

NDE
Network Defense Essentials

Module 06

Virtualization and Cloud Computing

Module Objectives

01 Understanding Virtualization, its Components, and Virtualization Enablers

02 Understanding OS Virtualization Security and Concerns

03 Understanding the Best Practices for OS Virtualization Security

04 Understanding Cloud Computing and its Benefits

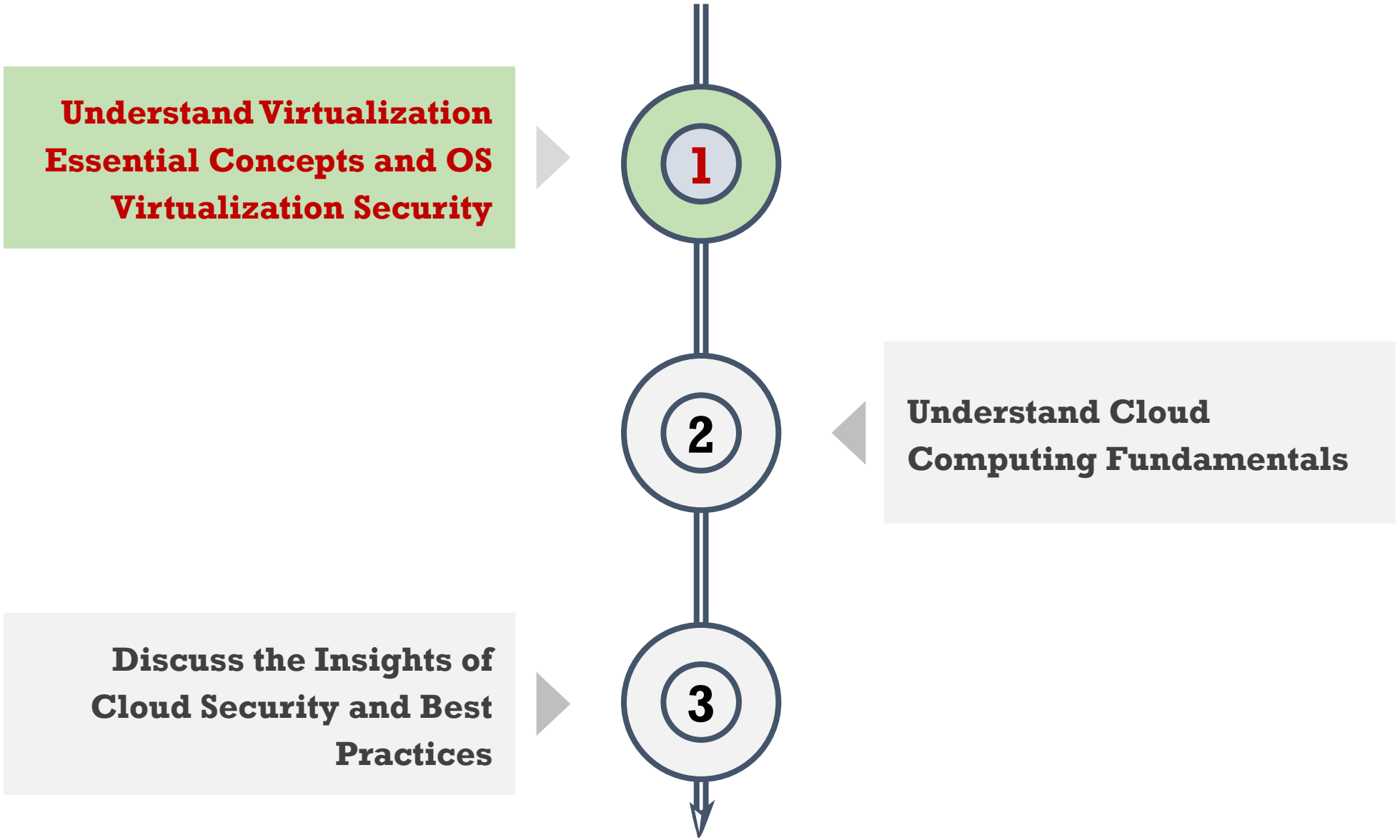
05 Overview of Different Types of Cloud Computing Services

06 Overview of Cloud Deployment Models

08 Understanding Importance of Cloud Security and its Best Practices



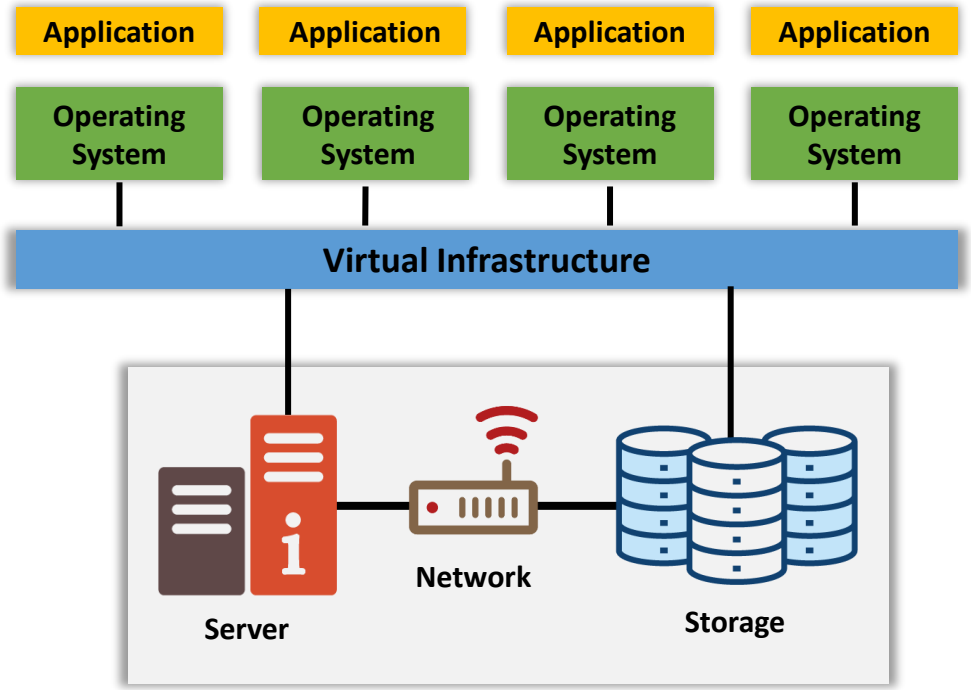
Module Flow


Understand Virtualization Essential Concepts and OS Virtualization Security
1
2
Understand Cloud Computing Fundamentals
Discuss the Insights of Cloud Security and Best Practices
3

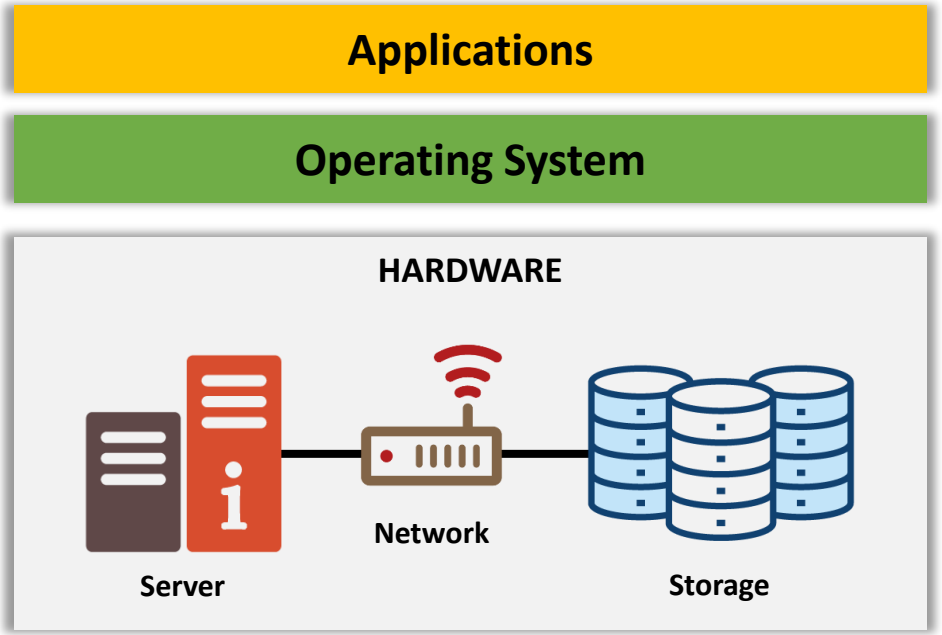
Virtualization

- Virtualization refers to a software-based virtual representation of an IT infrastructure that includes network, devices, applications, storage, etc.
- The virtualization framework divides the **physical resources** which are traditionally bound to hardware, into **multiple individual simulated environments**

Virtual Architecture



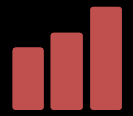
Traditional Architecture



Virtualization (Cont'd)



Virtualization Approaches



Levels of Virtualization



Types of Virtualization

Virtualization Components

01

Hypervisor / Virtual Machine Monitor

- An **application** or **firmware** that enables multiple guest operating systems to share a host's hardware resources

02

Guest Machine / Virtual Machine

- **Independent** instance of an operating system created by virtual machine monitor

03

Host Machine / Physical Machine

- **Real physical machine** that provides computing resources to support virtual machines

04

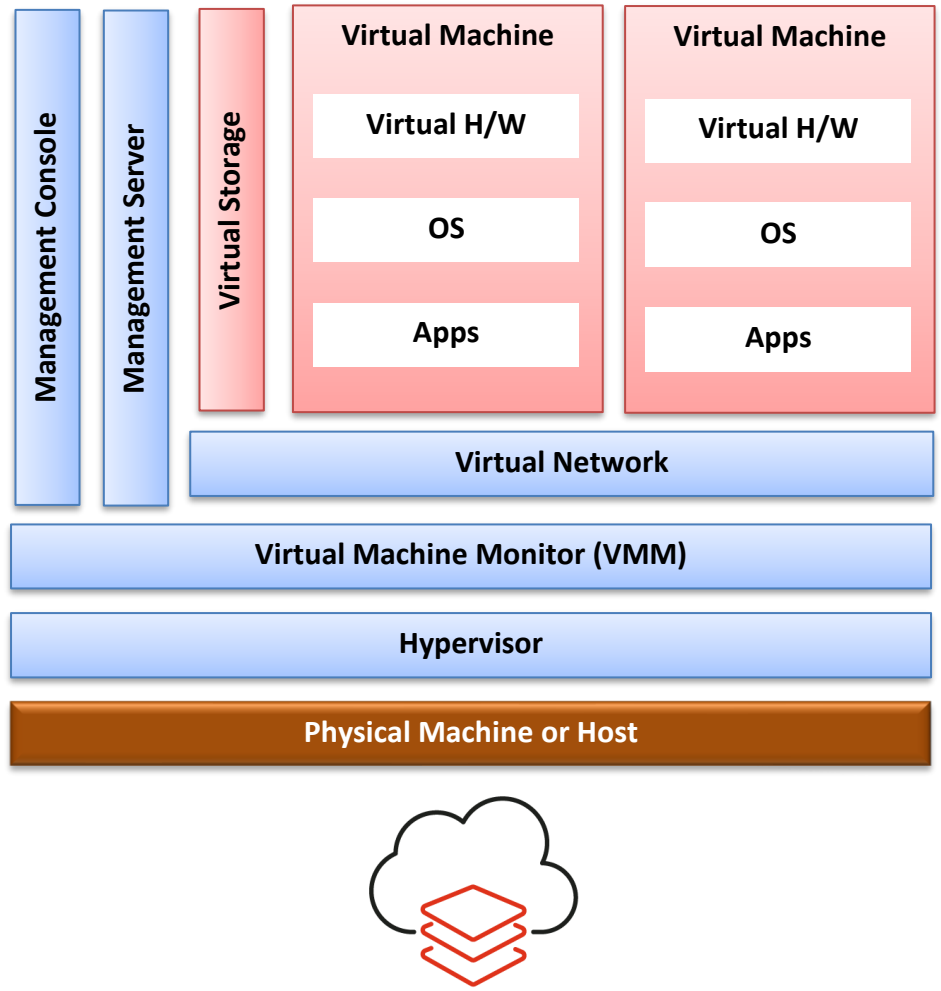
Management Server

- **Virtualization platform** components used to directly manage the virtual machines

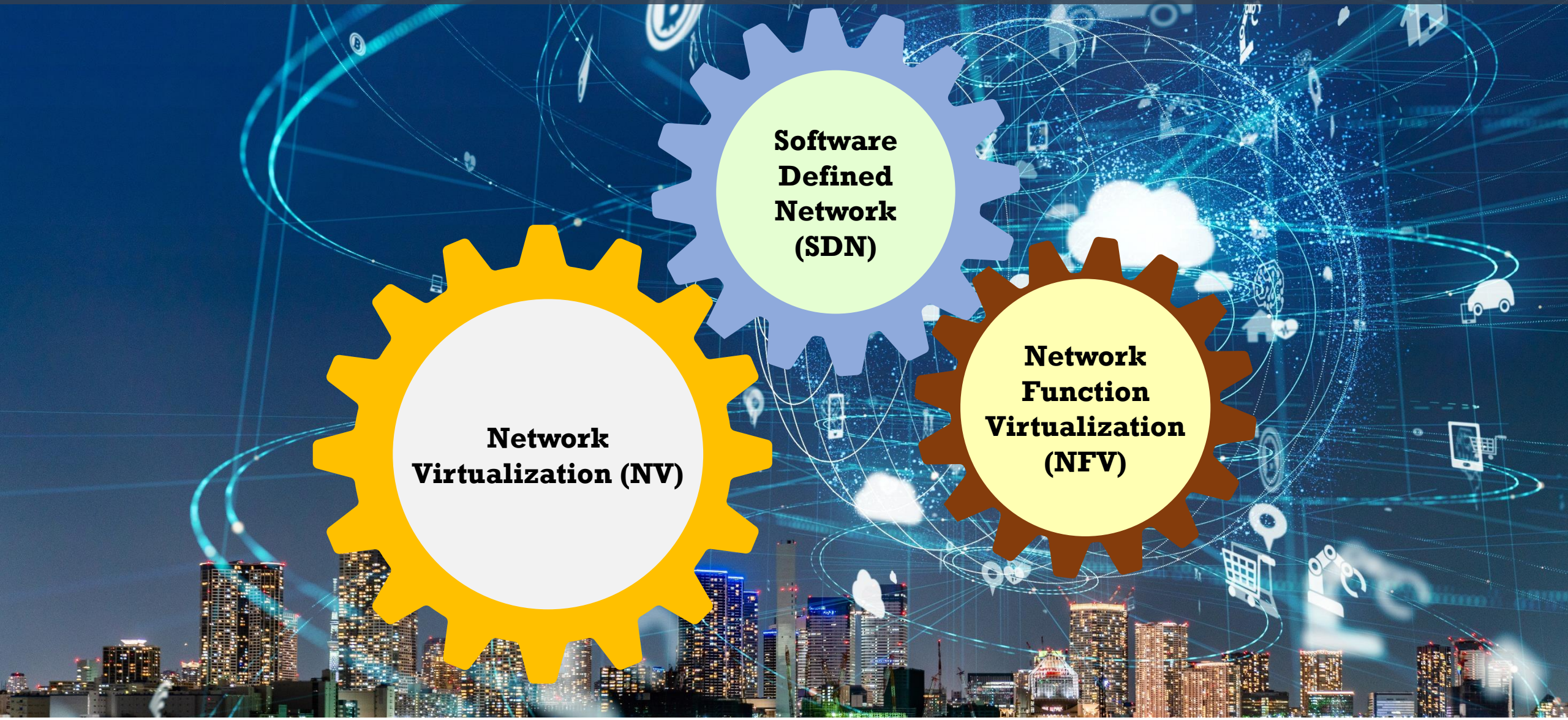
05

Management Console

- **Interface** used to access, configure, and manage the virtualization product



Virtualization Enablers



Common Virtualization Vendors



VMware ESXi
(*https://www.vmware.com*)



Citrix Hypervisor
(*https://www.citrix.com*)



Virtual Iron
(*https://www.oracle.com*)



Microsoft Hyper-V Server
(*https://www.microsoft.com*)



VirtualBox
(*https://www.virtualbox.org*)



OS Virtualization Security and Concerns

Container

- Virtualization based on an **operating system**, in which the kernel's operating system functionality is replicated on multiple instances of isolated user space, called **containers**, **software containers** or **virtualization engines**
- Containers as a service (CaaS) includes the virtualization of containers and container management through **orchestrators**
- Using CaaS, subscribers can develop rich, scalable containerized applications through the cloud or on-site data centers

Container Engine

- Managed environment for deploying containerized applications

Container Orchestration

- An automated process of managing the lifecycles of software containers and their dynamic environment

