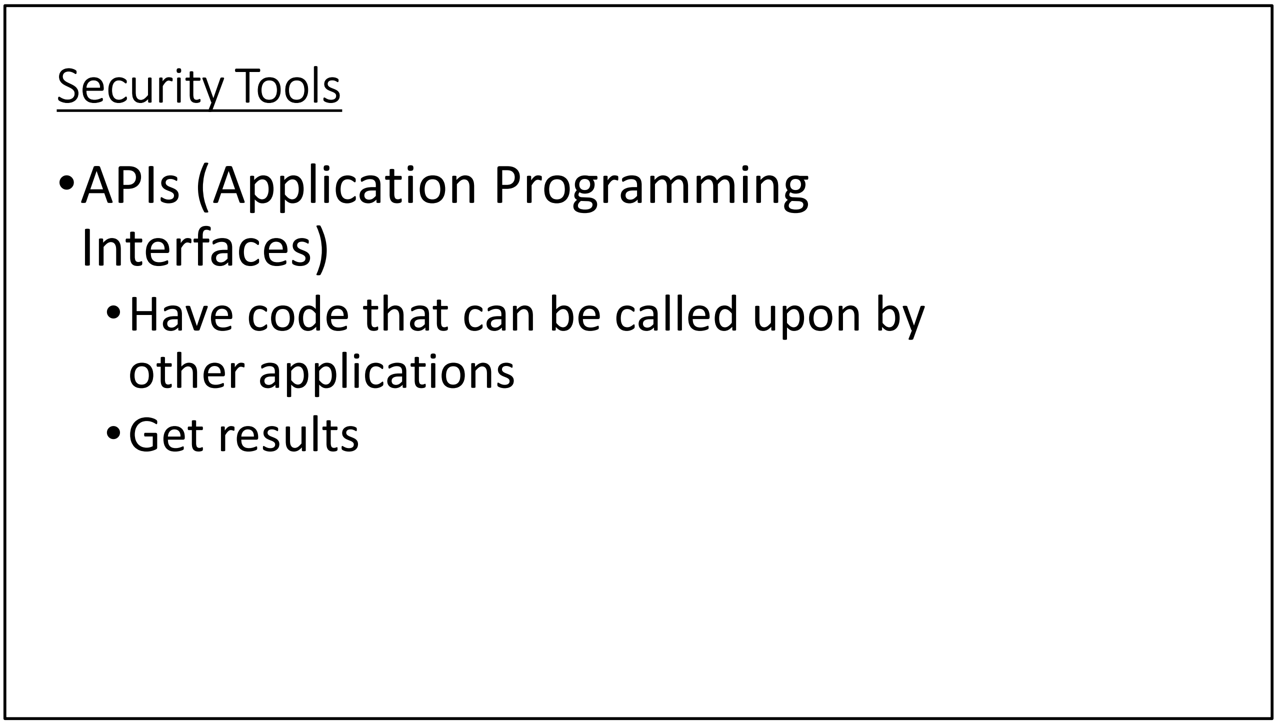


## Segmentation

- Network
  - Separate virtual private clouds
  - Subnets within a virtual private cloud
- Storage
  - Different physical locations/regions
  - Separation based on content to restrict access
- Compute
  - Different instances do different compute processes

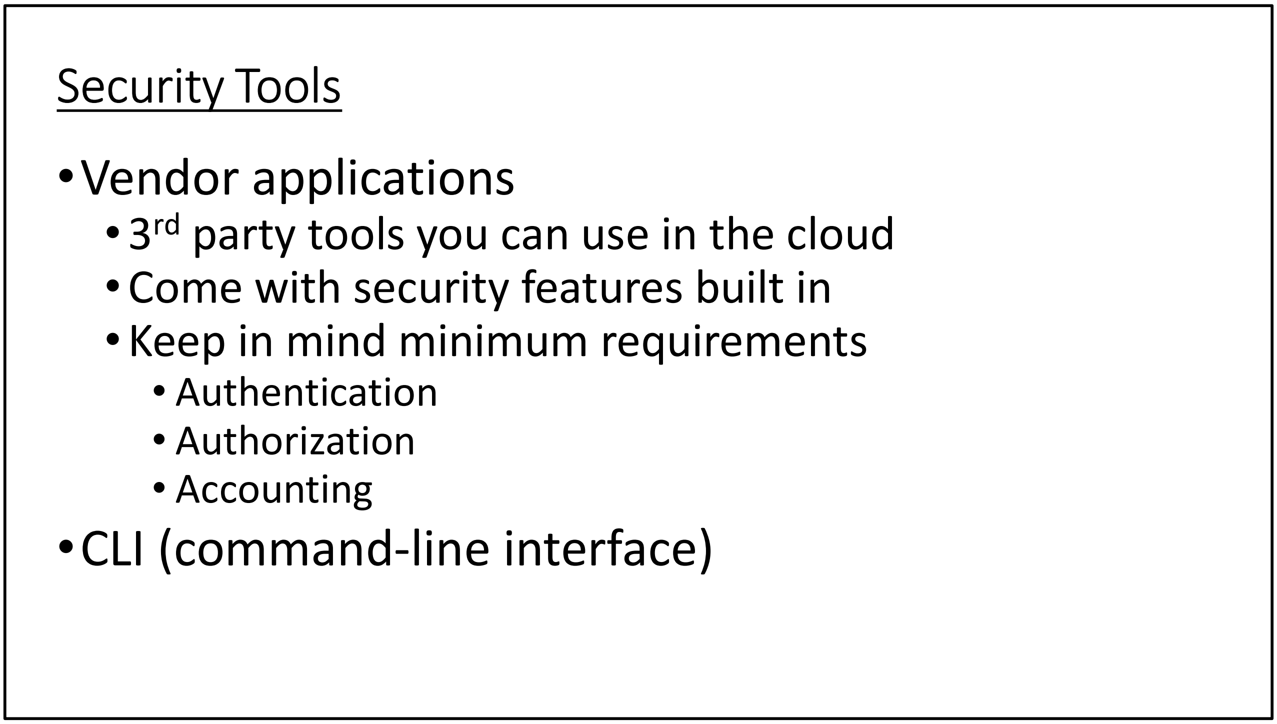
# 6.10 Security Tools (Demo)

