Cloud Computing

Google Class room Code:

rhezfdl

S.M SOHAIB UR REHMAN

S. No.	Topics
1	What's in it for you? Before Cloud Computing About Hypervisors and virtualization
2	What is cloud computing? Types of Cloud Computing Public Cloud Private Cloud Hybrid Cloud IP Addressing with Types
3	Cloud Architecture Benefits IaaS, PaaS, SaaS
4	Benefits Of Cloud Computing
5	Cloud Management
6	Microservices Architecture How MicroServices Works? Benefits Microservices Challenges of MicroServices Characteristics of MicroServices MicroServices in Cloud Benefits of using Microservices in cloud

S. No.	Topics
7	Cloud VS on-prem Security Introduction On-prem Security Benefits Cost of On-prem Security Benefits of Cloud Security Cons of Cloud Security
8	Cloud Computing Security Deep Dive What is Cloud Security Principal of Cloud Computing Security Cloud Computing Security Best practice
9	Module Review AWS Certification Road Map Azure Certification Road Map

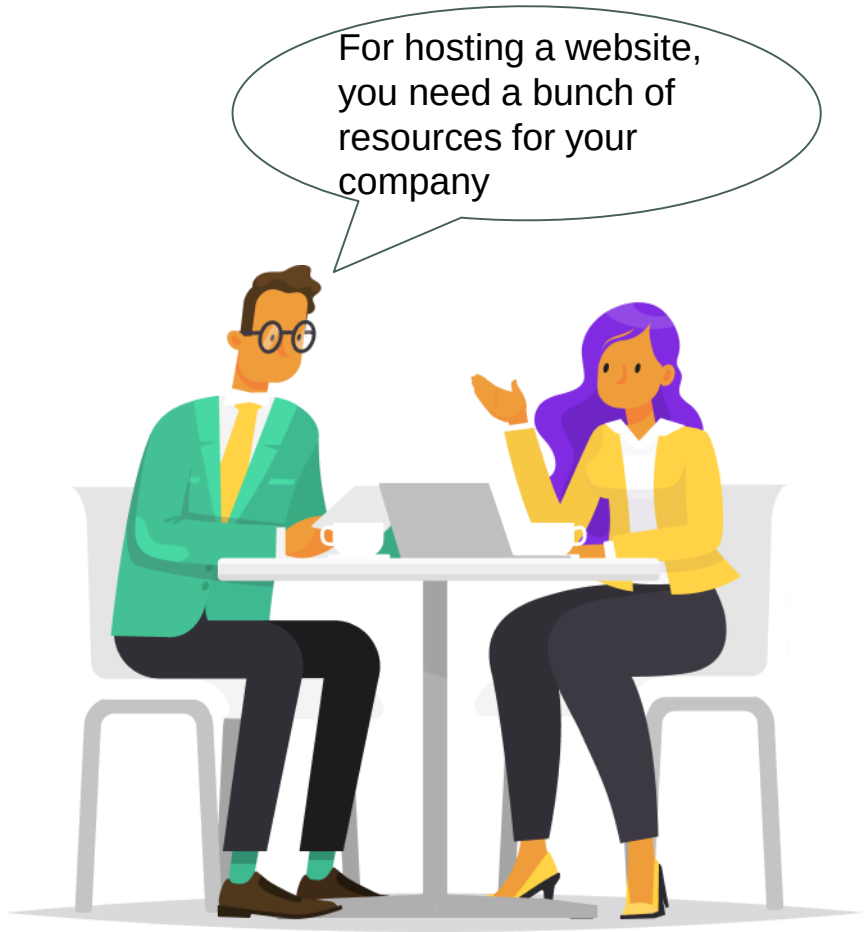
What’s in it for you:

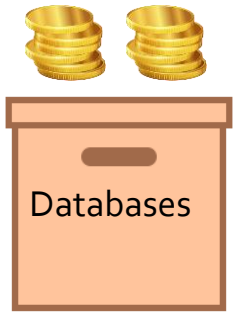
What's in it for you:

- Before Cloud Computing
- What is Cloud Computing
- Benefits of Cloud Computing
- Types of Cloud Computing
- Categories of Cloud Computing

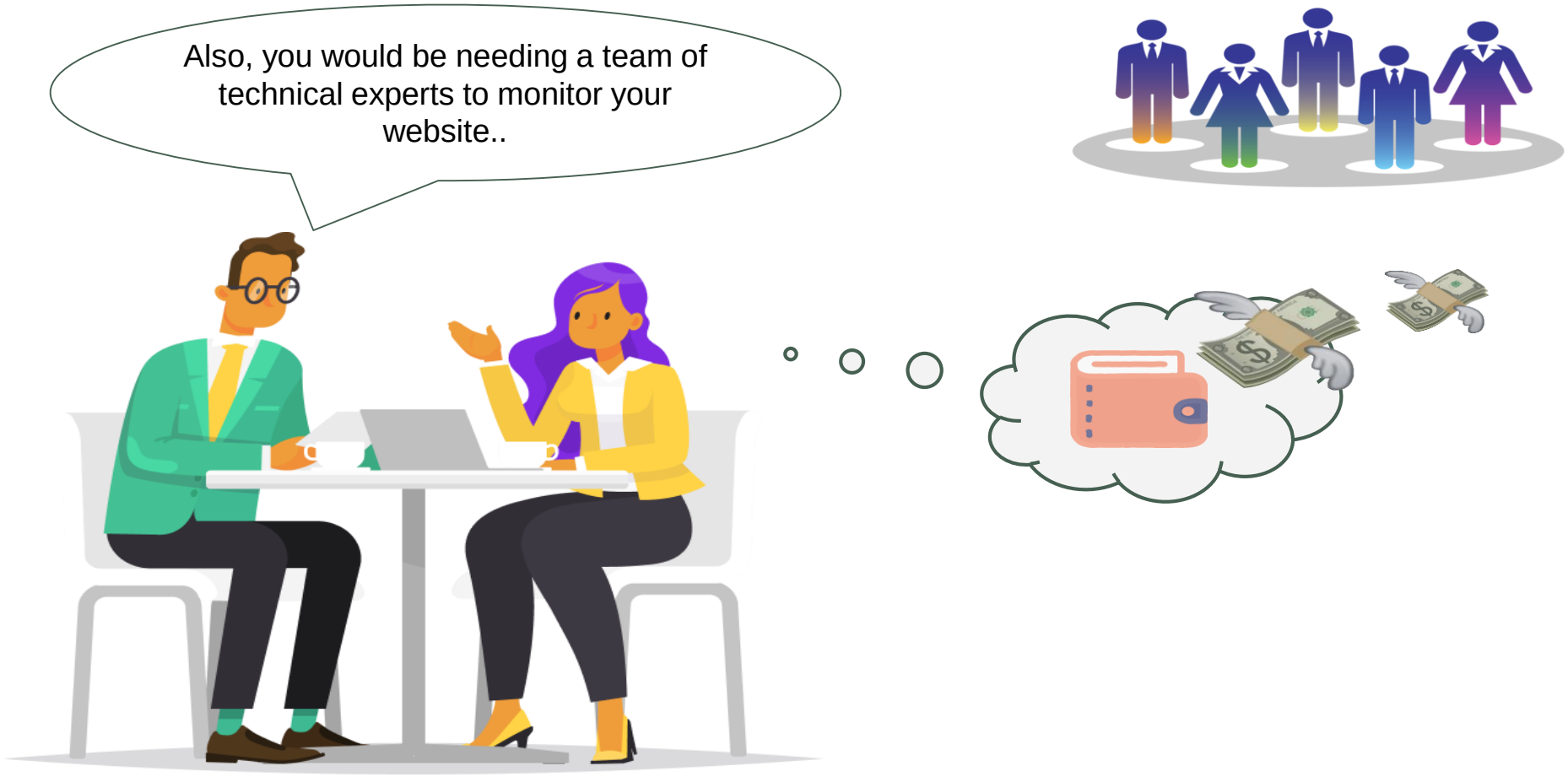
Before Cloud Computing:

Before Cloud Computing:



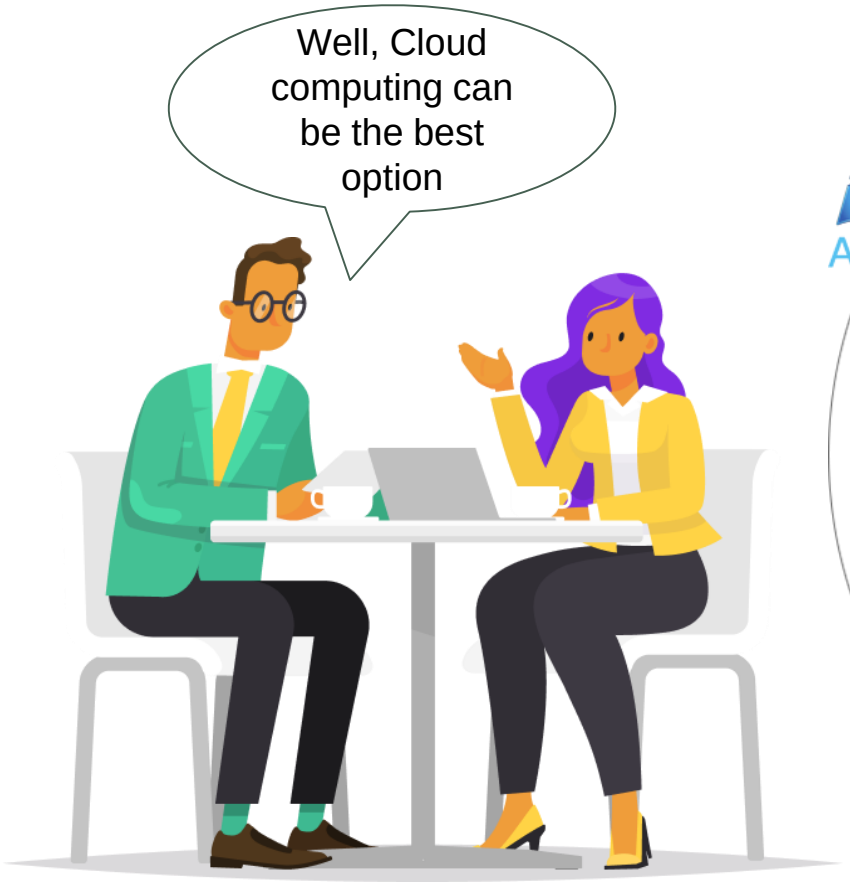


Before Cloud Computing:



Before Cloud Computing:

Before Cloud Computing:



What is cloud computing

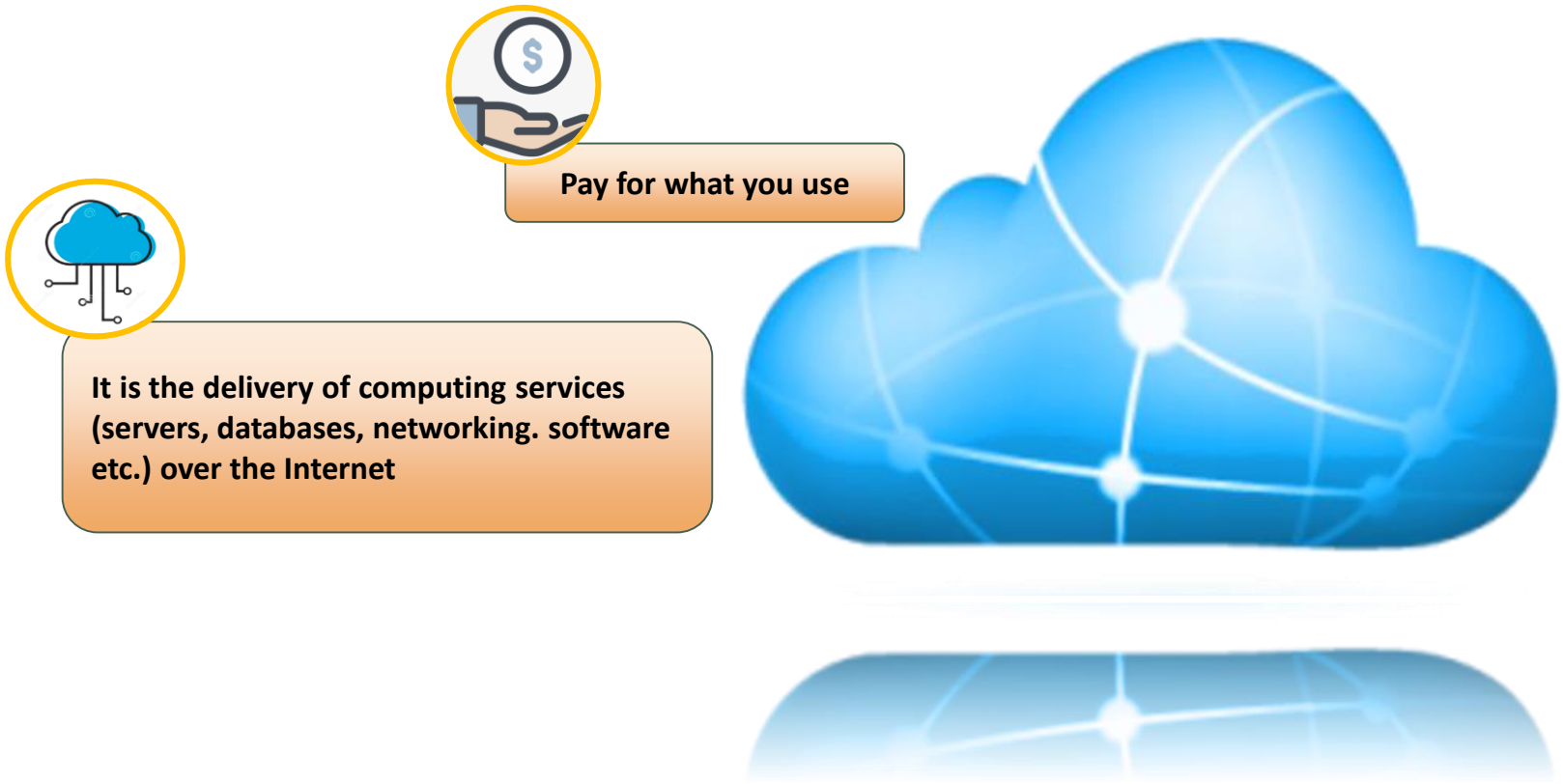
What is cloud Computing?

Cloud Computing is the use of a network of remote servers hosted on the Internet to store, manage and process data rather than a local server

What is cloud Computing?

It is the delivery of computing services (servers, databases, networking, software etc.) over the Internet

What is cloud Computing?



What is cloud Computing?

What is cloud Computing?

Cloud computing service providers give the ability to manage applications and services through a global network

Example: Amazon Web Services and Microsoft Azure

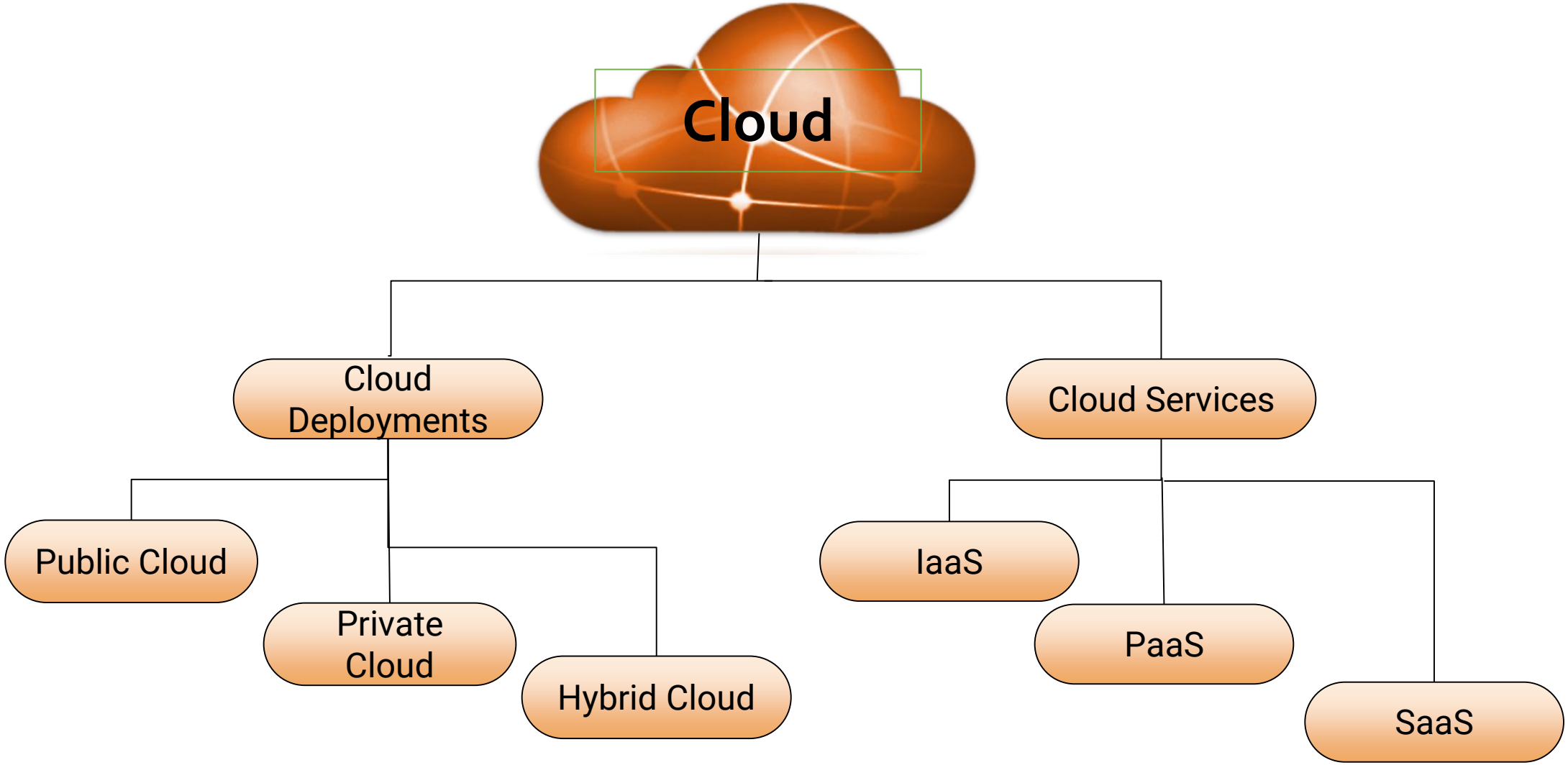
Q&A Session

1. What is one benefit of cloud computing?
   a. Computer resources can be quickly provisioned.
   b. A workload can quickly move to a cloud computing environment.
   c. There is no operational cost for a cloud computing environment.
   d. The resources can quickly move from one cloud environment to another.

1. What is one benefit of a cloud computing environment?
   a. It improves server performance.
   b. It minimizes network traffic to the virtual machines.
   c. It automatically transforms physical servers into virtual machines.
   d. It maximizes server utilization by implementing automated provisioning.

3. What is the role of virtualization in cloud computing?
   a. It removes operating system inefficiencies.
   b. It improves the performance of web applications.
   c. It optimizes the utilization of computing resources.
   d. It adds extra load to the underlying physical infrastructure and has no role in cloud computing.

Type(s) Of **Cloud Computing**


Cloud
Cloud Deployments
Cloud Services
Public Cloud
Private Cloud
Hybrid Cloud
IaaS
PaaS
SaaS

Types of Cloud Deployment

Public Cloud

Typically have massive amounts of available space, which translates into easy scalability. Recommended for software development and collaborative projects.

Private Cloud

Usually reside behind a firewall and are utilized by a single organization. Recommended for businesses with very tight regulatory requirements

Hybrid Cloud

Combine public clouds with private clouds to allow the two platforms to interact seamlessly. Recommended for businesses balancing big data analytics with strict data privacy regulations.

Community Cloud

A collaborative, multi-tenant platform used by several distinct organizations to share the same applications. Users are typically operating within the same industry or field.

Deployment Models

PUBLIC CLOUD : The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

PRIVATE CLOUD : The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

COMMUNITY CLOUD : The Community Cloud allows systems and services to be accessible by group of organizations.