Container Orchestration Software



Docker Swarm



OPENSHIFT



Kubernetes

Container Technology Architecture

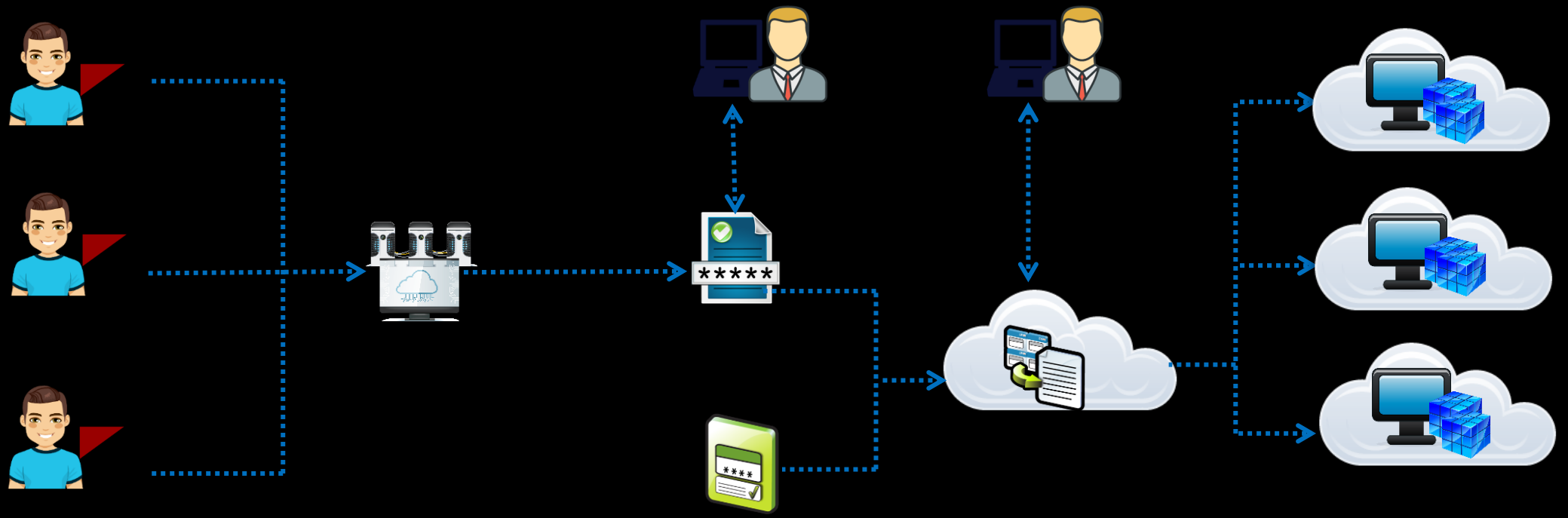


Image Creation, Testing and Accreditation

Storage and Retrieval of Image

Deployment and Management of Container

Types of Containers



OS Containers

multiple

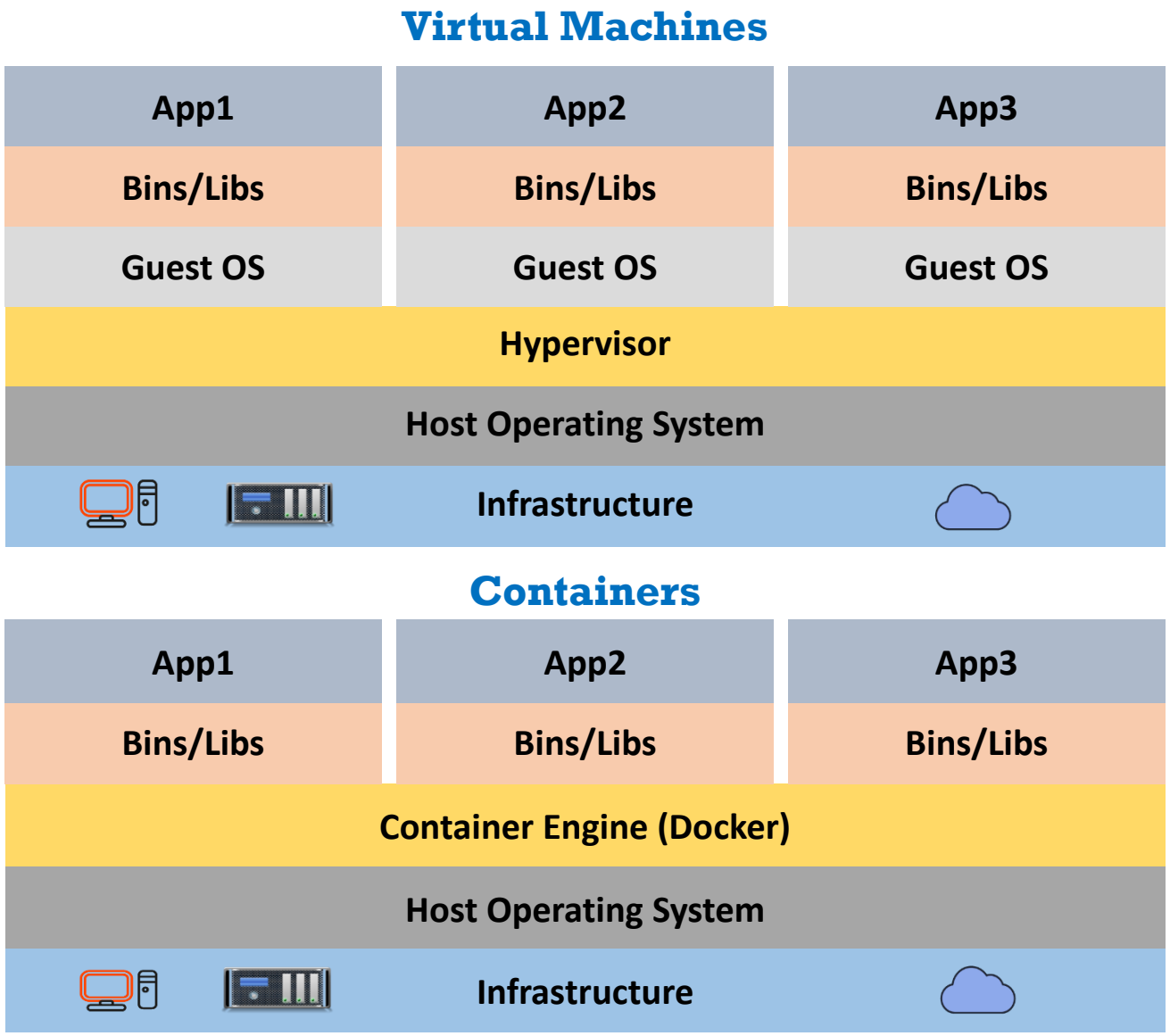


Application Containers

single

Containers v/s Virtual Machine

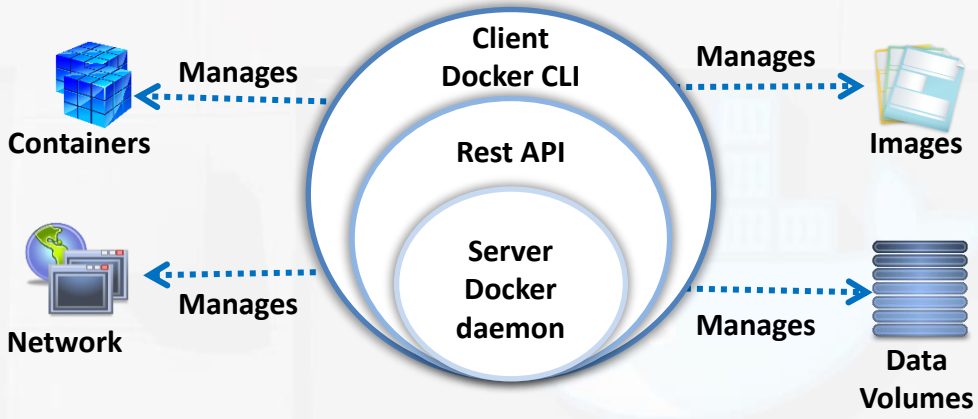
Container	Virtual Machine
Provides OS-level virtualization	Provides hardware-level virtualization
Lightweight	Heavyweight
All containers share the host OS	Each virtual machine runs in its own OS
Requires less memory space	Allocates required memory
Fully isolated (more secure)	Process-level isolation (less secure)
Example: LXC, LXD, CGManager, Docker	**Example**: VMWare, Hyper-V, vSphere, Virtual Box



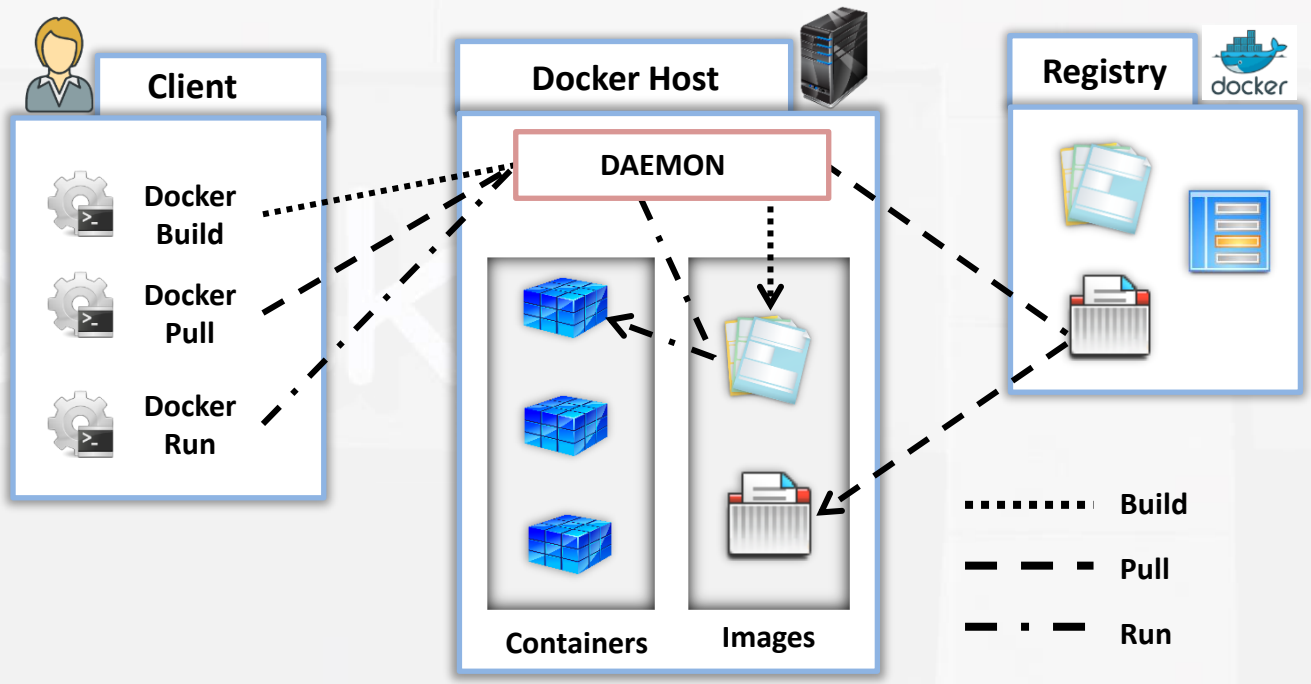
Docker

- Docker is an open source technology used for developing, packaging, and running applications and all its dependencies in the **form of containers**, to ensure that the application works in a seamless environment
- Docker provides a Platform-as-a-Service (PaaS) through **OS-level virtualization** and delivers containerized software packages

Docker Engine

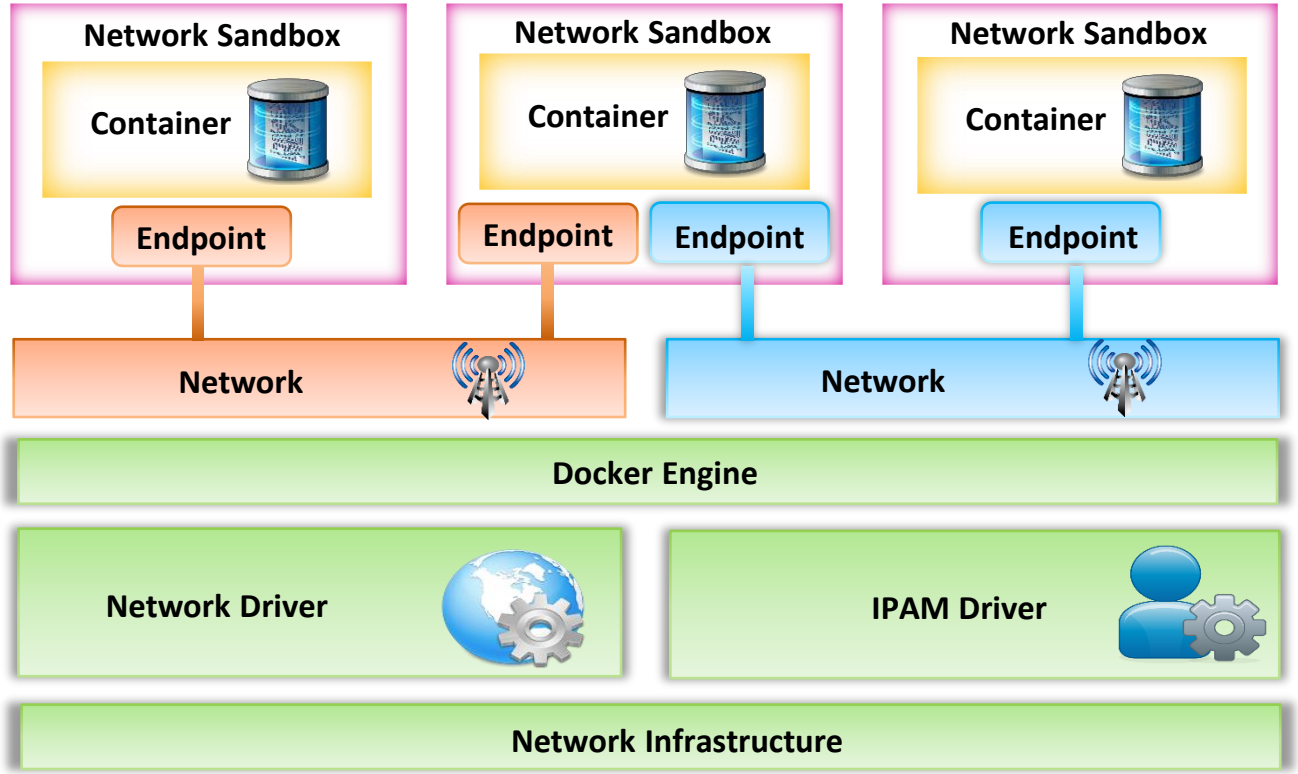


Docker Architecture



Docker Networking

- Docker **connects multiple containers** and services or other non-Docker workloads together
- The Docker networking architecture is developed on a set of interfaces known as the **Container Network Model** (CNM)
- The CNM provides application portability across heterogeneous infrastructures

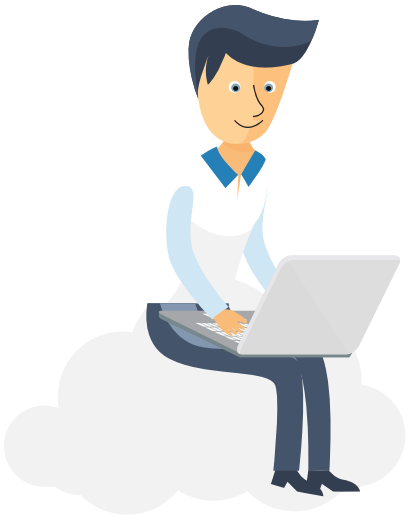


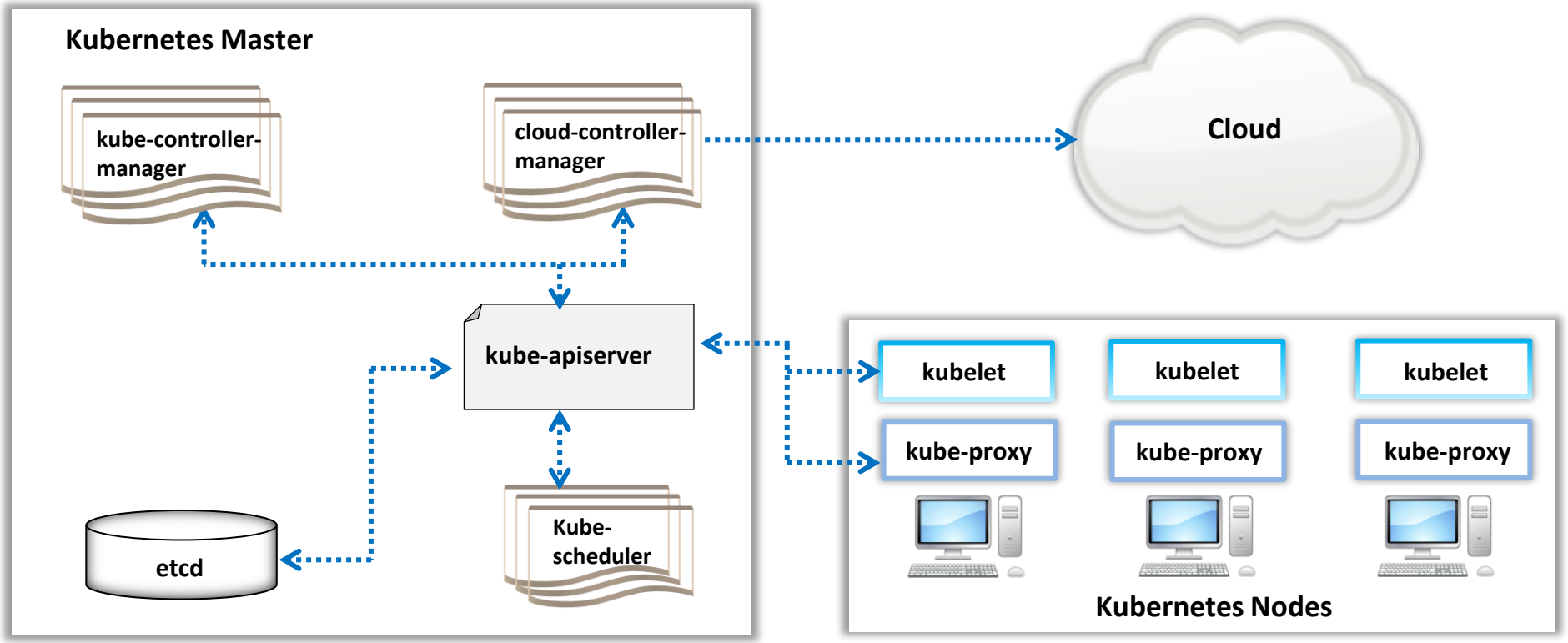


Kubernetes

- Kubernetes, also known as K8s, is an open-source, portable, extensible, orchestration platform developed by Google for **managing containerized applications** and microservices
- Kubernetes provides a **resilient framework** for managing distributed containers, generating deployment patterns, and performing failover and redundancy for the applications

Kubernetes Cluster Architecture





Container Security Challenges

1. Inflow of vulnerable source code
2. Large attack surface
3. Lack of visibility
4. Compromising secrets
5. DevOps speed
6. Noisy neighboring containers
7. Container breakout to the host
8. Network-based attacks
9. Bypassing isolation
10. Ecosystem complexity

Container Security Threats

Image Threats

- Image vulnerabilities
- Image **configuration defects**
- Embedded malware
- Embedded **clear text secrets**
- Use of untrusted images

Registry Threats

- **Insecure connections** to registries
- Stale images in registries
- **Insufficient authentication** and **authorization** restrictions

Container Threats

- Vulnerabilities within the **runtime software**
- Unbounded **network access** from containers
- Insecure container runtime configurations
- App vulnerabilities
- Rogue containers

Container Security Threats (Cont'd)

Orchestrator Threats

- Unbounded **administrative access**
- Unauthorized access
- Poorly separated inter-container network traffic
- Mixing of **workload sensitivity levels**
- Orchestrator node trust



Host OS Threats

- Large attack surface
- Shared kernel
- Host OS **component vulnerabilities**
- Improper user access rights
- Host OS **file system tampering**