CH06: Cloud Security



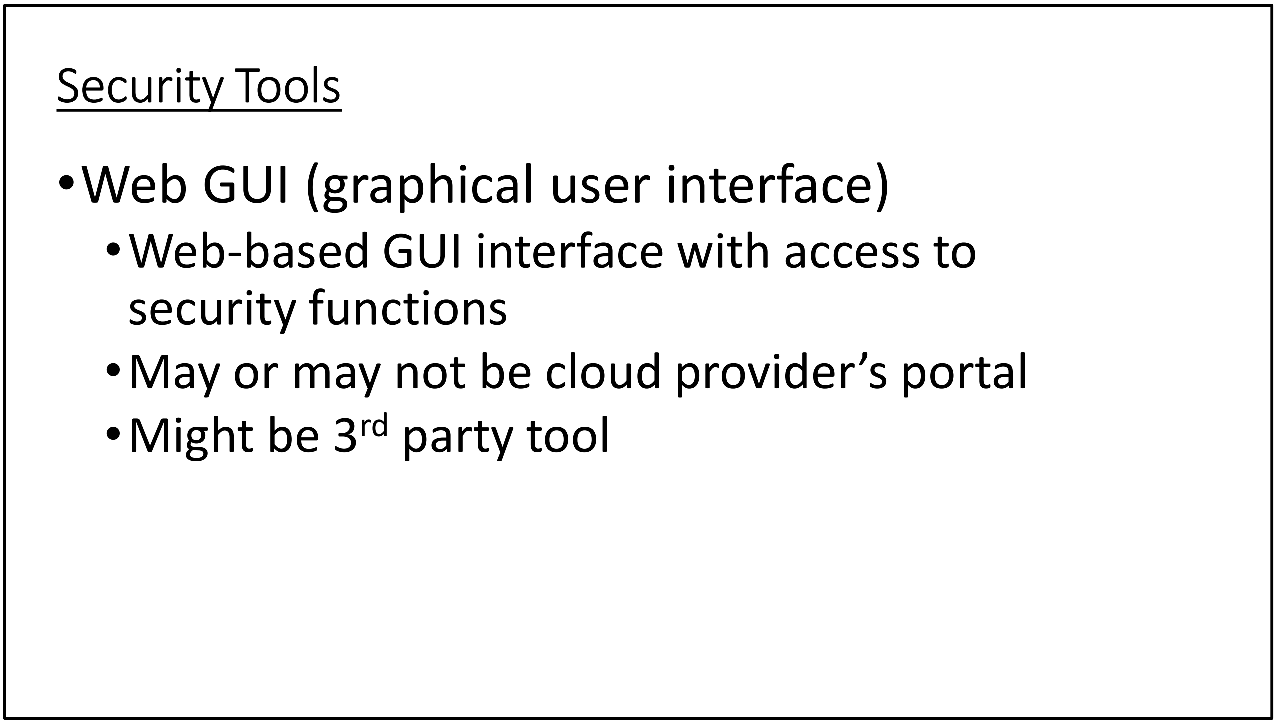
## Security Tools

- APIs (Application Programming Interfaces)
  - Have code that can be called upon by other applications
  - Get results



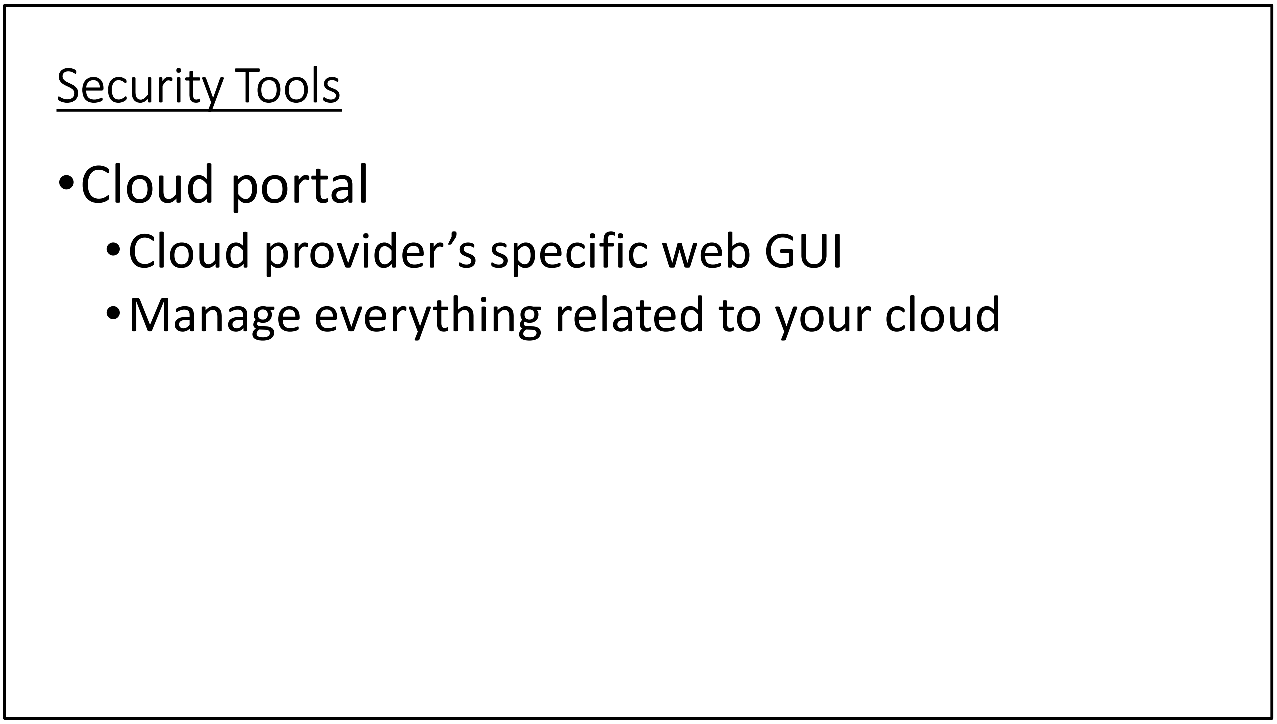
## Security Tools

- Vendor applications
  - 3rd party tools you can use in the cloud
  - Come with security features built in
  - Keep in mind minimum requirements
    - Authentication
    - Authorization
    - Accounting
- CLI (command-line interface)



