

Module 11

Cloud Computing Threats and Countermeasures

Module Objectives

Understanding Cloud Computing Concepts

Overview of Container Technology

Understanding Cloud Computing Threats

Overview of Cloud Attacks and Tools

Understanding Cloud Attack Countermeasures

Overview of Various Cloud Computing Security Tools



Module Flow



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

1

On-demand self-service

2

Distributed storage

3

Rapid elasticity

4

Automated management



5

Broad network access

6

Resource pooling

7

Measured service

8

Virtualization technology

Types of Cloud Computing Services

SYS ADMINS

Infrastructure-as-a-Service (IaaS)

- Provides **virtual machines** and other abstracted hardware and operating systems which may be **controlled through a service API**
- E.g., Amazon EC2, Microsoft OneDrive, or Rackspace

DEVELOPERS

Platform-as-a-Service (PaaS)

- 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

END CUSTOMERS

Software-as-a-Service (SaaS)

- Offers **software to subscribers** on-demand **over the Internet**
- E.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, or Freshbooks

Types of Cloud Computing Services (Cont'd)

SYS ADMINS

Identity-as-a-Service (IDaaS)

- Offers **IAM services** including SSO, MFA, IGA, and intelligence collection
- E.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, or Okta

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

Security-as-a-Service (SECaaS)

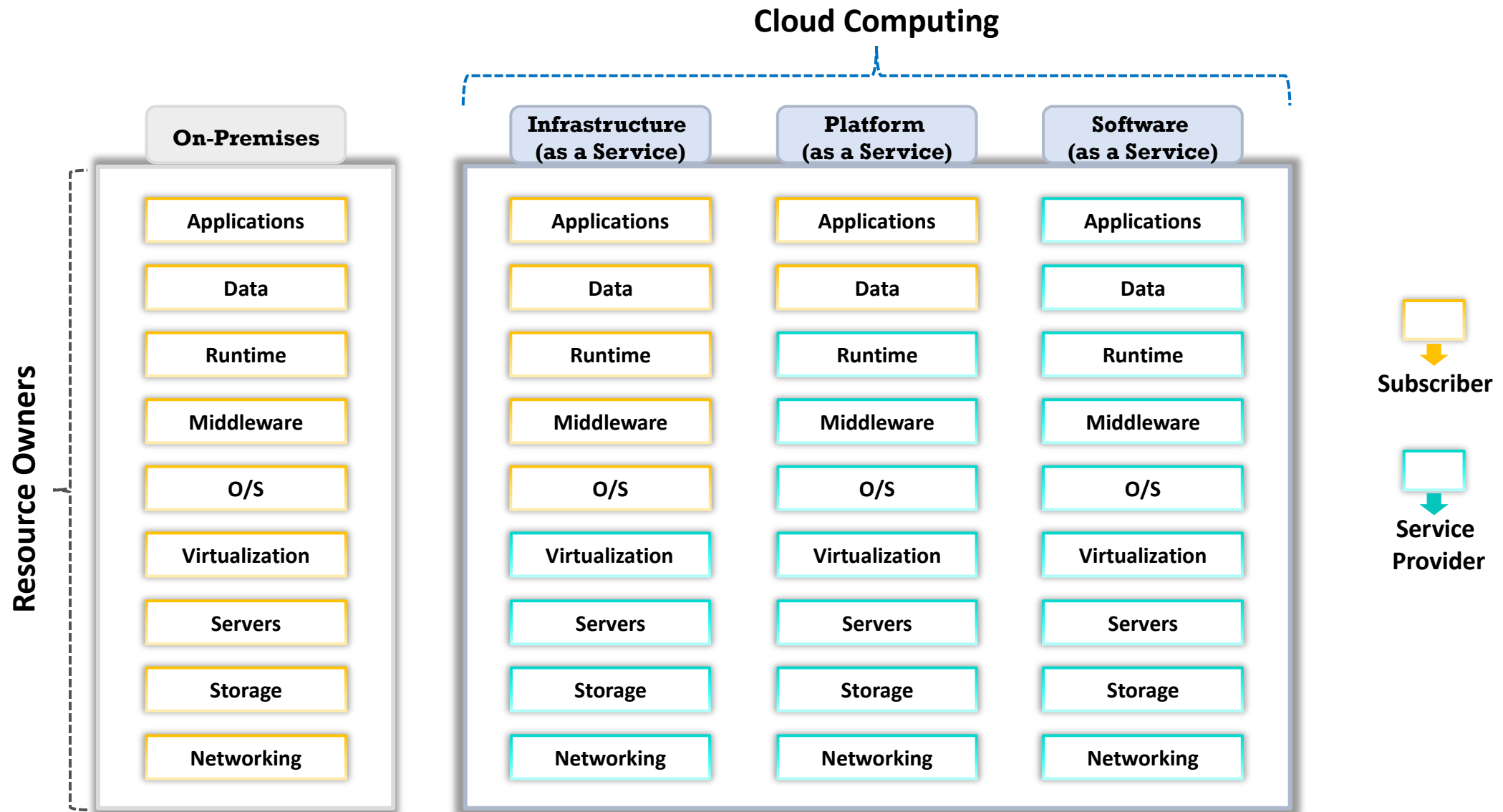
- Provides **penetration testing, authentication, intrusion detection**, anti-malware, security incident, and event management services
- E.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, or McAfee Managed Security Services

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

Separation of Responsibilities in Cloud

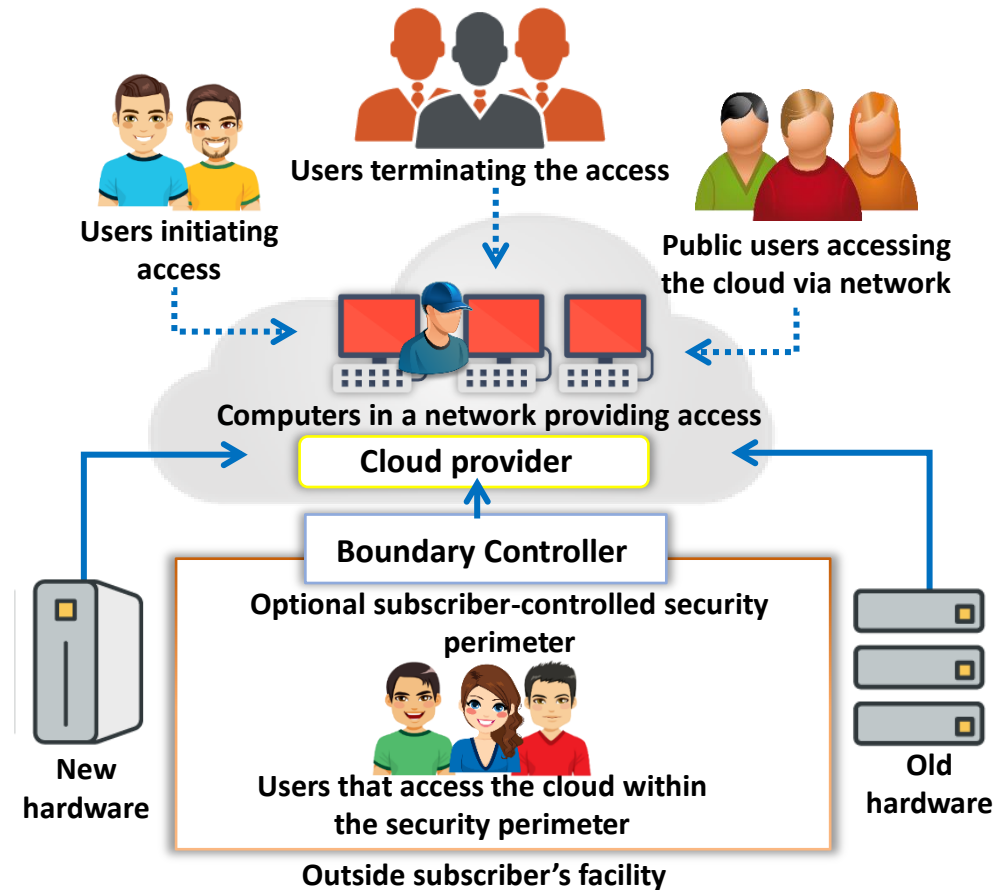


Cloud Deployment Models



Public Cloud

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

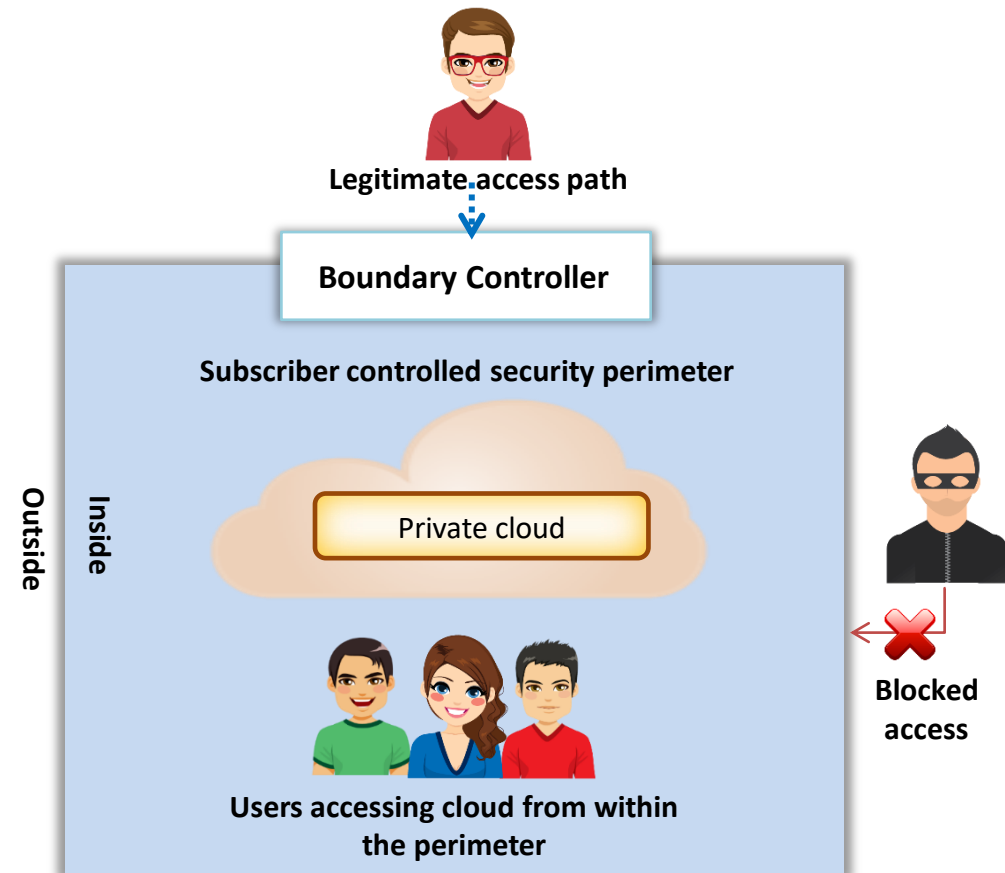


Cloud Deployment Models (Cont'd)

Private Cloud



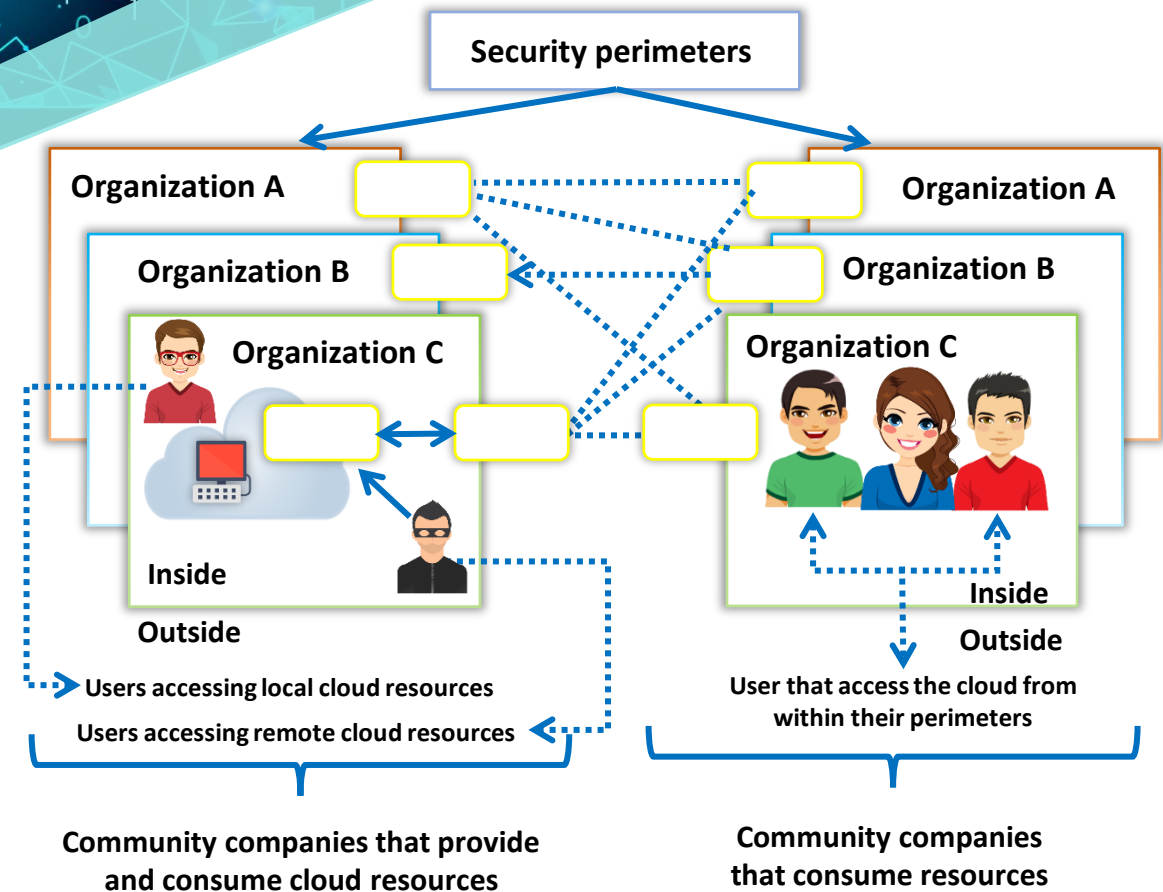
Cloud infrastructure is operated for a **single organization only**