Docker Security Threats



Escaping

Gaining of root access

Cross-Container Attacks

DDoS Attacks

unpatched exploits

Inter-Container Attacks

unauthorized access

Docker Registry Attacks

docker registry

Kubernetes Security Challenges and Threats

01

Explosion of east-west traffic

02

Increased attack surface

03

Automating security to keep pace

04

Too many containers

05

Communication between containers

06

Default configuration settings

07

Runtime security challenges

08

Compliance issues

OS Virtualization Security Best Practices

Best Practices for Container Security

1

Regularly **monitor the CVEs** of the container runtime and remediate, if any vulnerabilities are detected

2

Employ **app-aware tools** to monitor container network interfaces, network traffic, and network anomalies

3

Configure applications to **run as normal users** to prevent privilege escalation

4

Configure the **host's root file system in read-only mode** to restrict the write access

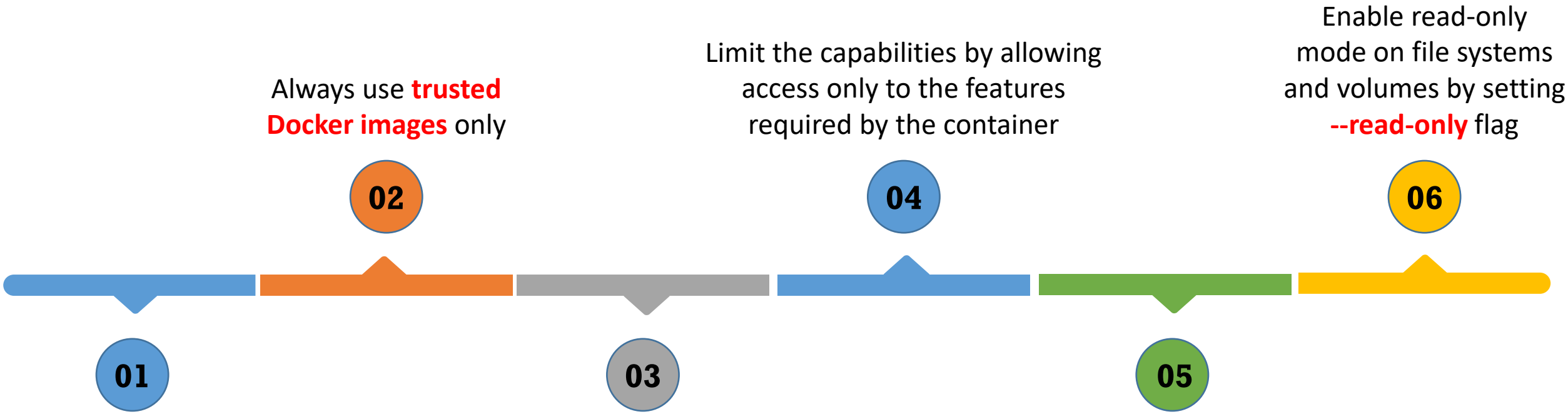
5

Employ **application security scanning tools** to protect containers from malicious software

6

Perform regular **scanning of the images** in the repository to identify vulnerabilities or misconfigurations

Best Practices for Docker Security



Best Practices for Kubernetes Security

01 Ensure proper validation of **file contents** and their path at every stage of processing

02 Implement the **configuration method** for the credential paths

03 Raise errors explicitly after each step of a **compound operation**

04 Use the well-tested JSON library and type structures for constructing JSON objects

05 Never use compound shell commands without proper validations

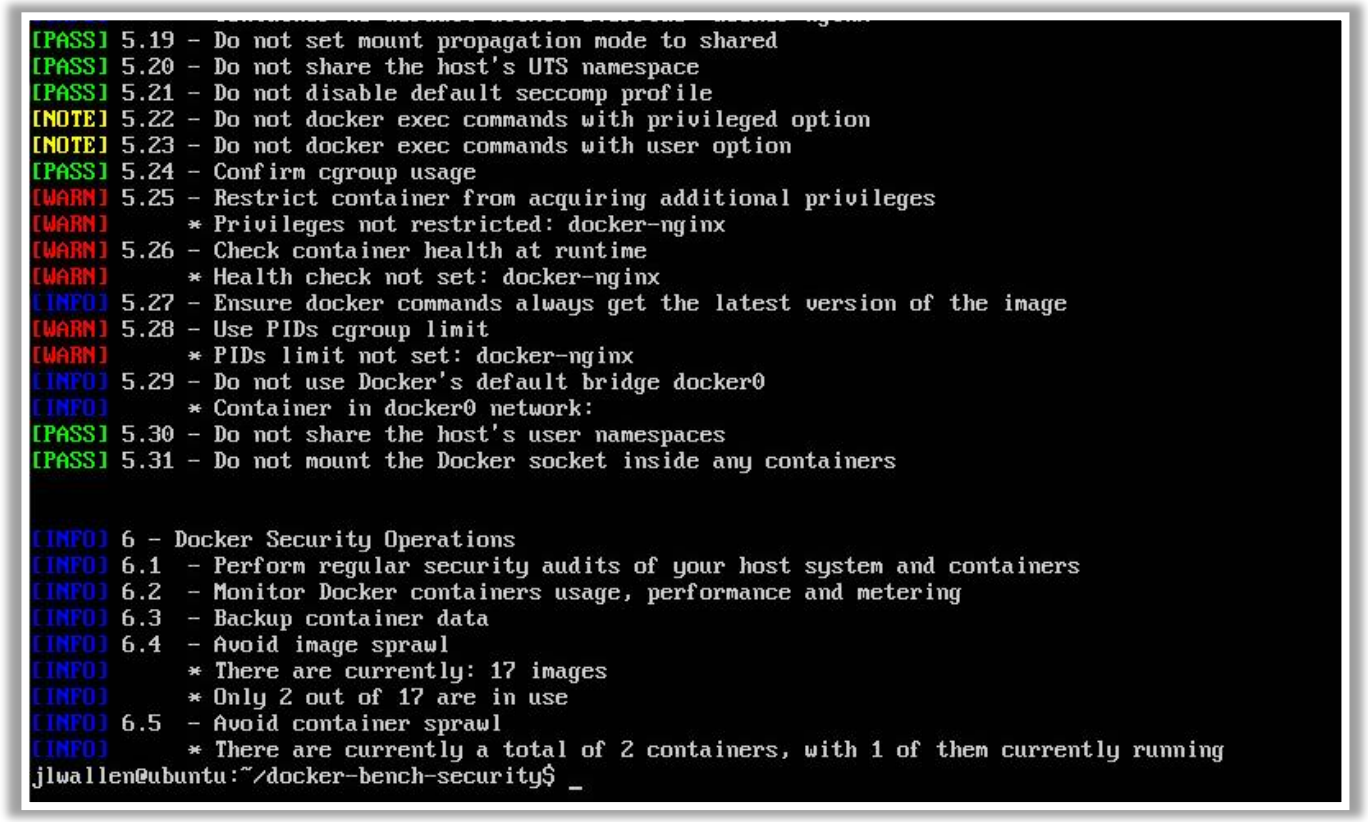
06 Use common parsing functions such as ParsePort across the codebase to **increase code readability**

Docker Security Tools

Docker Bench for Security

A script that enables checking:

- Host Configuration
- Docker Daemon Configuration
- Docker Daemon Configuration Files
- Container Images and Build Files
- Container Runtime



https://github.com

Twistlock
https://github.com

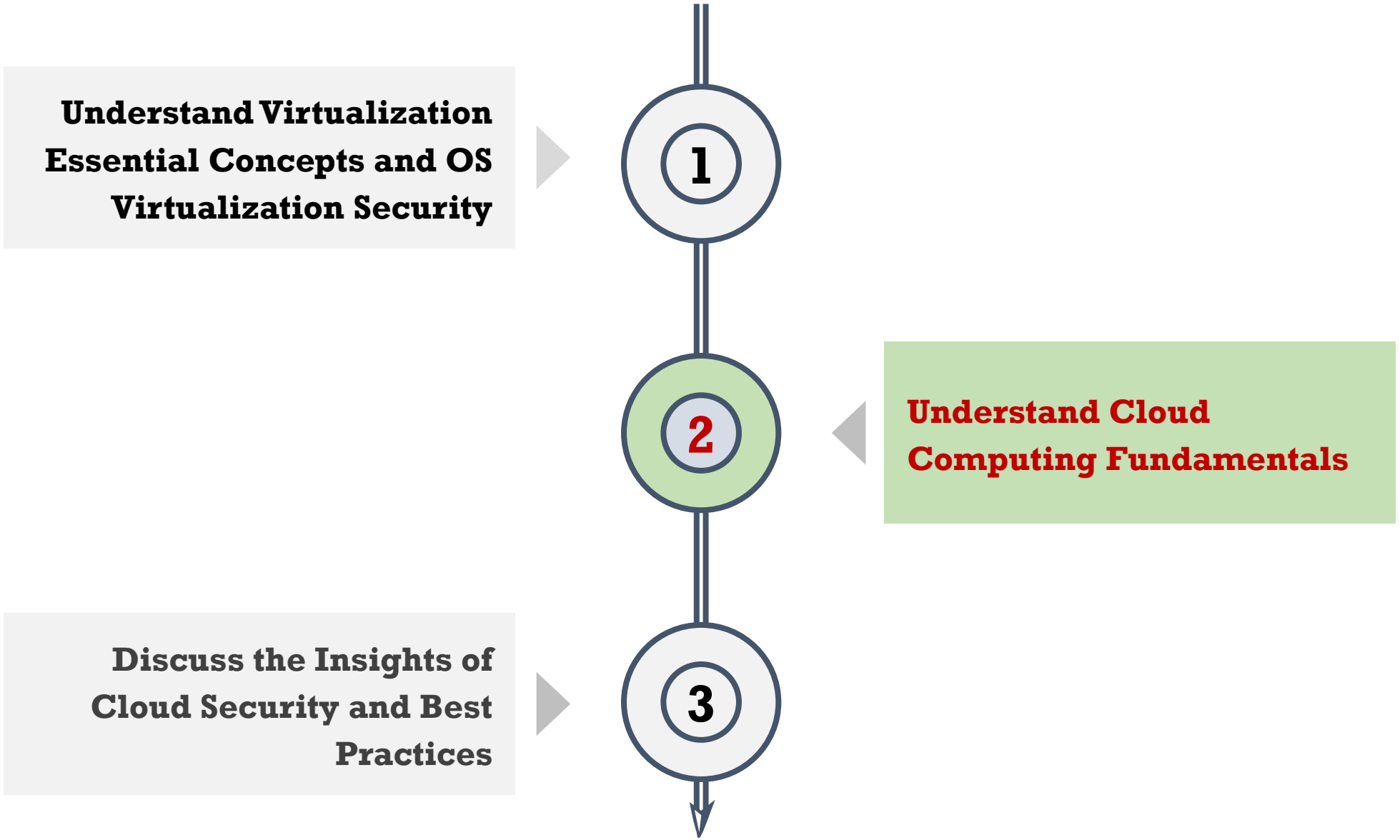
Aqua
https://www.aquasec.com

Anchore
https://anchore.com

NeuVector
https://neuvector.com

CloudPassage Halo
https://www.cloudpassage.com

Module Flow

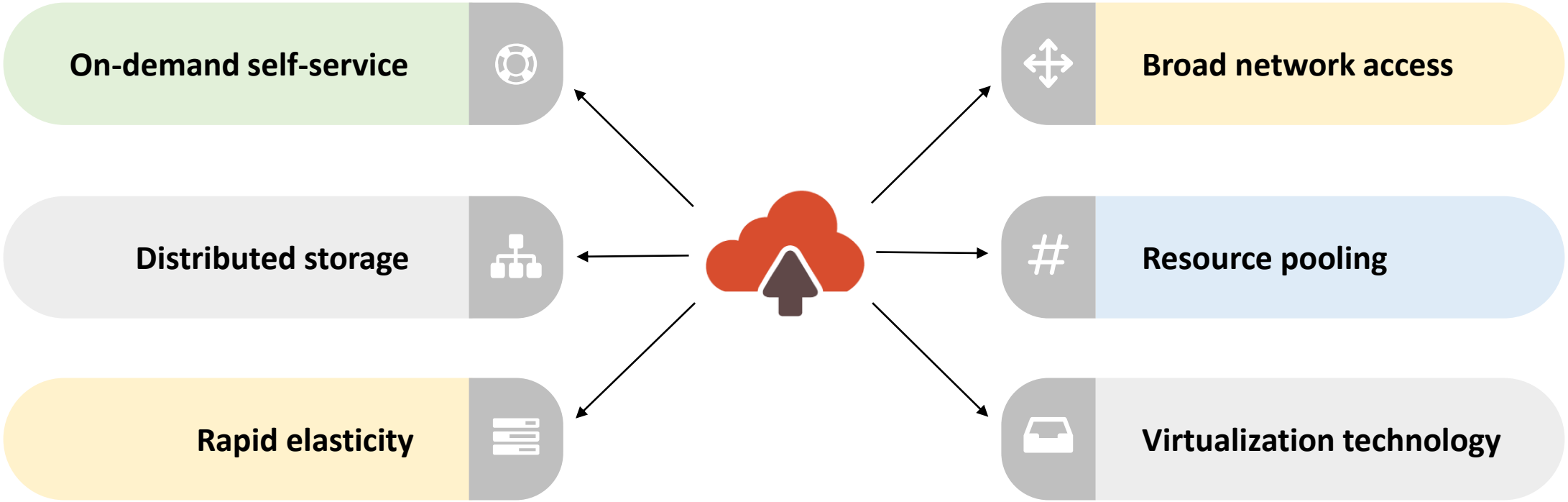

Understand Virtualization Essential Concepts and OS Virtualization Security
1
2
Understand Cloud Computing Fundamentals
Discuss the Insights of Cloud Security and Best Practices
3

Introduction to Cloud Computing



- Cloud computing is an on-demand delivery of **IT capabilities** where IT infrastructure and applications are provided to **subscribers** as a metered service over a network

Characteristics of Cloud Computing



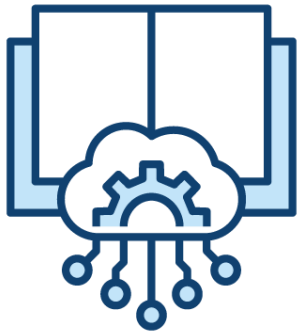
Cloud Computing Benefits

Economic

- ✓ Business agility
- ✓ Less maintenance costs
- ✓ Acquire economies of scale
- ✓ Less capital expense
- ✓ Huge storage facilities for organizations

Operational

- ✓ Flexibility and efficiency
- ✓ Resilience and redundancy
- ✓ Scale as required
- ✓ Less operational problems
- ✓ Deploy applications quickly



Staffing

- ✓ Streamline processes
- ✓ Efficient usage of resources
- ✓ Less personnel training
- ✓ Less IT Staff
- ✓ Multiple users can utilize cloud resources

Security

- ✓ Less investment in security controls
- ✓ Efficient, effective, and swift response to security breaches
- ✓ Standardized open interface for managed security services (MSS)
- ✓ Effective patch management and implementation of security updates
- ✓ Better disaster recovery preparedness

Types of Cloud Computing Services

SYS ADMINS	DEVELOPERS	END CUSTOMERS	END CUSTOMERS
Infrastructure-as-a-Service (IaaS)	**Platform-as-a-Service (PaaS)**	**Software-as-a-Service (SaaS)**	**Identity-as-a-Service (IDaaS)**
▪ Provides **virtual machines** and other abstracted hardware and operating systems which may be **controlled through a service API** ▪ E.g., Amazon EC2, GoGrid, Microsoft OneDrive, or Rackspace	▪ Offers **development tools**, **configuration management**, and **deployment platforms** on-demand that can be used by subscribers to **develop custom applications** ▪ E.g., Google App Engine, Salesforce, or Microsoft Azure	▪ Offers **software to subscribers** on-demand **over the Internet** ▪ E.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, or Freshbooks	▪ Offers **IAM services** including SSO, MFA, IGA, and intelligence collection ▪ E.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, or Okta

Types of Cloud Computing Services (Cont'd)

END CUSTOMERS

Security-as-a-Service (SECaaS)

- Provides **penetration testing**, **authentication**, **intrusion detection**, anti-malware, security incident, and event management services
- E.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, or McAfee Managed Security Services

END CUSTOMERS

Function-as-a-Service (FaaS)

- Provides a platform for developing, running, and managing **application functionalities for microservices**
- E.g., AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, or Oracle Cloud Fn

END CUSTOMERS

Container-as-a-Service (CaaS)

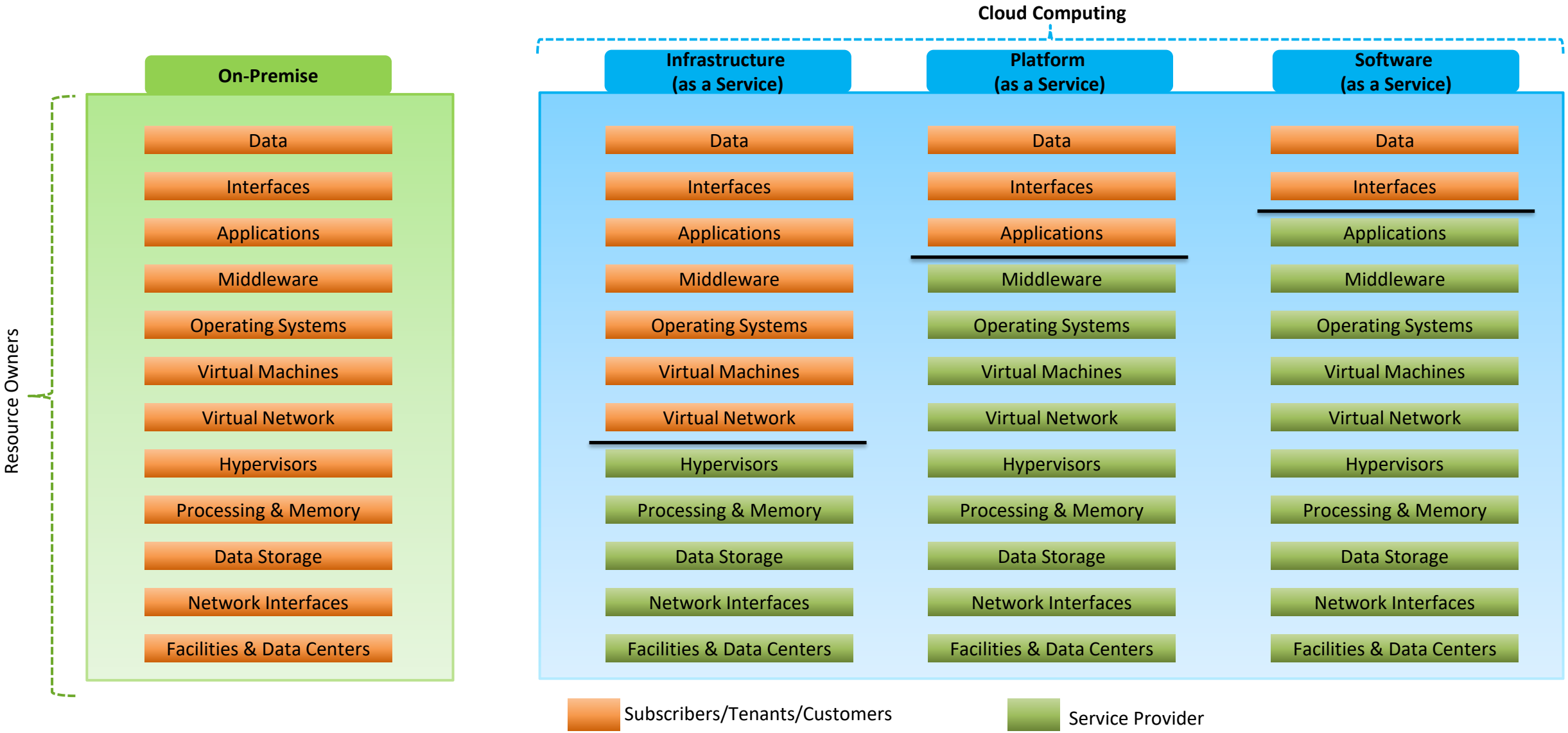
- Offers **virtualization of container engines**, and management of containers, applications, and clusters, through a web portal or API
- E.g., Amazon AWS EC2, or Google Kubernetes Engine (GKE)