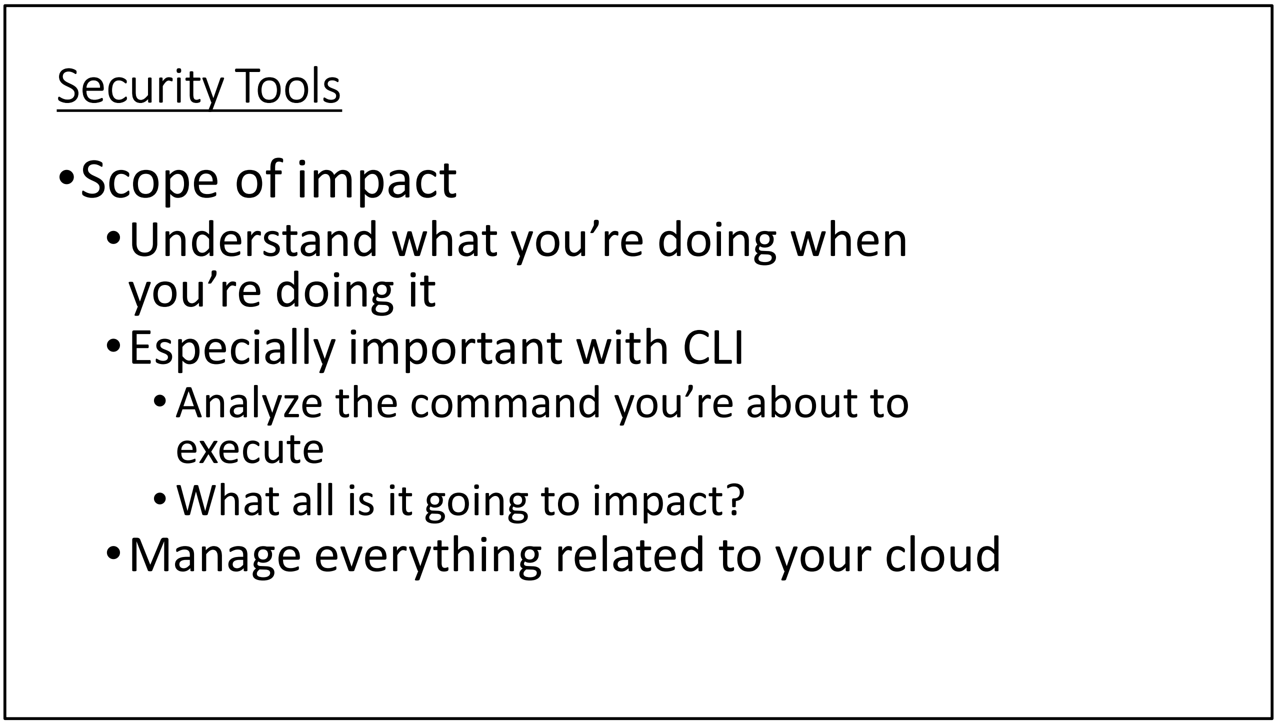
## Security Tools

- Web GUI (graphical user interface)
  - Web-based GUI interface with access to security functions
  - May or may not be cloud provider’s portal
  - Might be 3rd party tool



## Security Tools

- Cloud portal
  - Cloud provider’s specific web GUI
  - Manage everything related to your cloud

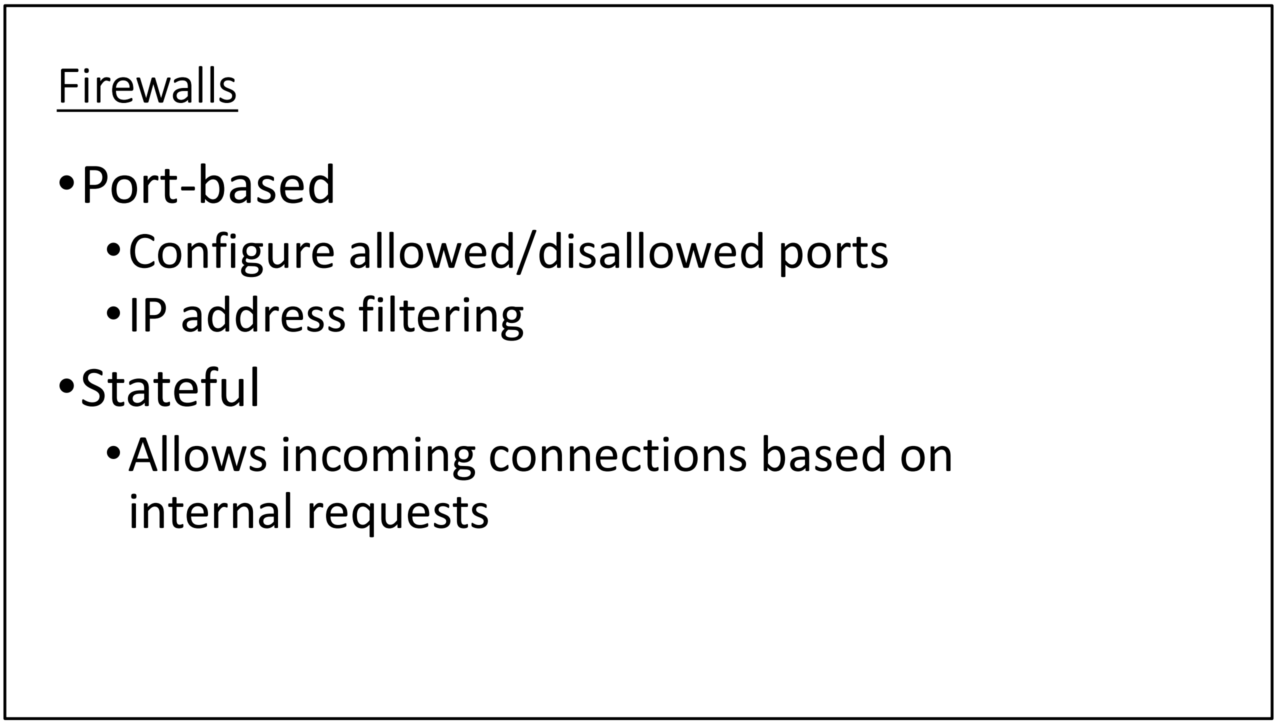


## Security Tools

- Scope of impact
  - Understand what you’re doing when you’re doing it
  - Especially important with CLI
    - Analyze the command you’re about to execute
    - What all is it going to impact?
  - Manage everything related to your cloud