Cloud Deployment Models (Cont'd)

Community Cloud

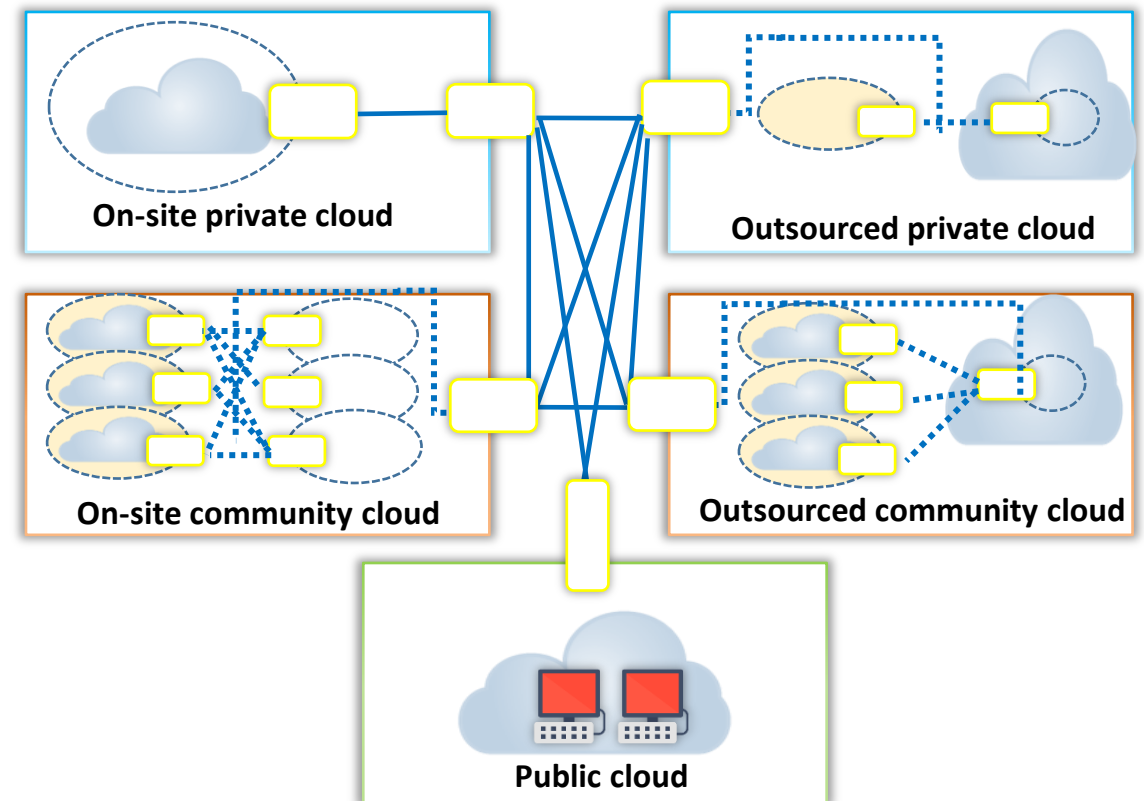
- ❑ Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)



Cloud Deployment Models (Cont'd)

Hybrid Cloud

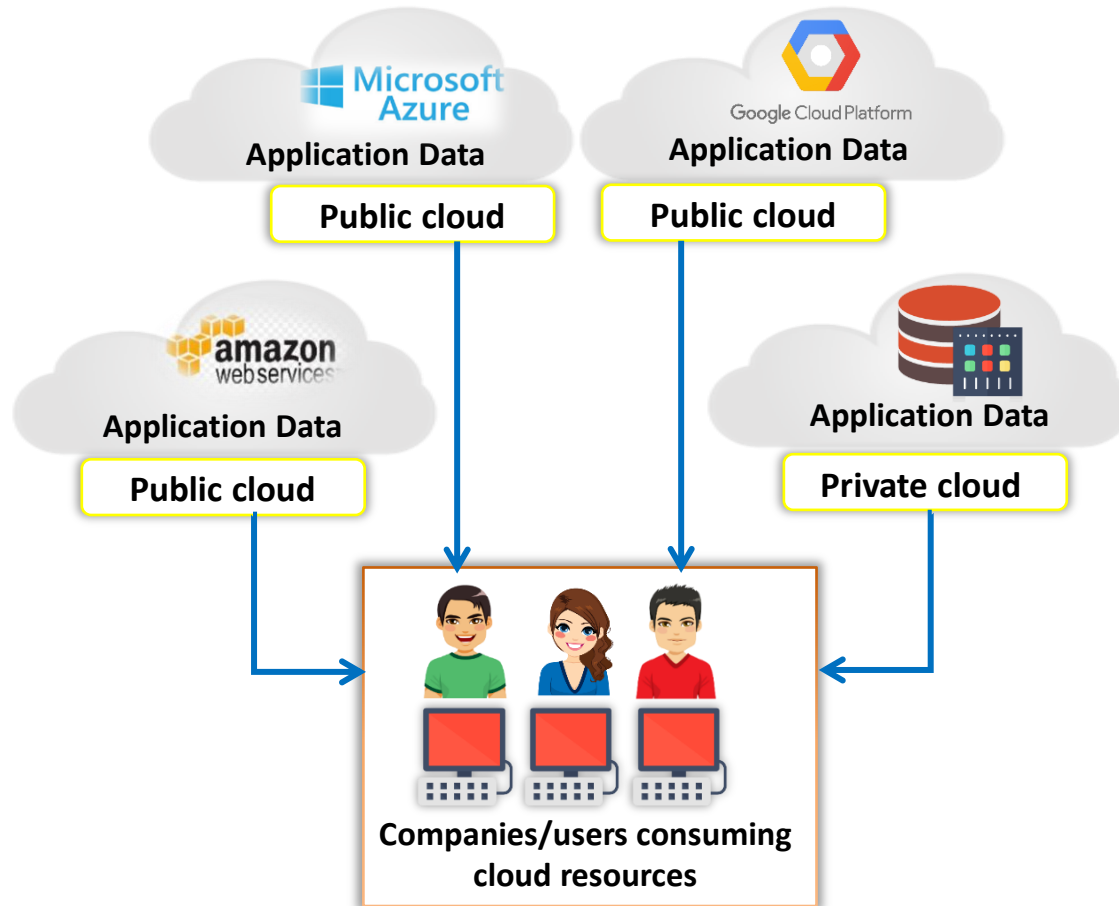
Combination of two or more clouds (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models