END CUSTOMERS

Anything-as-a-Service (XaaS)

- Offers anything as a service over the **Internet** based on the **user's demand** like digital products, food, transportation, medical consultations, etc.
- E.g., Salesforce, AWS, Google Compute Engine, Azure, O365 and G Suite, JumpCloud

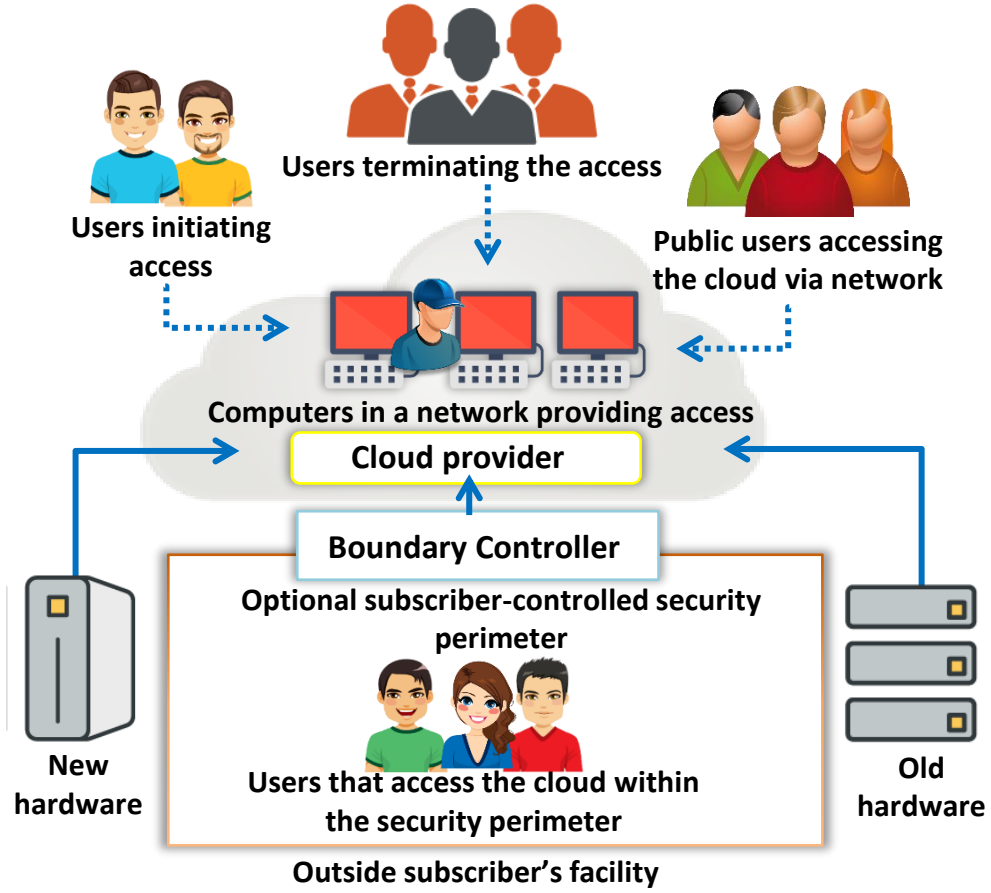
Customer vs. CSP Shared Responsibilities in IaaS, PaaS, and SaaS



Cloud Deployment Models

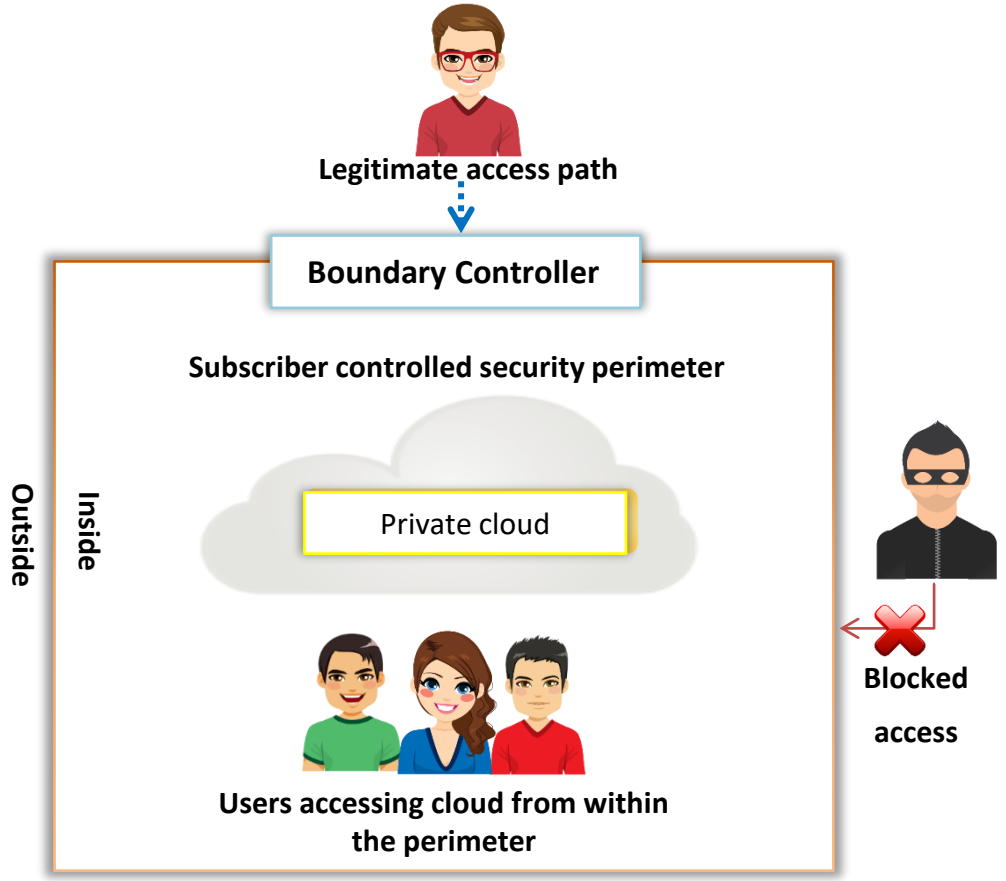
Public Cloud

Services are rendered over a network that is **open for public use**



Private Cloud

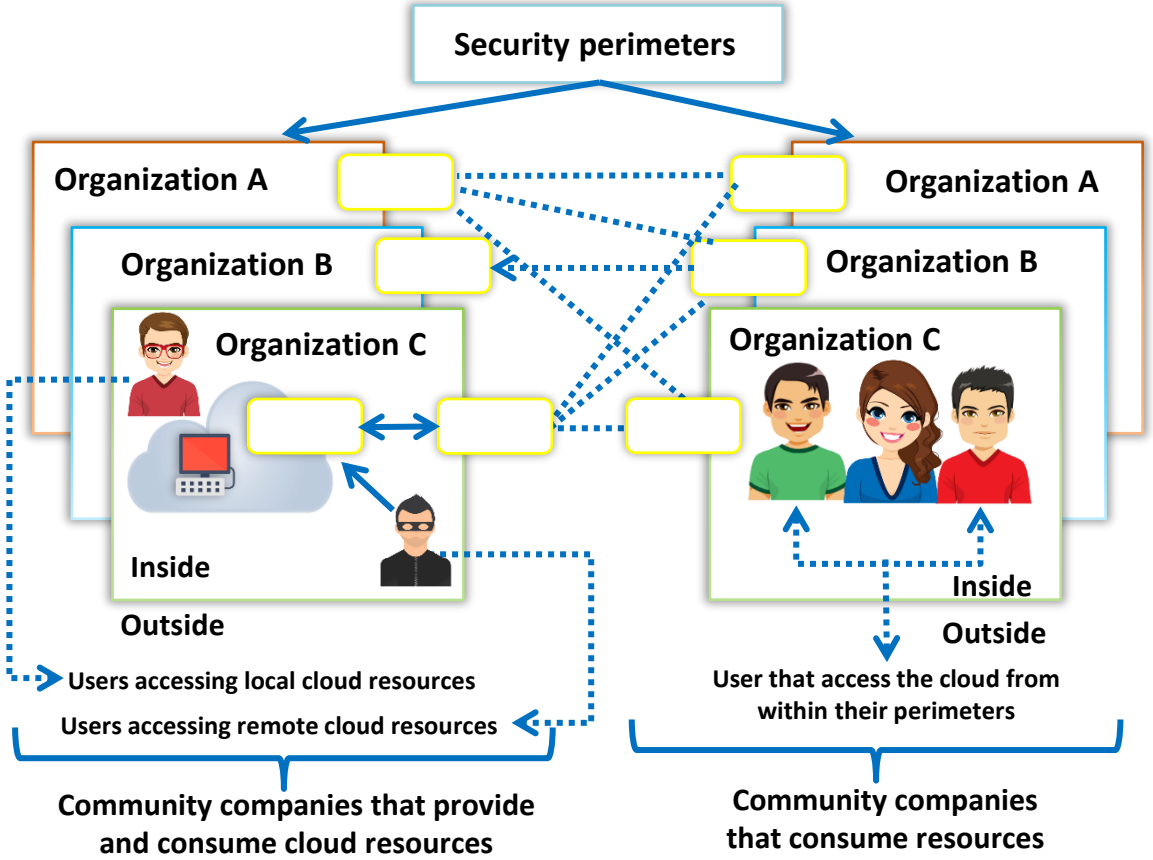
Cloud infrastructure is operated for a **single organization only**



Cloud Deployment Models (Cont'd)

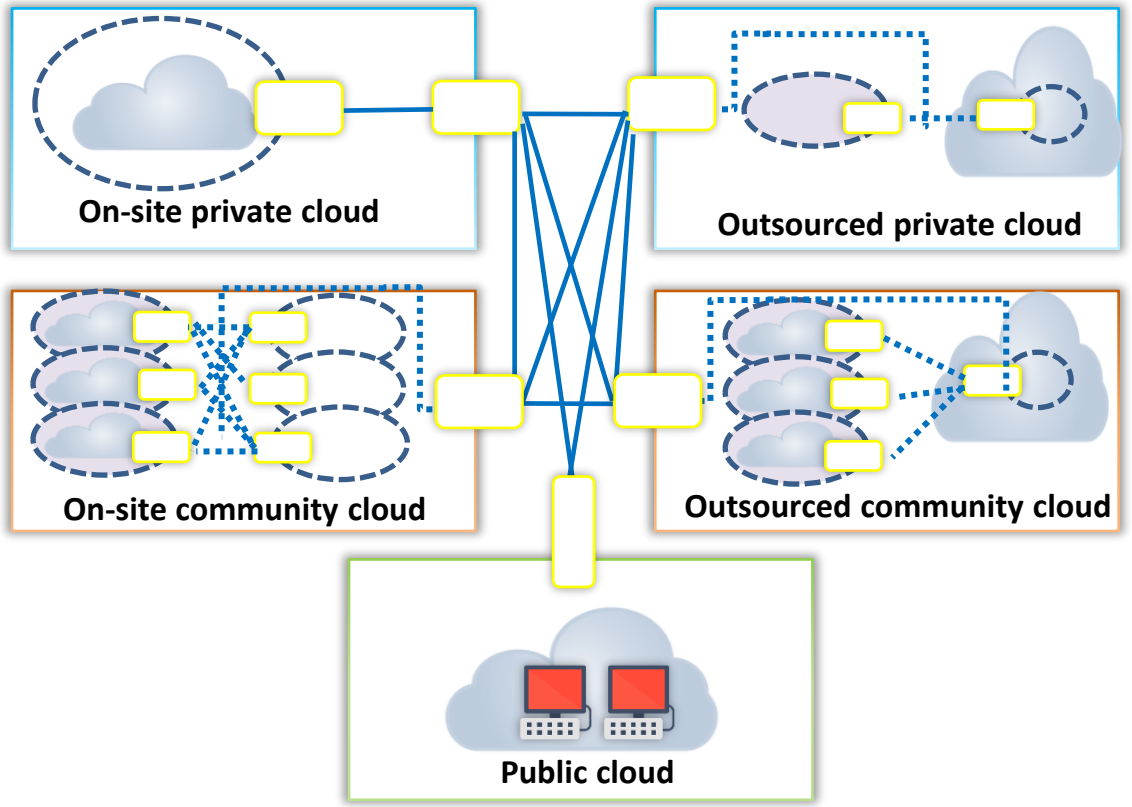
Community Cloud

Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)



Hybrid Cloud

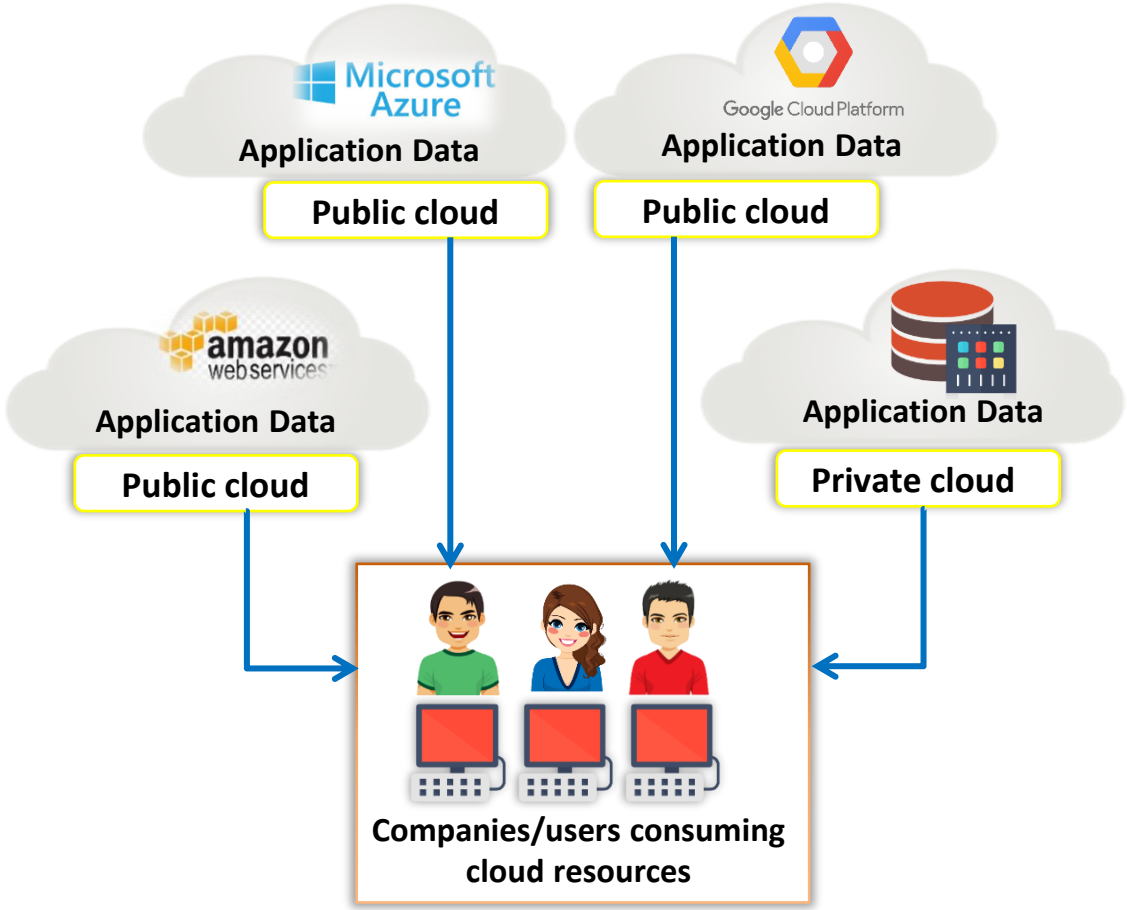
Combination of two or more clouds (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models



Cloud Deployment Models (Cont'd)