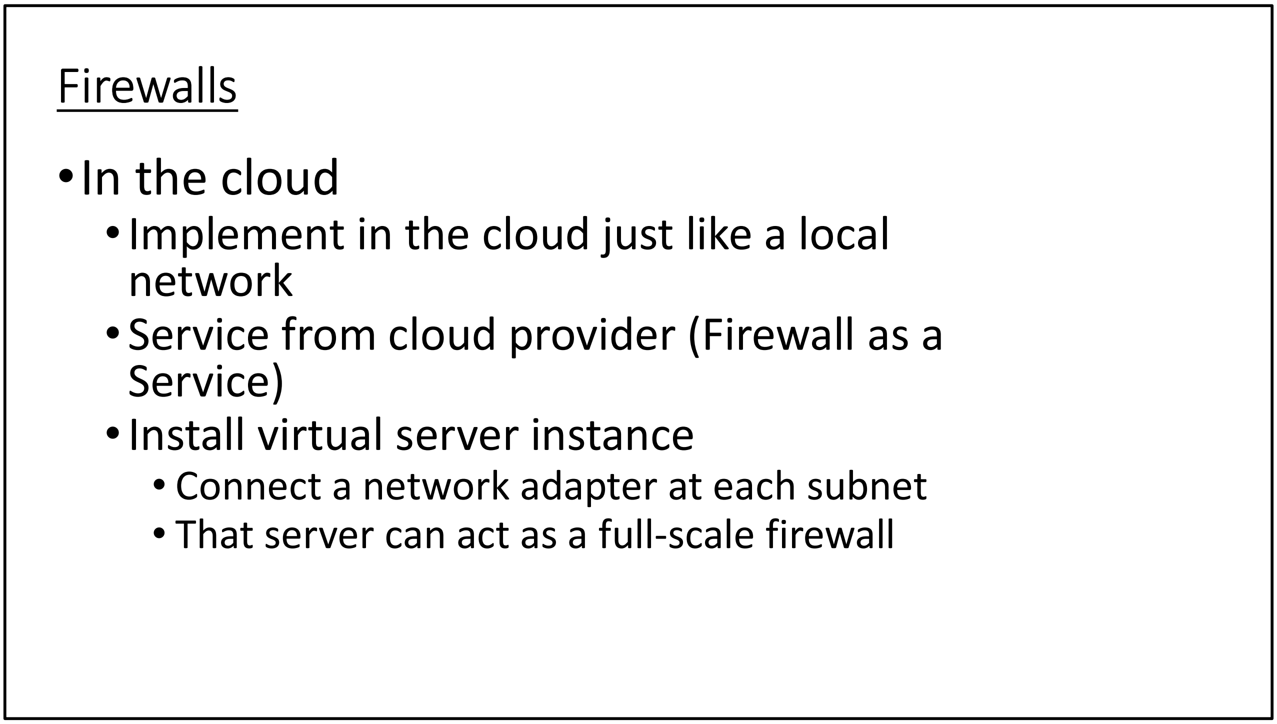
## 6.11 Security Services

CH06: Cloud Security



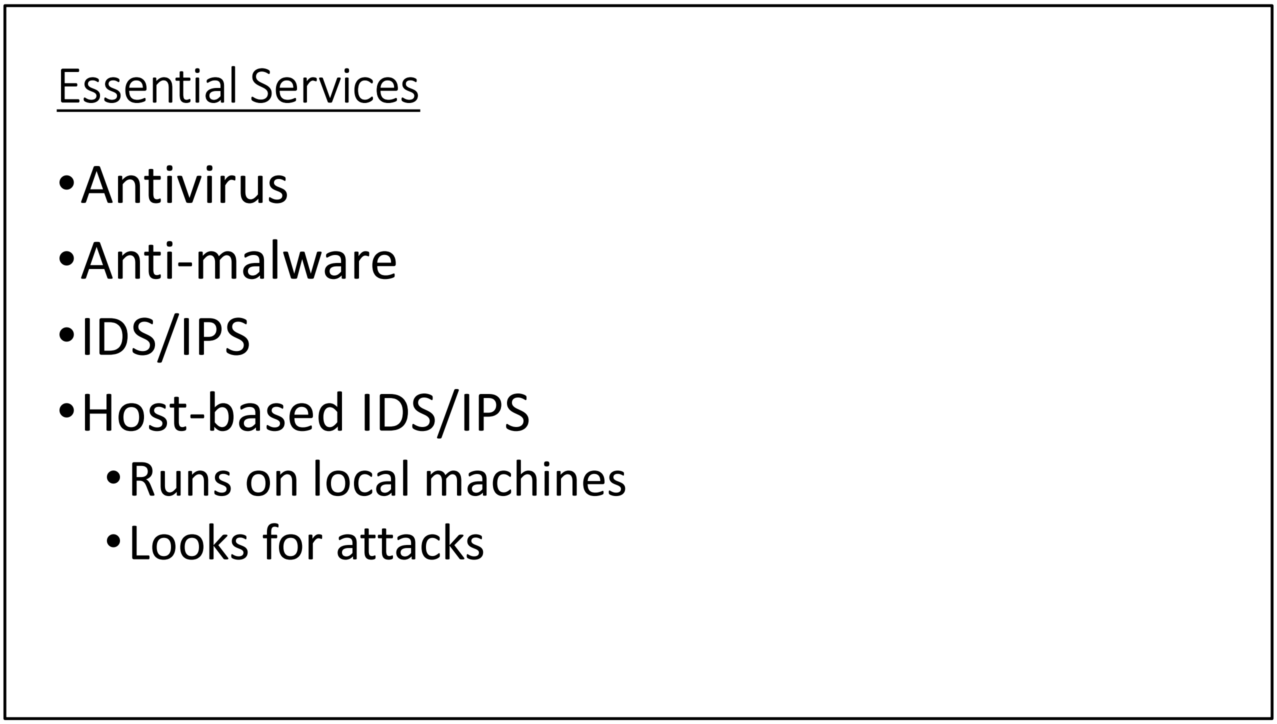
## Firewalls

- Port-based
  - Configure allowed/disallowed ports
  - IP address filtering
- Stateful
  - Allows incoming connections based on internal requests



## Firewalls

- In the cloud
  - Implement in the cloud just like a local network
  - Service from cloud provider (Firewall as a Service)
  - Install virtual server instance
    - Connect a network adapter at each subnet
    - That server can act as a full-scale firewall