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



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



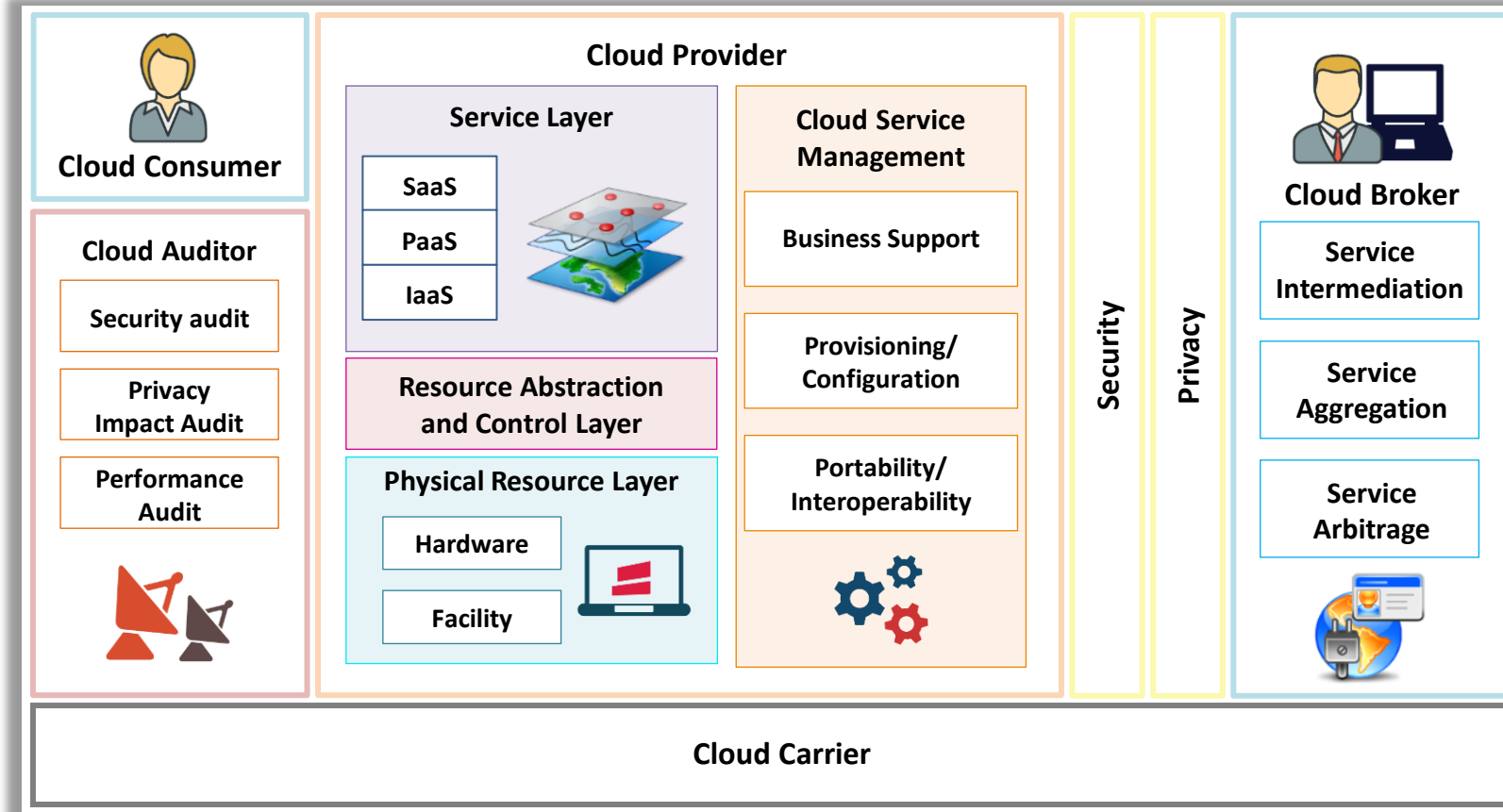
Cloud Auditor

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



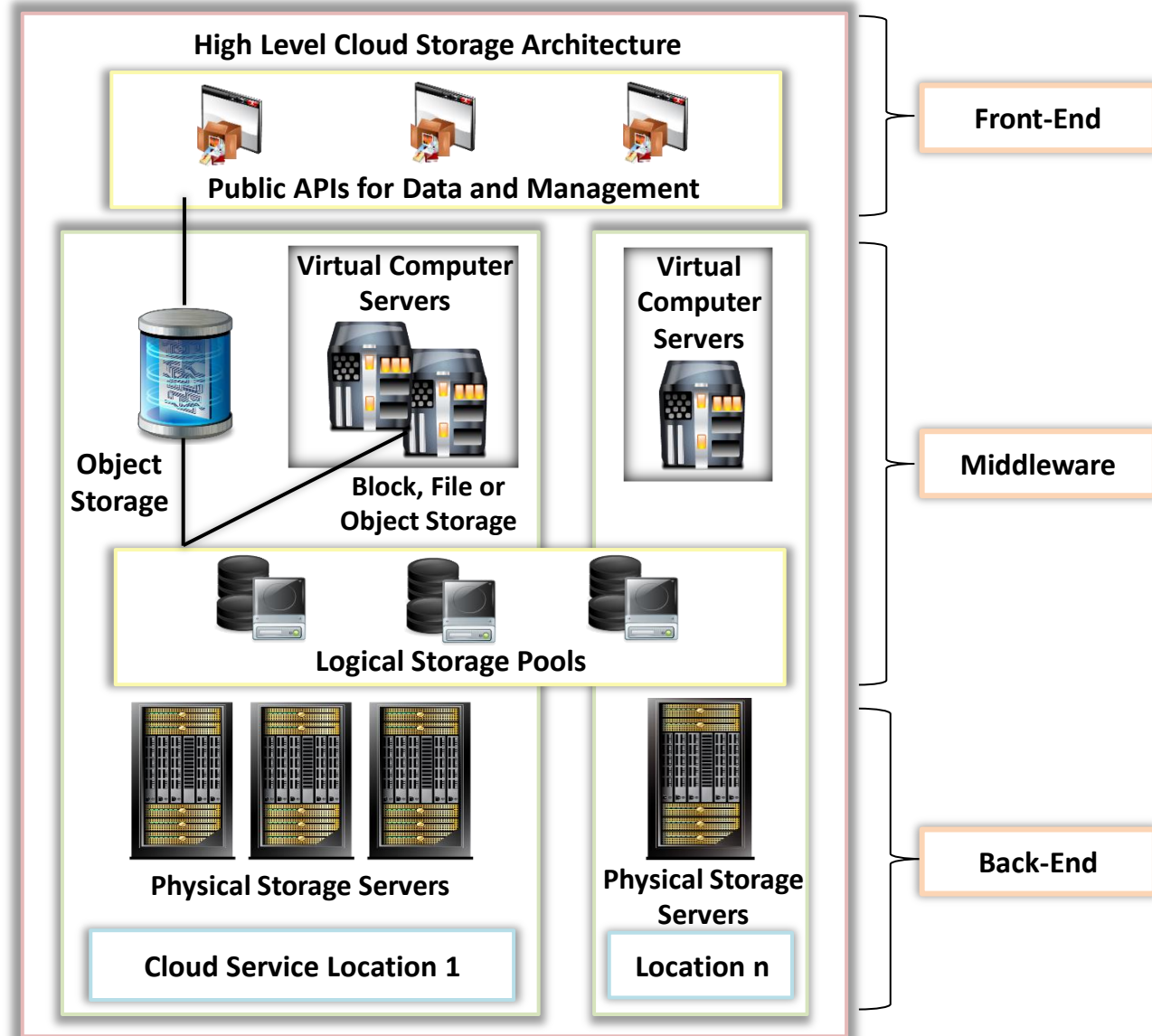
The **Front-end** layer is accessed by the **end user** where it provides APIs for the management of data storage



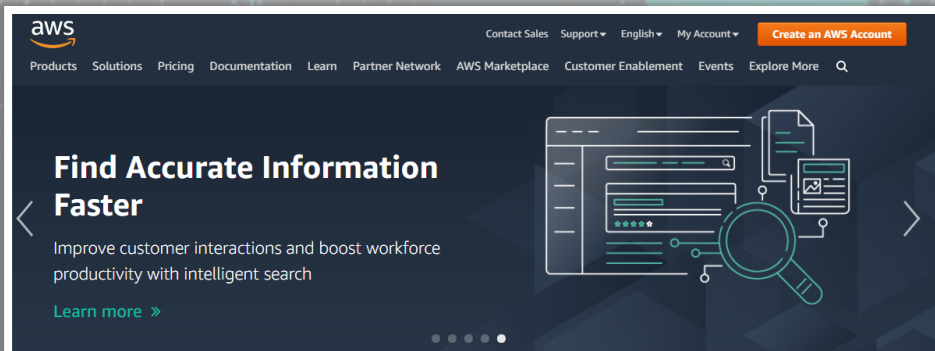
The **Middleware** layer performs several **functions** such as data de-duplication and replication of data



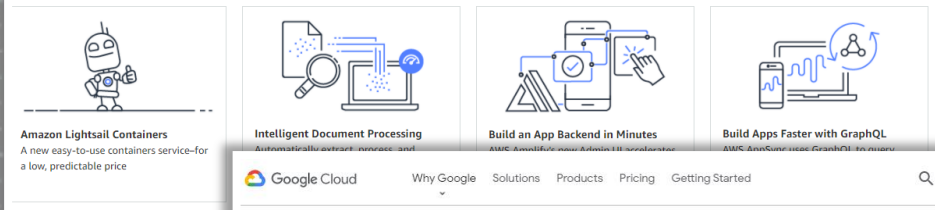
The **Back-end** layer is where the **hardware** is implemented



Cloud Service Providers

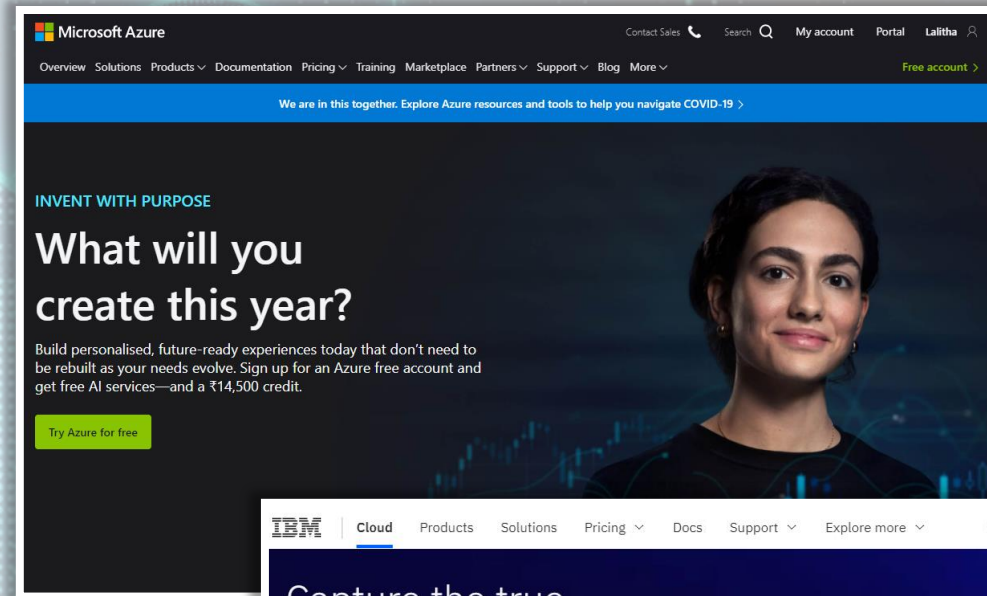


The screenshot shows the AWS homepage with a dark blue header containing navigation links like 'Products', 'Solutions', 'Pricing', 'Documentation', 'Learn', 'Partner Network', 'AWS Marketplace', 'Customer Enablement', 'Events', and 'Explore More'. A prominent orange button says 'Create an AWS Account'. The main hero section features the text 'Find Accurate Information Faster' and 'Improve customer interactions and boost workforce productivity with intelligent search', accompanied by an illustration of a magnifying glass over a document.



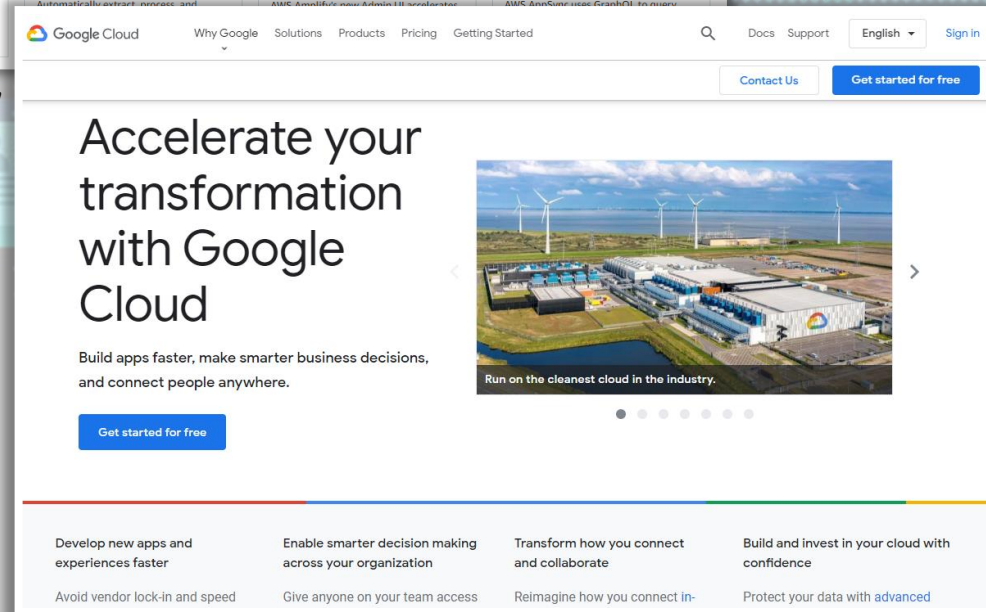
This section displays four service tiles from the AWS homepage: 'Amazon Lightsail Containers' (described as a new easy-to-use containers service), 'Intelligent Document Processing', 'Build an App Backend in Minutes', and 'Build Apps Faster with GraphQL'. Each tile includes a small icon representing the service.

<https://aws.amazon.com>



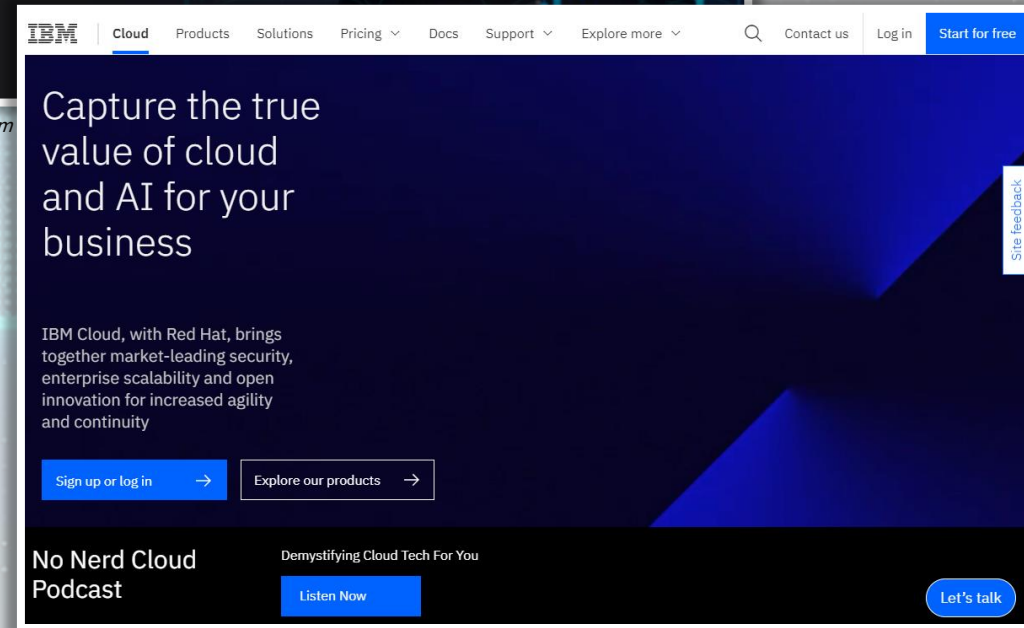
The screenshot shows the Microsoft Azure homepage with a dark blue header. The main hero section features a woman's portrait and the text 'What will you create this year?' with the subtext 'Build personalised, future-ready experiences today that don't need to be rebuilt as your needs evolve. Sign up for an Azure free account and get free AI services—and a \$14,500 credit.' A green button says 'Try Azure for free'.

<https://azure.microsoft.com>



The screenshot shows the Google Cloud homepage with a white header. The main hero section features the text 'Accelerate your transformation with Google Cloud' and 'Build apps faster, make smarter business decisions, and connect people anywhere.' Below this is a blue button 'Get started for free' and an image of a modern building with wind turbines in the background, with the text 'Run on the cleanest cloud in the industry.' The footer contains four columns of text describing various cloud services.

<https://cloud.google.com>



The screenshot shows the IBM Cloud homepage with a dark blue header. The main hero section features the text 'Capture the true value of cloud and AI for your business' and 'IBM Cloud, with Red Hat, brings together market-leading security, enterprise scalability and open innovation for increased agility and continuity.' Below this are two buttons: 'Sign up or log in' and 'Explore our products'. The footer contains two sections: 'No Nerd Cloud Podcast' and 'Demystifying Cloud Tech For You', each with a 'Listen Now' button.