HYBRID CLOUD : The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

Benefits

Public Cloud	Private Cloud	Hybrid Cloud
No maintenance costs	Dedicated, secure	Policy-driven deployment
High scalability, flexibility	Regulation compliant	High scalability, flexibility
Reduced complexity	Customizable	Minimal security risks
Flexible pricing	High scalability	Workload diversity supports high reliability
Agile for innovation	Efficient	Improved security

Drawbacks

Public Cloud	Private Cloud	Hybrid Cloud
Potential for high TCO	Expensive with high TCO	Potential for high TCO
Decreased security and availability	Minimal mobile access	Compatibility and integration
Minimal control	Limiting infrastructure	Added complexity

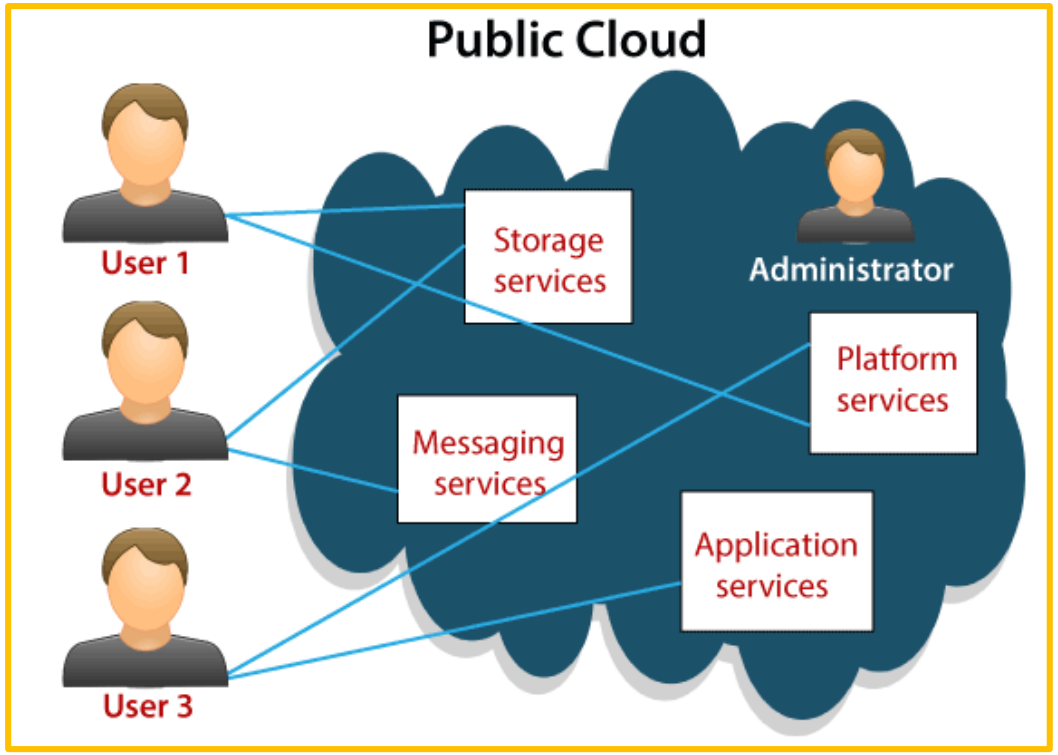
What Is Public Cloud?

The public cloud refers to the cloud computing model in which **IT services are delivered via the internet.**

The public cloud offers vast choices in terms of solutions and computing resources.

The defining features of a public cloud solution include:

- ➔ High elasticity and scalability
- ➔ A low-cost subscription-based pricing tier



What Is Public Cloud?

When To Use Public Cloud?

The public cloud is most suitable for these types of environments:

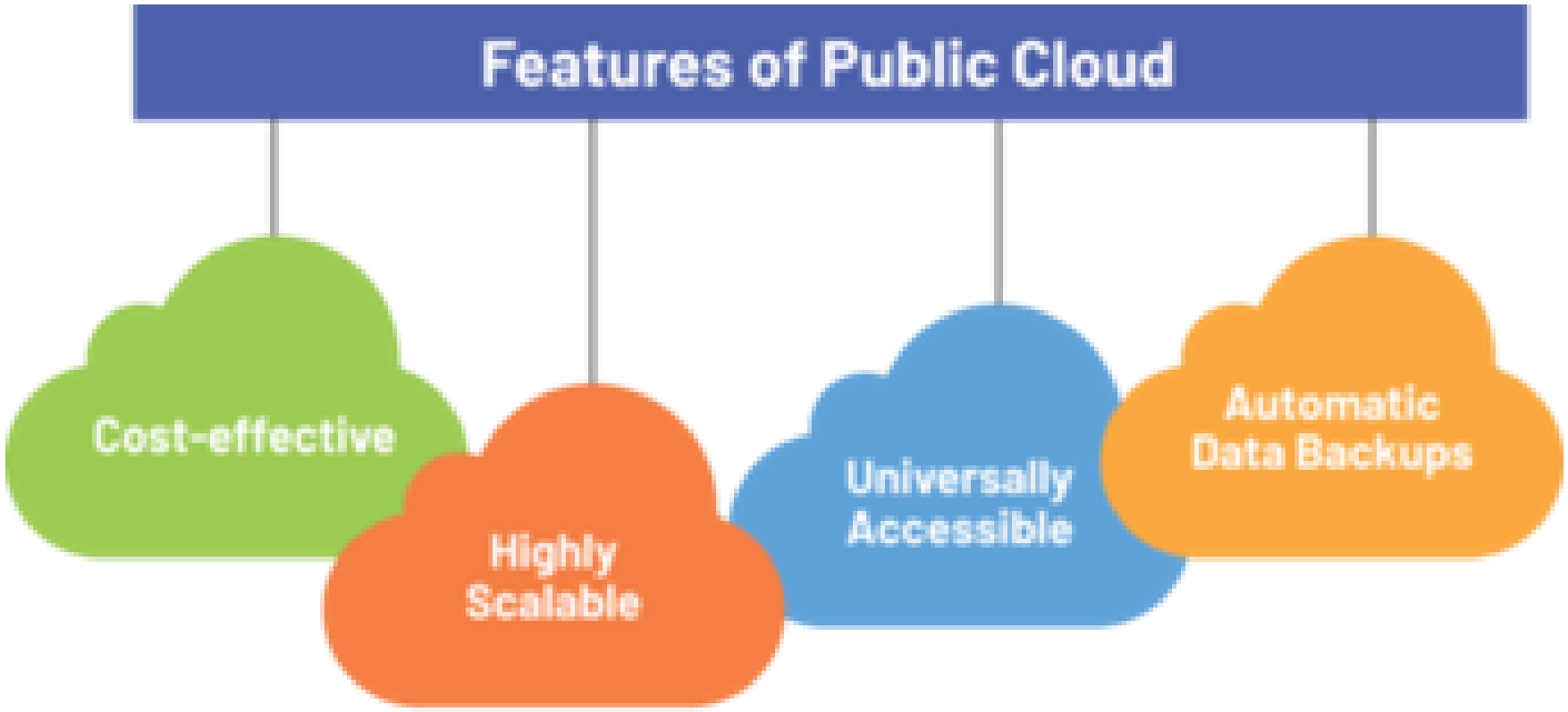
- ➔ Predictable computing needs, such as communication services for a specific number of users
- ➔ Apps and services necessary to perform IT and business operations (elasticity & scalability)
- ➔ Additional resource requirements to address varying peak demands.
- ➔ Software development and test environments

Advantages Of Public Cloud?

People appreciate these public cloud benefits:

- **No CapEx**. No investments required to deploy and maintain the IT infrastructure.
- **Technical agility.** High scalability and flexibility to meet unpredictable workload demands.
- **Business focus.** The reduced complexity and requirements on in-house IT expertise is minimized, as the cloud vendor is responsible for infrastructure management.
- **Affordability.** Flexible pricing options based on different SLA offerings
- **Cost agility.** The cost agility allows organizations to follow lean growth strategies and focus their investments on innovation projects

Advantages Of Public Cloud?



Drawbacks Of Public Cloud?

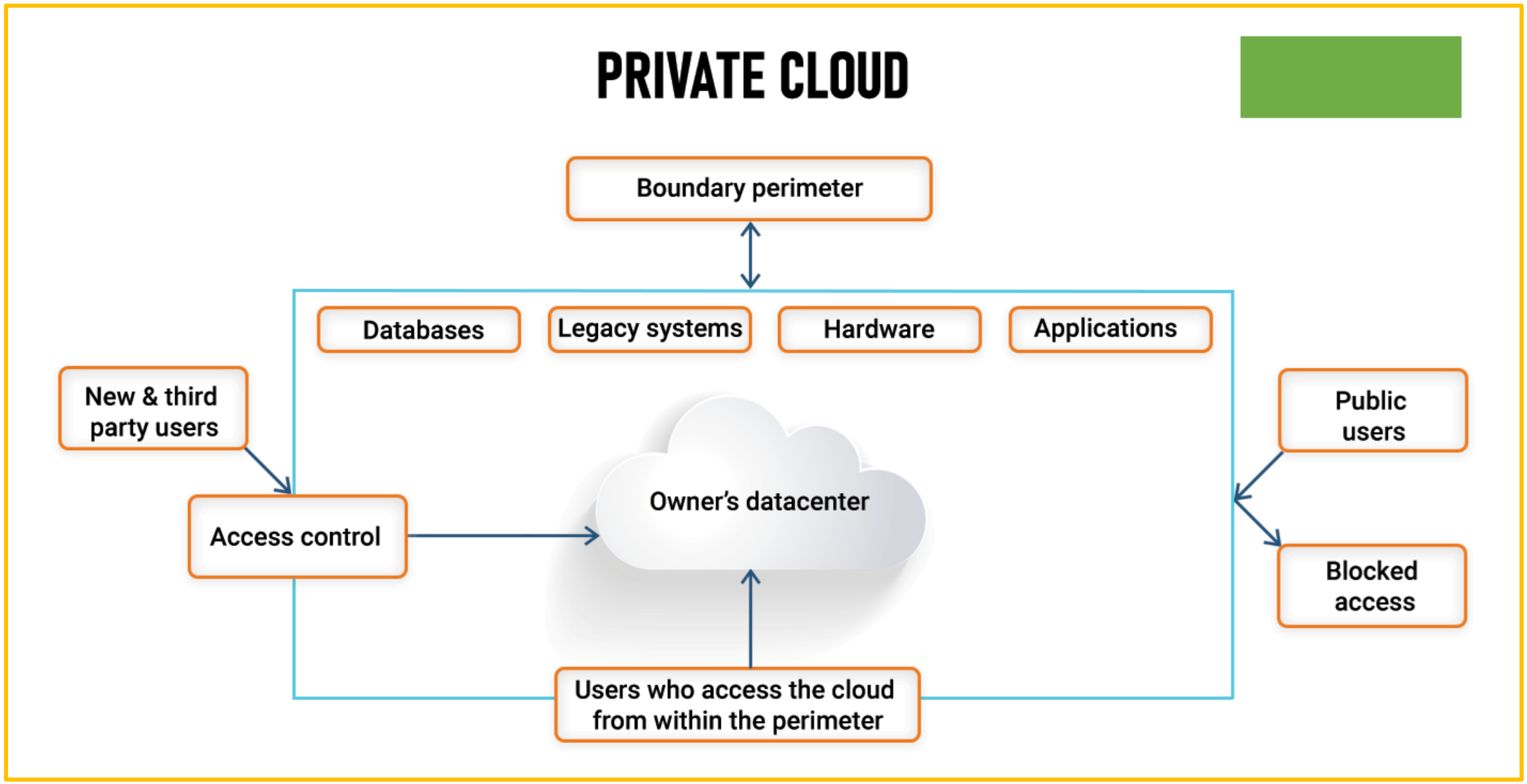
The public cloud does come with limitations:

- **Lack of cost control**. The total cost of ownership (TCO) can rise exponentially for large-scale usage, specifically for midsize to large enterprises.

- **Lack of security.** Public cloud is the least secure by nature this is the reason it isn't best for sensitive mission-critical IT workloads.

What Is Private Cloud?

- The private cloud refers to any cloud solution dedicated for use by a single organization.
- In the private cloud, you're not sharing cloud computing resources with any other organization.
- The data center resources may be located on-premise or operated by a third-party vendor off-site.
- The computing resources are isolated and delivered via a secure private network, and not shared with other customers.
- Private cloud is customizable to meet the unique business and security needs of the organization.


PRIVATE CLOUD
Boundary perimeter
Databases
Legacy systems
Hardware
Applications
New & third party users
Access control
Owner's datacenter
Public users
Blocked access
Users who access the cloud from within the perimeter

When To Use Private Cloud?

The private cloud is best suited for:

- Highly regulated industries and government agencies
- Securing Sensitive data
- Companies that require strong control and security over their IT workloads and the underlying infrastructure
- Large enterprises that require advanced data center technologies to operate efficiently and cost-effectively
- Organizations that can afford to invest in high performance and available technologies

Advantages Of Private Cloud?

The most popular benefits of private cloud include:

- **Exclusive environments.** Dedicated and secure environments that cannot be accessed by other organizations.

- **Custom security.** Compliance to stringent regulations as organizations can run protocols, configurations, and measures to customize security based on unique workload requirements

- **Scalability without tradeoffs**. High scalability and efficiency to meet unpredictable demands without compromising on security and performance

- **Efficient performance.** The private cloud provides high SLA performance and efficiency.

- **Flexibility**. The private cloud is flexible as you transform the infrastructure based on ever-changing business and IT needs of the organization.

DrawBacks Of Private Cloud?

The private cloud has drawbacks that might limit use cases:

- **Price.** The private cloud is an expensive solution with a relatively high TCO compared to public cloud alternatives, especially for short-term use cases.
- **Mobility difficulty**. Mobile users may have limited access to the private cloud considering the high security measures in place.
- **Scalability depends**. The infrastructure may not offer high scalability to meet unpredictable demands if the cloud data center is limited to on-premise computing resources

DrawBacks Of Private Cloud?

Cost

Prices square measure substantial within the case of building Associate in Nursing on-premise personal cloud. The running value would come with personnel value and periodic hardware upgrade prices. within the case of outsourced personal cloud, operating expense can embody per resource usage and subject to vary at the discretion of the service supplier.

Under-utilization

In some instances the resources signed will be under-utilized. Hence, optimizing the use of all resources may be a challenge.

Capacity Ceiling

Because of physical hardware limitations with the service supplier, there can be a capability ceiling to handle solely specific amount of servers or storage.

Vendor Lock-in

This could be a serious impediment privately cloud adoption particularly once the hardware and infrastructure is outsourced.

What Is Hybrid Cloud?

The hybrid cloud is any cloud infrastructure environment that combines both public and private cloud solutions.
The resources are typically orchestrated as an integrated infrastructure environment.
Apps and data workloads can share the resources between public and private cloud deployment based on organizational business and technical policies around aspects like:

- ➔ Security
- ➔ Performance
- ➔ Scalability
- ➔ Cost
- ➔ Efficiency


Hybrid Cloud
App Loads
App Loads
App Loads
Management
Cloud OS
Federation & Choice
Management
Cloud OS
Private Clouds
Public Clouds

When To Use Hybrid Cloud?

Here's who the hybrid cloud might suit best:

- Organizations serving multiple verticals facing different IT security, regulatory, and performance requirements
- Optimizing cloud investments without compromising on the value that public or private cloud technologies can deliver
- Improving security on existing cloud solutions such as SaaS offerings that must be delivered via secure private networks
- Strategically approaching cloud investments to continuously switch and tradeoff between the best cloud service delivery model available in the market

Example:
Netflix, Hulu, Uber and Airbnb all rely heavily on hybrid cloud data storage due to its on-demand and pay-per-use features. Netflix and Hulu experience spikes in bandwidth demand when a new bingeable series debuts on their respective platforms.

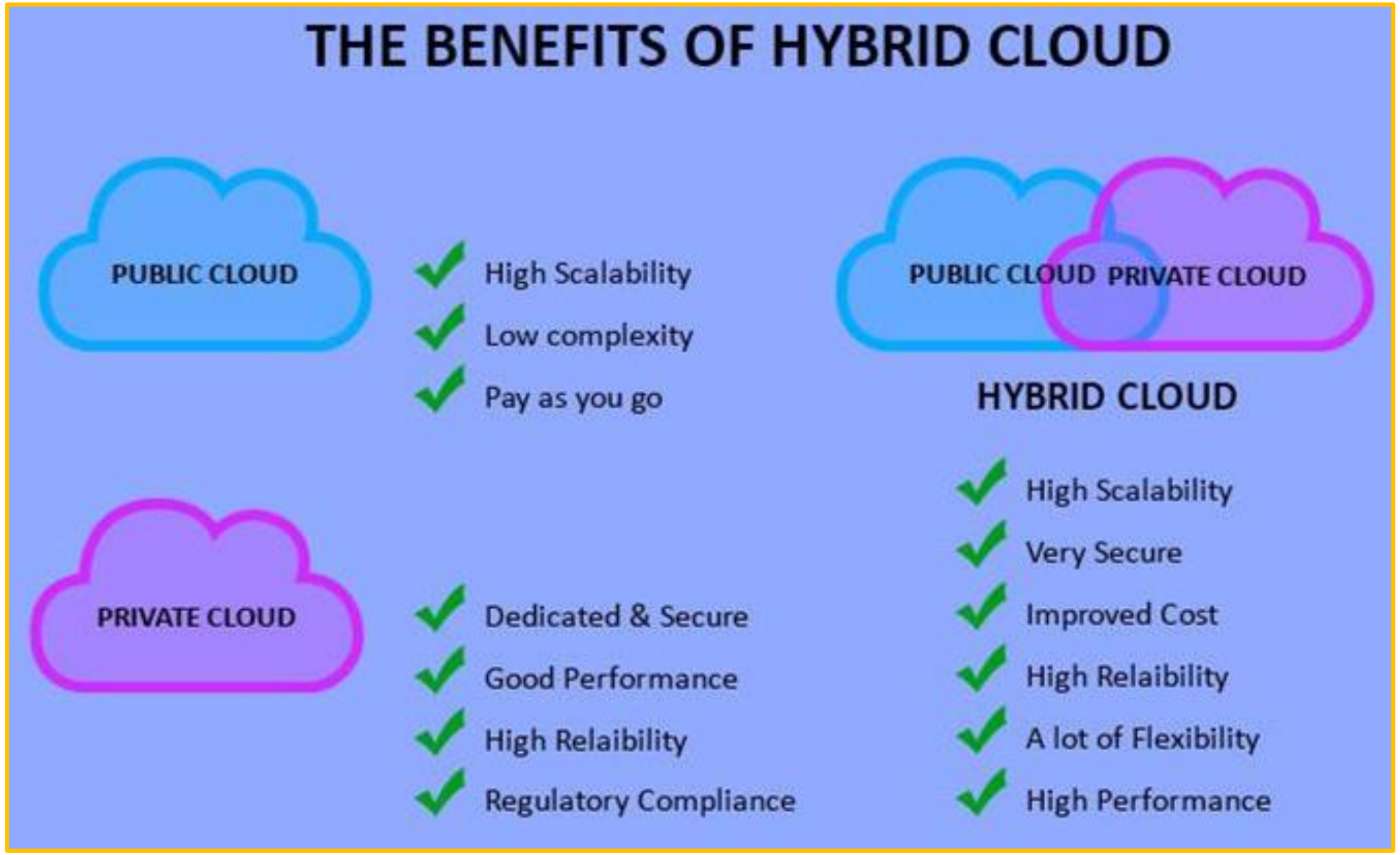
Advantages Of Hybrid Cloud?

Policy-driven option. Flexible policy-driven deployment to distribute workloads across public and private infrastructure environments based on security, performance, and cost requirements.

Scale with security. Scalability of public cloud environments is achieved without exposing sensitive IT workloads to the inherent security risks.

Reliability. Distributing services across multiple data centers, public and private, results in maximum reliability.

Cost control. Improved security posture as sensitive IT workloads run on dedicated resources in private clouds while regular workloads are spread across inexpensive public cloud infrastructure to tradeoff for cost investments


THE BENEFITS OF HYBRID CLOUD
PUBLIC CLOUD
High Scalability
Low complexity
Pay as you go
PUBLIC CLOUD
PRIVATE CLOUD
HYBRID CLOUD
High Scalability
Very Secure
Improved Cost
High Relaibility
A lot of Flexibility
High Performance
PRIVATE CLOUD
Dedicated & Secure
Good Performance
High Relaibility
Regulatory Compliance

Drawbacks Of Hybrid Cloud?