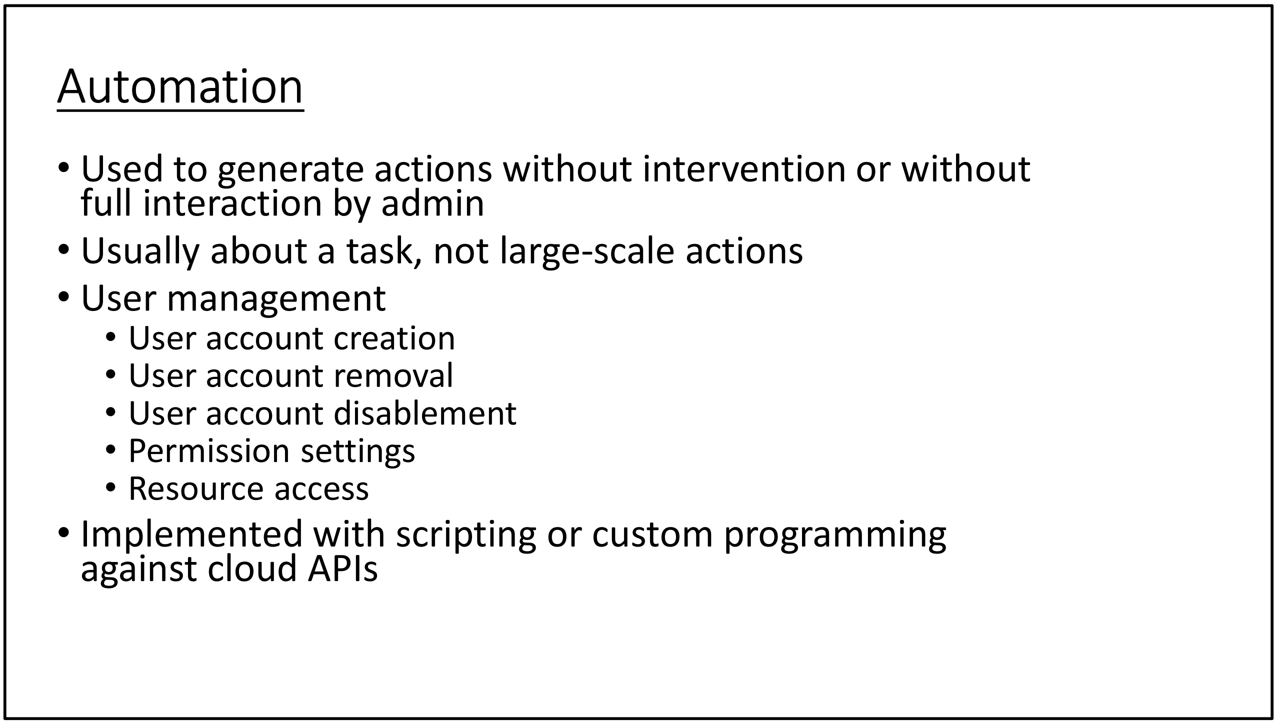


## Essential Services

- Antivirus
- Anti-malware
- IDS/IPS
- Host-based IDS/IPS
  - Runs on local machines
  - Looks for attacks

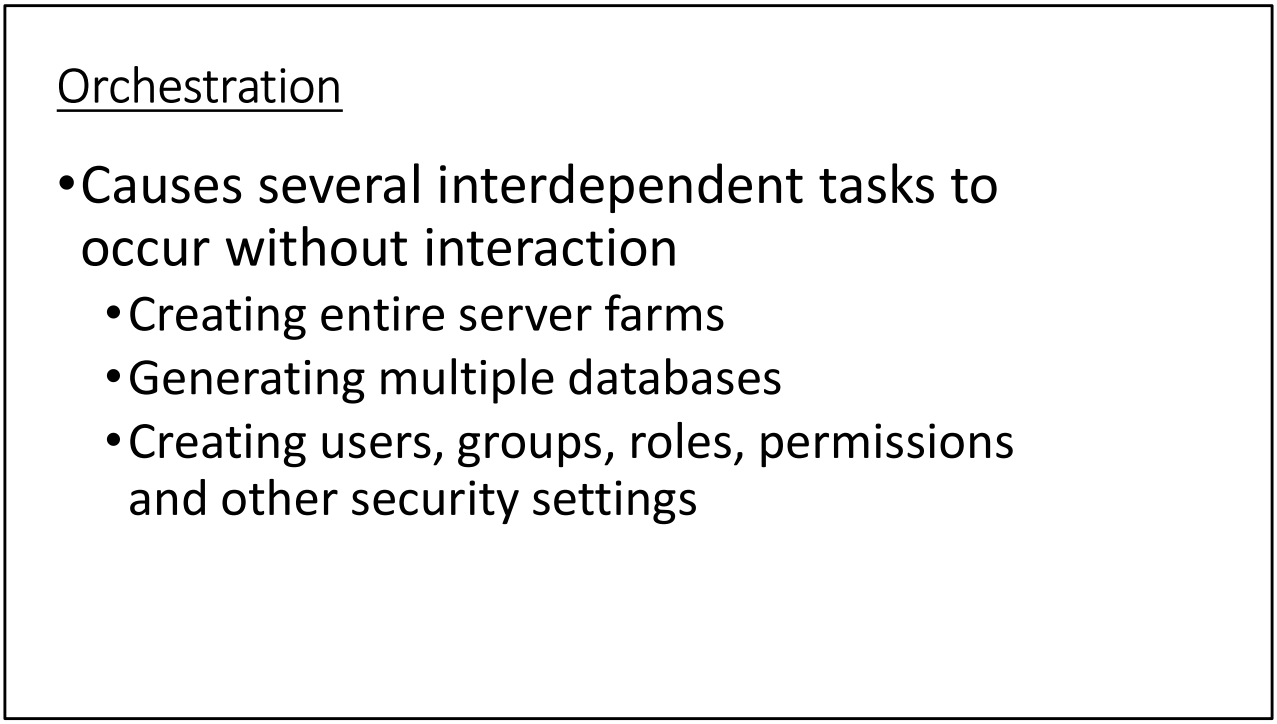
# 6.12 Security Automation and Orchestration