<https://www.ibm.com>

Module Flow

**Understand Cloud
Computing Concepts**

01



02

**Understand Container
Technology**

**Discuss Cloud Attack
Countermeasures**

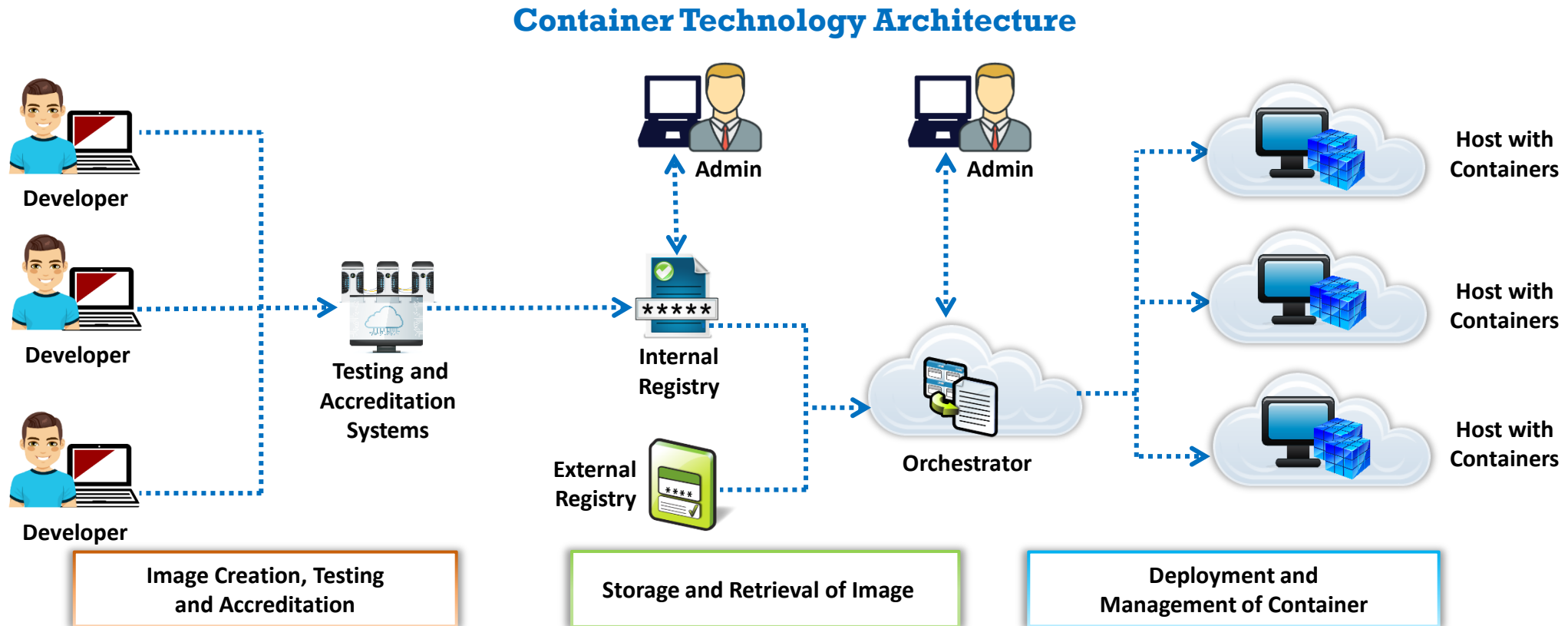
04

03

**Discuss Cloud
Computing Threats**

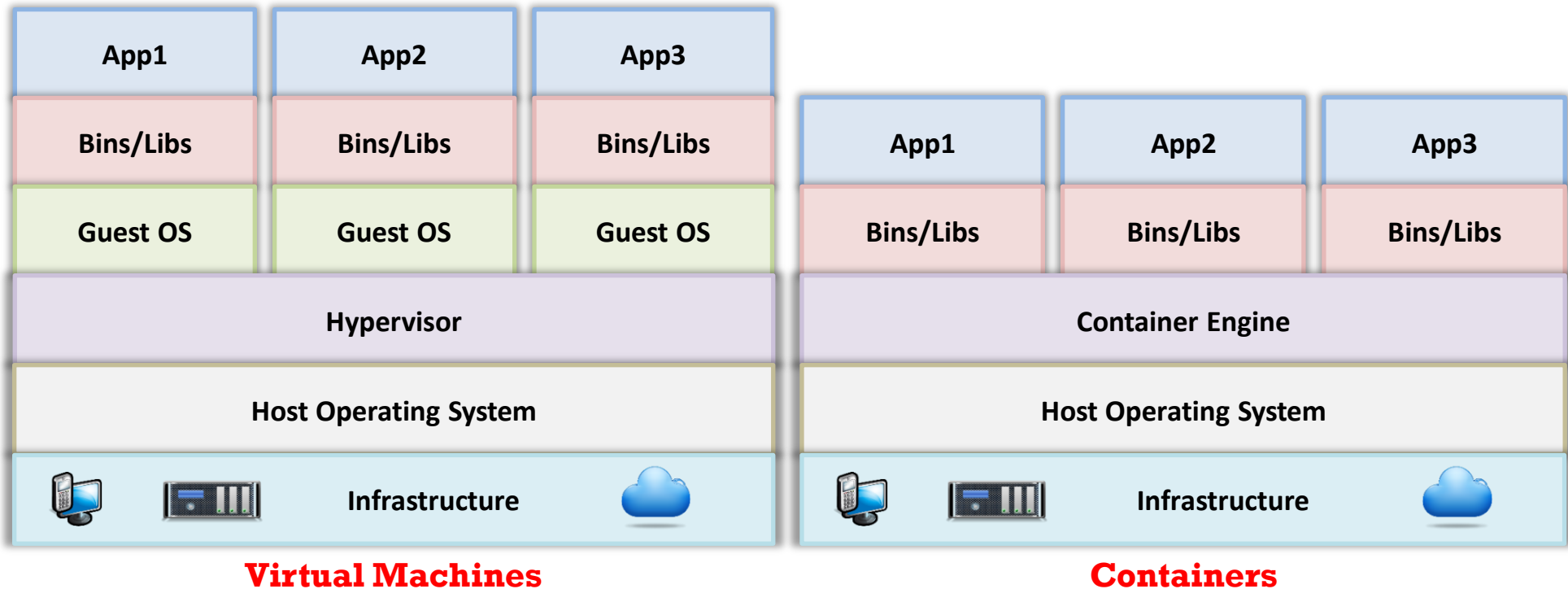
What is a Container?

- ❑ A container is a package of an **application/software** including all its dependencies such as library files, configuration files, binaries, and other resources that run independently of other processes in the cloud environment
- ❑ CaaS is a service that includes the virtualization of containers and container management through **orchestrators**



Containers Vs. Virtual Machines

- ❑ Virtualization is the ability to **run multiple operating systems on a single physical system** and share the underlying resources such as a server, storage device, or network
- ❑ Containers are placed on the top of one physical server and host operating system, and **share the operating system's kernel binaries and libraries**, thereby reducing the need for reproducing the OS



What is Docker?

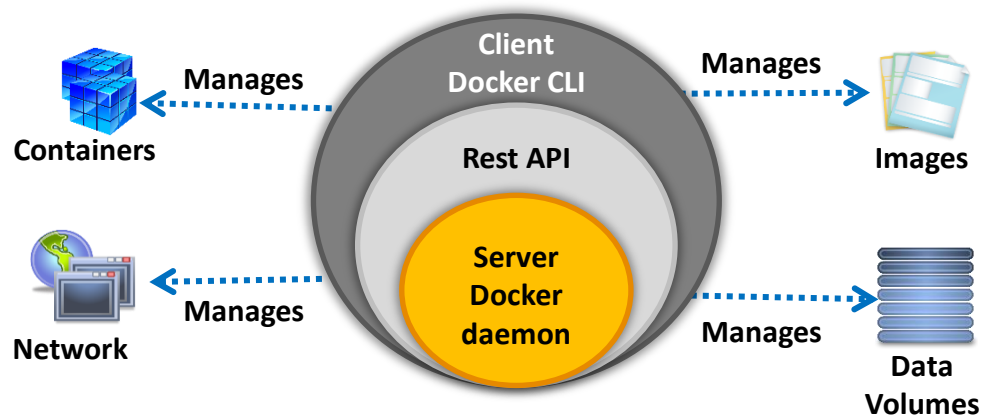


Docker is an open source technology used for developing, packaging, and running applications and all its dependencies in the **form of containers**, to ensure that the application works in a seamless environment

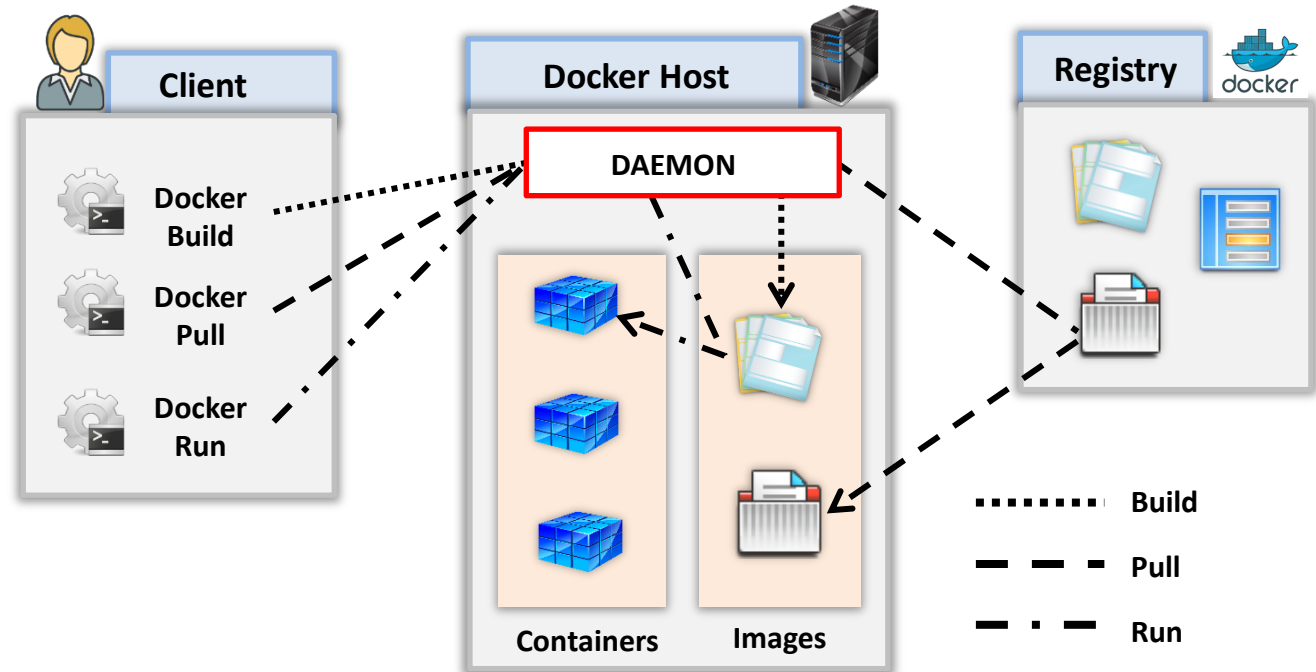


Docker provides a Platform-as-a-Service (PaaS) through **OS-level virtualization** and delivers containerized software packages

Docker Engine



Docker Architecture



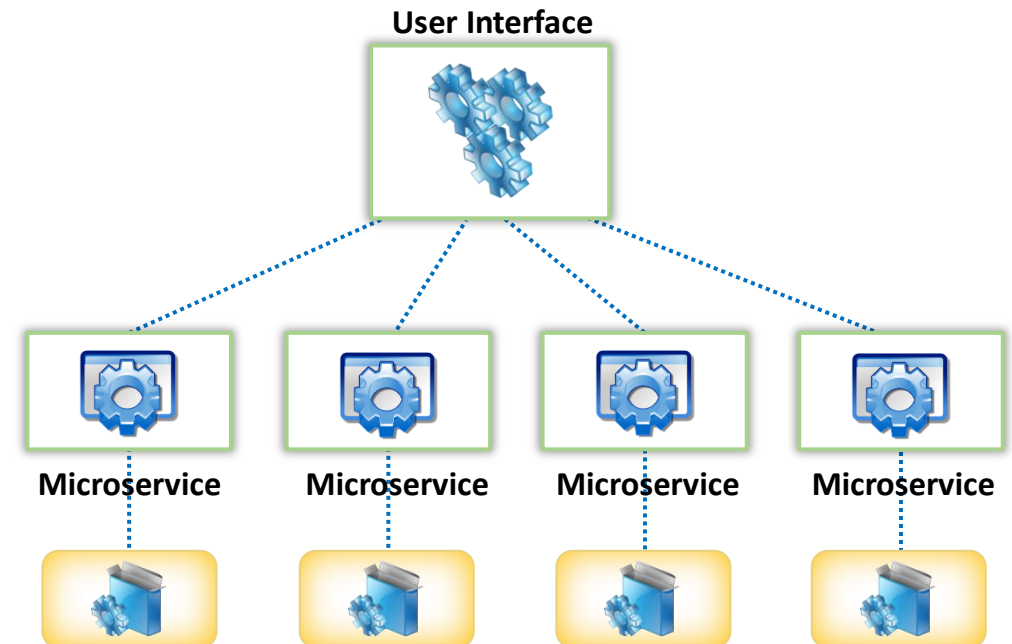
Microservices Vs. Docker

- ❑ Monolithic applications are broken down into cloud-hosted sub-applications called **microservices** that work together, each performing a unique task
- ❑ As each microservice is packaged into the **Docker container** along with the required libraries, frameworks, and configuration files, microservices belonging to a single application can be developed and managed using multiple platforms