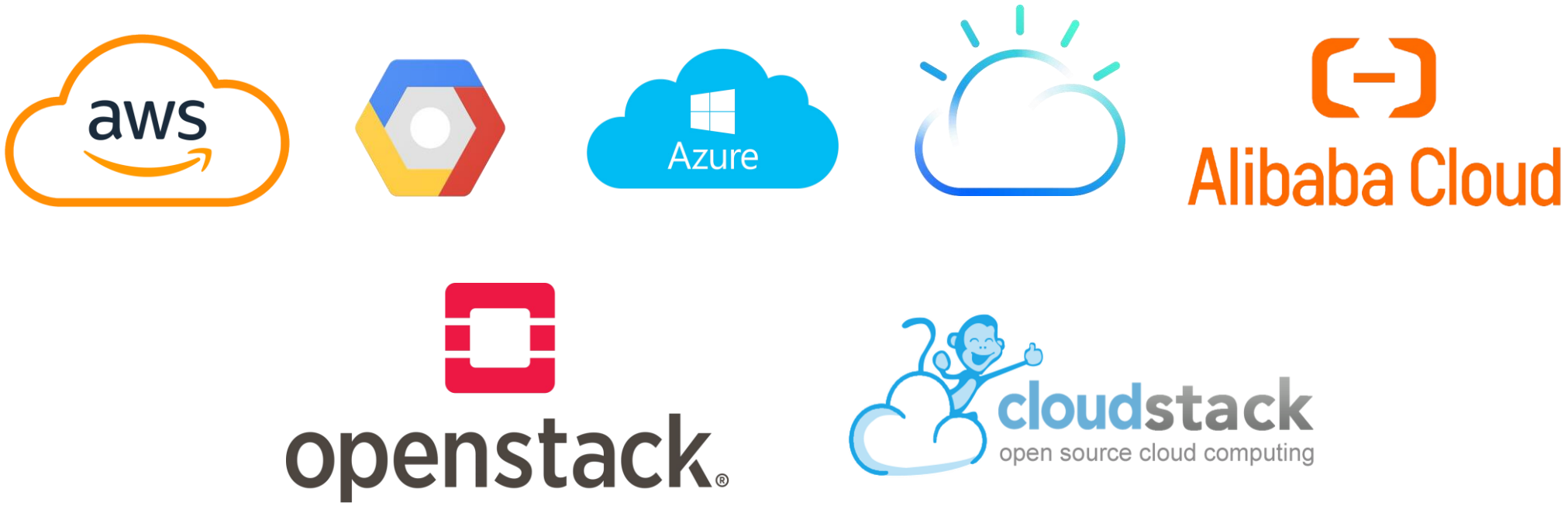
Common drawbacks of the hybrid cloud include:

Price. Toggling between public and private can be hard to track, resulting in wasteful spending.

Management. Strong compatibility and integration is required between cloud infrastructure spanning different locations and categories (cloud to cloud spanning, on-prem and cloud spanning).

Added complexity. Additional infrastructure complexity is introduced as organizations operate and manage an evolving mix of private and public cloud architecture.

Types of Cloud Computing



Q&A Session

1. A company would like to leverage cloud computing to provide advanced collaboration services (i.e., video, chat, and web conferences) for its employees but does not have the IT resources to deploy such an infrastructure. Which cloud computing model would best fit the company needs?

a. Hybrid Cloud
b. Public Cloud
c. Private Cloud
d. Virtual Private Cloud.

2. A company is considering a cloud environment to improve the operating efficiency for its data and applications. The company is part of an industry where strict security and data privacy issues are of the highest importance. Which type of cloud would be a good choice?

a. Hybrid cloud
b. Public cloud
c. Private cloud
d. Governed cloud

Q&A Session

3. What is a public cloud?
    a. A cloud formation that can be seen across the globe
    b. A cloud service that can only be accessed from a publicly shared computer
    c. A multi-tenant cloud environment accessed over the internet
    d. A cloud environment owned, operated and controlled by a public company

IP address with Types

IP Address

- An IP address is a unique number assigned to every device on a TCP/IP network.
- **IP addresses identify computers and devices and lets them communicate with each other.**

Types:

- Public IP Address
- Private IP Address
- Static IP Address
- Dynamic IP Address

Types Of IP Address

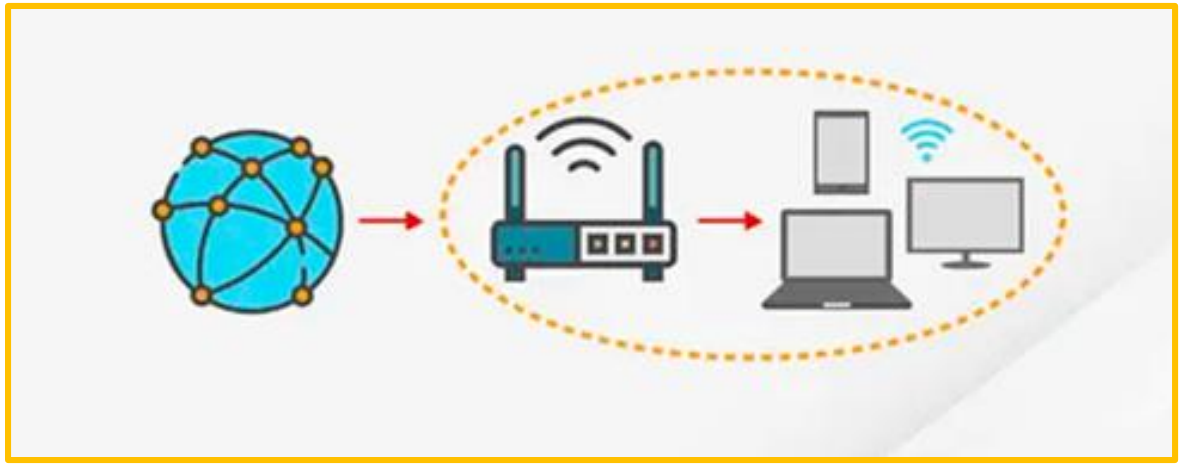
Public IP Address

- A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP).
- Your personal device also has a private IP that remains hidden when you connect to the internet through your router's public IP.

Types Of IP Address

Private IP Address

- A private IP address is a range of non-internet facing IP addresses used in an internal network.
- Private IP addresses are provided by network devices, such as routers, using network address translation.

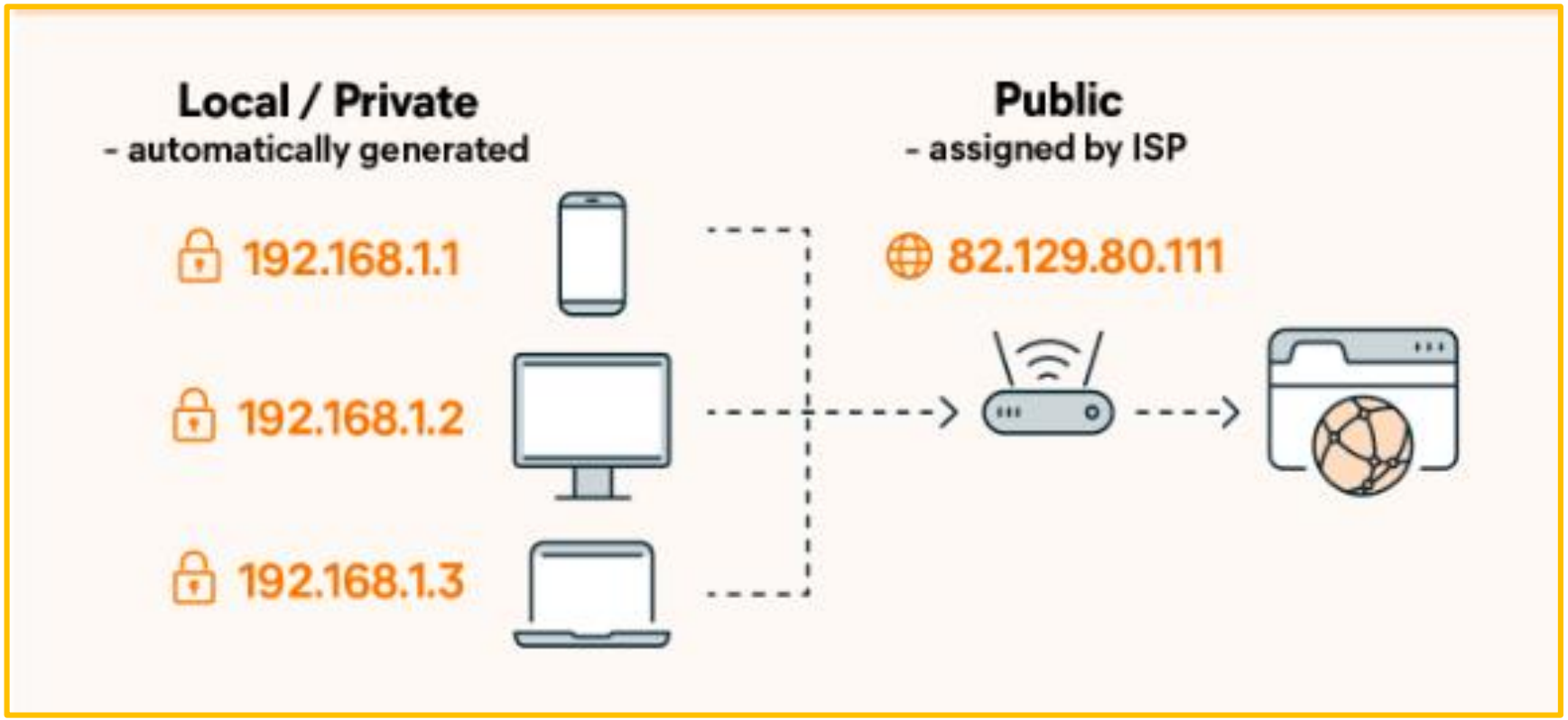


Difference Between Public and Private IP Address

Private	Public
Used for communicating within a private network. Cannot be directly contacted over the internet.	Used to communicate over the public internet—outside a private network.
Addresses can be reused per network.	Addresses are unique and cannot be reused.
Assigned to a device by a router.	Assigned by an ISP.
Has a small set range of possible addresses.	Addresses can be any combination of numbers not within the private IP range.

Types Of IP Address

Difference Between Public and Private IP Address



Types Of IP Address

Static IP Address

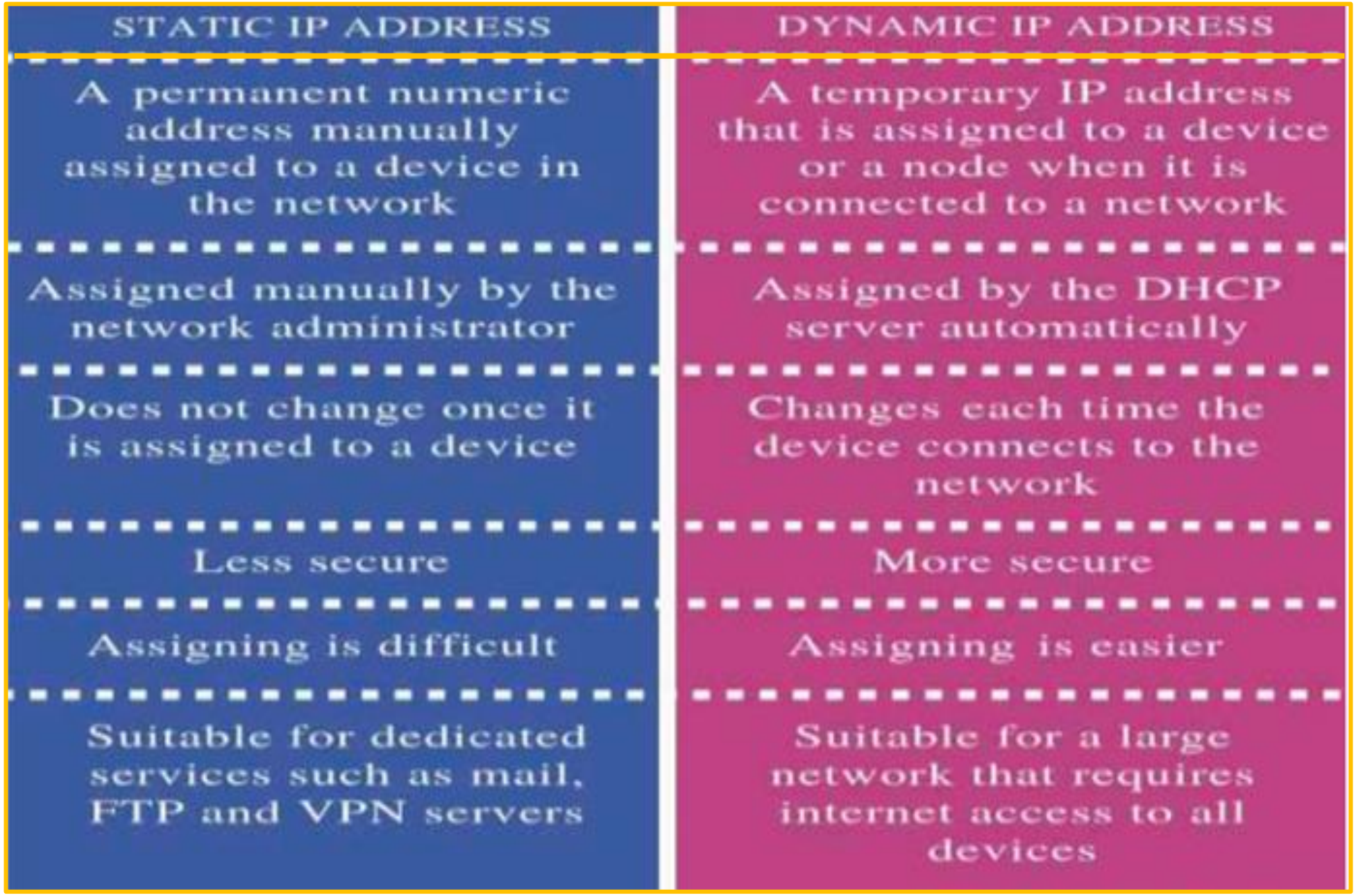
- An IP address that a person manually configures and fixes to their device's network is referred to as a static IP address.
- A static IP address cannot be changed automatically.

Types Of IP Address

Dynamic IP Address

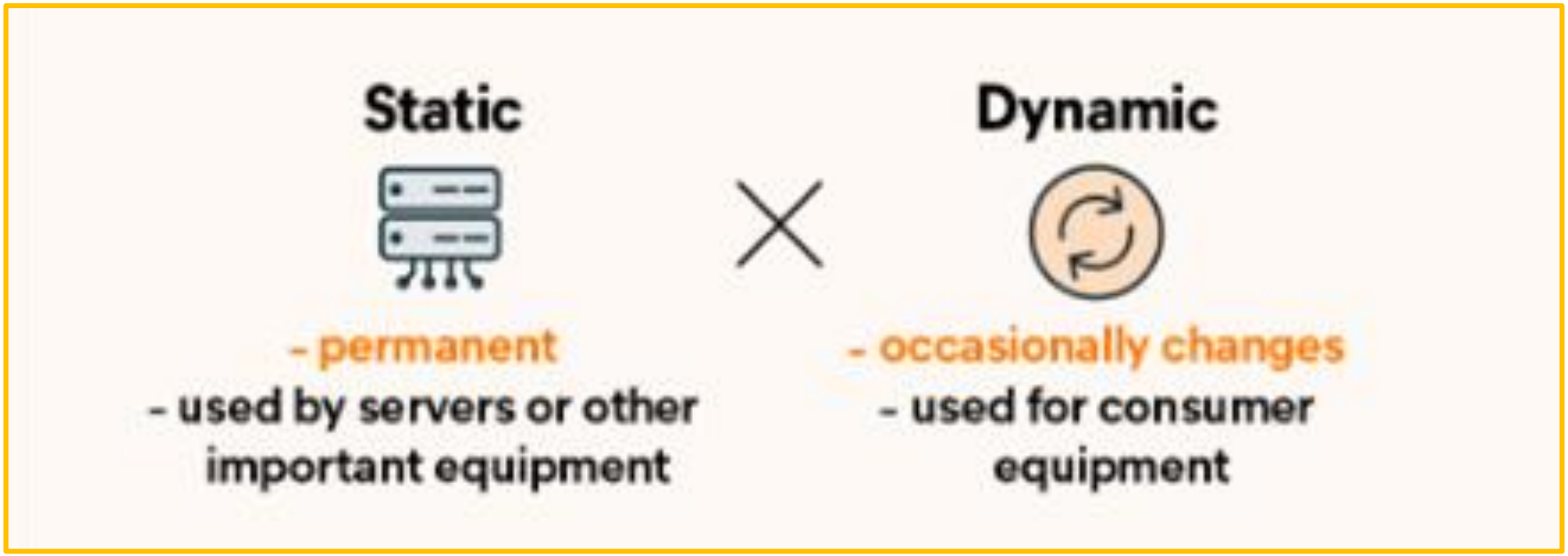
- A dynamic IP address is automatically assigned to a network when a router is set up.
- The Dynamic Host Configuration Protocol (DHCP) assigns the distribution of this dynamic set of IP addresses.
- The DHCP can be the router that provides IP addresses to networks across a home or an organization.

Difference Between Static and Dynamic IP Address



Types Of IP Address

Difference Between Static and Dynamic IP Address



Cloud Architecture

Cloud Computing Architecture:

Cloud architecture is the way technology components combine to build a cloud, in which resources are pooled through virtualization technology and shared across a network.

The components of a cloud architecture include:

- A front-end platform (the client or device used to access the cloud)
- A back-end platform (servers and storage)
- A cloud-based delivery model (SaaS, PaaS, IaaS)
- A network (IP addresses ,routing etc)

Together, these technologies create a cloud computing architecture on which applications can run, providing end-users with the ability to leverage the power of cloud resources.

Benefits Of Cloud Architecture:

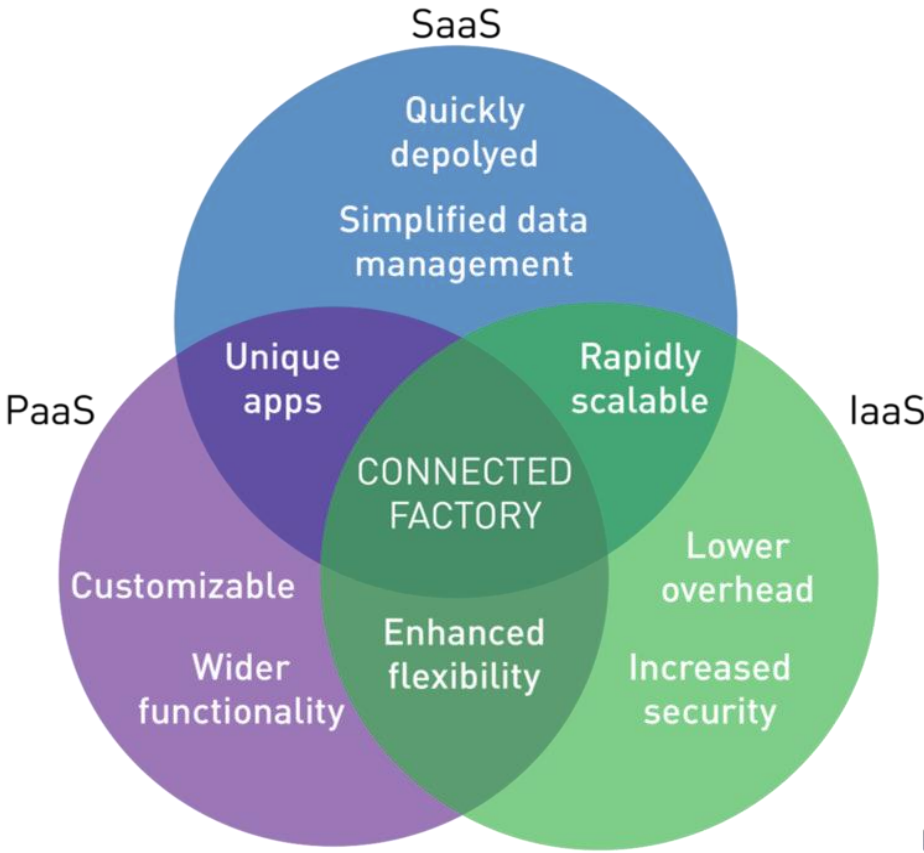
- It reduces or eliminate their reliance on on-premises server, storage, and networking infrastructure.
- Organizations adopting cloud architecture often shift IT resources to the public cloud, **eliminating the need for on-premises servers and storage, and reducing the need for IT data center real estate, cooling, and power, and replacing them with a monthly IT expenditure.**
- This shift from capital expenditure to operating expense is a major reason for the popularity of cloud computing today.