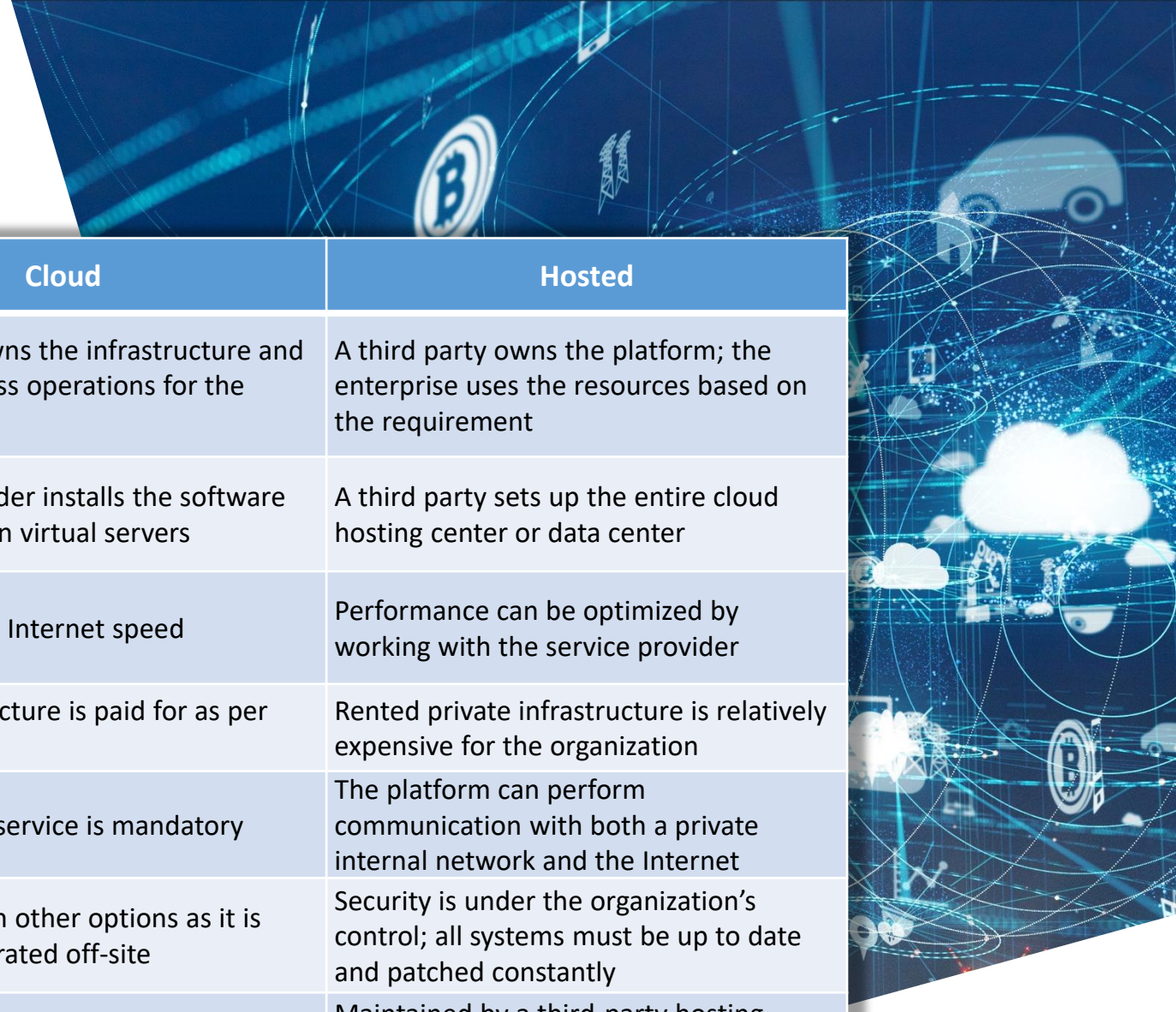
Multi Cloud

- Dynamic heterogeneous environment that **combines workloads across multiple cloud vendors**, managed via one proprietary interface to achieve long term business goals





On-premises vs. Hosted vs. Cloud



Parameters	On-premises	Cloud	Hosted
Ownership	The organization establishes the infrastructure and runs all the business operations	A third party owns the infrastructure and runs the business operations for the organization	A third party owns the platform; the enterprise uses the resources based on the requirement
Deployment	The software or application is installed on internal physical servers	The cloud provider installs the software or application on virtual servers	A third party sets up the entire cloud hosting center or data center
Performance	Depends on the skills of internal employees	Depends on the Internet speed	Performance can be optimized by working with the service provider
Cost	Physical infrastructure and initial setup are expensive	Virtual infrastructure is paid for as per usage	Rented private infrastructure is relatively expensive for the organization
Connectivity	Systems can work without the Internet	Active Internet service is mandatory	The platform can perform communication with both a private internal network and the Internet
Security	Depends on the skills of the administration team	Less secure than other options as it is completely operated off-site	Security is under the organization's control; all systems must be up to date and patched constantly
Maintenance	Maintained by an internal team	Maintained by the cloud provider	Maintained by a third-party hosting agency
Scalability	Offers limited scalability	Easily and highly scalable	Scalability depends on the availability of applications on the cloud

NIST Cloud Deployment Reference Architecture

NIST cloud computing reference architecture defines five major actors:

Cloud Consumer

A person or organization that uses **cloud computing services**

Cloud Provider

A person or organization providing services to interested parties

Cloud Carrier

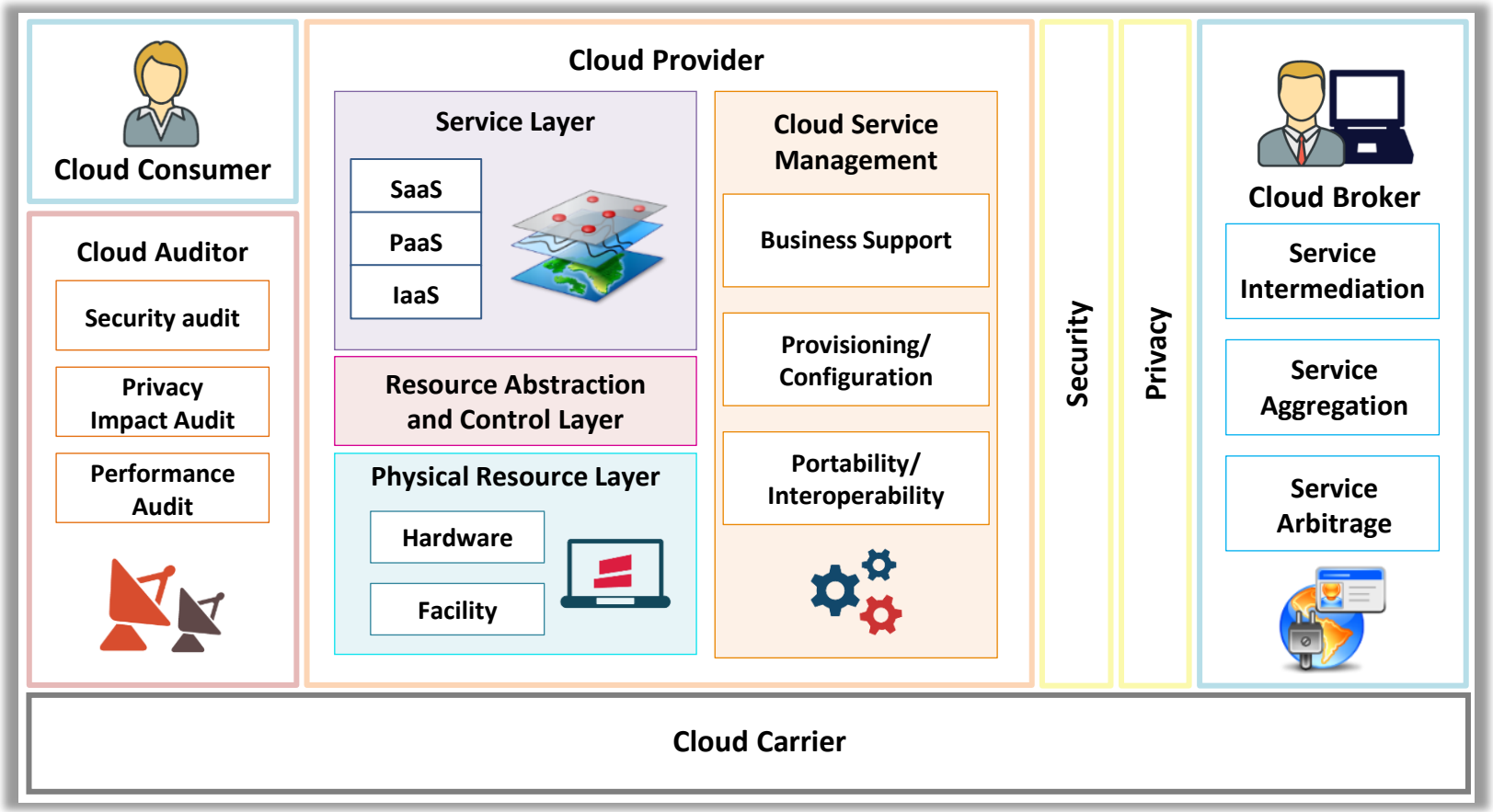
An intermediary for **providing connectivity** and **transport services** between cloud consumers and providers

Cloud Auditor

A party for making **independent assessments** of **cloud service controls** and taking an opinion thereon

Cloud Broker

An entity that **manages cloud services** in terms of use, performance, and delivery, and maintains the relationship between cloud providers and consumers



Cloud Storage Architecture

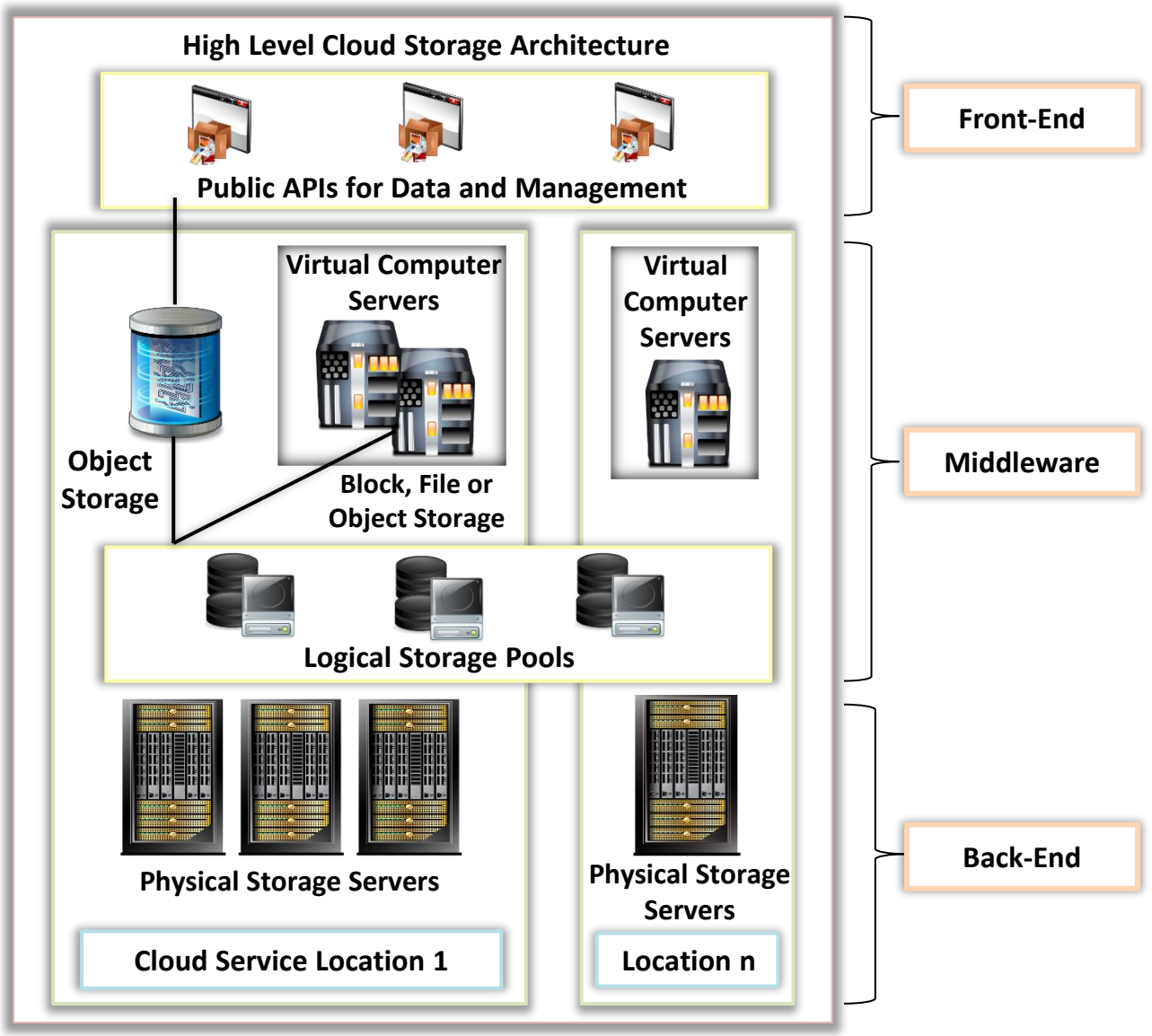
Cloud storage is a data storage medium used to **store digital data in logical pools** using a network

The cloud storage architecture **consists of three main layers** namely, front-end, middleware, and back-end

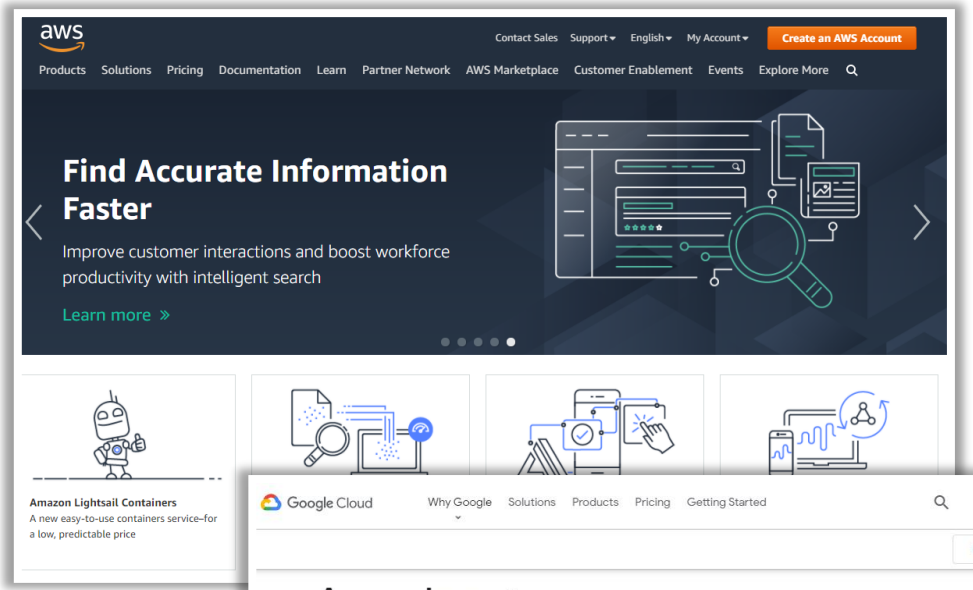
The **Front-end** layer is accessed by the **end user** where it provides APIs for the management of data storage

The **Middleware** layer performs several **functions** such as data de-duplication and replication of data

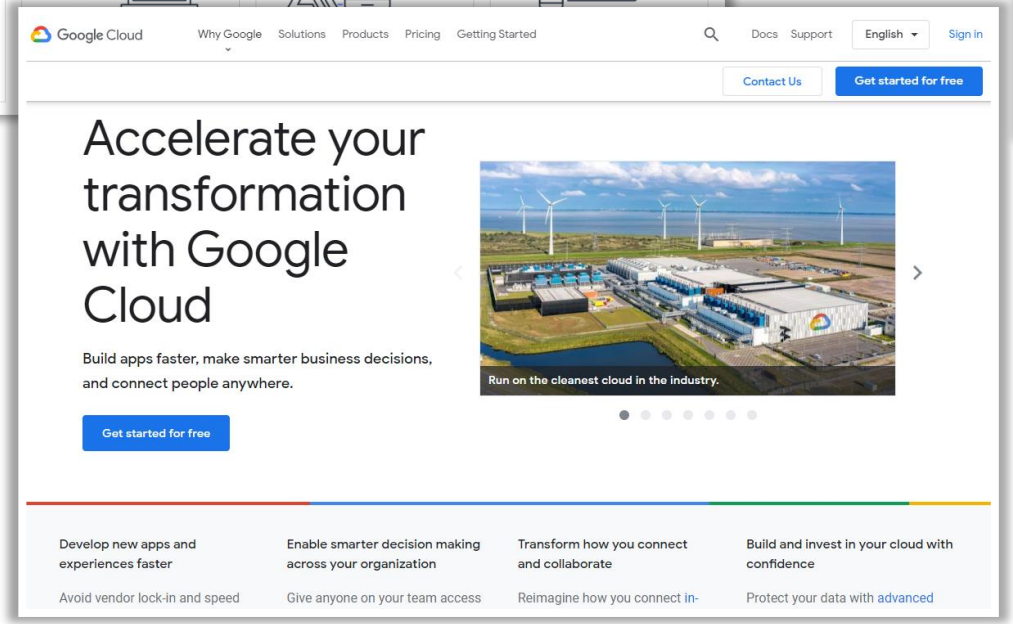
The **Back-end** layer is where the **hardware** is implemented