Monolithic Application



Microservices Application



Docker Networking



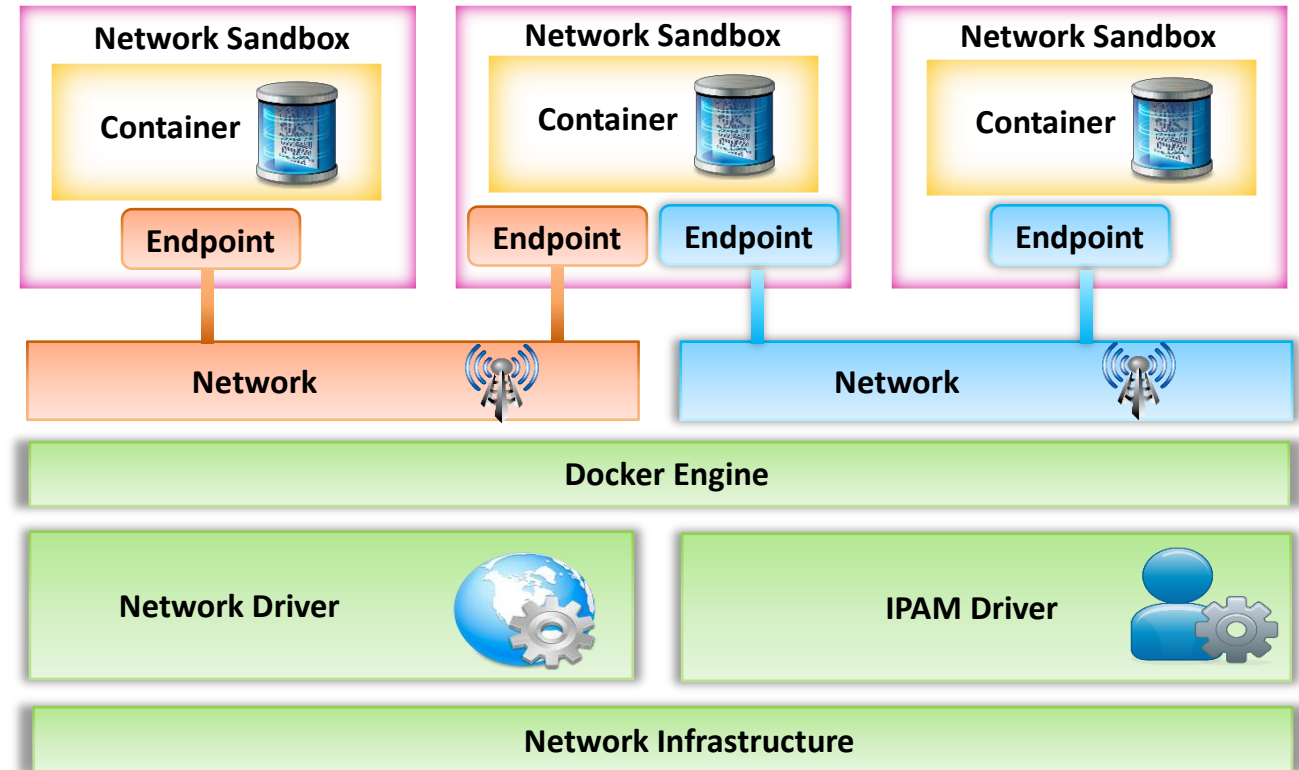
Docker **connects multiple containers** and services or other non-Docker workloads together



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



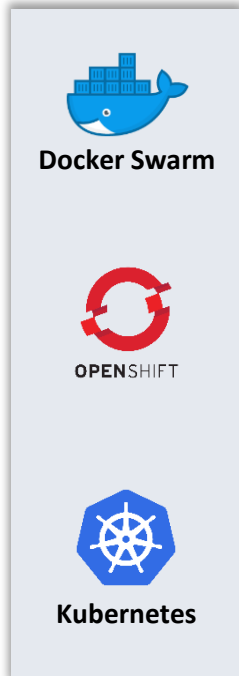
Container Orchestration

- ❑ An automated process of managing the **lifecycles of software containers** and their dynamic environments
- ❑ It is used for **scheduling and distributing** the work of individual containers for microservices-based applications spread across multiple clusters

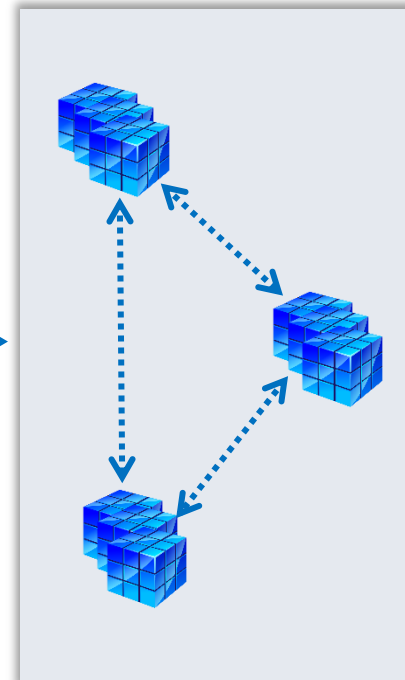
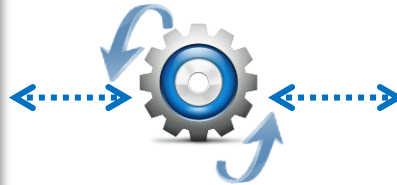
Container Orchestration Software

Automate Tasks

Application environment with multiple containers



- Scaling
- Provisioning
- Deployment
- Configuration
- Availability
- Security
- Health monitoring
- Load balancing
- Resource allocation



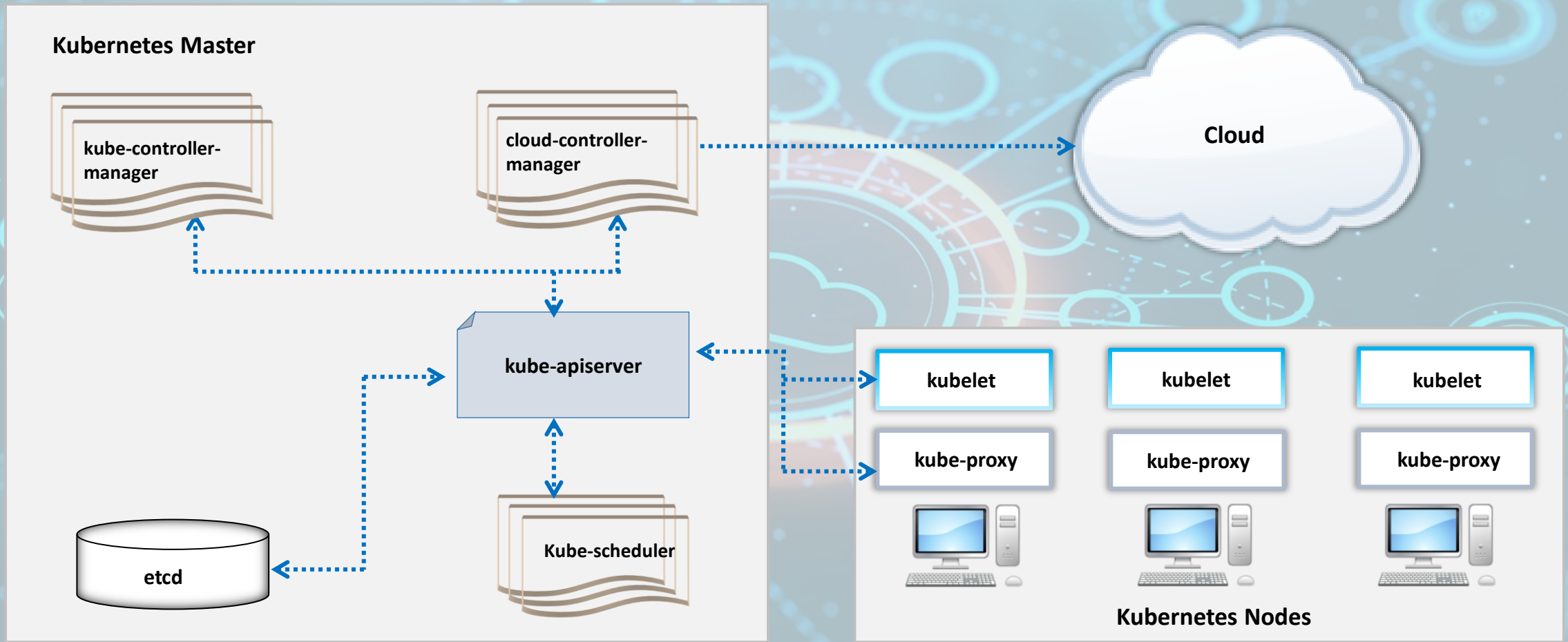
What is Kubernetes?

- ❑ 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 Features:

- ❖ Service discovery
- ❖ Load balancing
- ❖ Storage orchestration
- ❖ Automated rollouts and rollbacks
- ❖ Automatic bin packing
- ❖ Self-healing
- ❖ Secret and configuration management

Kubernetes Cluster Architecture



Kubernetes Vs. Docker

01

Docker is open source software that can be installed on any host to build, deploy, and **run containerized applications** on a single operating system

02

When Docker is installed on multiple hosts with different operating systems, you can use **Kubernetes** to manage these Docker hosts

03

Kubernetes is a **container orchestration platform** that automates the process of creating, managing, updating, scaling, and destroying containers

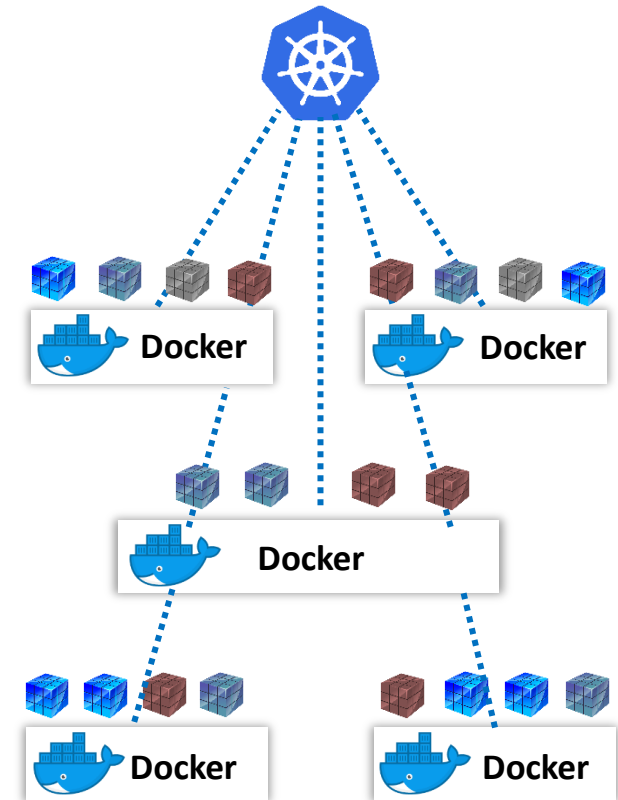
04

Kubernetes can be coupled with any containerization technology such as Docker, Rkt, RunC, and cri-o

05

Both Dockers and Kubernetes are based on microservices architecture, and built using the **Go programming language** to deploy small, lightweight binaries, and YAML files for specifying application configurations and stacks