Cloud Computing Architecture:

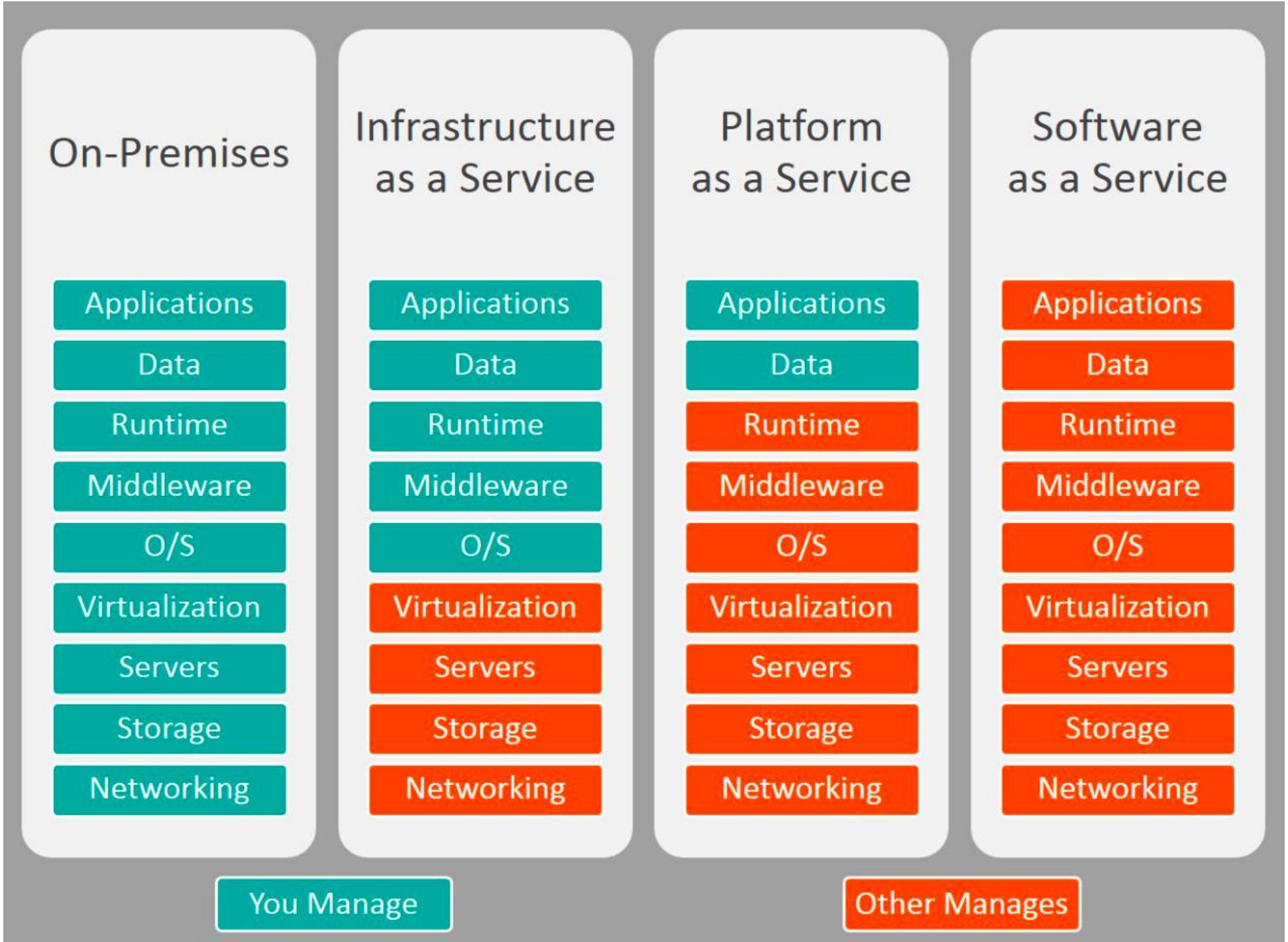
IaaS (Infrastructure as a Service)
Eg: Compute, Storage, Network.

PaaS (Platform as a Service)
Eg: Application development & deployment, Serverless.

SaaS (Software as a Service).
Eg: Email , Docs, App stream



TULIP


On-Premises
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Infrastructure as a Service
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Platform as a Service
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Software as a Service
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You Manage
Other Manages

Benefits Of Cloud Architecture:

There are three major models of cloud architecture that are driving organizations to the cloud. Each of these has its own benefits and key features.

Infrastructure as a Service (IaaS):

- In this, cloud at its simplest form, a third-party provider eliminates the need for organizations to purchase servers, networks or storage devices by providing the necessary infrastructure.
- In turn, organizations manage their software and applications, and only pay for the capacity they need at any given time.

Benefits Of Cloud Architecture:

IaaS:

Advantages

- Offers great flexibility of all cloud computing models
- Highly scalable as per business requirements
- Enables easy automation of deploying networking, processing power, servers & storage
- Flexibility to purchase only need-based hardware and other resources
- Clients retain complete infrastructure control

Characteristics

- Cost depends on the consumption
- Scalable services
- Resources are made available as a service
- Multiple users can be included on a single unit of hardware
- Organizations retain full control of infrastructure
- Flexible and dynamic

Benefits Of Cloud Architecture:

Platform as a Service (PaaS):

- ➔ In this cloud model, the service provider offers a computing platform and solution stack, often including middleware, as a service. Organizations can build upon that platform to create an application or service.
- ➔ The cloud service provider delivers the networks, servers and storage required to host an application while the end user oversees software deployment and configuration settings.

Benefits Of Cloud Architecture:

PaaS:

Advantages

- High availability
- Scalability
- Enabling developers to focus on the creation of custom applications without the responsibility of software maintenance
- Reduced coding time
- Automated business policy
- Enables easy migration to a hybrid model

Characteristics

- Easy scalability
- Offers several services to help in developing, testing and deploying the applications
- The same development app can be accessed by several users
- Integrated databases and web services

Benefits Of Cloud Architecture:

Software as a Service (SaaS):

- SaaS architecture providers deliver and maintain applications and software to organizations over the Internet, thereby eliminating the need for end users to deploy the software on servers.
- SaaS applications are typically accessed via a web interface available from a broad variety of devices and OSes.

Benefits Of Cloud Architecture:

SaaS:

Advantages

SaaS reduces the expenditure and time spent on installation and management of the software.

Characteristics

- Centrally located and managed
- Remote server hosting
- Accessible through the internet
- Hardware and software updates are not the user's responsibility

Why Adopt Cloud Architecture:

Organizations have many reasons for adoption of a cloud architecture, includes:

- ➔ Accelerate the **delivery of new apps**
- ➔ Take advantage of cloud-native architecture such as **Kubernetes and docker** to modernize applications and accelerate digital transformation.
- ➔ Ensure **compliance** with the latest regulations
- ➔ Deliver greater transparency into resources to **cut costs and prevent data breaches**
- ➔ Enable **faster provisioning of resources.**
- ➔ Utilize hybrid cloud architecture to **support real-time scalability** for applications as business needs change.
- ➔ Meet **service targets** consistently.
- ➔ **Leverage cloud reference architecture** to gain insight into IT spending patterns and cloud utilization


SaaS
PaaS
IaaS
BIGCOMMERCE
HubSpot
salesforce
zendesk
Google Apps
MailChimp
slack
DocuSign
Azure
apache
Stratos
heroku
force.com
platform as a service
rackspace

Q&A Session

1. Which delivery model is an example of a cloud computing environment that provides users with a web-based email service?
   a. Software as a Service
   b. Platform as a Service
   c. Computing as a Service
   d. Infrastructure as a Service

2. How can company leverage the Platform as a Service cloud computing delivery model?

   a. A company requires more processing power to perform its financial analysis calculations and acquires additional computational resources.
   b. A company requires a customer relationship management solution and obtains an application that addresses its requirements from a cloud provider.
   c. A company is running out of storage space to store a customer database and dynamically request additional space via the cloud provider web services interface.
   d. A company obtains an environment with a software stack from a cloud provider, develops custom application, and makes that application available to its customers on the Internet.

Q&A Session

3. A cloud provider offers an environment for building applications that will run from the customer's environment. Which cloud computing delivery model are they using?

a. Platform as a Service
b. Software as a Service
c. Development as a Service
d. Infrastructure as a Service

4. A company interested in cloud computing is looking for a provider who offers a set of basic services such as virtual server provisioning and ondemand storage that can be combined into a platform for deploying and running customized applications. What type of cloud computing model fits these requirements?

a. Platform as a Service
b. Software as a Service
c. Application as a Service
d. Infrastructure as a Service

Benefits of cloud computing

Benefit Of Cloud Computing

SPEED

Vast amount of computing resources can be provisioned in minutes.

Benefit Of Cloud Computing

COST

It eliminates the expense of buying computer hardware and software

SPEED

Vast amount of computing resources can be provisioned in minutes.

Benefit Of Cloud Computing

SPEED

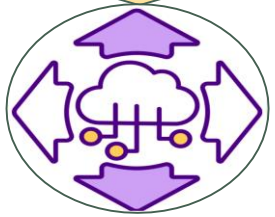
Vast amount of computing resources can be provisioned in minutes.

COST

It eliminates the expense of buying computer hardware and software

SCALABILITY

Easy to scale up your cloud capacity



Benefit Of Cloud Computing

SPEED

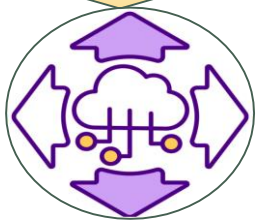
Vast amount of computing resources can be provisioned in minutes.

COST

It eliminates the expense of buying computer hardware and software

SCALABILITY

Easy to scale up your cloud capacity



ACCESSIBILITY

Easy to access data from anywhere

Benefit Of Cloud Computing

SPEED

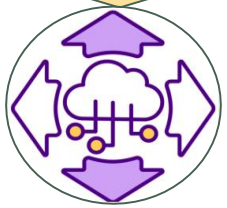
Vast amount of computing resources can be provisioned in minutes.

COST

It eliminates the expense of buying computer hardware and software

SCALABILITY

Easy to scale up your cloud capacity



ACCESSIBILITY

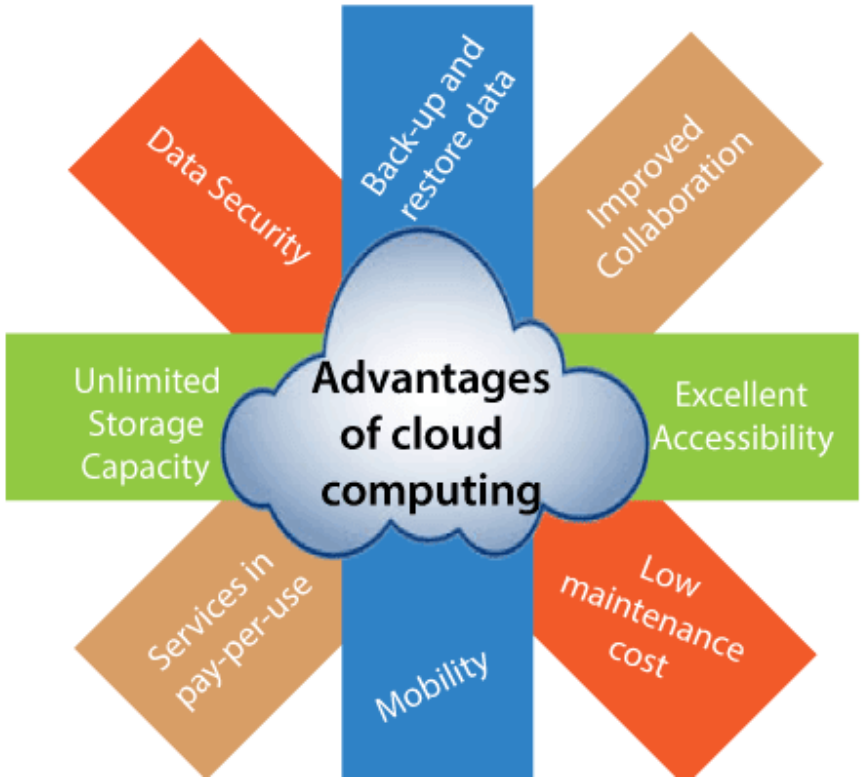
Easy to access data from anywhere

BETTER SECURITY

In cloud, data is secured in a centralized secure location

Advantages and Characteristics Of Cloud Computing

- On-Demand.
- No-Single point of failure.
- Scalable.
- Pay as you go service(s).
- Agile (Go global in minutes).
- Highly available and durable.
- Secure.



Q&A Session

1. Which feature of Cloud services makes it possible to manage computing infrastructure better and more efficiently?
   a. Scalability
   b. Cloud economics
   c. Computing services
   d. None of the above
2. Which of these is an advantage of cloud storage?
   a. Many programs can be run at the same time, regardless of the processing power of your device
   b. Accessible anywhere with an internet connection
   c. Portability
   d. The user has no control over their data
3. Which of the following isn't an advantage of cloud?
   a. Easier to maintain a cloud network
   b. No worries about running out of storage
   c. Immediate access to computing resources
   d. Paying only for what you use

Cloud Management

What Is Cloud Managment:

Changing infrastructure and moving to the cloud is disruptive and introduces other changes within organizations.

Cloud management is the methodology and processes used by organizations to plan and manage these changes.

Through cloud management, you can protect your company from some of the typical pitfalls and challenges associated with moving to the cloud.

Cloud Management Components

What Is Cloud Managment:

Cloud Management Impacts:

- ➔ Cloud adoption and frequent changes impact different areas of your organization differently and to different degrees.
- ➔ Some departments may only use your cloud for storage as an alternative to old-school filing cabinets while others are using extensive resources for DevOps including CICD pipelines and automation.
- ➔ These use cases have different needs and should be approached and planned differently.

What Is Cloud Managment:

Compliance

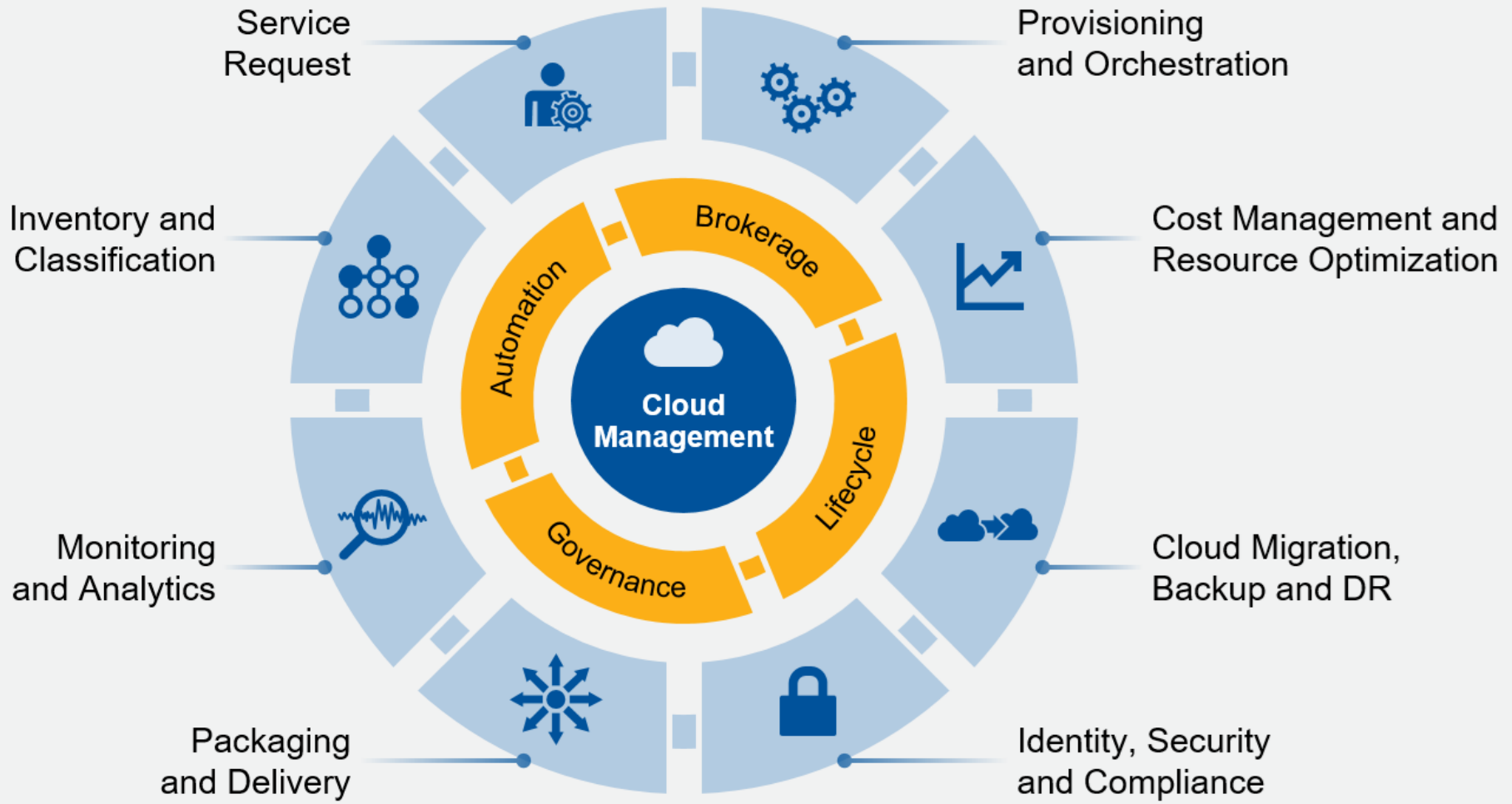
- With the cloud in use, your organization may have to set new internal policies for employees and should consider how changing compliance should be managed.
- For example, your organization is subject to PCI, GDPR, or HIPAA compliance, part of your change management would involve anticipating how these regulations impact your cloud transition and use.
- You will also need a policy restricting cloud use—so no one uploads their unnecessary video collection to their personal work cloud account.

What Is Cloud Managment:

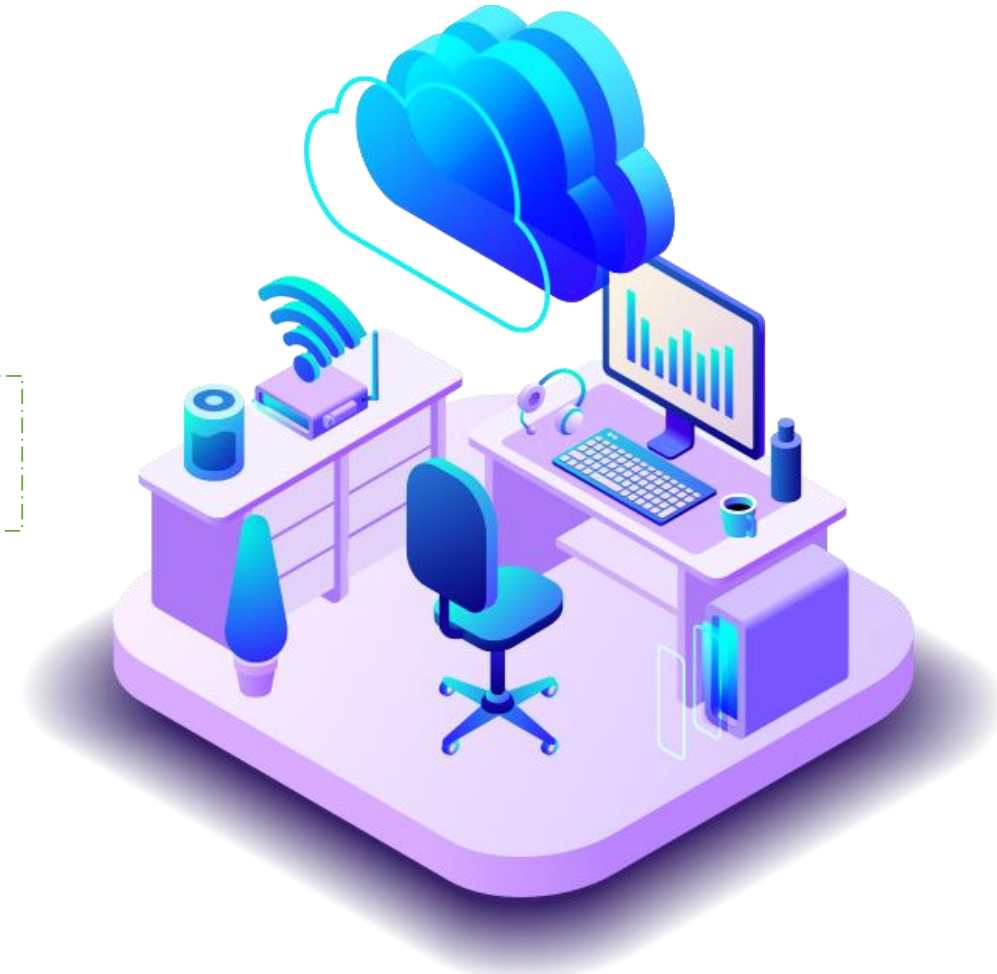
Cloud management goals

- Setting goals for how you transition and optimize the cloud is important.
- Understanding how cloud management works in your organization can help you choose the right goals and decide how you want to track and implement them.
- By building clarity, your organization is in a better position to manage change moving forward.