CH06: Cloud Security



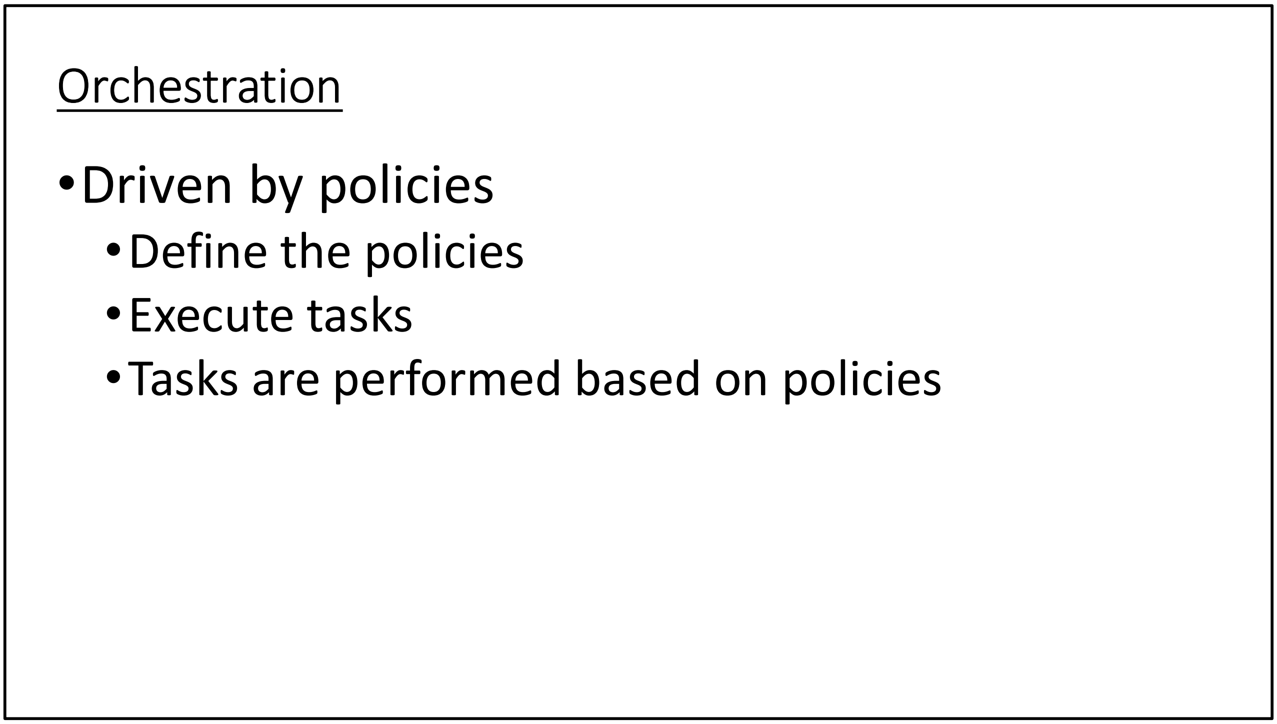
## Automation

- Used to generate actions without intervention or without full interaction by admin
- Usually about a task, not large-scale actions
- User management
    - User account creation
    - User account removal
    - User account disablement
    - Permission settings
    - Resource access
- Implemented with scripting or custom programming against cloud APIs



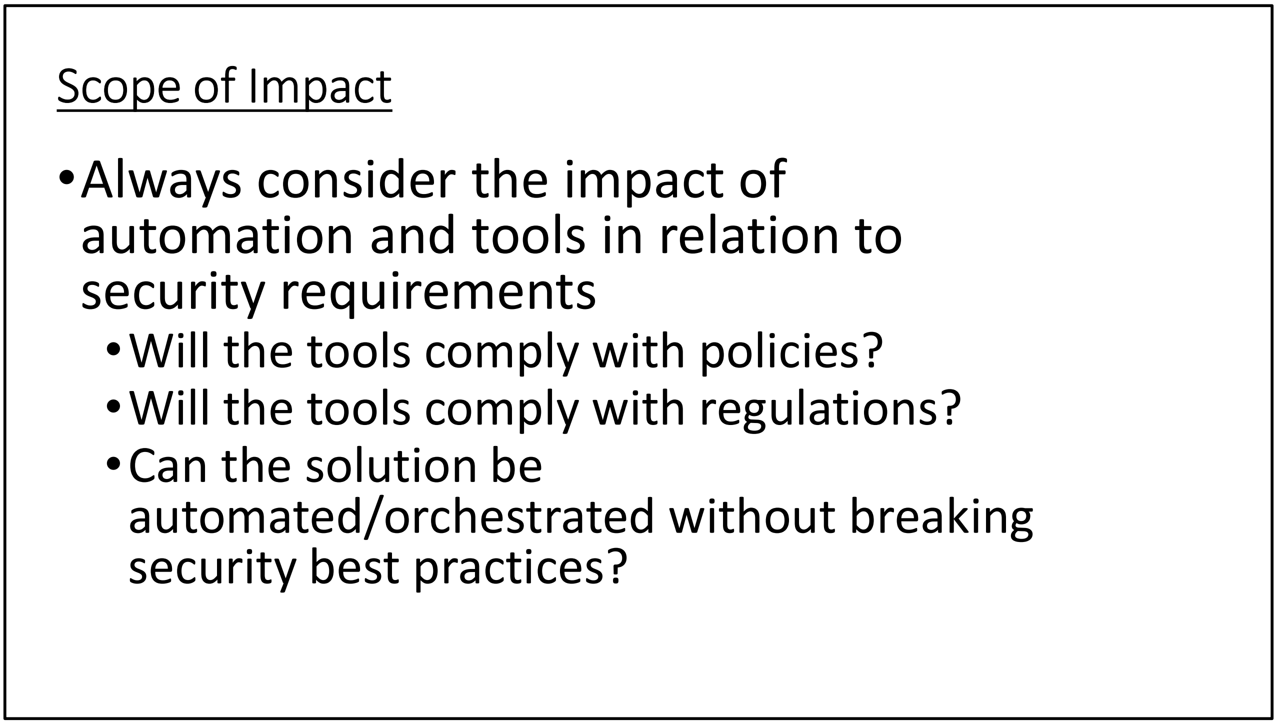
Orchestration

- Causes several interdependent tasks to occur without interaction
  - Creating entire server farms
  - Generating multiple databases
  - Creating users, groups, roles, permissions and other security settings