Kubernetes Deployment



Kubernetes and Docker run together to build and run containerized applications

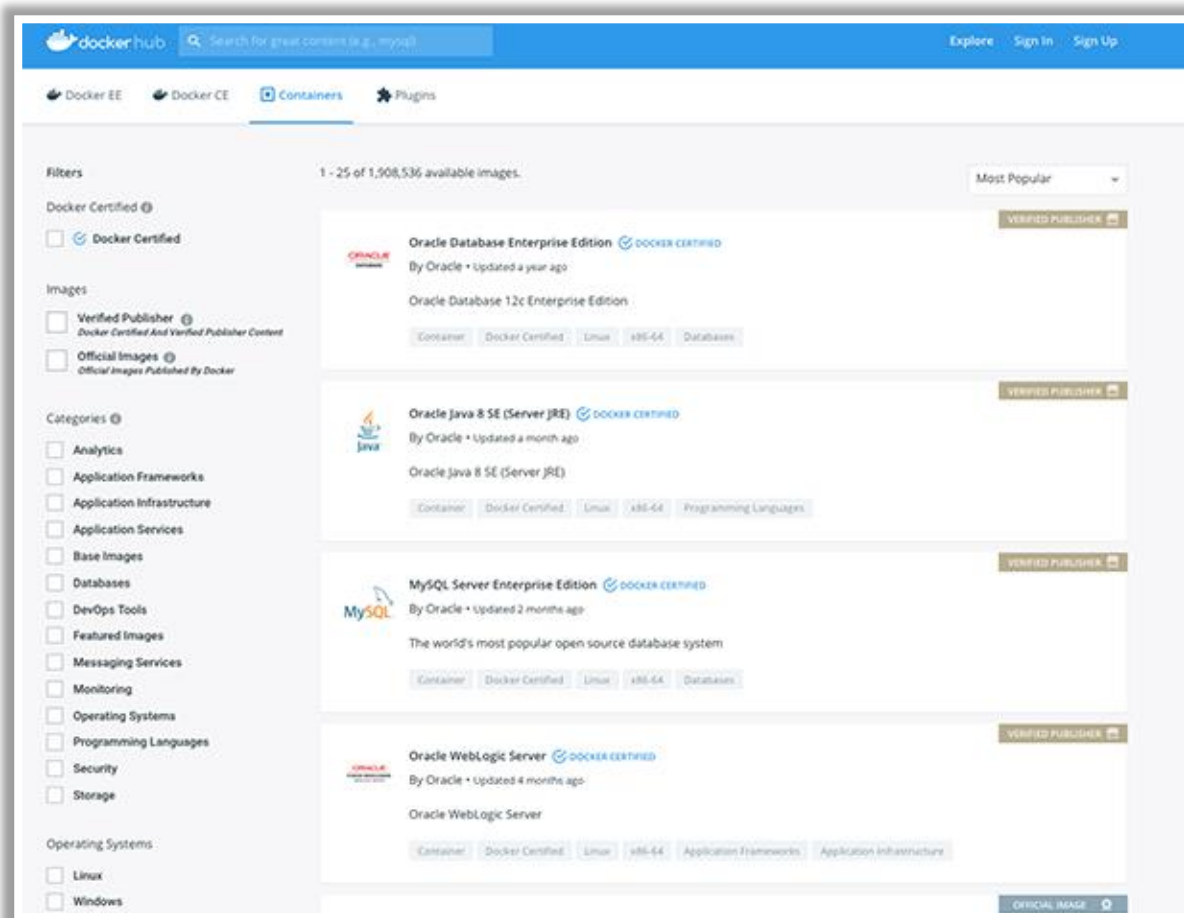
Container Security Challenges



Container Management Platforms

Docker

A **container platform** that helps in building, managing, and securing all the applications and deploying them across cloud environments



<https://www.docker.com>



Amazon Elastic Container Service (ECS)

<https://aws.amazon.com>



Microsoft Azure Container Instances (ACI)

<https://azure.microsoft.com>



Red Hat OpenShift Container Platform

<https://www.openshift.com>



Portainer

<https://www.portainer.io>



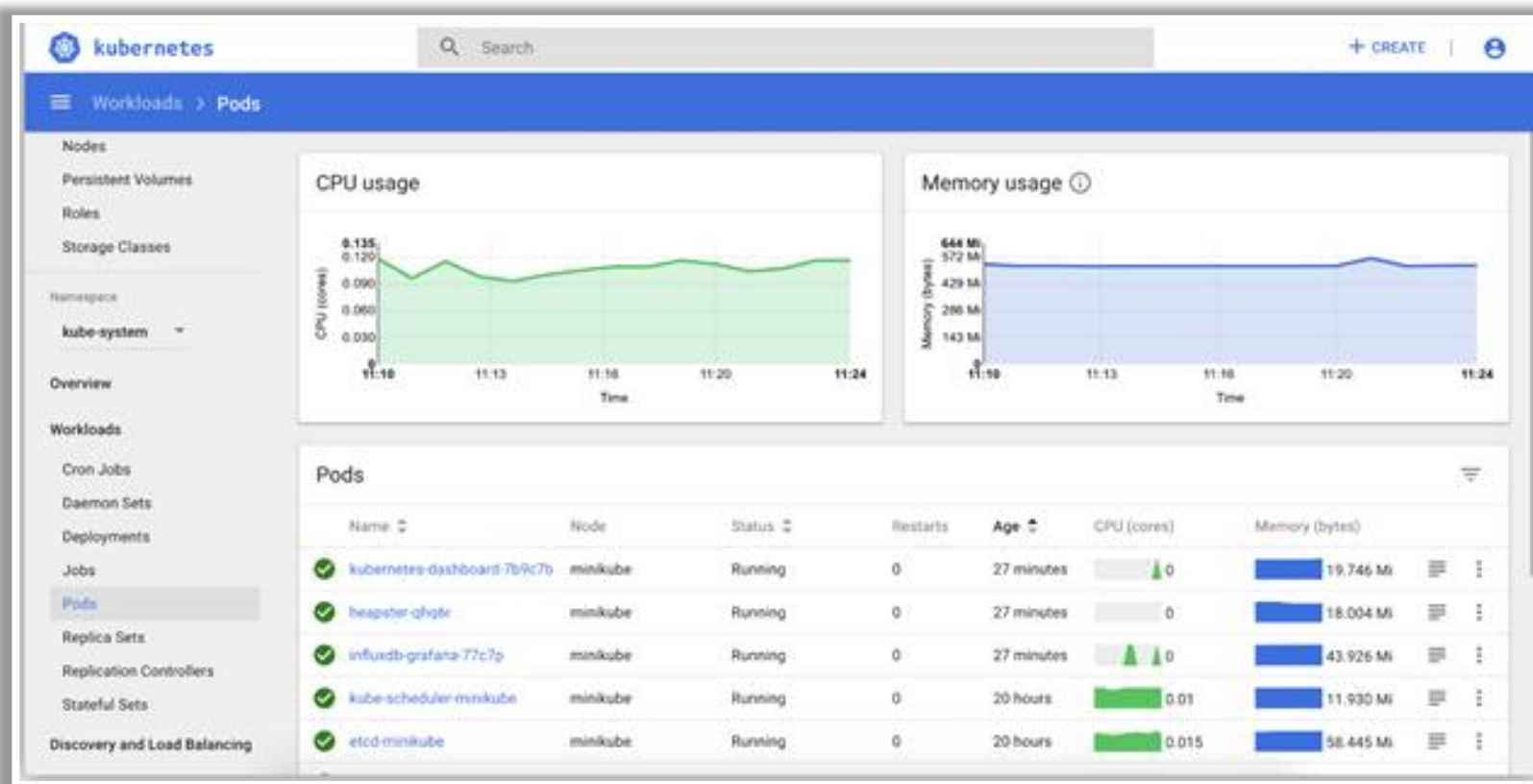
HPE Ezmeral Container Platform

<https://www.hpe.com>

Kubernetes Platforms

Kubernetes

An open-source **container orchestration engine** for automating deployment, scaling, and management of containerized applications



<https://kubernetes.io>



Amazon Elastic Kubernetes Service (EKS)

<https://aws.amazon.com>



Docker Kubernetes Service (DKS)

<https://www.docker.com>



Knative

<https://cloud.google.com>



IBM Cloud Kubernetes Service

<https://www.ibm.com>



Google Kubernetes Engine (GKE)

<https://cloud.google.com>

Module Flow

**Understand Cloud
Computing Concepts**

01



02

**Understand Container
Technology**

03

**Discuss Cloud
Computing Threats**

**Discuss Cloud Attack
Countermeasures**

04

OWASP Top 10 Cloud Security Risks

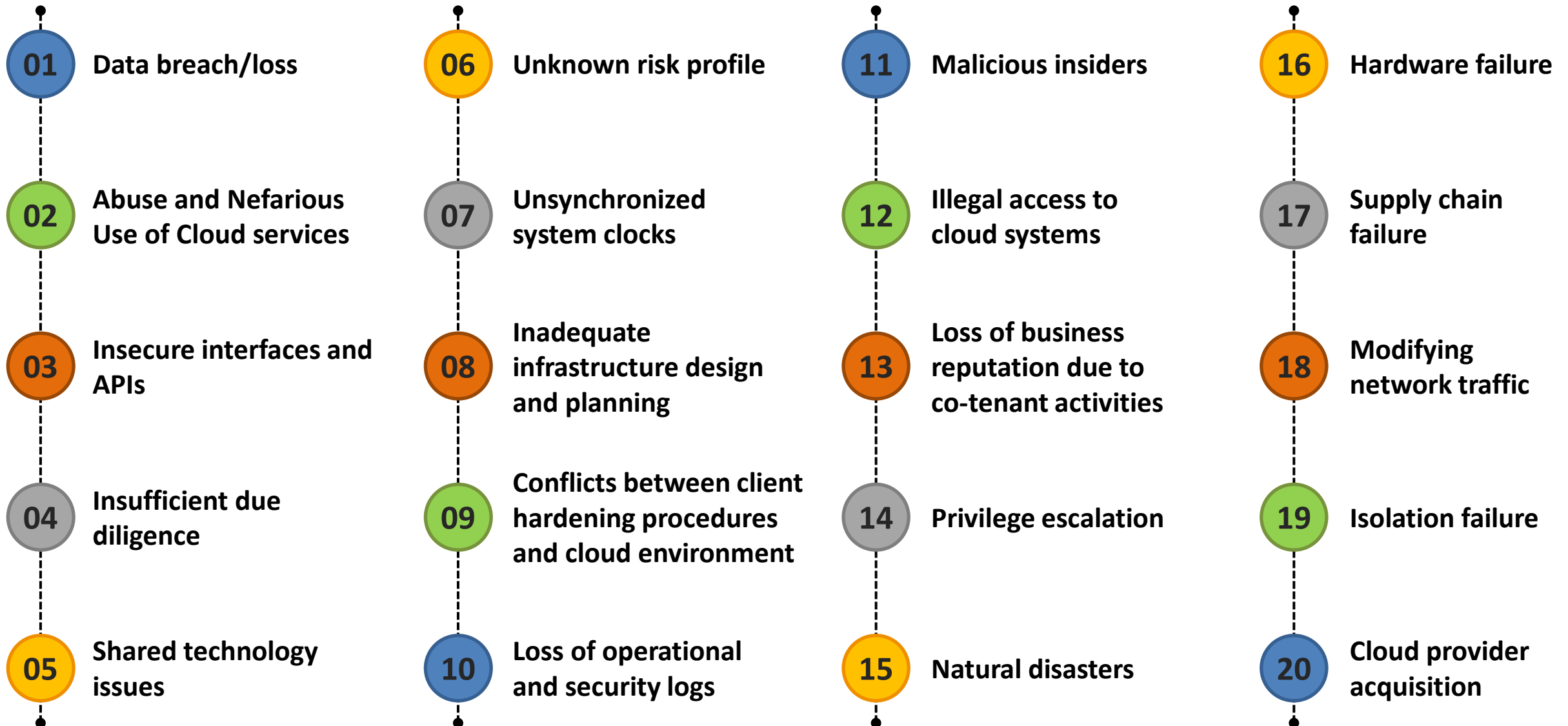
Risks	Description
R1 - Accountability and Data Ownership	Using the public cloud for hosting business services can cause severe risk for the recoverability of data
R2 - User Identity Federation	Creating multiple user identities for different cloud providers makes it complex to manage multiple user IDs and credentials
R3 - Regulatory Compliance	There is a lack of transparency, and there are different regulatory laws in different countries
R4 - Business Continuity and Resiliency	There can be business risk or monetary loss if the cloud provider handles the business continuity improperly
R5 - User Privacy and Secondary Usage of Data	The default share feature in social web sites can jeopardize the privacy of user's personal data

<https://www.owasp.org>

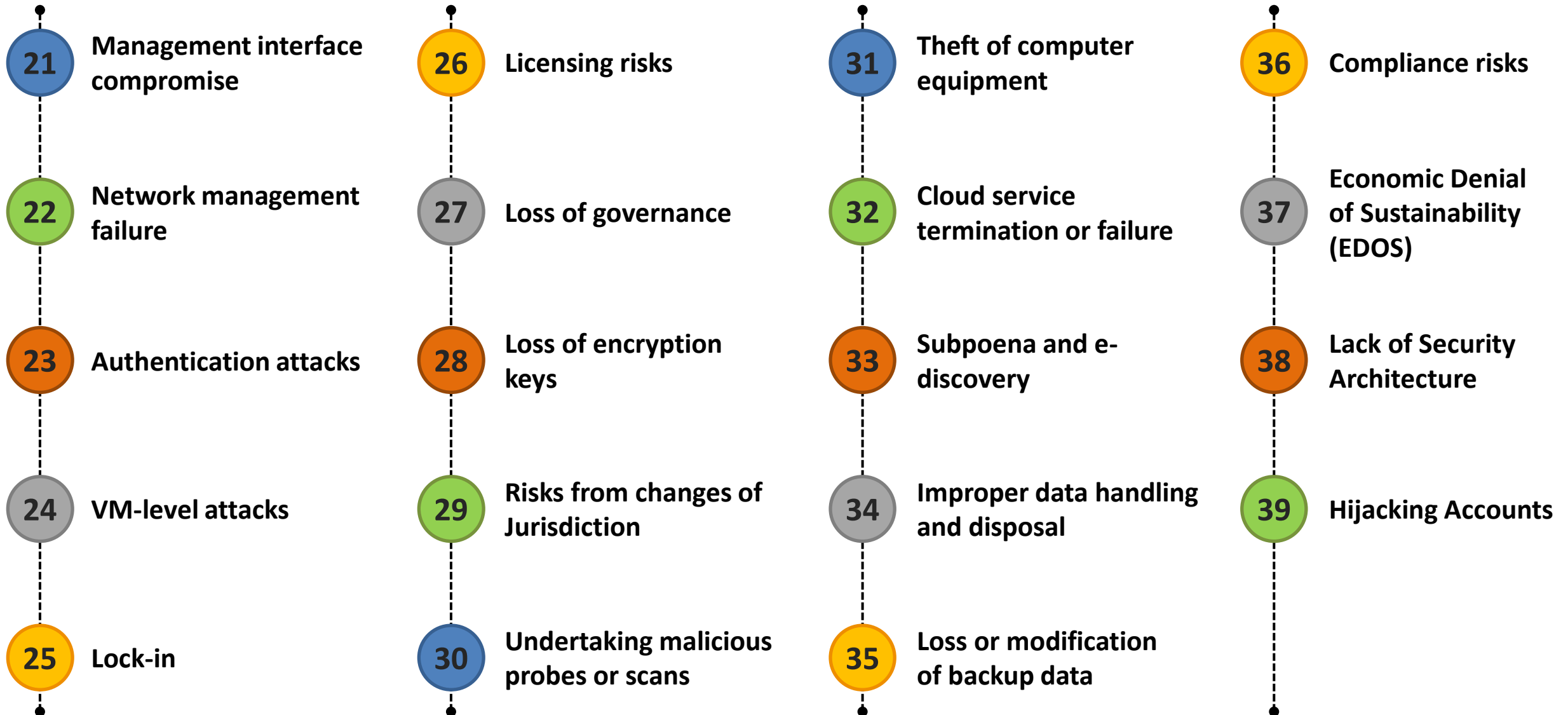
OWASP Top 10 Cloud Security Risks (Cont'd)