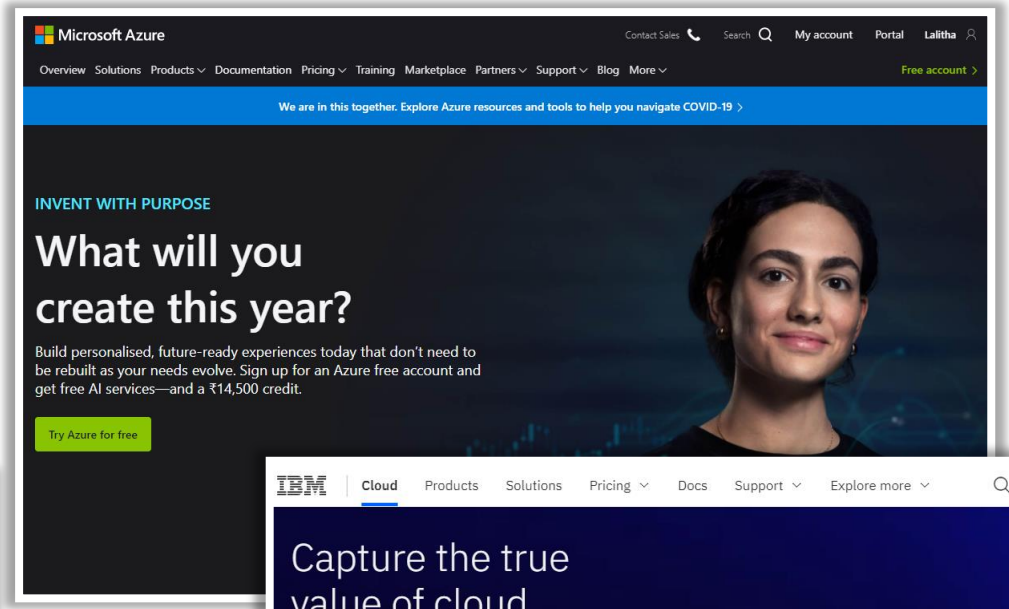
Cloud Service Providers



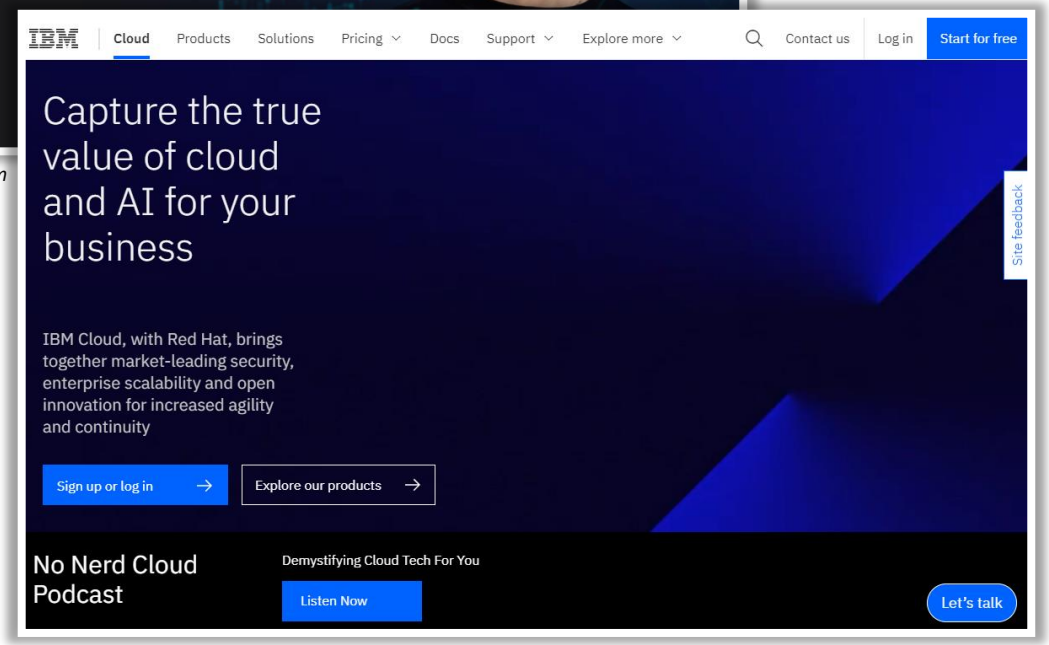
https://aws.amazon.com



https://cloud.google.com

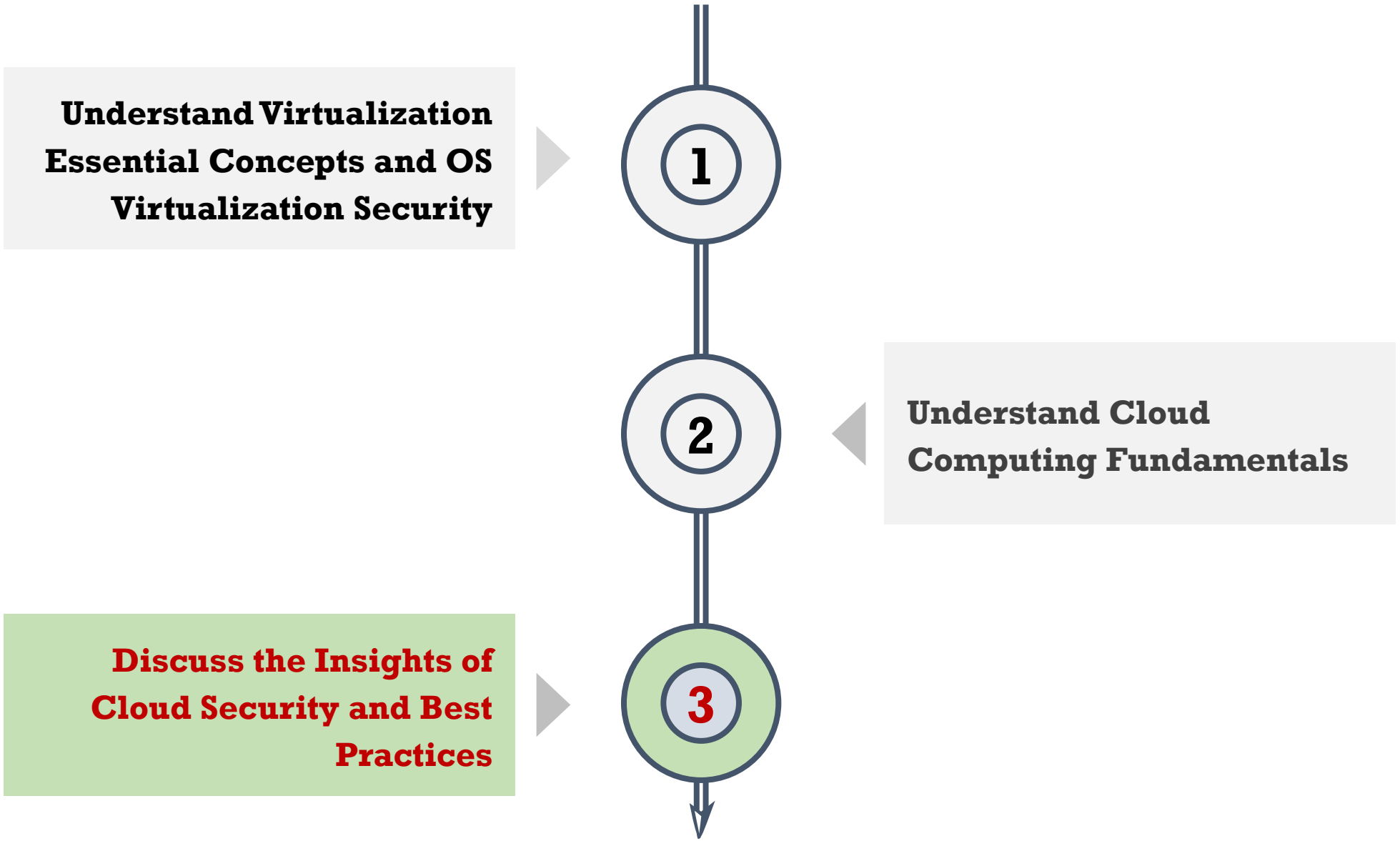


https://azure.microsoft.com



https://www.ibm.com

Module Flow

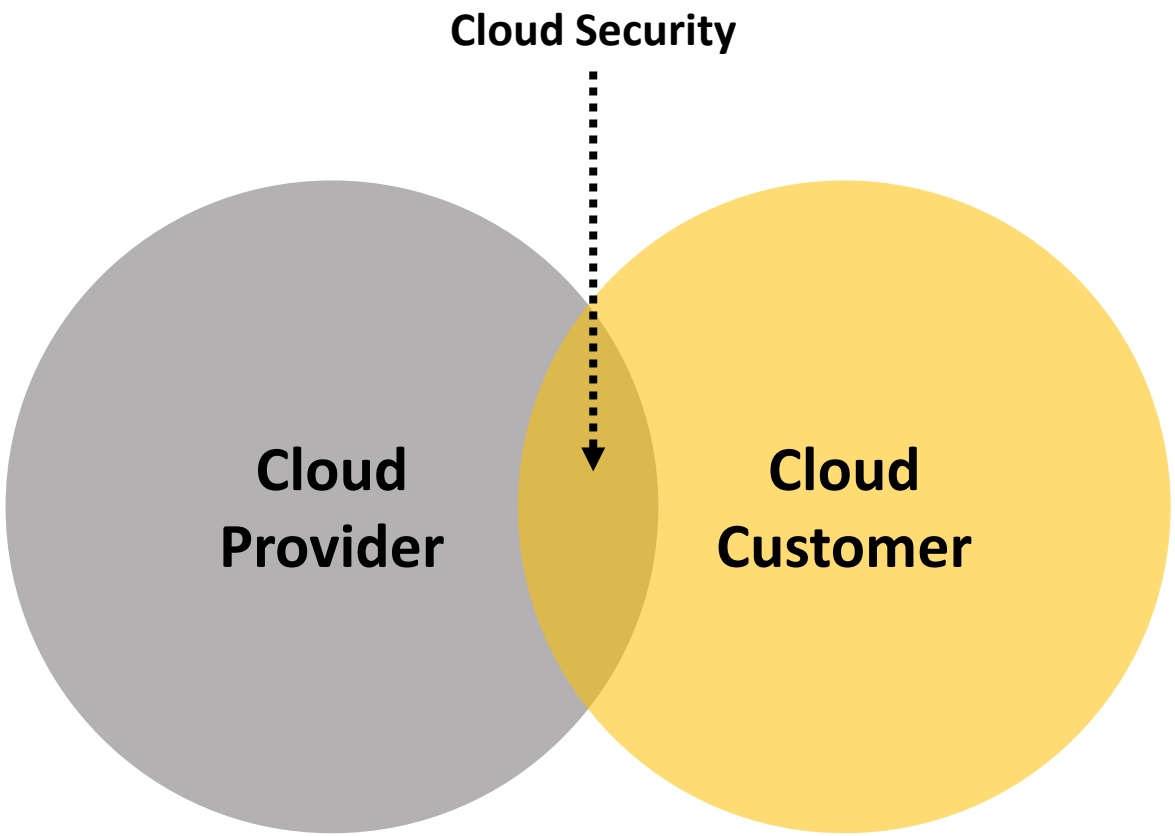

Understand Virtualization Essential Concepts and OS Virtualization Security
1
2
Understand Cloud Computing Fundamentals
Discuss the Insights of Cloud Security and Best Practices
3

Cloud Security: Shared Responsibility

1. Cloud security and compliance are the **shared responsibility** of the cloud provider and consumer

2. According to the selected cloud module, security responsibilities are divided based on the **shared responsibility model**

3. If the **consumers do not secure their functions**, the entire cloud security model will **fail**



Cloud Security: Shared Responsibility (Cont'd)

Shared Responsibility Model for Security in the Cloud				
Responsibility	**On-Premises (for reference)**	**IaaS (Infrastructure-as-a-service)**	**PaaS (Platform-as-a-serve=ice)**	**SaaS (Software-as-a-service)**
User Access				
Data				
Applications				
Operating System				
Network Traffic				
Infrastructure				
Physical				

 **Customer Responsibility**

 **Cloud Provider Responsibility**

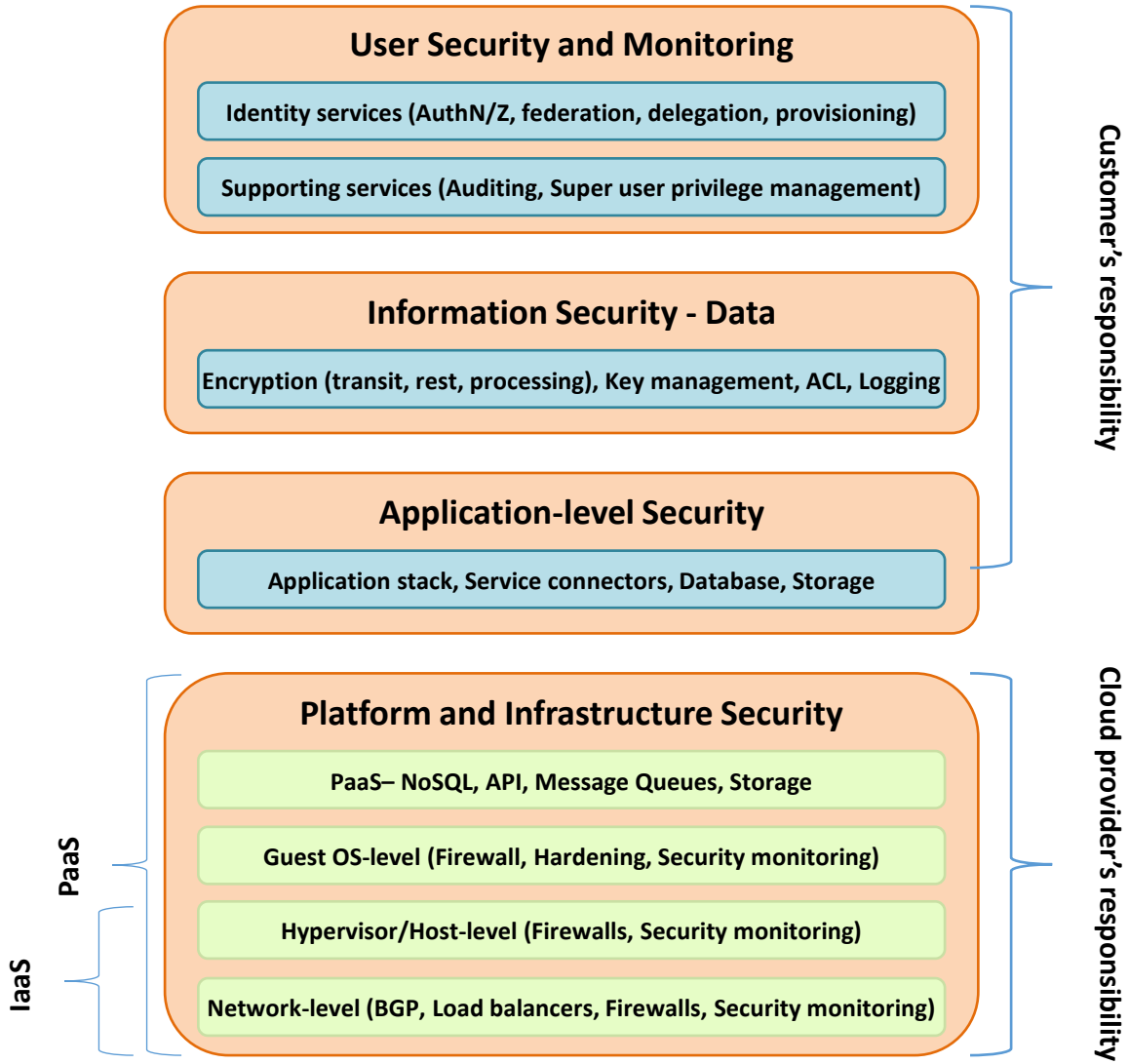
Elements of Cloud Security

Cloud Service Consumers

- Cloud service consumers are responsible for:
  - ✓ User security and monitoring (identity and access management (IAM)
  - ✓ Information security–data (encryption and key management)
  - ✓ Application-level security
  - ✓ Data storage security
  - ✓ Monitoring, logging, and compliance

Cloud Service Providers

- Cloud service providers are responsible for **securing the shared infrastructure**, including routers, switches, load balancers, firewalls, hypervisors, storage networks, management consoles, DNS, directory services, and cloud API

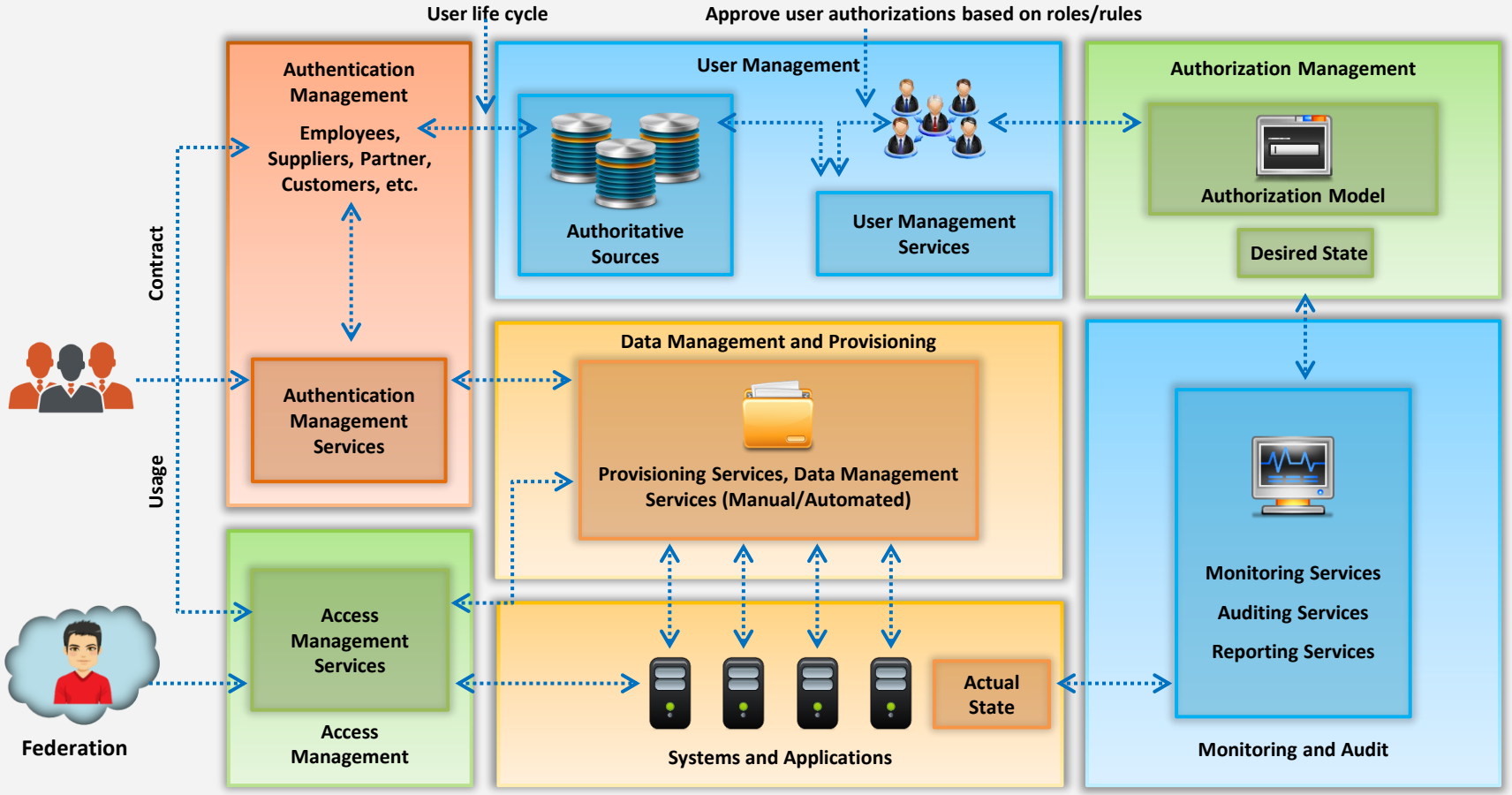


Elements of Cloud Security (Cont'd)

Identity and Access Management (IAM)

- IAM is the management of the **digital identities of users** and their **rights** to access cloud resources
- It includes creating, managing, and removing digital identities, as well as the authorization of users





Elements of Cloud Security (Cont'd)

Compliance

- A clear idea about the **regulation standards** that an organization wants to comply with along with its associated requirements allows organizations benefit from the business agility and growth

- **Compliance considerations** for the organizations to integrate their compliance programs with their cloud providers:

  - ✓ Know the requirements that impact an organization to know about the jurisdictions of an organization, industry, or activities employed by the organization to conduct business

  - ✓ Conduct regular compliance risk assessments to help the organizations to adopt the updated and revised risk assessment processes regularly

  - ✓ Monitoring and auditing the organization compliance program before a crisis hits helps organizations to determine the gaps and improving their compliance position



Elements of Cloud Security (Cont'd)