Evaluation Criteria Categories and Attributes: The Cloud Management Wheel



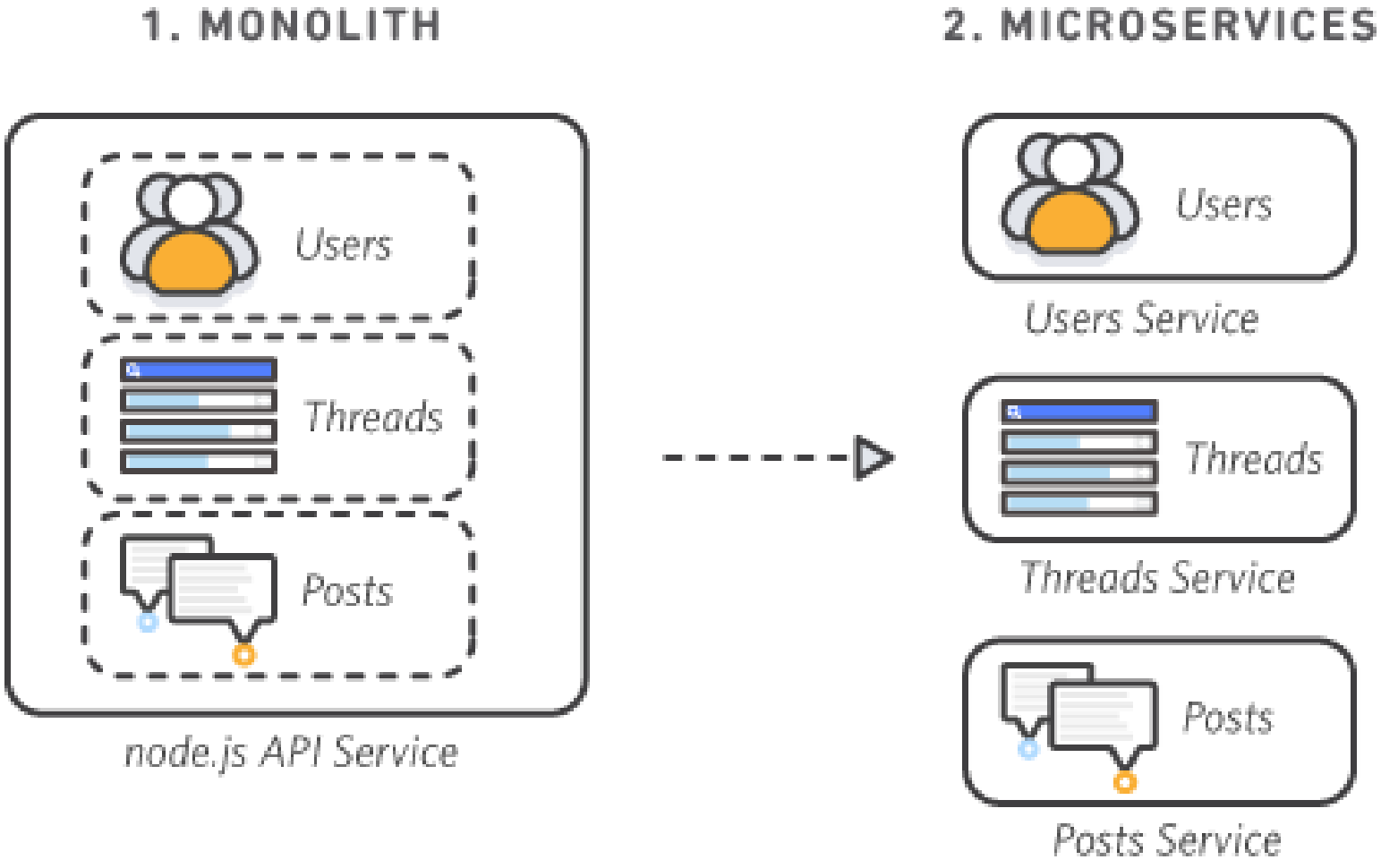
ID: 342611



What Are Microservices:

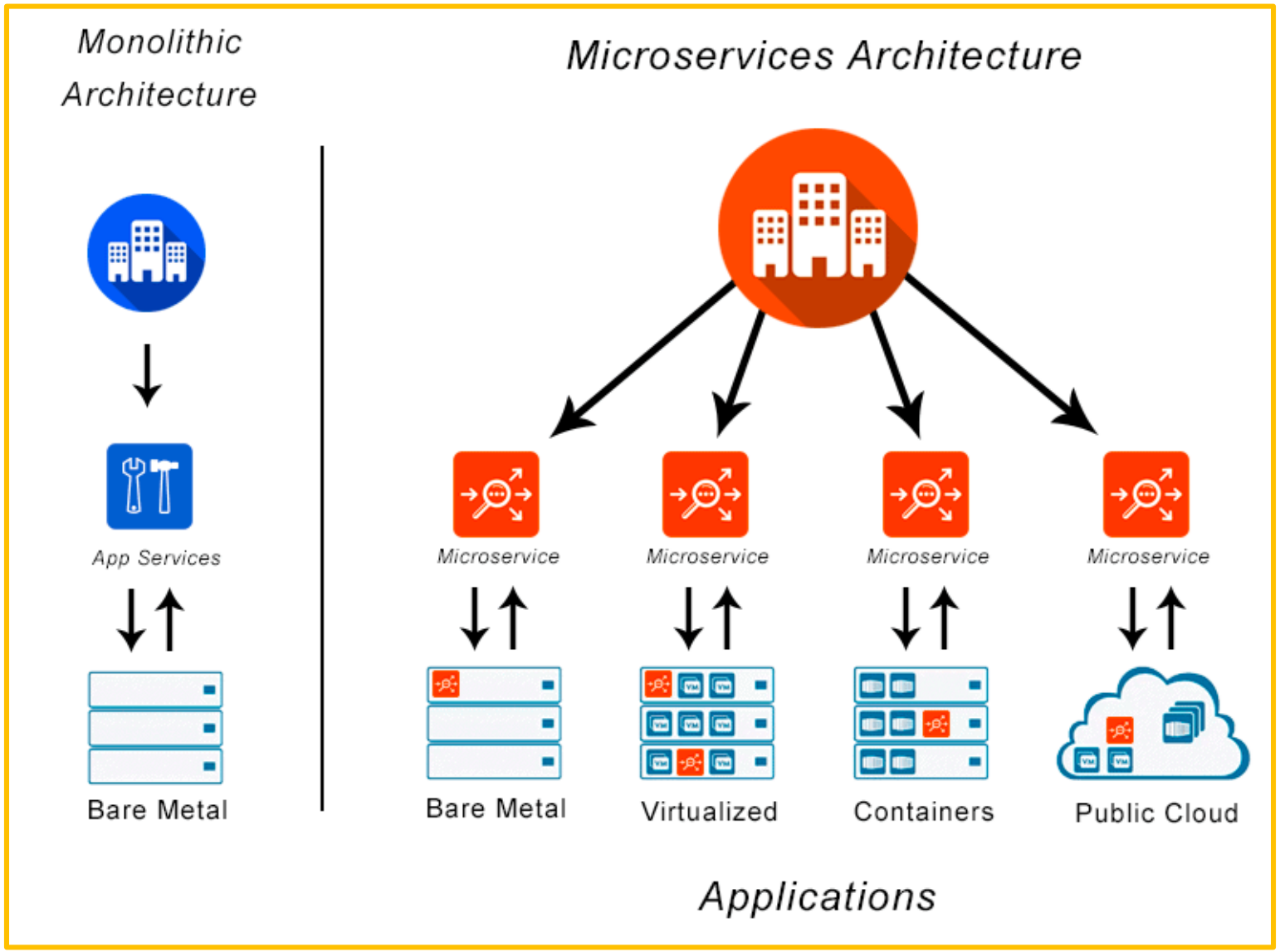
Microservices, or microservices architecture, is an approach to application development in which a large application is built from modular components or services.

Each module supports a specific task or business goal and uses a simple, well-defined interface, such as an application programming interface (API), to communicate with other sets of services.


1. MONOLITH
Users
Threads
Posts
node.js API Service
2. MICROSERVICES
Users
Users Service
Threads
Threads Service
Posts
Posts Service

How Microservices Work:

- In a microservices architecture, an application is divided into services.
- Each service runs a unique process and usually manages its own database.
- A service can generate alerts, log data, support user interfaces (UIs), handle user identification or authentication and perform various other tasks.
- The microservices paradigm provides development teams with a more decentralized approach to building software.
- Each service can be isolated, rebuilt, redeployed and managed independently.


Monolithic Architecture
App Services
Bare Metal
Microservices Architecture
Microservice
Microservice
Microservice
Microservice
Bare Metal
Virtualized
Containers
Public Cloud
Applications

Benefits Of Microservices Architecture:

Advantages:

- ➔ Can be developed and deployed using different computing languages and tools
- ➔ Require less development time
- ➔ Can scale quickly
- ➔ Can be reused in different projects
- ➔ Contain better fault isolation
- ➔ Faster and less resource-intensive to deploy and load balance
- ➔ Can be deployed in relatively small teams
- ➔ Work well with Containers.

Challenges Of Microservices Architecture:

Drawbacks:

- Potentially too much granularity
- Extra effort designing for communication between services
- Complex testing
- Latency during heavy use
- Additional management and control
- Comprehensive security.

Challenges with Microservices

Business Impact

98% facing issues identifying root causes report direct business impacts

Troubleshooting

73% find troubleshooting harder in a microservices environment

Bigger Data

17% don't know how to manage the increase in data

Cost of Logs

21% see log aggregation bills climbing

Ops

56% say each additional microservice increases operational challenges

Skills

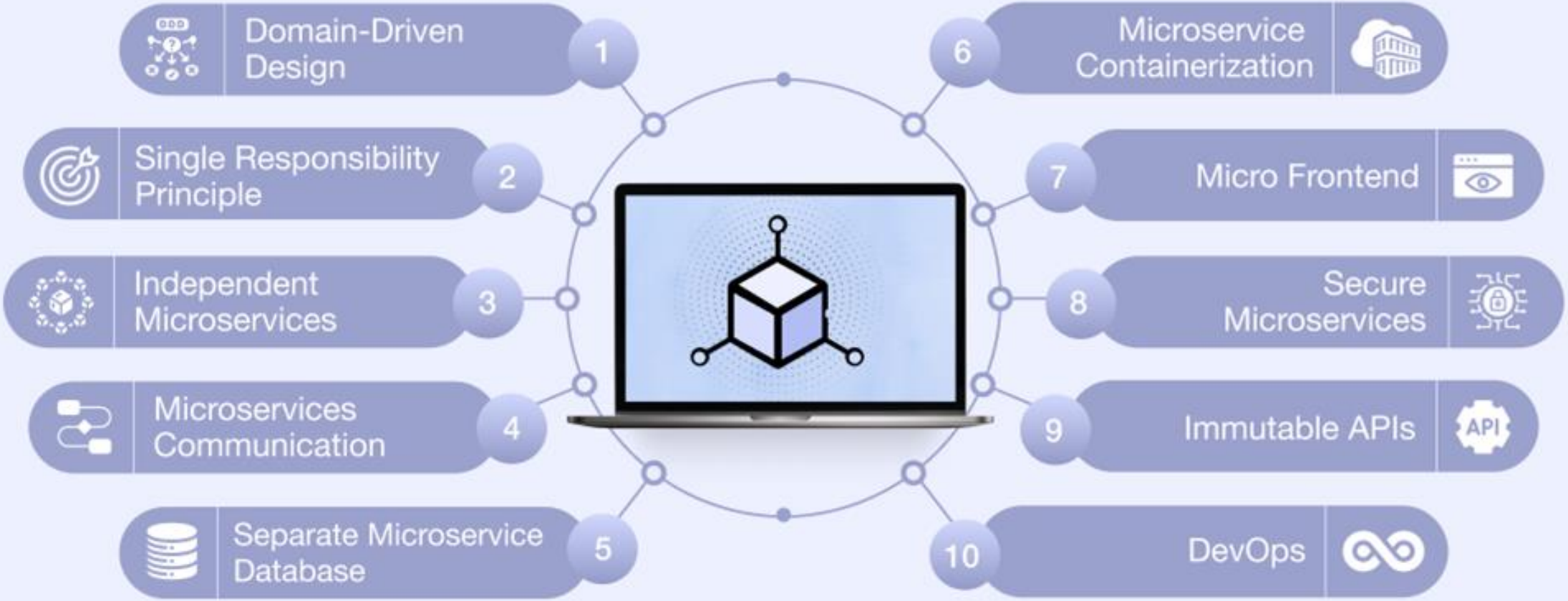
45% don't have the skills to build and manage a microservices architecture

Characteristics Of Microservices Architecture:

Typical characteristics of a microservices design and architecture include the following:

- **Decentralized.**
  Ideally services have few if any dependencies, although loose coupling requires frequent and extensive communication.
- **Resilient.**
  Design services for maximum fault tolerance. A single service failure shouldn't disable an entire application.
- **Use APIs.**
  A microservices architecture relies heavily on APIs and API gateways to facilitate communication.
- **Data separation.**
  Ideally, each service accesses its own database or storage volume.

Microservices Characteristics



Microservices Architecture

Characteristics Of Microservices Architecture:

➔ **Autonomous**

- Each component service in a microservices architecture can be developed, deployed, operated, and scaled without affecting the functioning of other services.
- Services do not need to share any of their code or implementation with other services.
- Any communication between individual components happens via well-defined APIs.

➔ **Specialized**

- Each service is designed for a set of capabilities and focuses on solving a specific problem.
- If developers contribute more code to a service over time and the service becomes complex, it can be broken into smaller services.

Microservices In Cloud:

COMPUTE SERVICES:

- **Container Service**
  AWS Elastic Container Service / Azure Container service

A highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon and Azure instances.

- **Serverless**
  AWS Lambda / Azure Functions

AWS and Azure serverless services lets you run code without provisioning or managing servers. Just upload your code and the serverless service manages everything that is required to run and scale your code with high availability.

Microservices In Cloud:

Storage And Databases:

- **Caching Services**
  AWS ElastiCache / Azure Cache

Caching improves service performance by allowing you to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases.

- **Object Storage**
  AWS Simple Storage Service / Blob Storage

Object storages provides developers and IT teams highly reliable, secure, and scalable object storage for all of their data, large or small.

Microservices In Cloud:

Databases:

- **NoSQL Databases**
  AWS DynamoDB / Azure DocumentDB

A fully managed, fast, and flexible NoSQL database service for all applications that need consistent, single-digit, millisecond latency at any scale.

- **Relational Databases**
  AWS Relational DB / Azure SQL DB

Easily setup, operate, and scale a relational database in the cloud. Choose from six familiar database engines, including Oracle, Microsoft SQL Server, PostgreSQL, MySQL and MariaDB.

Microservices In Cloud:

Networking:

- **Service Discovery**

  AWS Cloud Map / Azure DNS service Discovery

Service discovery is for all your cloud resources. With Cloud Map, you can define custom names for your application resources, and it maintains the updated location of these dynamically changing resources.

- **Service Mesh**

  AWS App Mesh / Azure Service Fabric

Service Mesh makes it easy to monitor and control microservices running on Cloud. Mesh services standardizes how your microservices communicate, giving you end-to-end visibility and helping to ensure high-availability for your applications

Microservices In Cloud:

Networking:

Load Balancers

AWS Elastic Load Balancer / Load Balancing for Azure

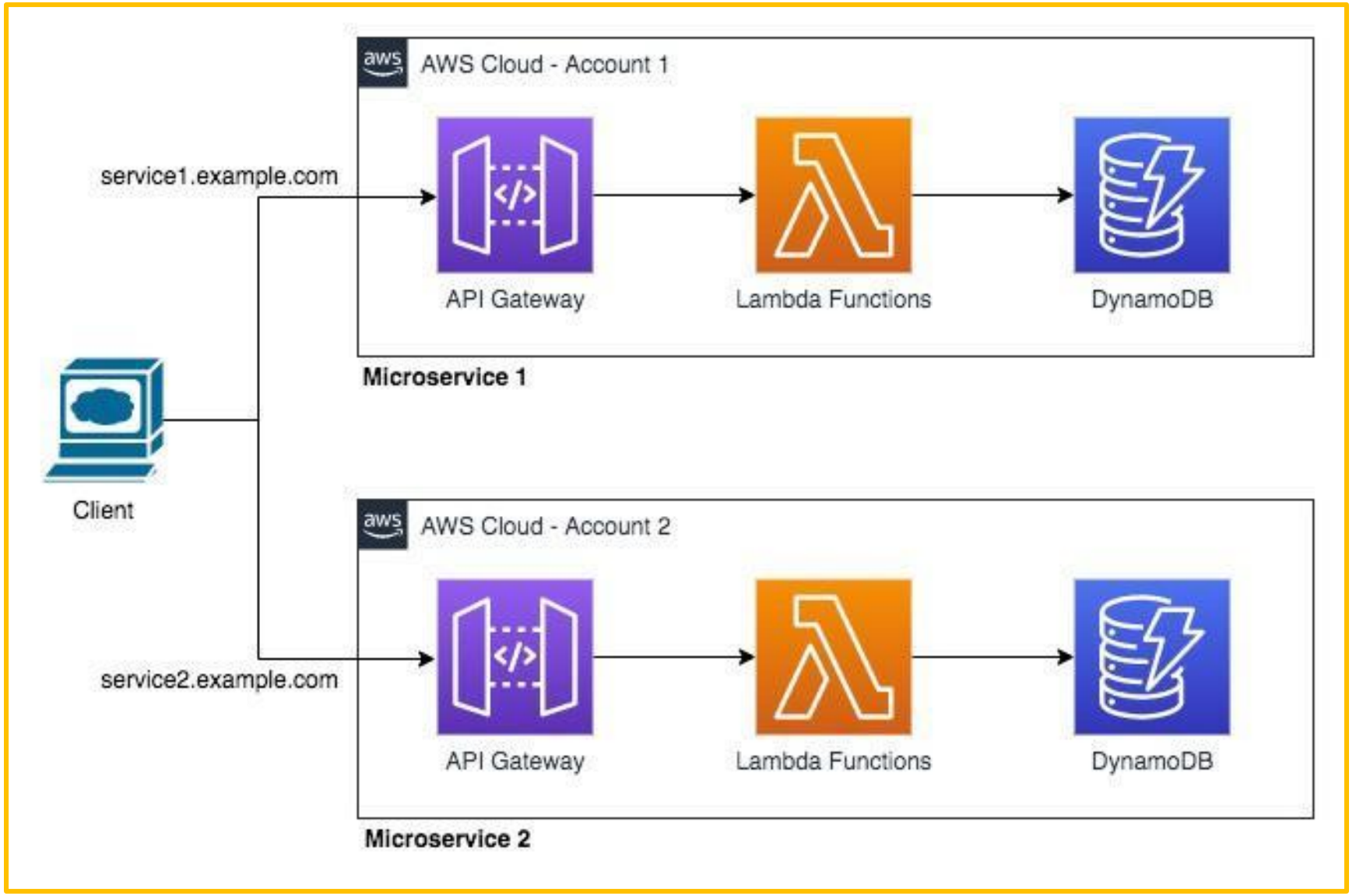
➔ **Application Load Balancer**

The Application Load Balancer load balances HTTP and HTTPS traffic at the application layer (level 7) providing advanced request routing that is targeted at the delivery of modern application architectures, including microservices and containers.