Risks	Description
R6 - Service and Data Integration	Unsecured data in transit is susceptible to eavesdropping and interception attacks
R7 - Multi Tenancy and Physical Security	Poor logical segregation may lead to tenants interfering with the security features of other tenants
R8 - Incident Analysis and Forensic Support	Due to the distributed storage of logs across the cloud, law enforcement agencies may face problems in forensics recovery
R9 - Infrastructure Security	Misconfiguration of infrastructure may allow network scanning for vulnerable applications and services
R10 - Non-Production Environment Exposure	Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification

Cloud Computing Threats

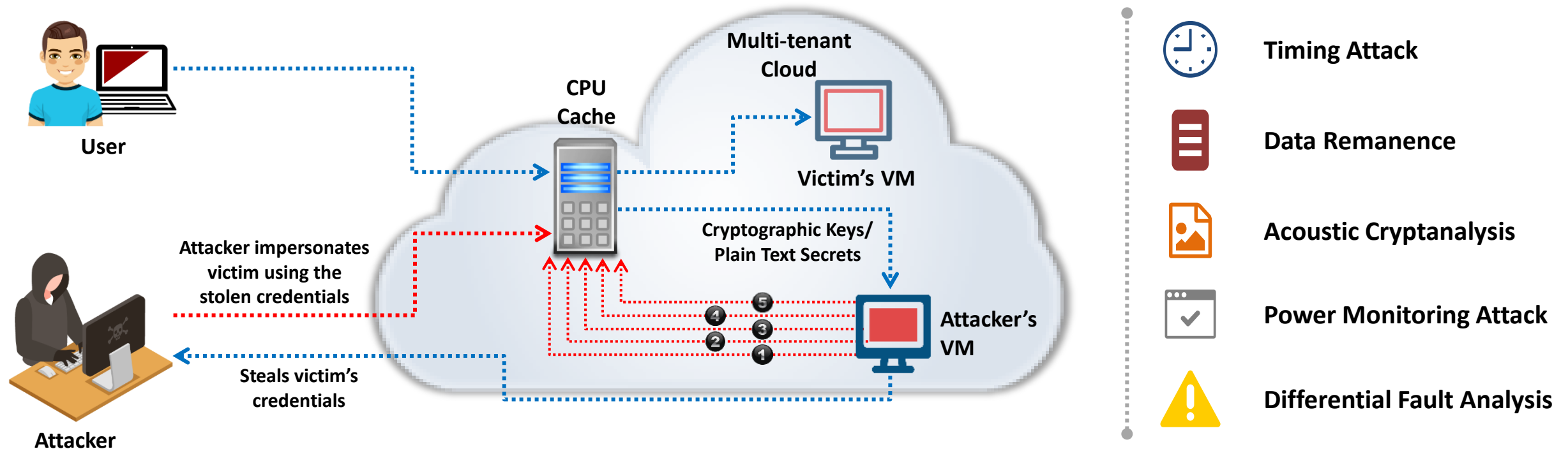


Cloud Computing Threats (Cont'd)



Cloud Attacks: Side-Channel Attacks or Cross-guest VM Breaches

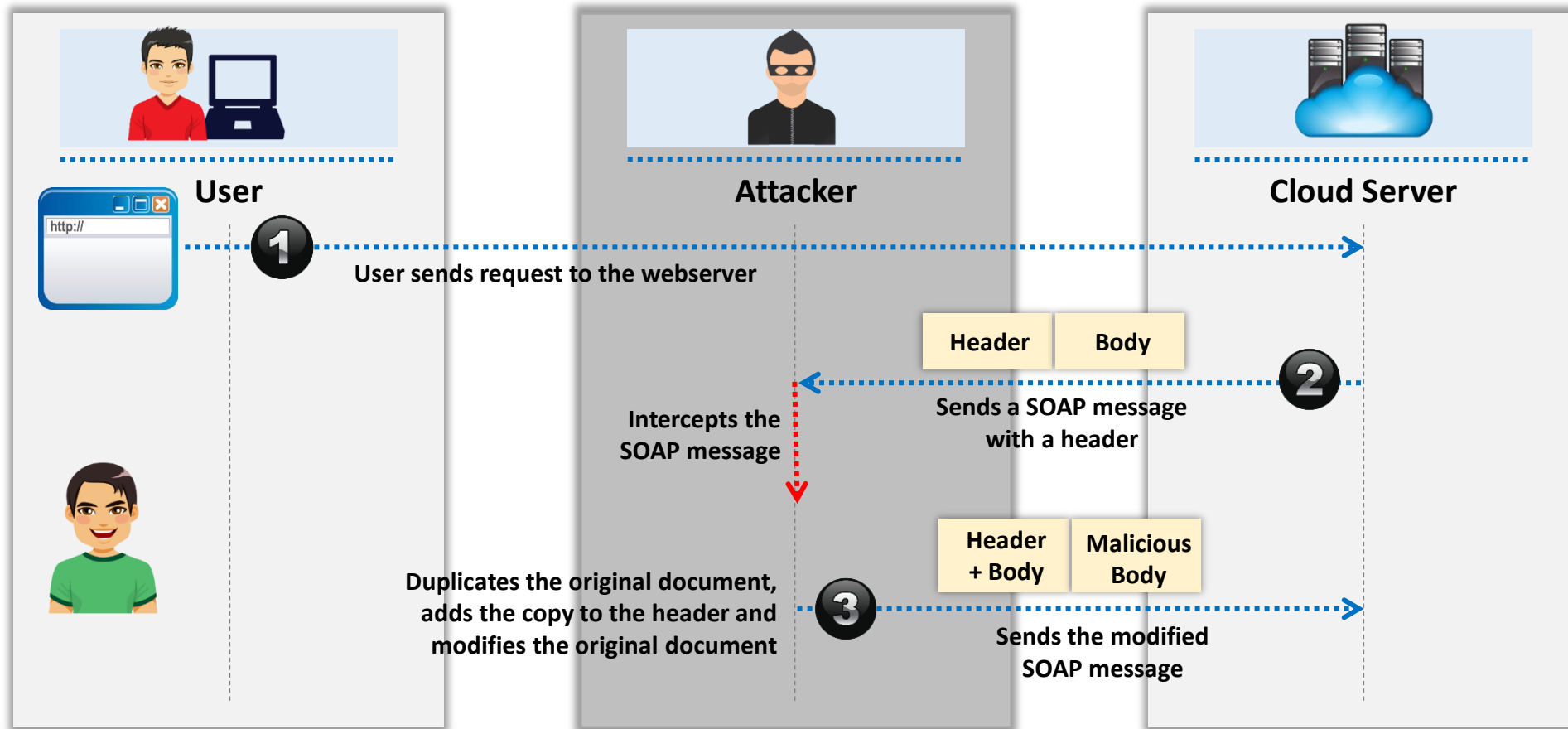
- ❑ The attacker compromises the cloud by placing a **malicious virtual machine** near to a target cloud server and then launches a side-channel attack
- ❑ In a side-channel attack, the attacker **runs a virtual machine on the same physical host as the victim's virtual machine** and takes advantage of the shared physical resources (processor cache) to **steal data** (cryptographic keys) from the victim
- ❑ Side-channel attacks can be implemented by any **co-resident user** due to the vulnerabilities in shared technology resources



Cloud Attacks: Wrapping Attack



A wrapping attack is performed during the **translation of the SOAP message** in the TLS layer where attackers duplicate the body of the message and sends it to the server as a legitimate user



Cloud Attacks: Man-in-the-Cloud (MITC) Attack

1

MITC attacks are an advanced version of Man-in-the-middle (MITM) attacks

2

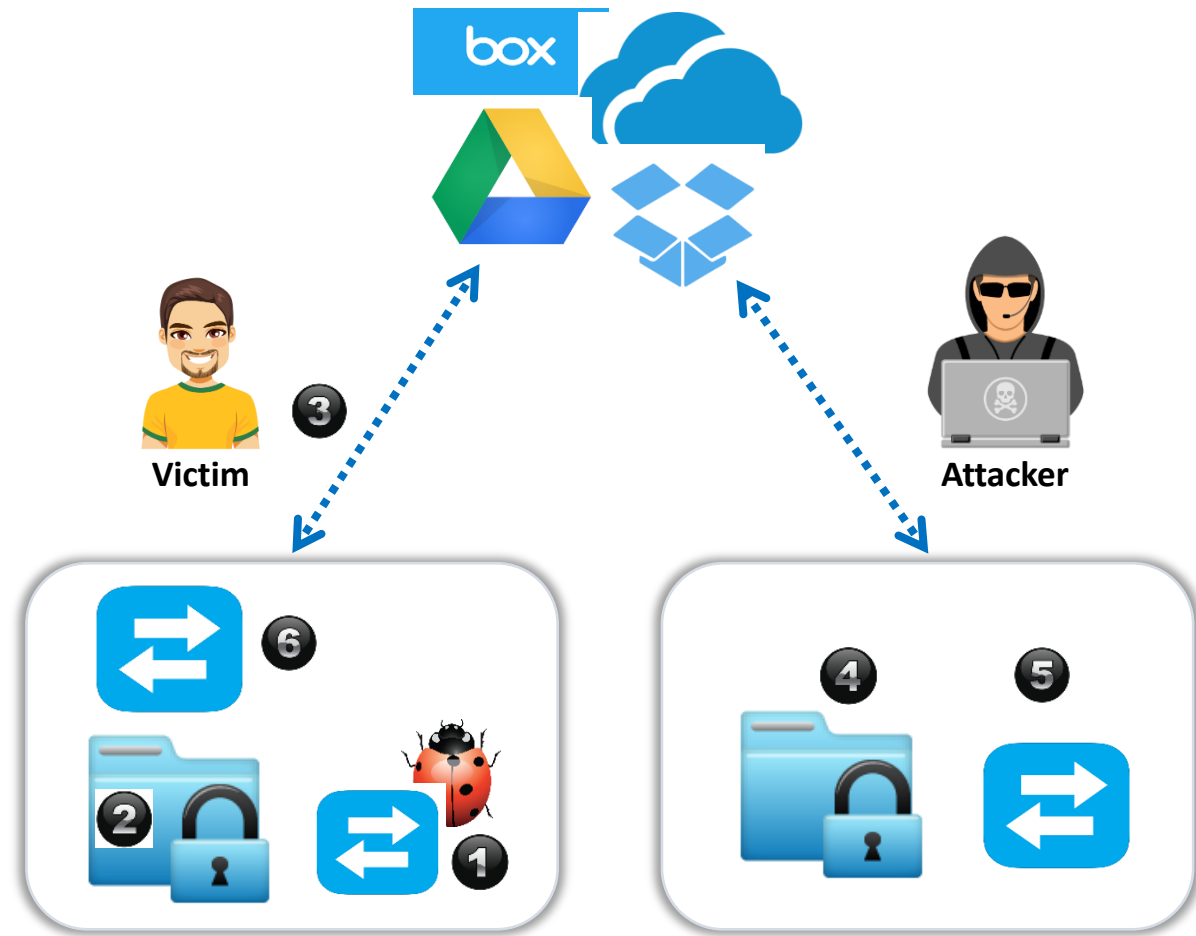
The attacker tricks the victim into **installing a malicious code**, which plants the attacker's **synchronization token** on the victim's drive

3

Then, the attacker steals the victim's synchronization token and uses the stolen token to **gain access** to the victim's files