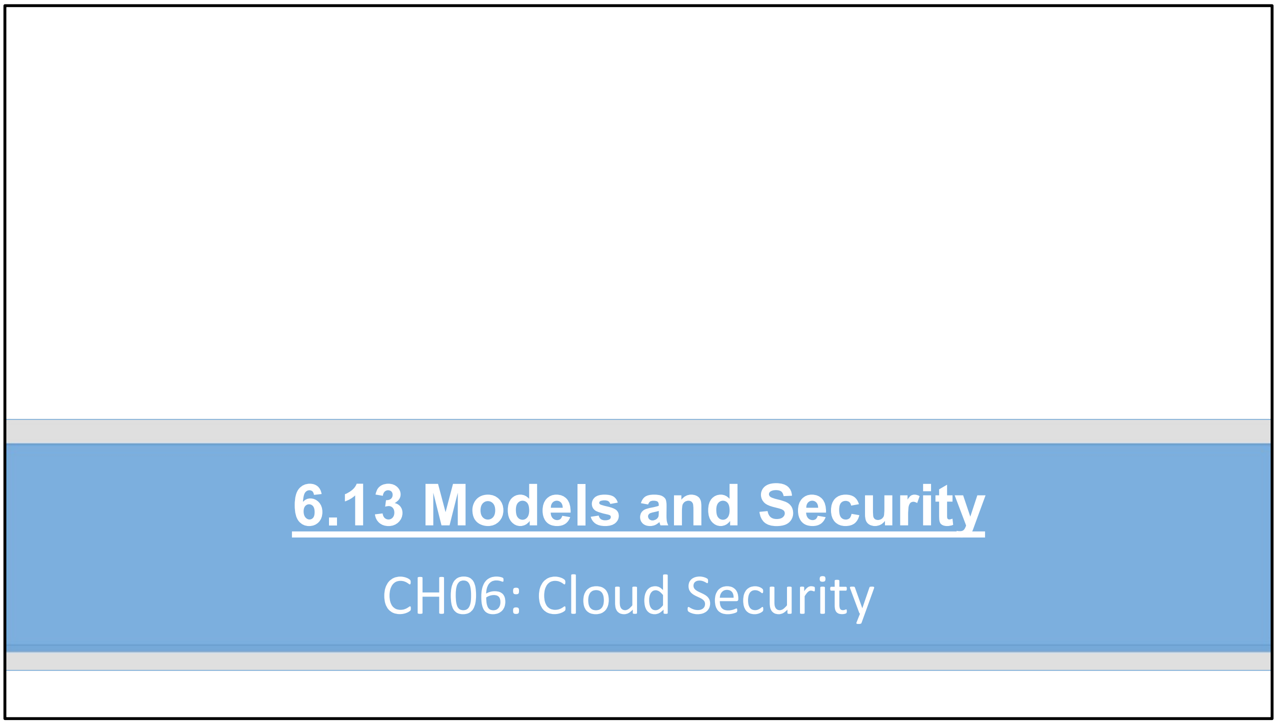
## Orchestration

- Driven by policies
  - Define the policies
  - Execute tasks
  - Tasks are performed based on policies



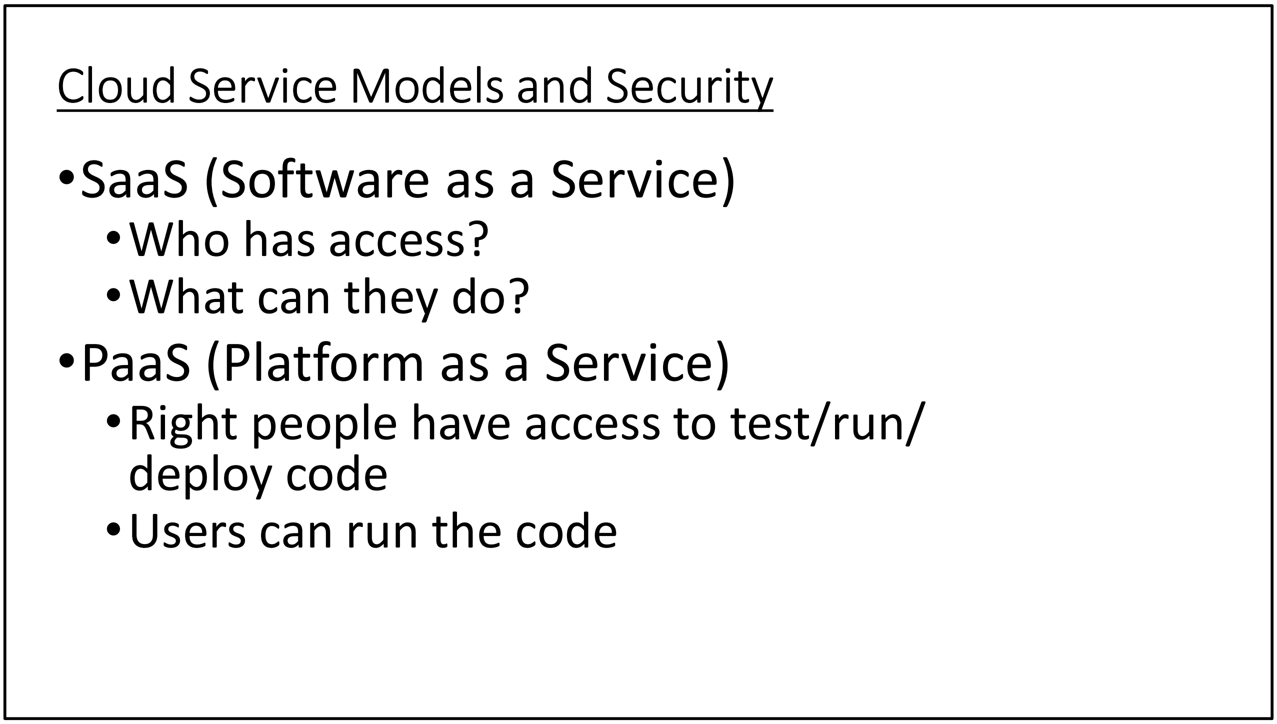
## Scope of Impact

- Always consider the impact of automation and tools in relation to security requirements
  - Will the tools comply with policies?
  - Will the tools comply with regulations?
  - Can the solution be automated/orchestrated without breaking security best practices?