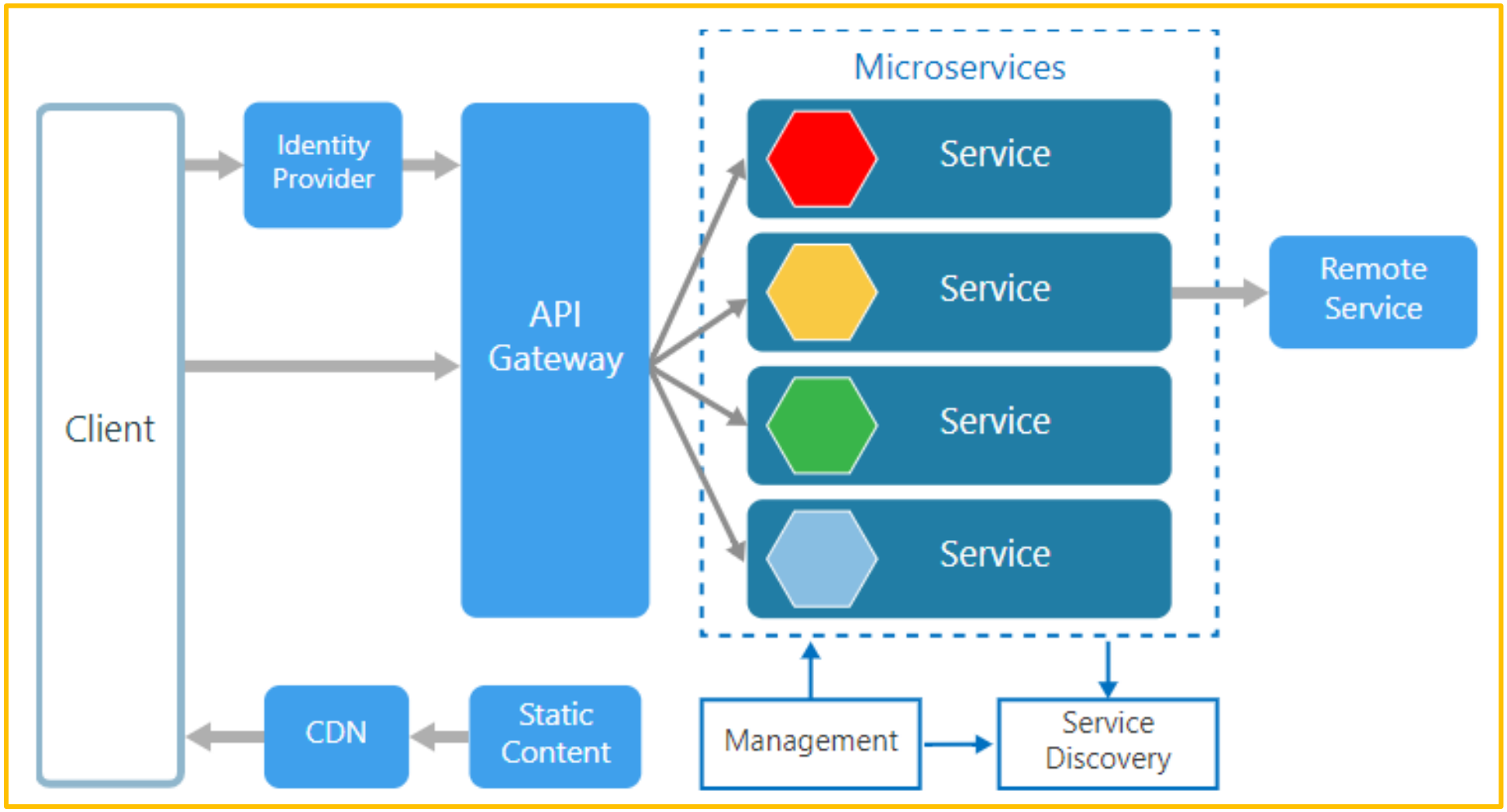
➔ **Network Load Balancer**

The Network Load Balancer offers high performance load balancing that operates at the network connection layer (level 4) and allows you to route connections to microservices based on IP protocol data. The Network Load Balancer can handle millions of requests per second while maintaining ultra-low latencies.

AWS:


AWS Cloud - Account 1
service1.example.com
API Gateway
Lambda Functions
DynamoDB
Microservice 1
Client
AWS Cloud - Account 2
service2.example.com
API Gateway
Lambda Functions
DynamoDB
Microservice 2

AZURE:


Microservices
Client
Identity Provider
API Gateway
Service
Service
Service
Service
Remote Service
CDN
Static Content
Management
Service Discovery

Microservices In Cloud:

Networking

➔ **API Proxy**

Amazon API Gateway / Azure API Management

API proxy services offers a comprehensive platform for API management. It allows you to process hundreds of thousands of concurrent API calls and handles traffic management, authorization and access control, monitoring, and API version management.

➔ **DNS**

Amazon Route 53 / Azure Traffic Manager

DNS service is a highly available and scalable cloud Domain Name System (DNS) web service that effectively connects requests to infrastructure that is running in AWS and Azure. It can be used for IP health checks and service discovery for microservices.

Microservices In Cloud:

Messaging:

- **Message Publishing & Subscription**
  Amazon Simple Notification Service / Azure Notification Hub - Service Bus

It is a fully managed pub/sub messaging service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.

- **Message Queueing**
  Amazon Simple Queue Service / Azure Queue Storage

It is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.

Microservices In Cloud:

Logging And Monitoring:

- **API Monitoring**
  AWS CloudTrail / Azure Operational Insights

API monitoring service provides continuous logging and monitoring, and retain account activity related to actions across your infrastructure. The event history simplifies security analysis, resource change tracking, and troubleshooting.

- **Application and Resource Monitoring**
  Amazon CloudWatch / Azure Application Insights

It collects and tracks metrics, collects and monitors log files, set alarms, and automatically react to changes across your running services and AWS and Azure resources.

Microservices In Cloud:

Logging And Monitoring:

➔ **Distributed Tracing**
AWS X-Ray / Azure Monitor

Get an end-to-end view of requests as they travel through your application and see a map of your application's underlying components. As a set of microservices works together to handle a request, this service can provide a centralized view of logs, allowing you to monitor and troubleshoot complex interactions.

Microservices In Cloud:

DevOps:

➔ **Container Image Repository**
Amazon Elastic Container Registry / Azure Container Registry

A fully managed Docker container registry that you can use to store, manage, and deploy Docker container images.

Container Image Repository is integrated with Container Service, simplifying development to production workflow for containers.

Microservices In Cloud:

DevOps:

Continuous Delivery

➔ **Cloud Developer Tools**

AWS Developer Tools / Azure Developer Tools

Cloud Developer Tools is a set of services that enable developers and IT operations professionals practicing DevOps to rapidly and safely deliver software.

These services help you securely store and version control your application's source code, and automatically build, test, and deploy your application to cloud or your on-premises environment.

BENEFITS OF A MICROSERVICES ARCHITECTURE

CONTINUOUS DELIVERY AND DEPLOYMENT

BETTER SCALABILITY

IMPROVED FAULT ISOLATION

GREATER FLEXIBILITY

SMALLER DEVELOPMENT TEAMS

HIGHER SOFTWARE TESTABILITY

IMPROVED MAINTAINABILITY

Companies using Microservices are:

- Comcast Cable
- Uber
- Netflix
- Amazon
- eBay
- Soundcloud
- Karma
- Karma
- Microsoft
- Groupon
- Hailo
- Gilt
- Zalando
- Lending Club
- AutoScout24

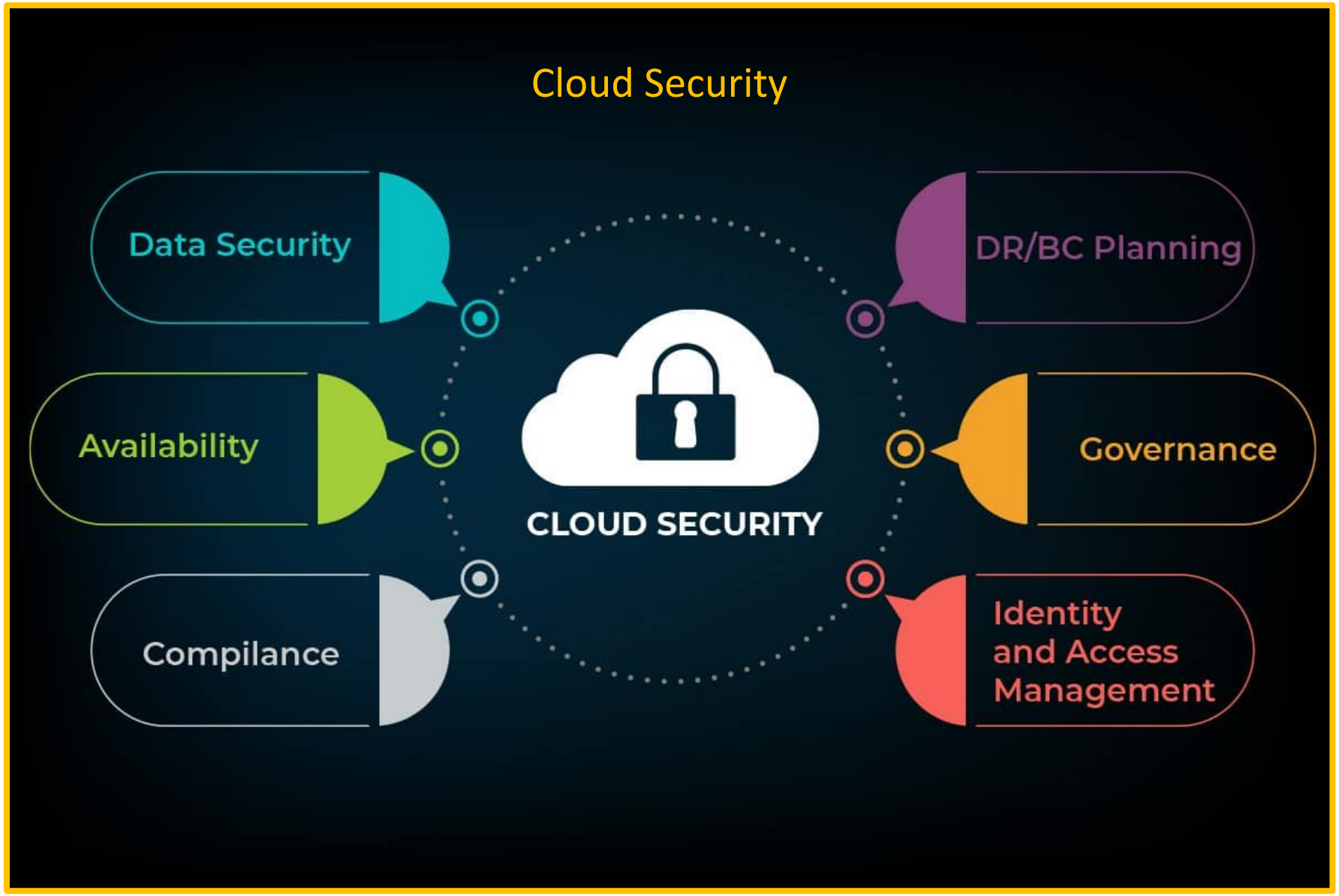
Q&A Session

1. What is a microservice?
    a. A design used primarily in functional programming and object-oriented programming
    b. A small program that represents discrete logic that executes within a well-defined boundary on dedicated hardware
    c. A style of design for enterprise systems based on a loosely coupled component architecture
    d. A very small piece of code that never gets any bigger than 10 lines

1. Which of the following responses is an advantage of microservices?
    a. Any microservice component can change independently from other components
    b. They don't require a lot of expertise to program
    c. They're so small that developers can typically write very powerful ones with a few lines of text
    d. They are easy to manage

1. Which of the following responses is a disadvantage of microservices?
    a. Microservices are very difficult to manage at scale
    b. Microservices require a lot of monitoring to operate effectively
    c. Neither A nor B
    d. Both A and B


VS


Cloud Security
Data Security
DR/BC Planning
Availability
Governance
CLOUD SECURITY
Compilance
Identity
and Access
Management

On Prem Vs Cloud Securtiy:

- The on-prem versus cloud security debate continues within the data center industry.
- The differences range from minor to substantial, but both on-prem and cloud advocates can agree that countless protections and threats exist in either environment.
- Beyond focusing solely on meeting IT security priorities.

The Question Is: **Which is more secure for my organization and its business objectives?**

On-Prem Securtiy:

On-premises servers are the traditional enterprise computing model. In this implementation, all hardware and software resides in house.

A business purchases and maintains its own servers, located in a secure, climate-controlled room onsite.

The company needs specialized IT support to manage the equipment, as well as appropriate HVAC systems, UPS, battery powers etc to keep the equipment in working order.

IT professionals must stay up-to-date with the latest software updates and perform regular backups. A continuous expansion in business needs to procure new hardware to meet its growing demands.

On-Prem Securtiy:

Benefits Of On-Prem Security:

- **Increased Control**
  More control over security is retained when a company manages services with its own on-prem servers.

- **Infinite Customization**
  On-Premises serves to allow network customization that is tailor-made for a company's needs.

- **More Reliable**
  On-prem servers do not rely on an internet connection.

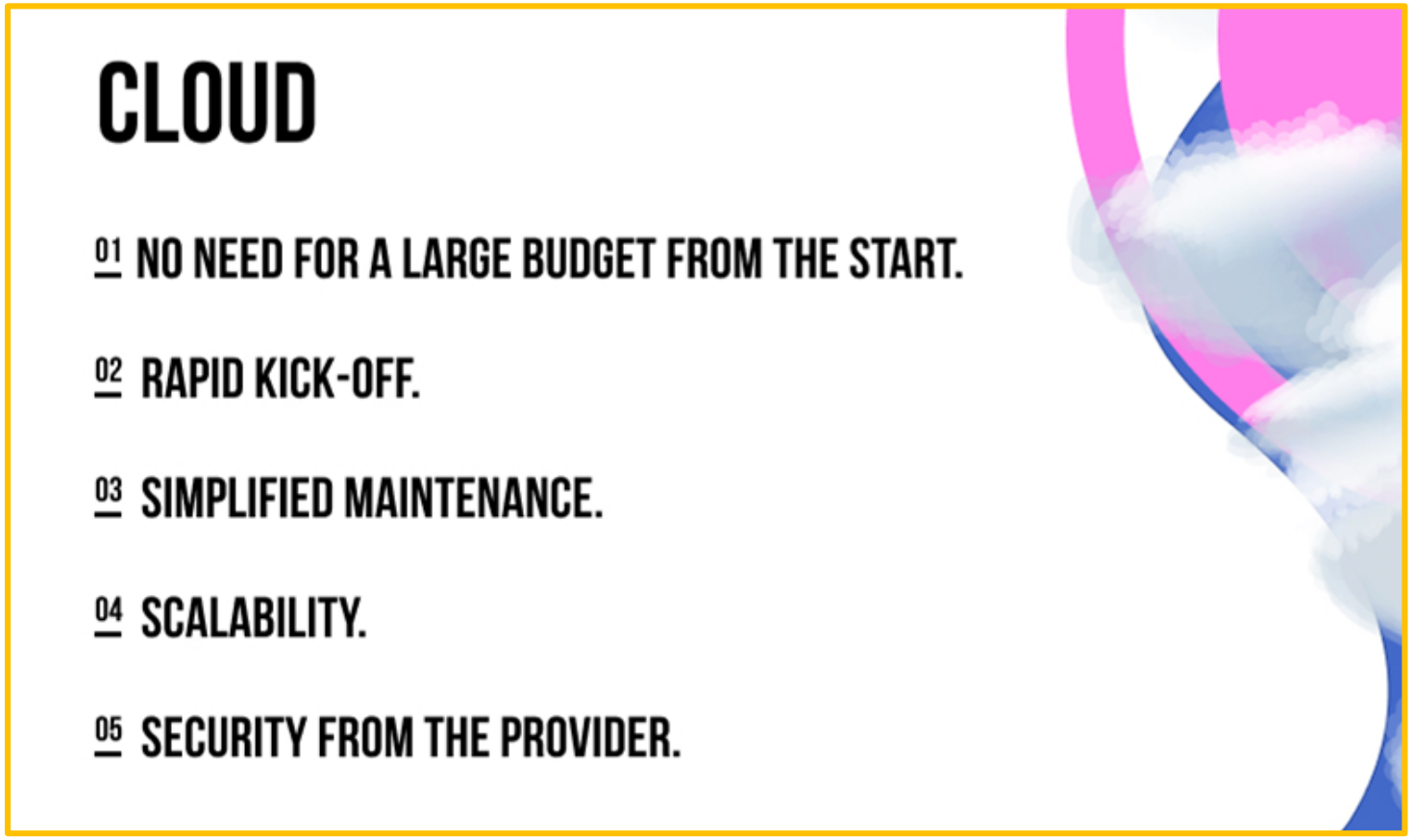
- **Quicker Learning Curve**
  The majority of IT professionals are better equipped to build security processes in this environment.

Cons Of On-Prem Security:

- **Timely To Scale**
  Procurement of IT hardware can take time and research to scale security for on-prem data centers.

- **Increases The Need For On-Site Security**
  Without the right team and safety controls in place, some businesses may be more vulnerable to physical threats such as damage to physical property.

Cloud Securtiy:



Benefits Of Cloud Securtiy:

- **Easier To Scale**
  Expanding storage for data in the cloud is as straightforward as upgrading a cloud storage package.

- **Faster Set-Up**
  Cloud-based security is more automated, which means set-up takes minutes rather than days.

- **Flexible Pricing Structure**
  Cloud computing often has a more flexible pricing structure with “pay-as-you-grow” fees.

Cons Of Cloud Securtiy:

- **Increased Vulnerabilities**
  The cloud's larger attack surface can make it particularly vulnerable to cyberattacks.

- **Limited Customization**
  Traditional monitoring and security tools do not always work in cloud environments.

- **Regulation Issues**
  Some regulations require that the shared responsibility of multi-tenant hardware is not used.

- **More Expensive**
  Cloud computing often has a more flexible pricing structure with "pay-as-you-grow" fees, but is less predictable for forecasting unforeseen costs and is more expensive in the long term.

	On-premise	Cloud
Installation	You manage	Automatic
Firewalls	You configure	Automatic
IT infrastructure	You provide	Included
Database security	You provide	Included
Virus protection	You provide	Included
Patches/ Updates	Manual	Included
Upgrades	Manual	Included
24/7 monitoring	You provide	Included
Mobile CMMS	You configure (if possible)	Included

SECURITY

CLOUD SECURITY

- Cloud provider is responsible for security on an equal footing with the client
- Security is automated, thanks to the presence of various APIs
- Adding additional features and requirements entails an increase in the cost of the cloud provider's services
- Some conditions in the work of the provider are immutable and may not suit you
- An initial investment in security is zero - this is included in the cost of the entire service On-Premise Security

ON-PREMISE SECURITY

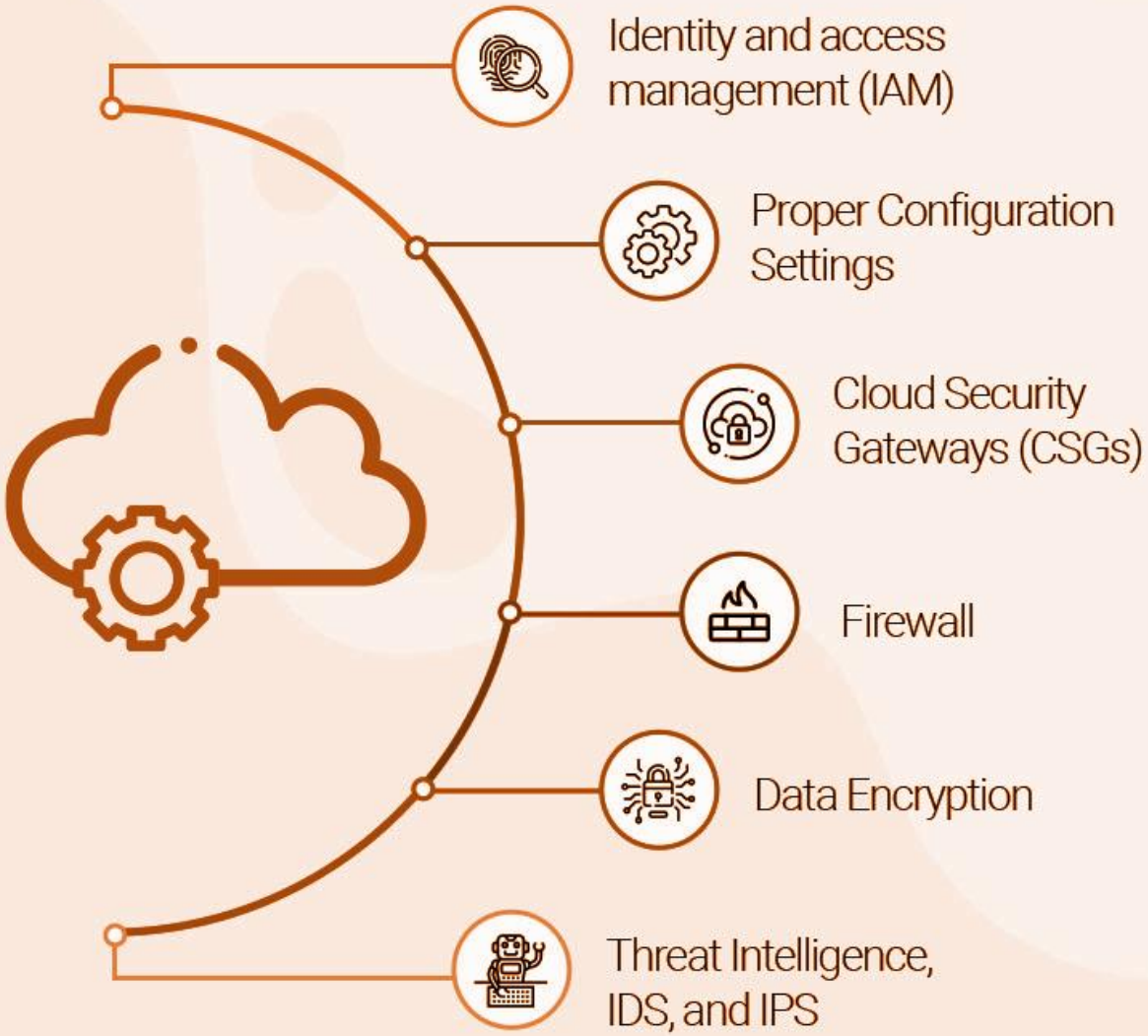
- Fully implemented by company resources
- Provides the need to ensure offline security too
- The high initial investment, but without the need for constant infusion of funds
- Custom server configuration for the specific needs of your business
- All control on your part

Q&A Session

1. During which phase of a cloud migration framework is security the most critical?
    a. Discovery phase
    b. Cloud migration phase
    c. Operations phase
    d. All of the above

1. Cloud security analytics can help enterprises:
    a. Predict account hijacking
    b. Detect malware with unknown signatures
    c. Monitor data for access
    d. All of the above

Cloud Security



Addressing Cloud Security: Why is it Important?