4

Later, the attacker **restores the malicious token** with the original synchronized token of the victim, thus returning the drive application to its **original state** and stays undetected



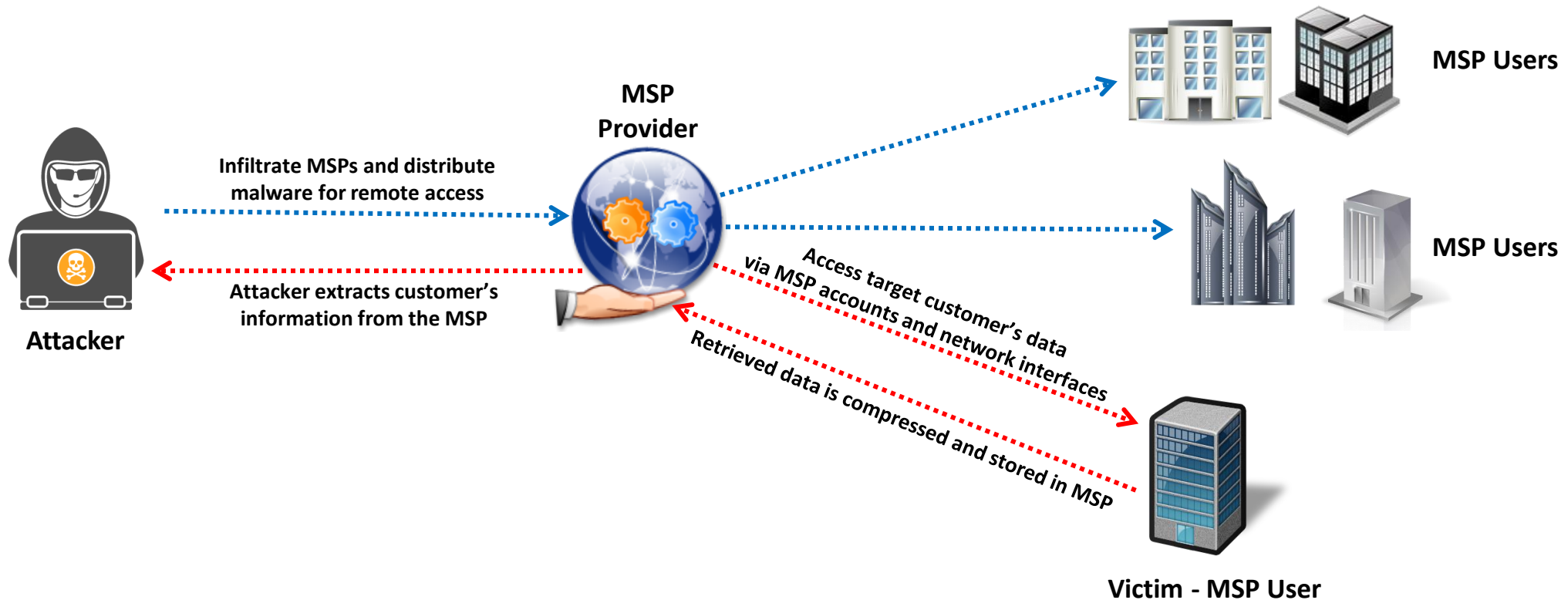
Cloud Attacks: Cloud Hopper Attack



Cloud Hopper attacks are **triggered at the managed service providers** (MSPs) and their users

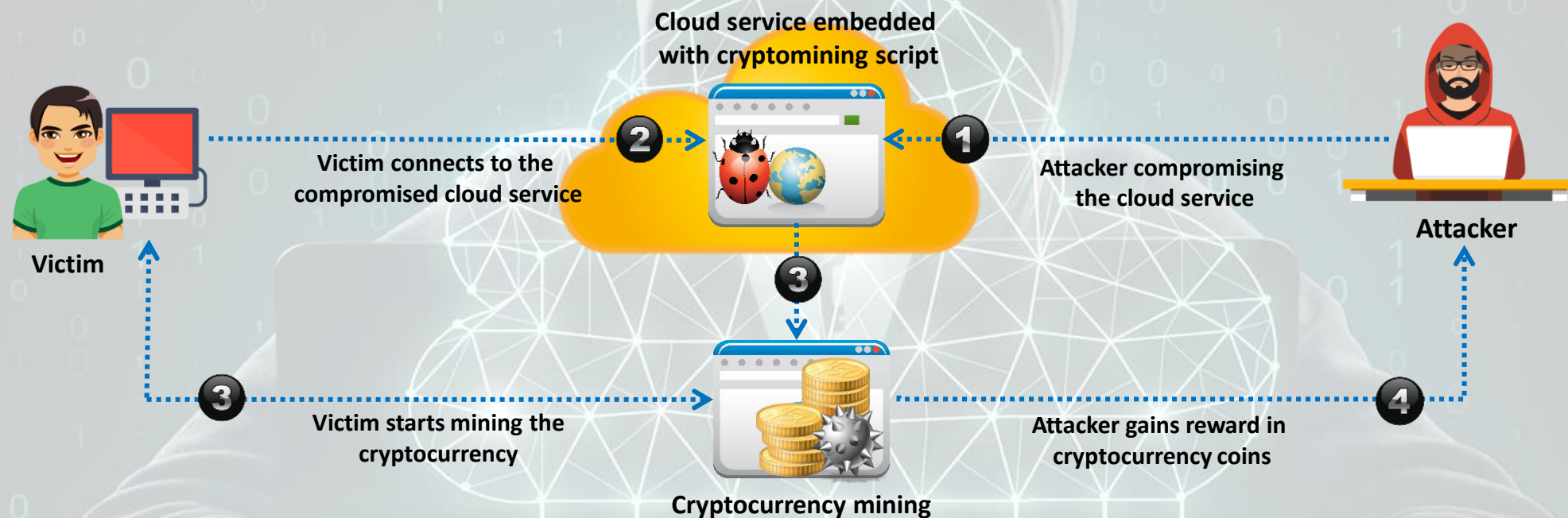


Attackers initiate **spear-phishing emails** with custom-made malware to compromise the accounts of staff or cloud service firms to obtain confidential information



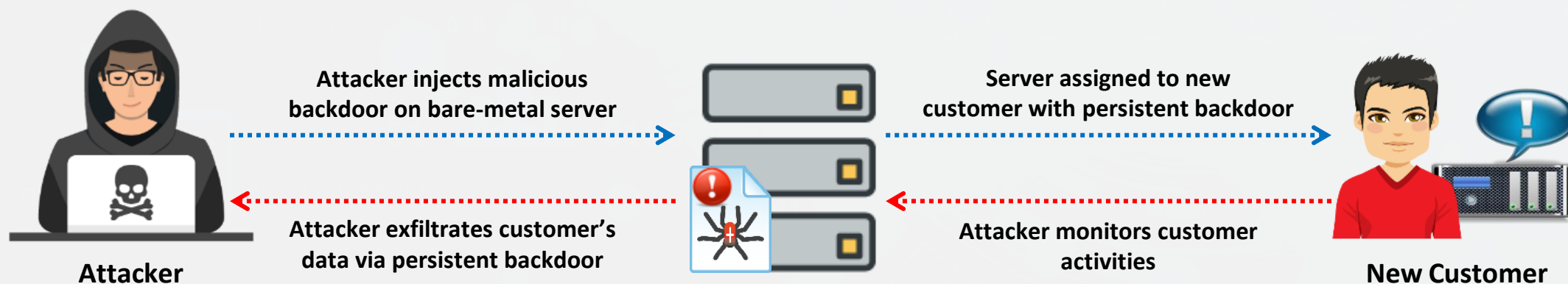
Cloud Attacks: Cloud Cryptojacking

- ❑ Cryptojacking is the unauthorized use of the victim's computer to **stealthily mine digital currency**
- ❑ Cryptojacking attacks are **highly lucrative**, which involve both external attackers and rogue insiders
- ❑ To perform this attack, the attackers leverage attack vectors like cloud misconfigurations, compromised websites, and client or server-side vulnerabilities



Cloud Attacks: Cloudborne Attack

- ❑ Cloudborne is a vulnerability residing in a **bare-metal cloud server** that enables the attackers to implant a malicious backdoor in its firmware
- ❑ The malicious backdoor can allow the attackers to **bypass the security mechanisms** and perform various activities such as watching new user's activity or behavior, disabling the application or server, and intercepting or stealing the data



Enumerating S3 Buckets using lazys3

lazys3



Simple storage service (S3) is a scalable **cloud storage service** used by Amazon AWS where files, folders, and objects are stored via web APIs



Attackers often try to the **find the bucket's location and name** to test its security and identify vulnerabilities in the bucket implementation

- ❑ lazys3 is a **Ruby script tool** that is used to brute-force AWS S3 buckets using different permutations

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~/lazys3]
#ruby lazys3.rb HackerOne
Generated wordlist from file, 9013 items...
Found bucket: HackerOne.admin-dev (404)
Found bucket: HackerOne-admin.staging (404)
Found bucket: HackerOne.admin-prod (404)
Found bucket: HackerOne-administration-dev (404)
Found bucket: HackerOne-administration-stage (404)
Found bucket: HackerOne.administration-production (404)
Found bucket: HackerOne-administration.test (404)
Found bucket: HackerOne-administrator.development (404)
Found bucket: HackerOne-administratordevelopment (404)
```

<https://github.com>

Cloud Attack Tools



Nimbostratus

- ❑ A tool used for **fingerprinting** and **exploiting** Amazon cloud infrastructures
- ❑ It allows attackers to **enumerate access to AWS services** for the current IAM role, extract the current AWS credentials from metadata, etc.

```
root@rrr0b0t:~/nimbostratus# ./nimbostratus -v dump-ec2-metadata --mangle-function=core.utils.mangle.mangle
Starting dump-ec2-metadata
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/ami-manifest-path
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/instance-type
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/instance-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/local-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/ami-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/instance-action
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/profile
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/reservation-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/security-groups
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/metrics/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/mac
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/public-ipv4
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/services/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/local-ipv4
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/placement/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/ami-launch-index
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/public-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/public-keys/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/block-device-mapping/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/info
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/Safe_way_to_distribute_aws_credentials
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/local-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/security-groups
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/public-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/vpc-ipv4-cidr-blocks
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/subnet-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/public-ipv4s
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/interface-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/mac
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/security-group-ids
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/vpc-ipv4-cidr-block
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/mac/02:da:ed:7d:28:12/owner-id
```

<https://andresriancho.github.io>



S3Scanner

<https://github.com>



Cloud Container Attack Tool (CCAT)

<https://github.com>



Pacu

<https://github.com>



DumpsterDiver

<https://github.com>



GCPBucketBrute

<https://rhinosecuritylabs.com>

Module Flow



Cloud Attack Countermeasures

1

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

2

Enforce **SLAs** for patching and vulnerability remediation

3

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

4

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

5

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

6

Implement **strong key generation**, storage and management, and destruction practices

Cloud Attack Countermeasures (Cont'd)

7

Ensure that the cloud undergoes regular **security checks and updates**

8

Ensure that physical security is a **24 x 7 x 365** affair

9

Enforce **security standards** in installation/configuration

10

Ensure that the memory, storage, and network access is **isolated**

11

Implement a baseline **security breach notification** process

12

Analyze **API dependency chain** software modules



Cloud Attack Countermeasures (Cont'd)

Side-Channel Attack

- ✓ Implement a **virtual firewall** in the cloud server back-end of the cloud computing
- ✓ Implement **random encryption** and decryption
- ✓ Lockdown **OS images** and application instances to prevent compromising vectors that might provide access

Wrapping Attack

- ✓ Use **XML schema** validation to detect SOAP messages
- ✓ Apply authenticated encryption in the **XML encryption** specification

MITC Attack

- ✓ Use an **email security** gateway to detect the social engineering attacks
- ✓ Harden the policies of **token expiration**
- ✓ Implement **cloud access security broker** (CASB) to monitor cloud traffic

Cloud Attack Countermeasures (Cont'd)



Cloud Hopper Attack

- ✓ Implement **multi-factor authentication** to prevent compromise of credentials
- ✓ Ensure mutual co-ordination between **customers and CSPs** in case of abnormal incidents or activities
- ✓ Ensure customers are aware and follow the **cloud service policies**



Cloud Cryptojacking

- ✓ Ensure to implement a **strong password** policy
- ✓ Always preserve three different copies of the data in different places and one copy **off-site**
- ✓ Implement **CoinBlocker URL** and IP Blacklist/blackholing in the firewall



Cloudborne Attack

- ✓ CSPs should keep the firmware **up-to-date**
- ✓ Sanitize the **server firmware** before it is assigned to new customers

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

1

In this module, we introduced the cloud computing concepts and various types of cloud computing services

2

We also discussed the importance of container technology

3

We fully examined the cloud computing threats and attacks



4

Additionally, we reviewed the various countermeasures to be employed to protect the cloud environment from hacking attempts by threat actors

5

Finally, we ended this module with a detailed discussion on various cloud security tools

6

In the next module, we will discuss in detail on penetration testing concepts