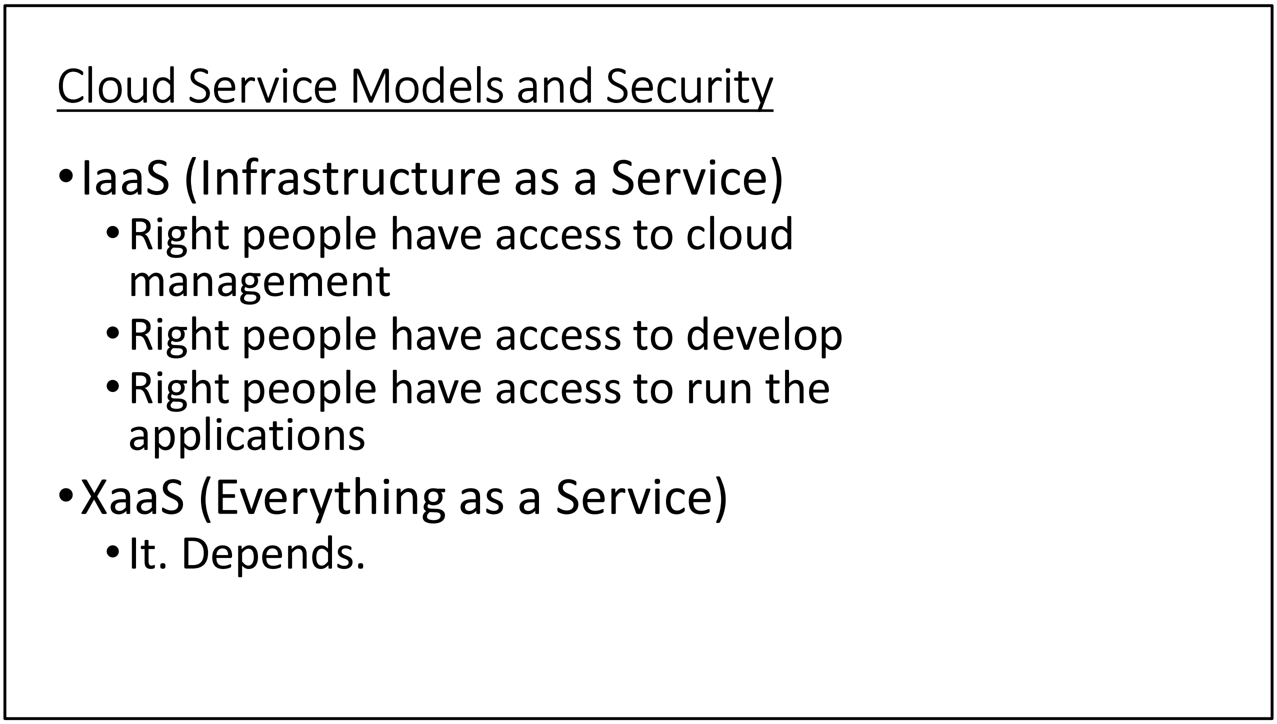
## 6.13 Models and Security

CH06: Cloud Security



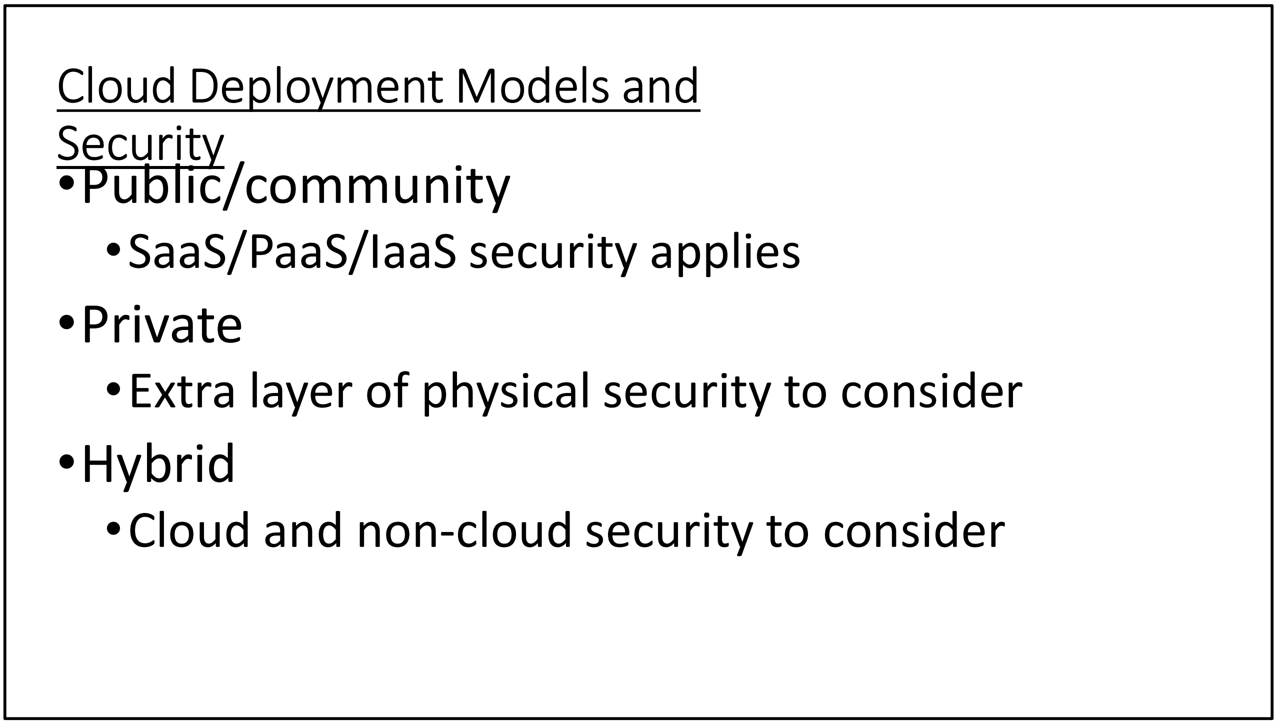
Cloud Service Models and Security

- SaaS (Software as a Service)
  - Who has access?
  - What can they do?
- PaaS (Platform as a Service)
  - Right people have access to test/run/ deploy code
  - Users can run the code



## Cloud Service Models and Security

- IaaS (Infrastructure as a Service)
  - Right people have access to cloud management
  - Right people have access to develop
  - Right people have access to run the applications
- XaaS (Everything as a Service)
  - It. Depends.



## Cloud Deployment Models and Security

- Public/community
  - SaaS/PaaS/IaaS security applies
- Private
  - Extra layer of physical security to consider
- Hybrid
  - Cloud and non-cloud security to consider