Data Storage Security

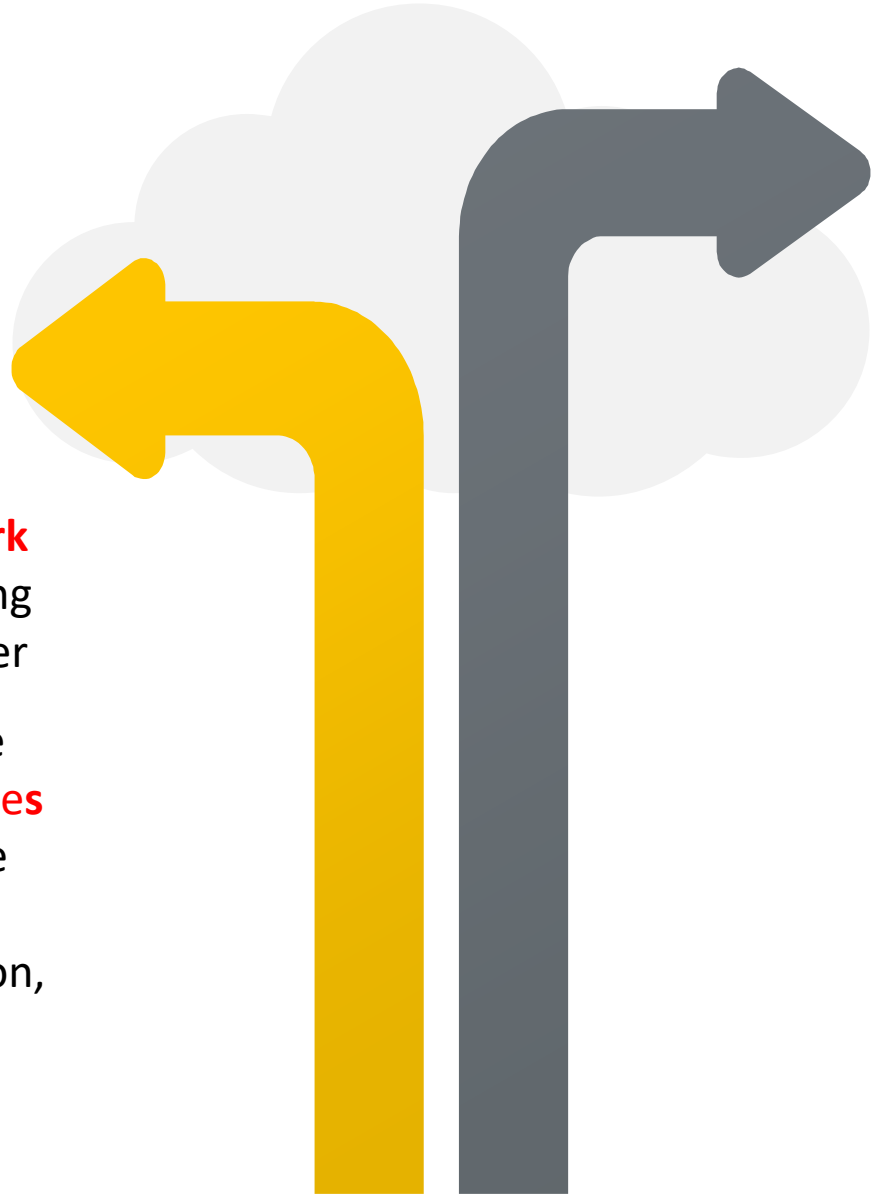
- In a cloud, data are stored on internet-connected servers in **data centers** and it is the responsibility of data centers to secure the data
- The data storage security techniques includes local data encryption, key management, strong password management, periodic security assessment of data security controls, cloud data backup, etc.

Monitoring

- Monitoring is required to manage **cloud-based services**, **applications**, and **infrastructure**
- Activity monitoring should observe the **activities** like data replication, data file name changes, data file classification changes, data ownership changes to monitor unauthorized data access, etc.



Elements of Cloud Security (Cont'd)



Network Security

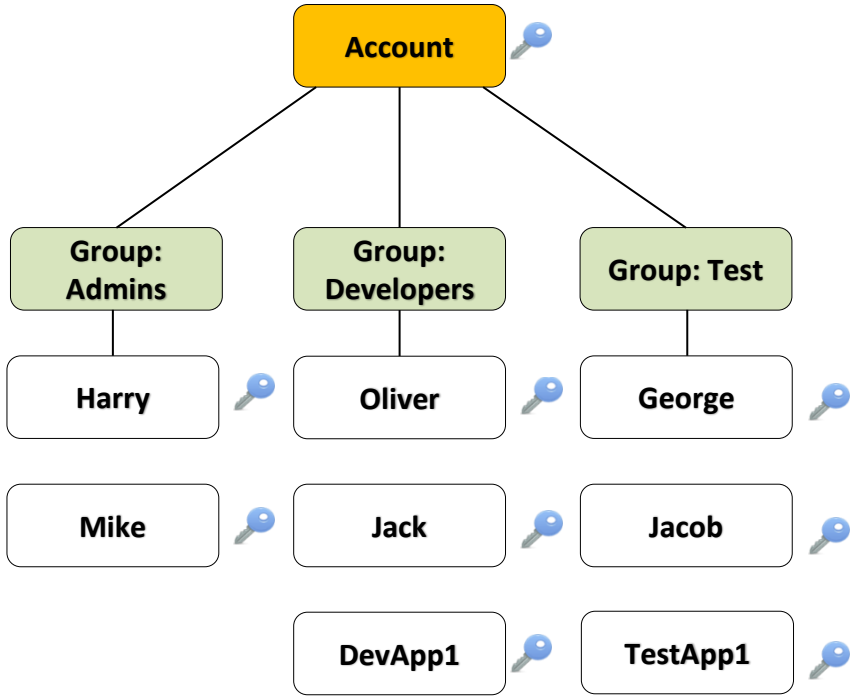
- Main challenge in cloud network security includes the **lack of network visibility** in monitoring and managing suspicious activities by the consumer
- Cloud network security requires the following **additional security features** like, encrypt data-in-transit, provide multi-factor authentication, install firewalls, enable data loss prevention, etc.

Logging

- **Security logs** are used for threat detection, data analysis, and compliance audits to enhance cloud security
- Efficient security log management for cloud includes aggregating all logs, capturing appropriate data, controlling log collection and distribution frequency, ensuring system scalability, etc.

AWS Identity and Access Management

- **IAM** enables users to securely control the access to AWS services and resources
- AWS IAM allows to establish **access rules** and **permissions** for specific users and applications





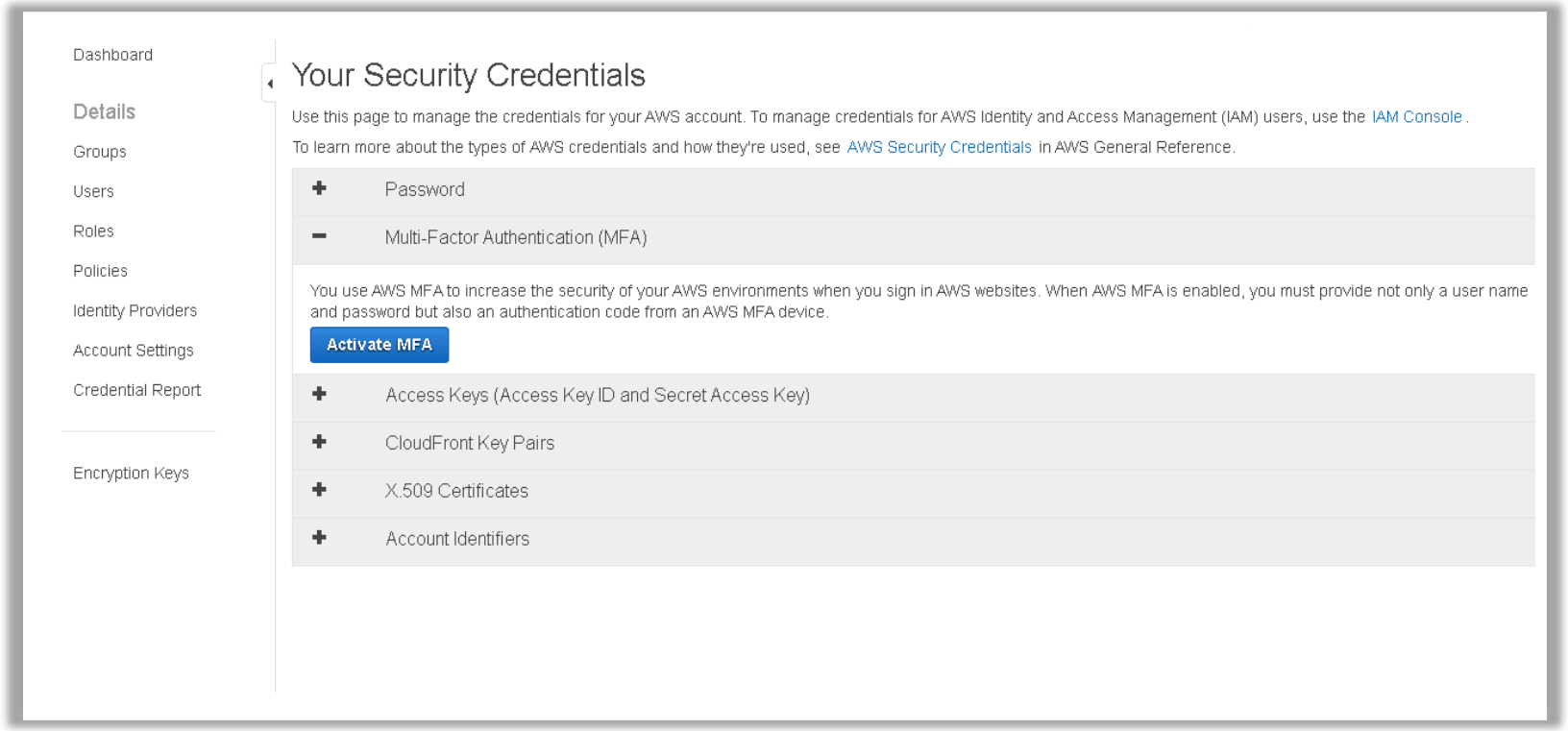
AWS IAM: Lock Your AWS Account Root User Access Keys

- The access key (an access key ID and secret access key) is used to make **programmatic requests** to AWS
- The access key of AWS root user account gives full access to all AWS resources

To protect root user access key:

- ✓ Do not create AWS root user account access keys unless required
- ✓ Change the AWS root user account access key regularly
- ✓ Never share the AWS root user account password or access keys
- ✓ Use strong passwords for logging into the AWS Management Console
- ✓ Enable AWS MFA on AWS root user account

Enabling AWS MFA on AWS root user account



AWS IAM: Create Individual IAM Users

1

Do not allow a user to use the **root user account**; instead, create individual user accounts for accessing AWS services

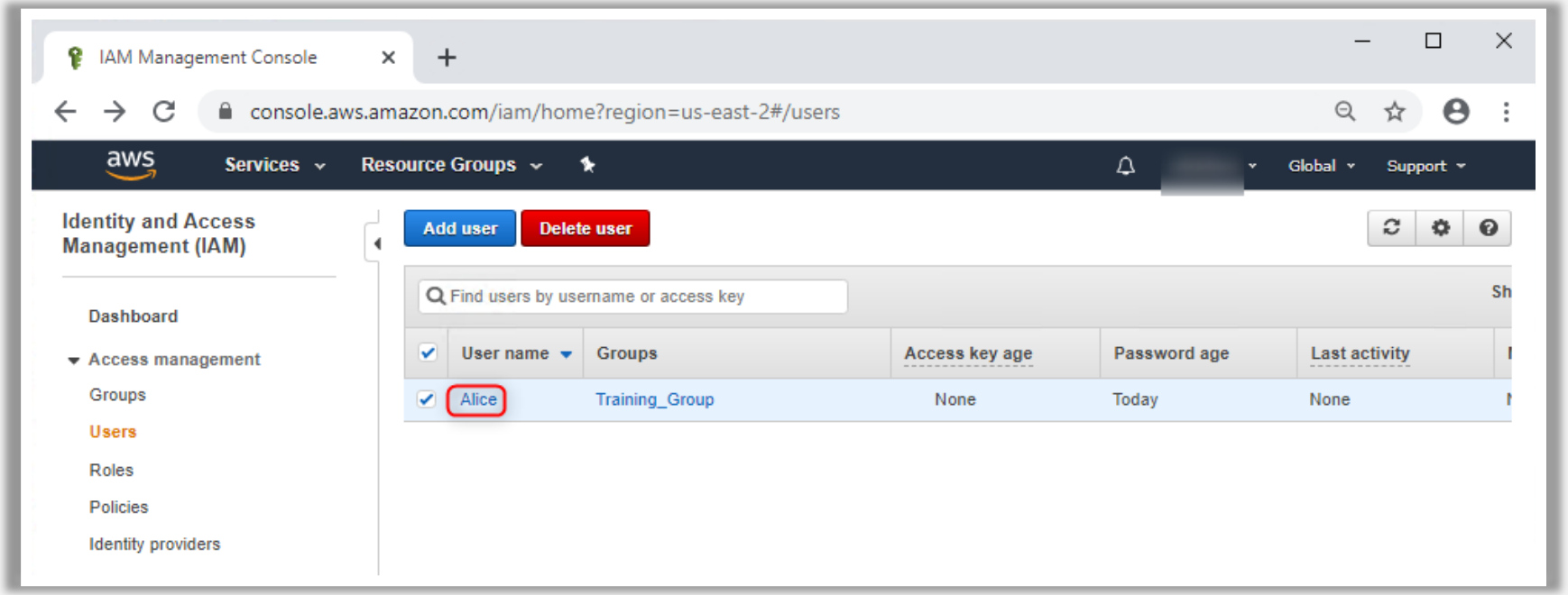
2

Provide a unique set of security credentials and appropriate permissions to the IAM users

3

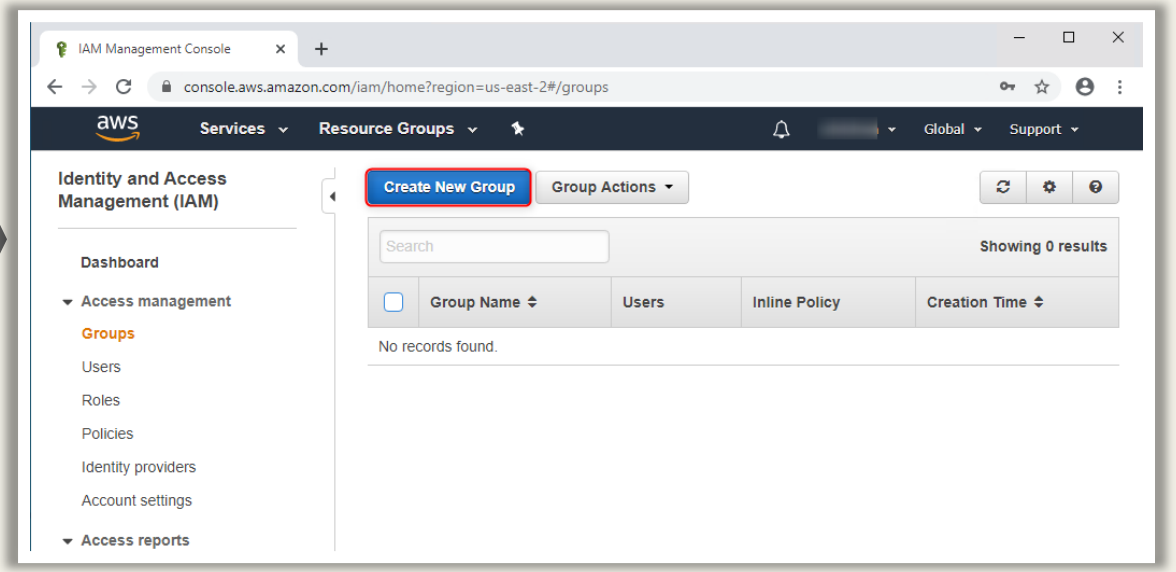
This will help in changing or revoking the permissions of IAM users as required





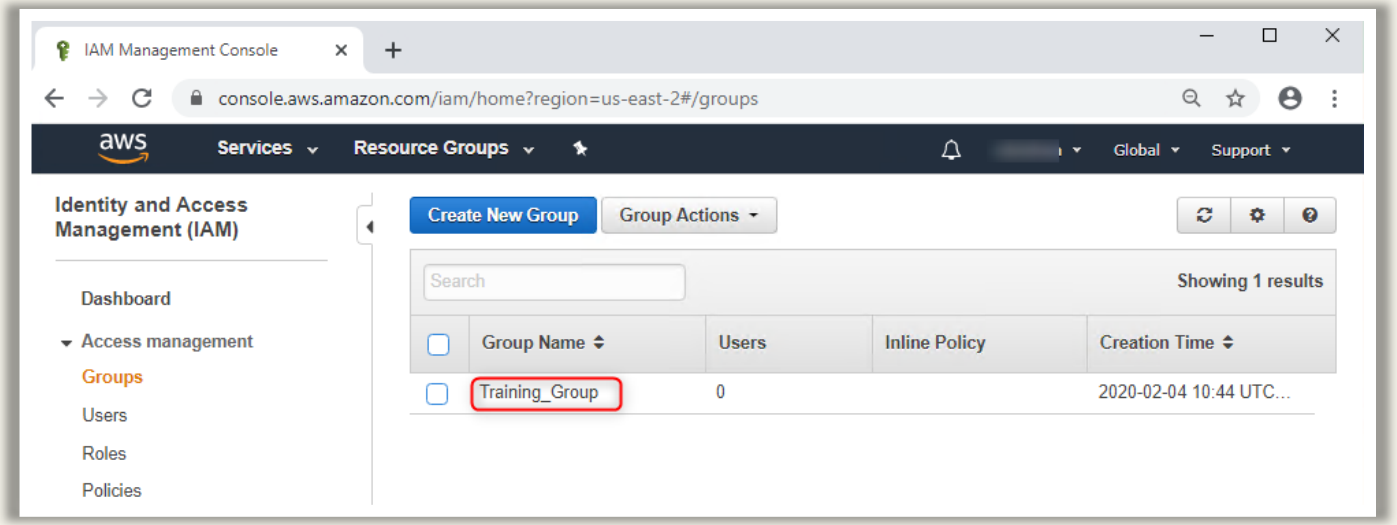
AWS IAM: Use Groups to Assign Permissions to IAM Users

- Create groups and assign appropriate permissions to reduce **access management complexity** for organizations with large number of users
- Create groups with similar job functions



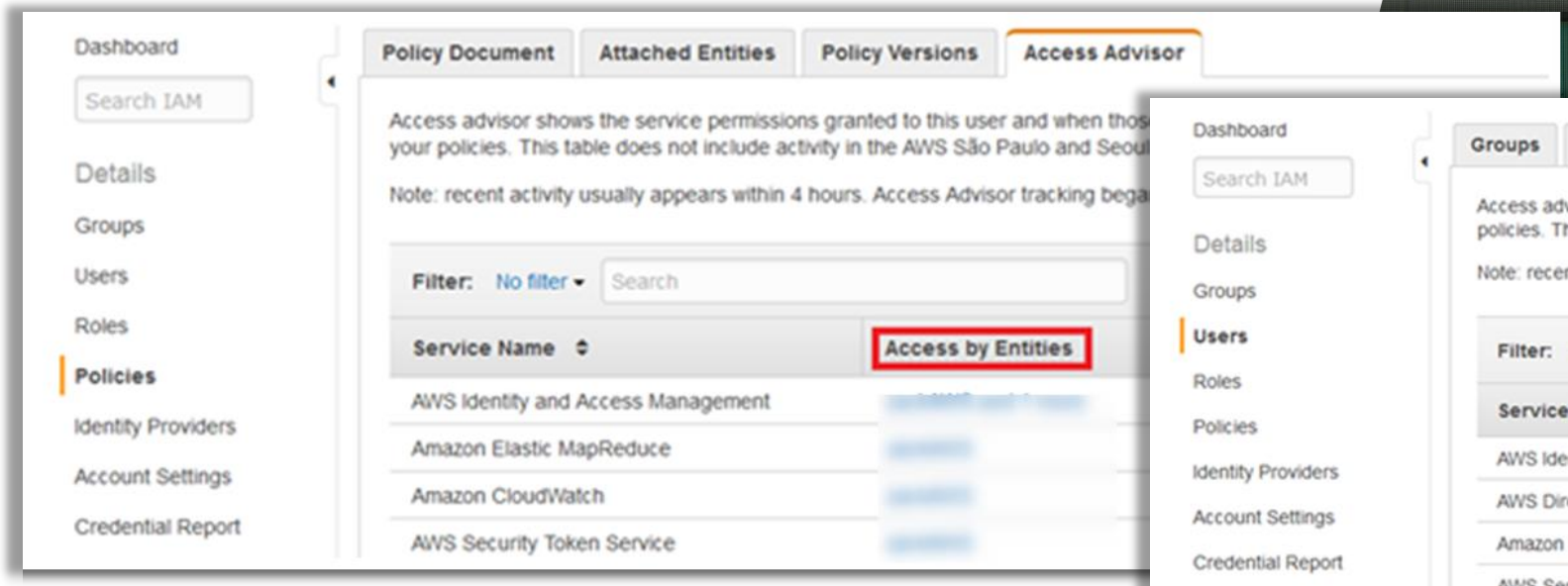
Advantages:

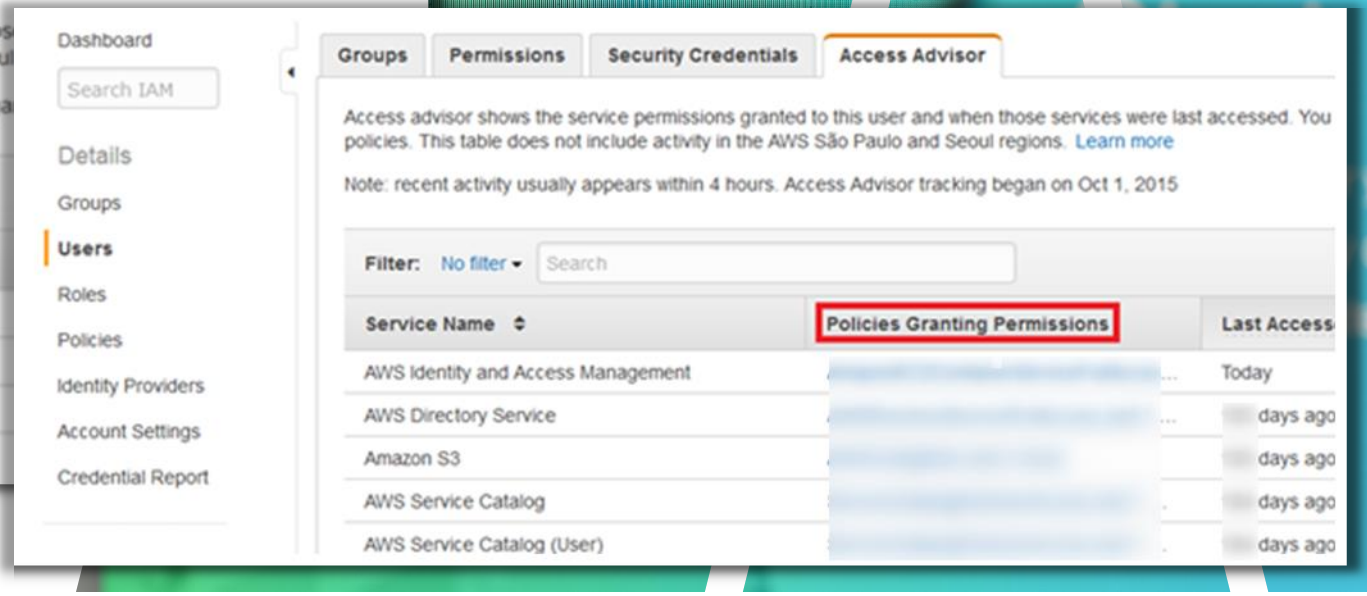
- Assigning and reassigning rights to groups is easy and less time consuming
- Reduces accidental assignment of greater privileges to users



AWS IAM: Grant Least Privilege

- ❑ To implement more granular access control, begin with minimum permissions and gradually add permissions as required
- ❑ Implement conditional access to restrict privileged access
- ❑ Use the **Access Advisor** tab to regularly monitor user access
- ❑ Implement resource-based policies to restrict access to specific resources

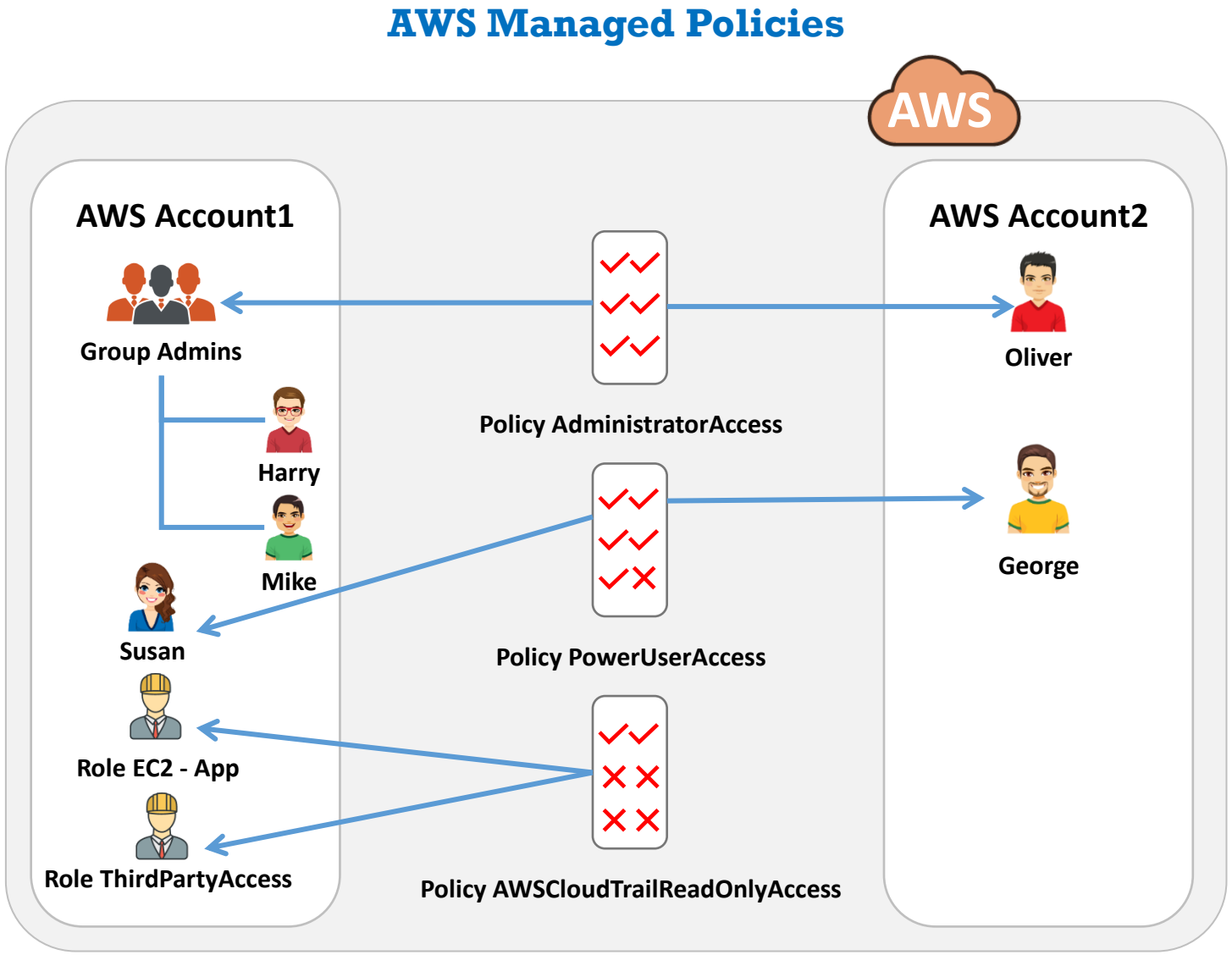




AWS IAM: Use AWS-managed Policies



- AWS managed policies are standalone policies that are created and administered by AWS
- AWS-managed policies are designed to provide **permissions** for common use cases
- Use AWS-managed policies while **designing** and **creating access policies**



Best Practices for Securing the Cloud

01 Enforce **data protection**, **backup**, and **retention** mechanisms

02 Enforce **SLAs** for patching and vulnerability remediation

03 Vendors should regularly undergo **AICPA SAS 70 Type II audits**

04 Verify one's own cloud in **public domain blacklists**



05 Enforce **legal contracts** in employee behavior policy

06 Prohibit **user credentials sharing** among users, applications, and services

07 Implement strong **authentication**, **authorization** and **auditing** controls

08 Check for **data protection** at both the design stage and at runtime

NIST Recommendations for Cloud Security

01 **Assess the risk** posed to the client's data, software and infrastructure

02 Select an appropriate **deployment model** according to the needs

03 Ensure **audit procedures** are in place for data protection and software isolation

04 **Renew SLAs** in case of **security gaps** found between the organization's security requirements and the cloud provider's standards

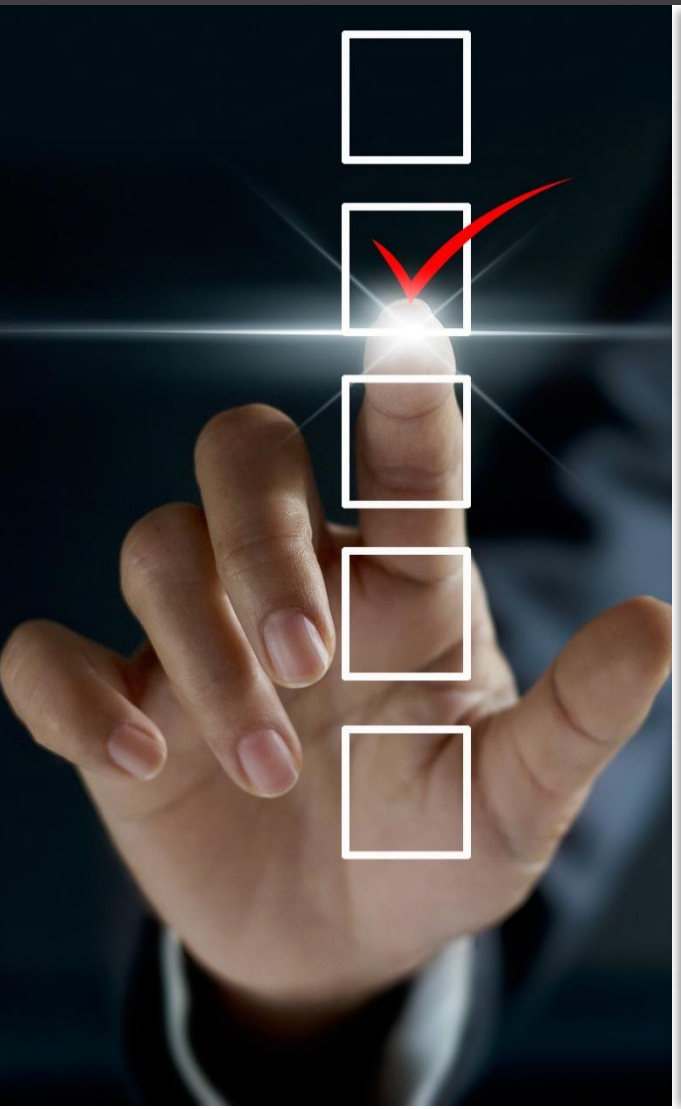
05 Establish appropriate **incident detection** and **reporting mechanisms**

06 Analyze what are the **security objectives** of the organization

07 Enquire about **who is responsible** for data privacy and security issues in the cloud



Organization/Provider Cloud Security Compliance Checklist

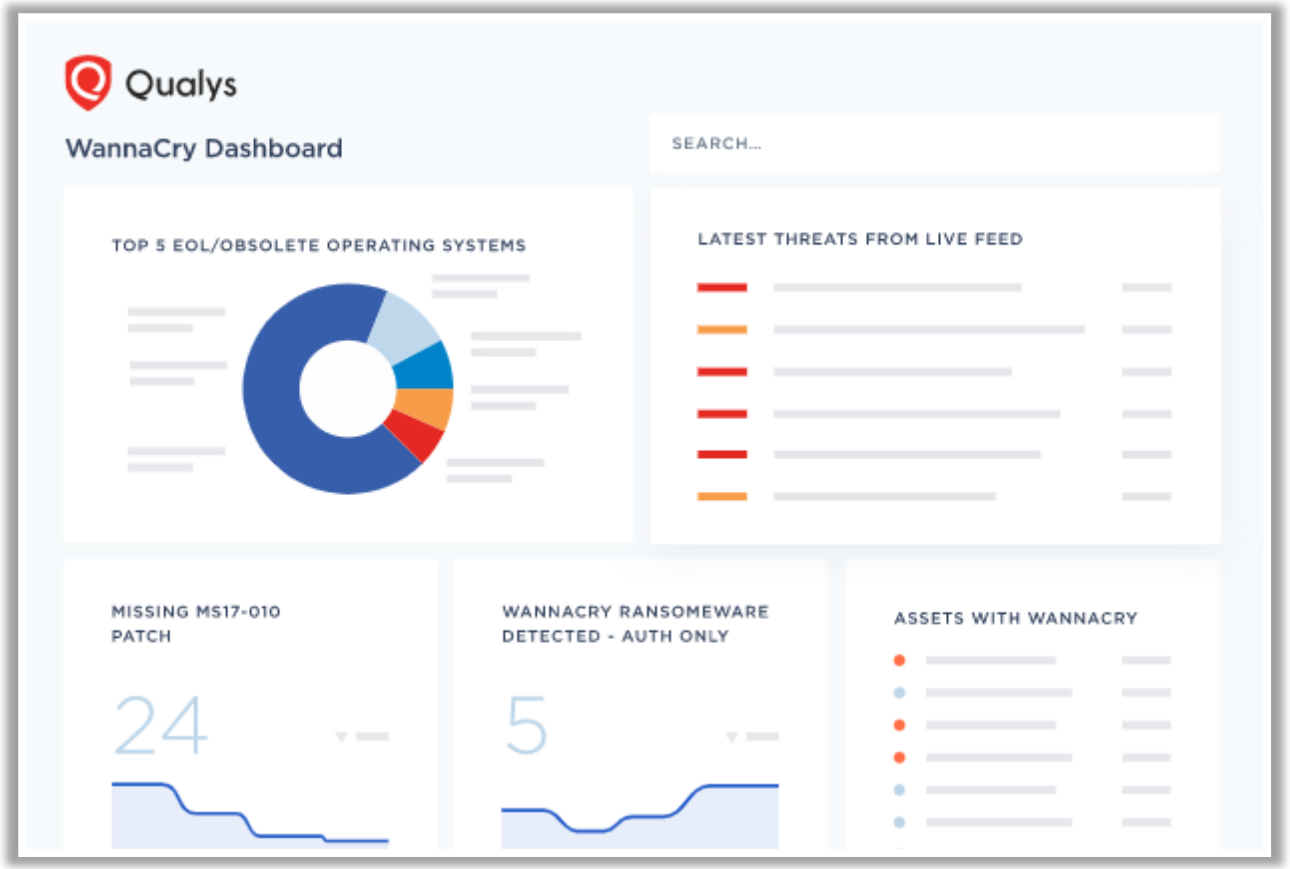


Management	Organization	Provider
Is everyone aware of his or her cloud security responsibilities?		
Is there a mechanism for assessing the security of a cloud service?		
Does the business governance mitigate the security risks that can result from cloud-based “shadow IT”?		
Does the organization know within which jurisdictions its data can reside?		
Is there a mechanism for managing cloud-related risks?		
Does the organization understand the data architecture needed to operate with appropriate security at all levels?		
Can the organization be confident of end-to-end service continuity across several cloud service providers?		
Does the provider comply with all relevant industry standards (e.g. the UK’s Data Protection Act)?		
Does the compliance function understand the specific regulatory issues pertaining to the organization's adoption of cloud services?		

Cloud Security Tools

Qualys Cloud Platform

An **end-to-end IT security solution** that provides a continuous, always-on **assessment of the global security** and compliance posture, with visibility across all IT assets irrespective of where they reside



https://www.qualys.com

- **CloudPassage Halo**
  https://www.cloudpassage.com
- **McAfee MVISION Cloud**
  https://www.mcafee.com
- **CipherCloud**
  https://www.ciphercloud.com
- **Netskope Security Cloud**
  https://www.netskope.com
- **Prisma Cloud**
  https://www.paloaltonetworks.com

Module Summary

- This module has discussed virtualization, its components, and virtualization enablers
- It has discussed OS virtualization security and concerns
- It has also discussed the best practices for OS virtualization security
- This module has discussed cloud computing and its benefits
- It has discussed different types of cloud computing services and cloud deployment models
- Finally, this module ended with a brief discussion on the importance of cloud security and its best practices
- In the next module, we will discuss on wireless network security in detail