What Is Cloud Securtiy:

- Cloud computing security refers to the discipline and practice of protection.
- Cloud security entails securing cloud environments
- While cloud security applies to security for cloud environments, the related term, cloud-based security, refers to the software as a service (SaaS) delivery model of security services, which are hosted in the cloud rather than deployed via on-premise hardware or software.

Principal Of Cloud Computing Securtiy:

Lack of Visibility & Shadow IT

- ➔ Cloud computing makes it easy for anyone to subscribe to a SaaS application or even to spin up new instances and environments.
- ➔ Users should adhere to strong acceptable use policies for obtaining authorization for, and for subscribing to, new cloud services or creating new instances.

Principal Of Cloud Computing Securtiy:

Lack of Control

- Leasing a public cloud service means an organization does not have ownership of the hardware, applications, or software on which the cloud services run.
- Ensure that you understand the cloud vendor's approach to these assets.

Principal Of Cloud Computing Securtiy:

Transmitting & Receiving Data

- ➔ Cloud applications often integrate and interface with other services, databases, and applications.
- ➔ This is typically achieved through an application programming interface (API).
- ➔ It’s vital to understand the applications and people who have access to API data and to encrypt any sensitive information.

Principal Of Cloud Computing Securtiy:

Embedded/Default Credentials & Secrets

- ➔ Cloud applications may contain embedded and/or default credentials.
- ➔ Default credentials post an increased risk as they may be guessable by attackers.
- ➔ Organizations need to manage these credentials as they would other types of privileged credentials.

Principal Of Cloud Computing Securtiy:

Incompatibilities

IT tools architected for on-premise environments or one type of cloud are frequently incompatible with other cloud environments.

Incompatibilities can translate into visibility and control gaps that expose organizations to risk from misconfigurations, vulnerabilities, data leaks, excessive privileged access, and compliance issues.

Multitenancy

Multi Tenancy is the backbone for many of the cloud benefits of shared resources (e.g., lower cost, flexibility, etc.), but it also introduces concerns about data isolation and data privacy.

Principal Of Cloud Computing Securtiy:

Scalability Cuts Both Ways

Automation and rapid scalability are chief benefits of cloud computing, but the flip side of cloud computing security is listed below:

- Vulnerabilities
- Misconfigurations
- Sharing of secrets–APIs
- Privileged credentials
- SSH keys
- Can also proliferate at speed and scale.

Principal Of Cloud Computing Securtiy:

Malware & External Attackers

Attackers can make a living by exploiting cloud vulnerabilities.

Rapid detection, and a multi-layered security approach (firewalls, data encryption, vulnerability management, threat analytics, identity management, etc.) will help you to reduce risk, while leaving you better poised to respond to withstand an attack

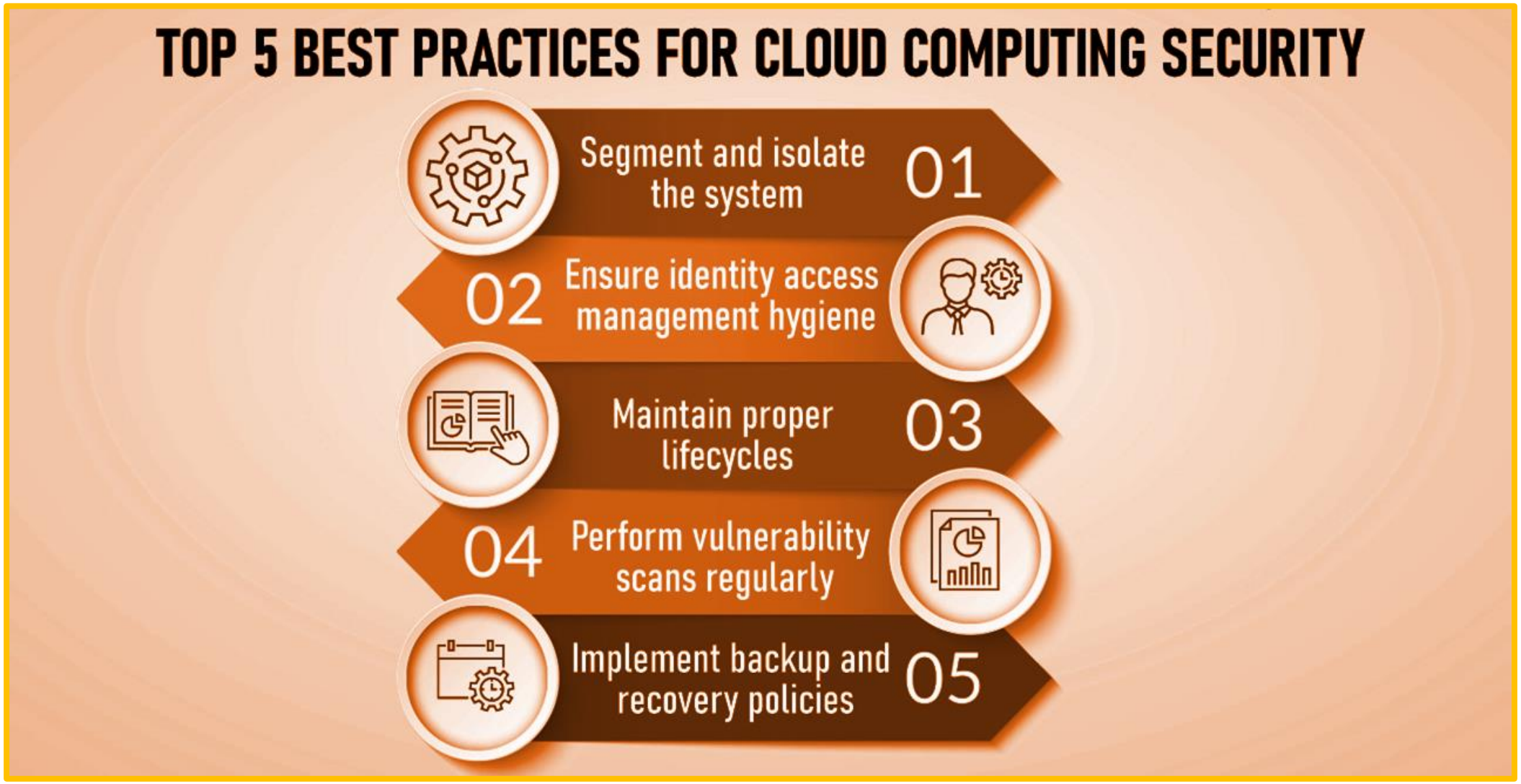
Principal Of Cloud Computing Securtiy:

Insider Threats – Privileges

Insider-related threats (either through negligence or malevolence), generally take the longest to detect and resolve, with the potential to be the most harmful.

A strong identity and access management framework along with effective privilege management tools are essential to eliminating these threats, and reducing the damage (such as by preventing lateral movement and privilege escalation) when they do occur.

Cloud Computing Security Best Practice


TOP 5 BEST PRACTICES FOR CLOUD COMPUTING SECURITY
Segment and isolate the system
01
02
Ensure identity access management hygiene
Maintain proper lifecycles
03
04
Perform vulnerability scans regularly
Implement backup and recovery policies
05

Best Practice Of Cloud Computing Securtiy:

Strategy & Policy

A holistic cloud security program should account for ownership and accountability (internal/external) of cloud security risks, gaps in protection/compliance, and identify controls needed to mature security and reach the desired end state.

Network Segmentation

In multi-tenant environments, assess what segmentation is in place between your resources and those of other customers, as well as between your own instances.

Leverage an isolation approach to isolate instances, containers, applications, and full systems from each other when possible.

Best Practice Of Cloud Computing Securtiy:

Identity and Access Management and Privileged Access Management

Leverage robust identity management and authentication processes to ensure only authorized users having access to the cloud environment, applications, and data.

Enforce least privilege to restrict privileged access and to harden cloud resources.

Ensure privileges are role-based, and that privileged access is audited and recorded via session monitoring.

Best Practice Of Cloud Computing Securtiy:

Discover and Onboard Cloud Instances and Assets

Once cloud instances, services, and assets are discovered and grouped, bring them under management (i.e. managing and cycling passwords, etc.).

Discovery and onboarding should be automated as much as possible to eliminate shadow Infrastructure.

Best Practice Of Cloud Computing Securtiy:

Password Control (Privileged and Non-Privileged Passwords)

Never allow the use of shared passwords. Combine passwords with other authentication systems for sensitive services. Ensure password management best practices.

Vulnerability Management

Regularly perform vulnerability scans and security audits, and patch known vulnerabilities.

Best Practice Of Cloud Computing Securtiy:

Encryption

Ensure your cloud data is encrypted, at rest, and in transit.

Disaster Recovery

Be aware of the data backup, retention, and recovery policies and processes for your cloud vendor(s).

Best Practice Of Cloud Computing Securtiy:

Monitoring, Alerting, and Reporting

Implement continual security and user activity monitoring across all environments and instances.

Integrate and centralize data from your cloud provider (if available) with data from in-house and other vendor solutions, so you have a holistic picture of what is happening in your environment.

Q&A Session

Q) What are the cloud security threats facing the public cloud?

A) Organizations rank the following threats as the largest obstacles for public clouds:

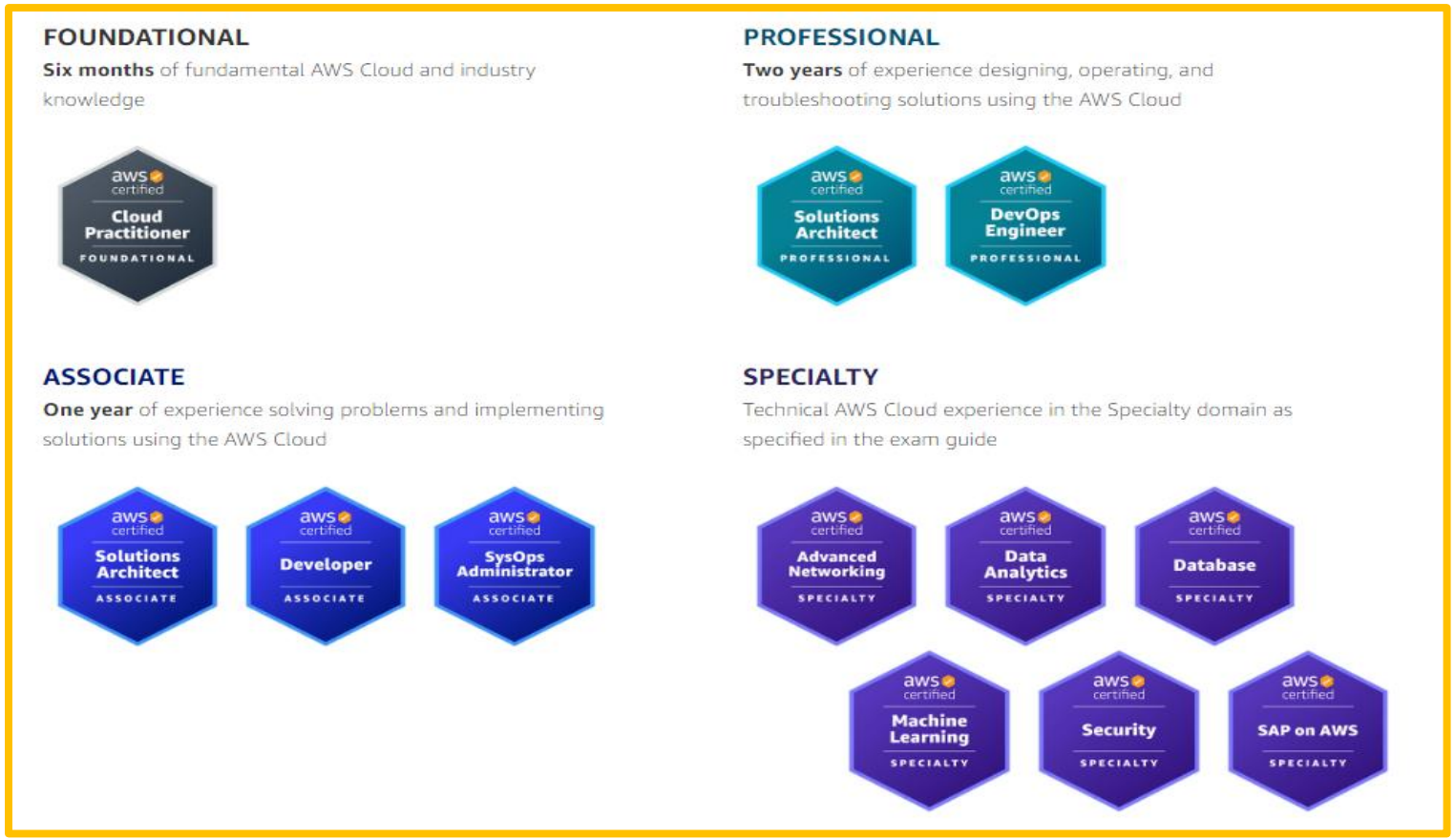
- Misconfigurations of the cloud platform/incorrect set up
- Unauthorized access
- Insecure interfaces/APIs

Q) Explain the Cloud Security controls?
A)

- Risk management
- Governance
- Data Protection
- Identity and Access Management
- Compliance


aws

AWS Certification Road Map:



AWS Certification Pricing:

AWS Certification exams:

The Cloud Practitioner exam is 100 USD. Associate-level exams are 150 USD. Professional-level and Specialty exams are 300 USD. You can renew your certification by using your 50% off voucher code to take the current, full exam at 50% off. Please note that taxes (such as Value Added Tax) may apply..

AWS Certified Solutions Architect,Developer and Sysops Administrator- Associate

Cost: $150

Format, Time: 65 questions, 130 minutes

AWS Certified Cloud Practitioner

Cost: $100

Format, Time: 65 questions, 90 minutes

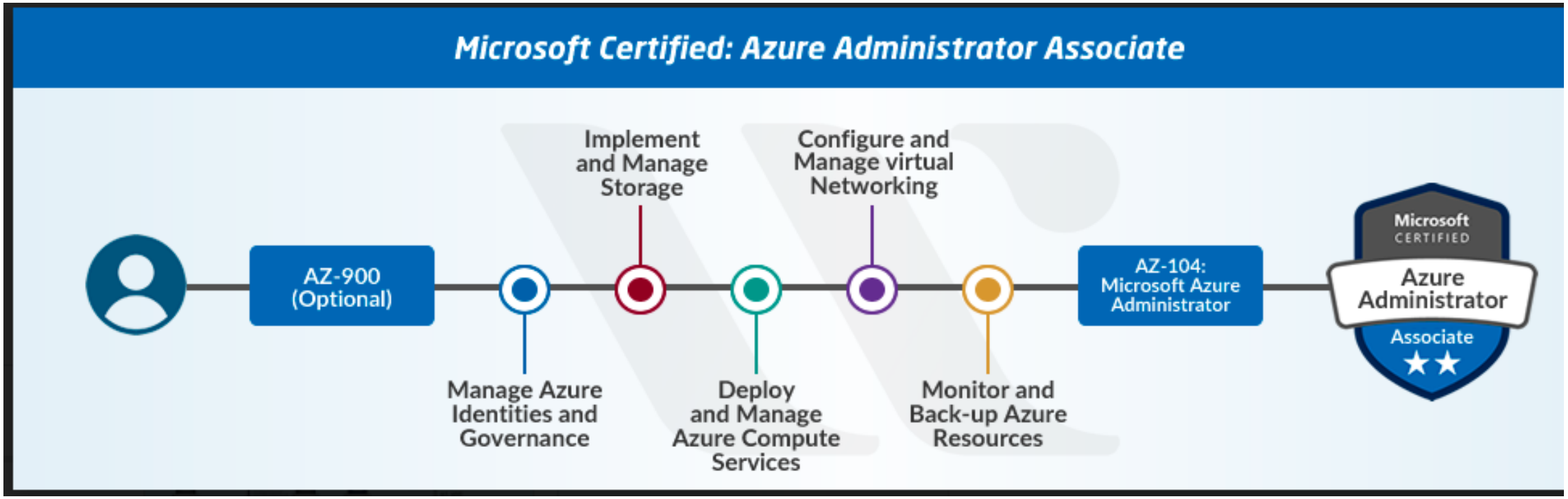
AWS Professional and Specialty Certification Exams

Cost: $300

Format, Time: 75 questions, 170 minutes

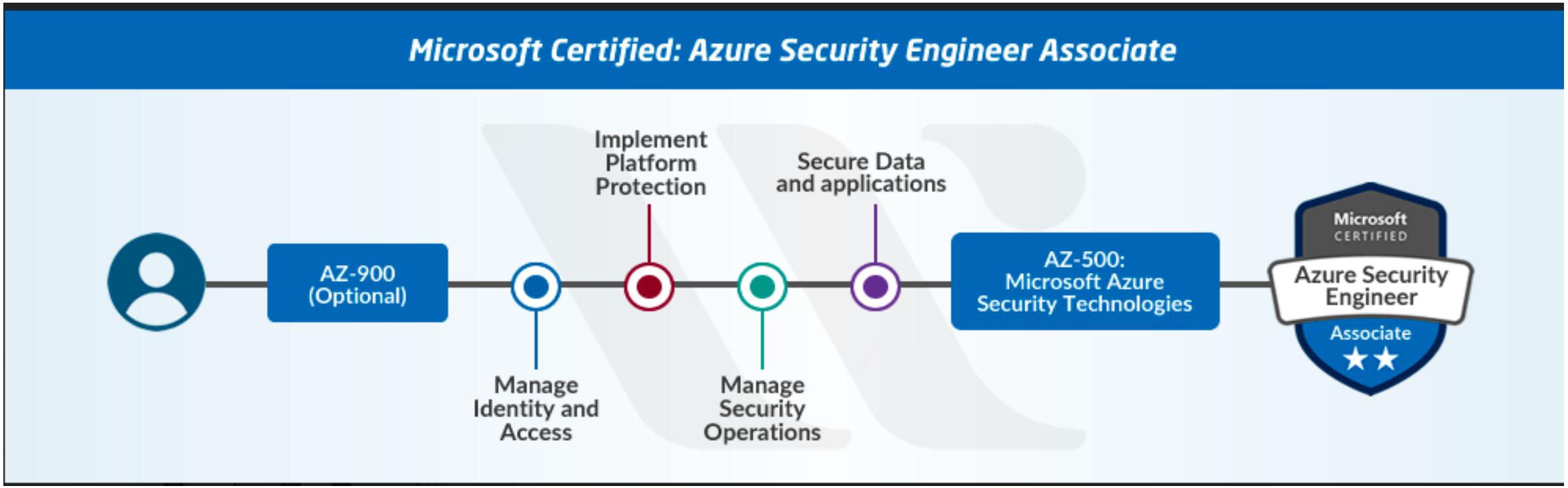
Azure Certification Road Map:

AZ104



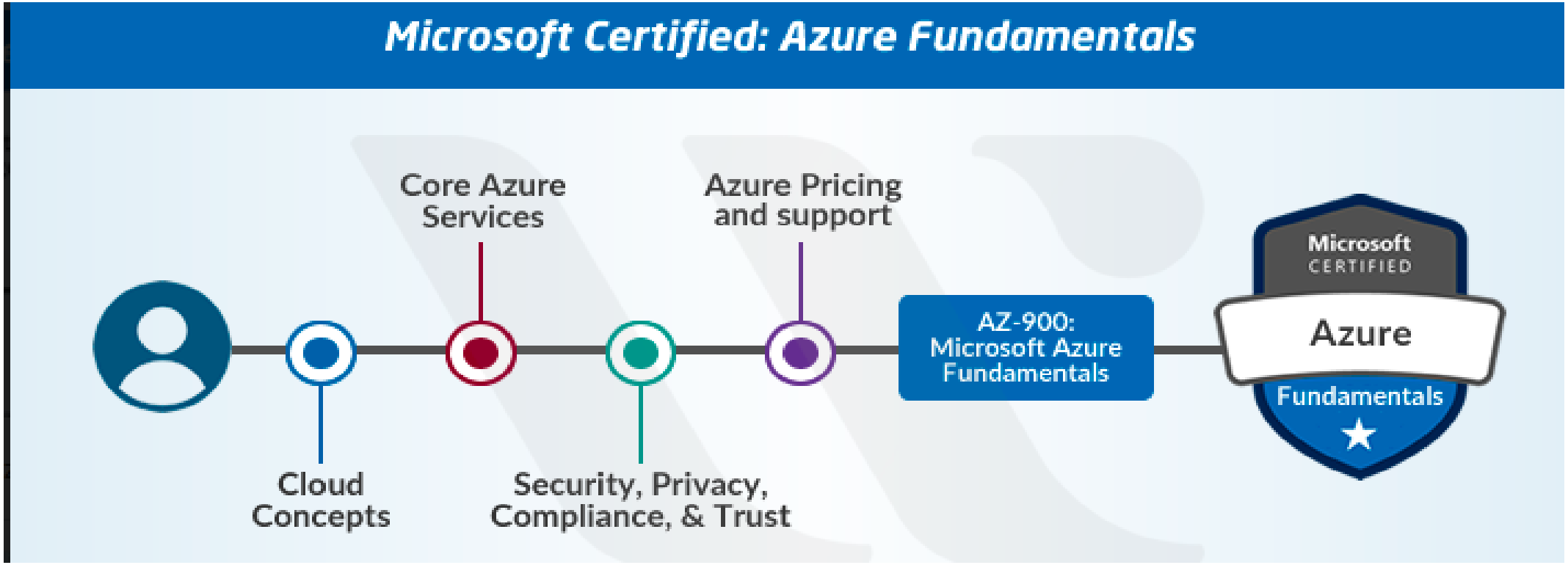
Azure Certification Road Map:

AZ500



Azure Certification Road Map:

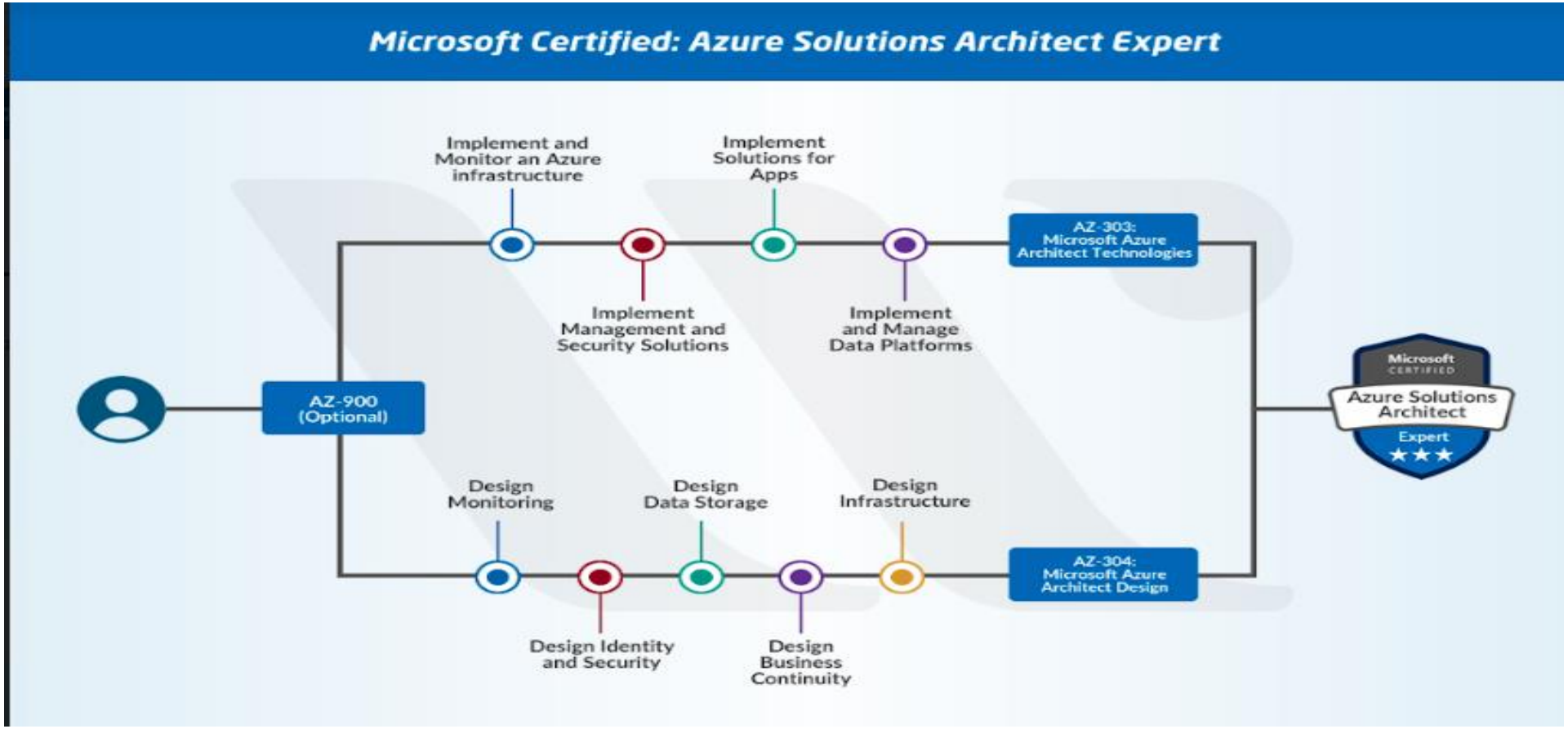
AZ900



Role Base Azure Certification Road Map:

AZ900

Azure Solution Architect Expert:



What we achieved?

Introducing the Cloud
Hypervisors
Types Of Cloud
Architecture of Cloud
Microservices
Cloud Security
AWS Certification RoadMap
Azure Certification RoadMap

Characteristics of **Virtualization**

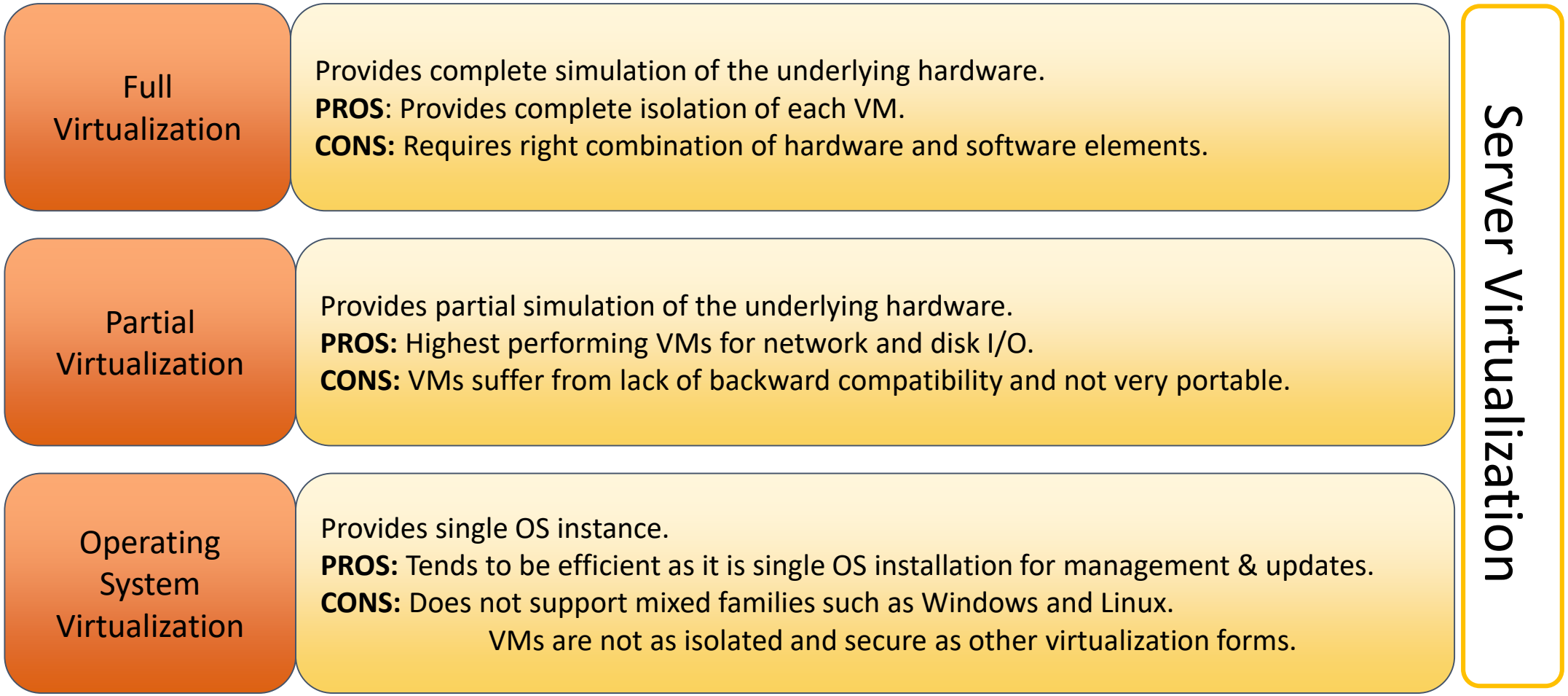
Distribution of resources: Virtualization and Cloud Computing technology ensure end-users develop a unique computing environment. It is achieved through the creation of one host machine. Through this host machine, the end-user can restrict the number of active users. They can also be used to bring down power consumption.

Accessibility of server resources: This feature ensures a boost to uptime, and there is less fault tolerance and availability of resources.

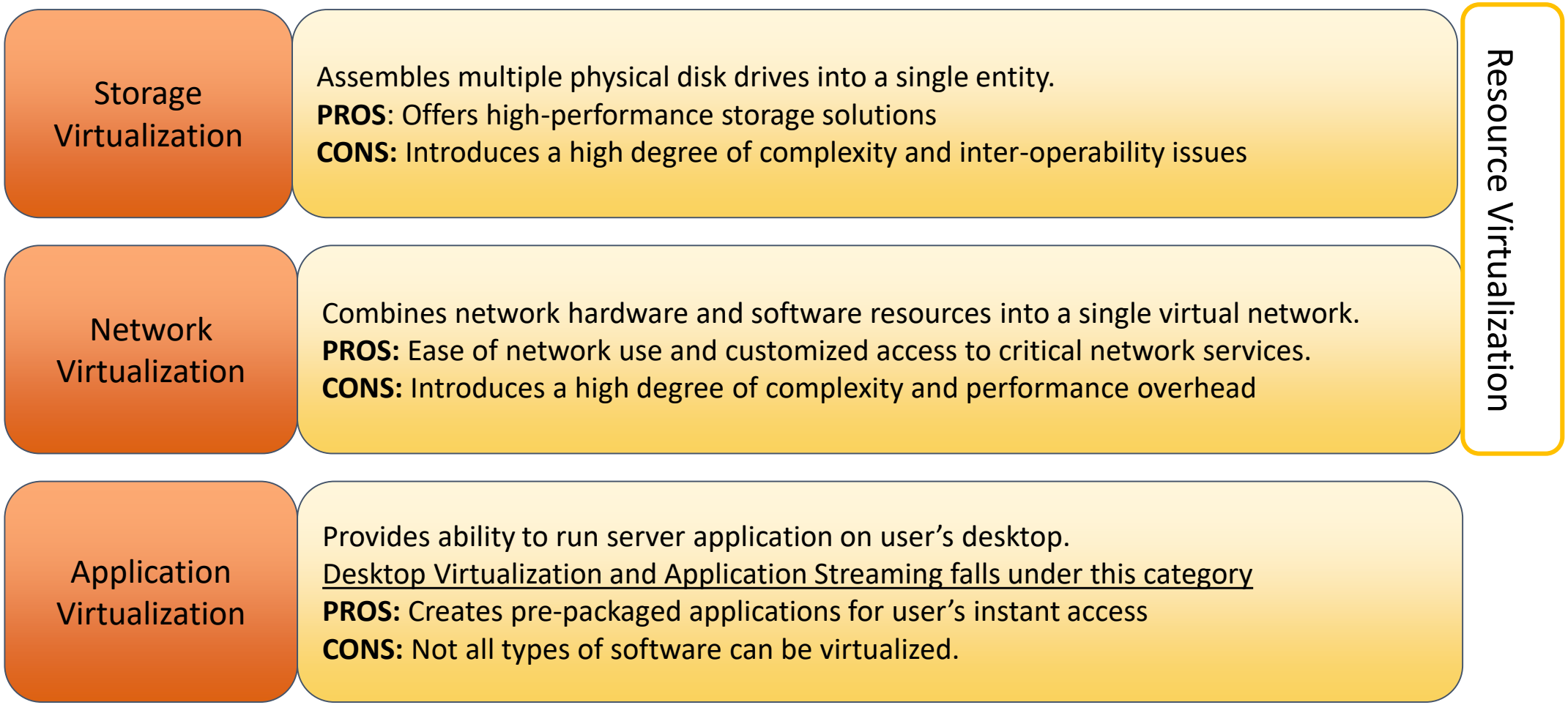
Characteristics of **Virtualization**

Resource Isolation: Virtualization provides isolated virtual machines. Each virtual machine can have many guest users, and guest users could be either operating systems, devices, or applications.
Security and authenticity: The virtualization systems ensure continuous uptime of systems, and it does automatic load balancing and ensures there is less disruption of services.
Aggregation: Aggregation in Virtualization is achieved through cluster management software. This software ensures that the homogenous sets of computers or networks are connected and act as one unified resource.

Types Of Virtualization



Types Of Virtualization

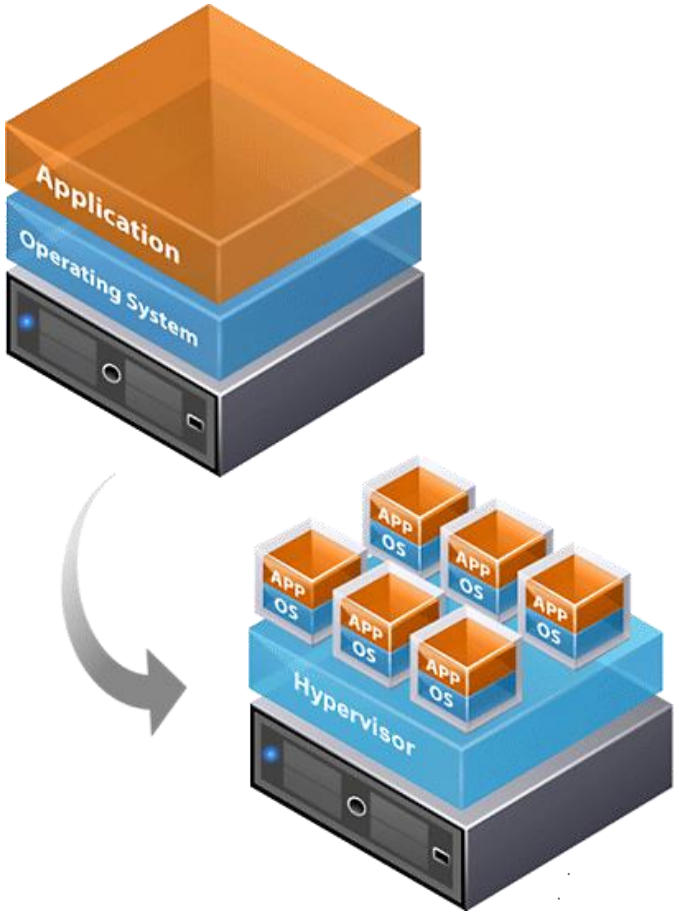


About Hypervisors

A hypervisor or virtual machine monitor (VMM) is **a piece of computer software, firmware or hardware that creates and runs virtual machines.**

A computer on which a hypervisor runs one or more virtual machines is called a **host machine**, and each virtual machine is called a **guest machine.**

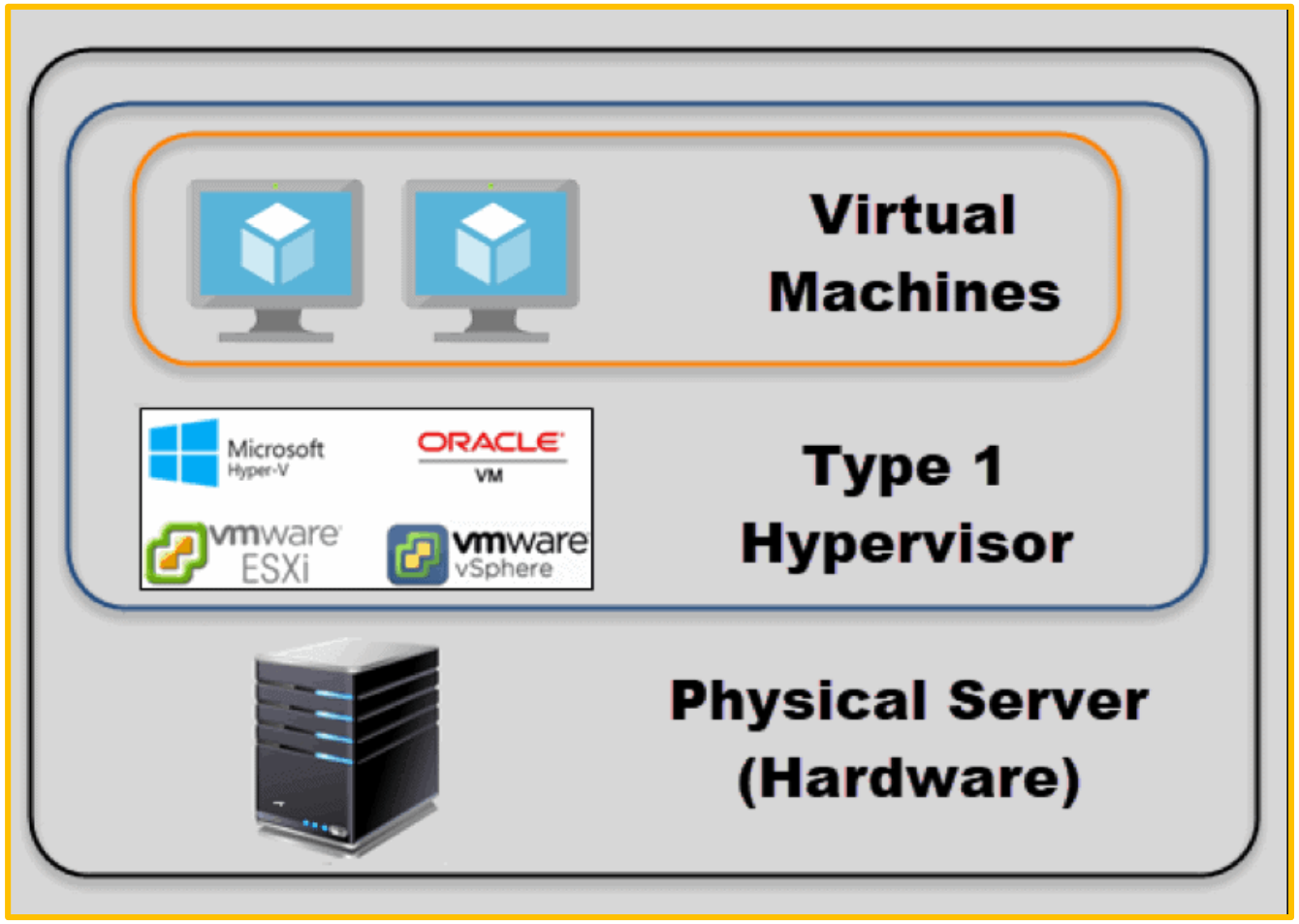
- Type 1 Hypervisor (bare metal or native)
- Type 2 Hypervisor (hosted hypervisors)



About Hypervisors (Types)

Type 1 Hypervisor

- A bare-metal hypervisor (Type 1) is a layer of software we install directly on top of a physical server and its underlying hardware.
- Type 1 hypervisors are an OS themselves, a very basic one on top of which you can run virtual machines.



About Hypervisors (Types)

Type 1 Hypervisor Vendors

- VMware vSphere with ESX/ESXi
- KVM (Kernel-Based Virtual Machine)
- Microsoft Hyper-V
- Oracle VM
- Citrix Hypervisor (formerly known as Xen Server)

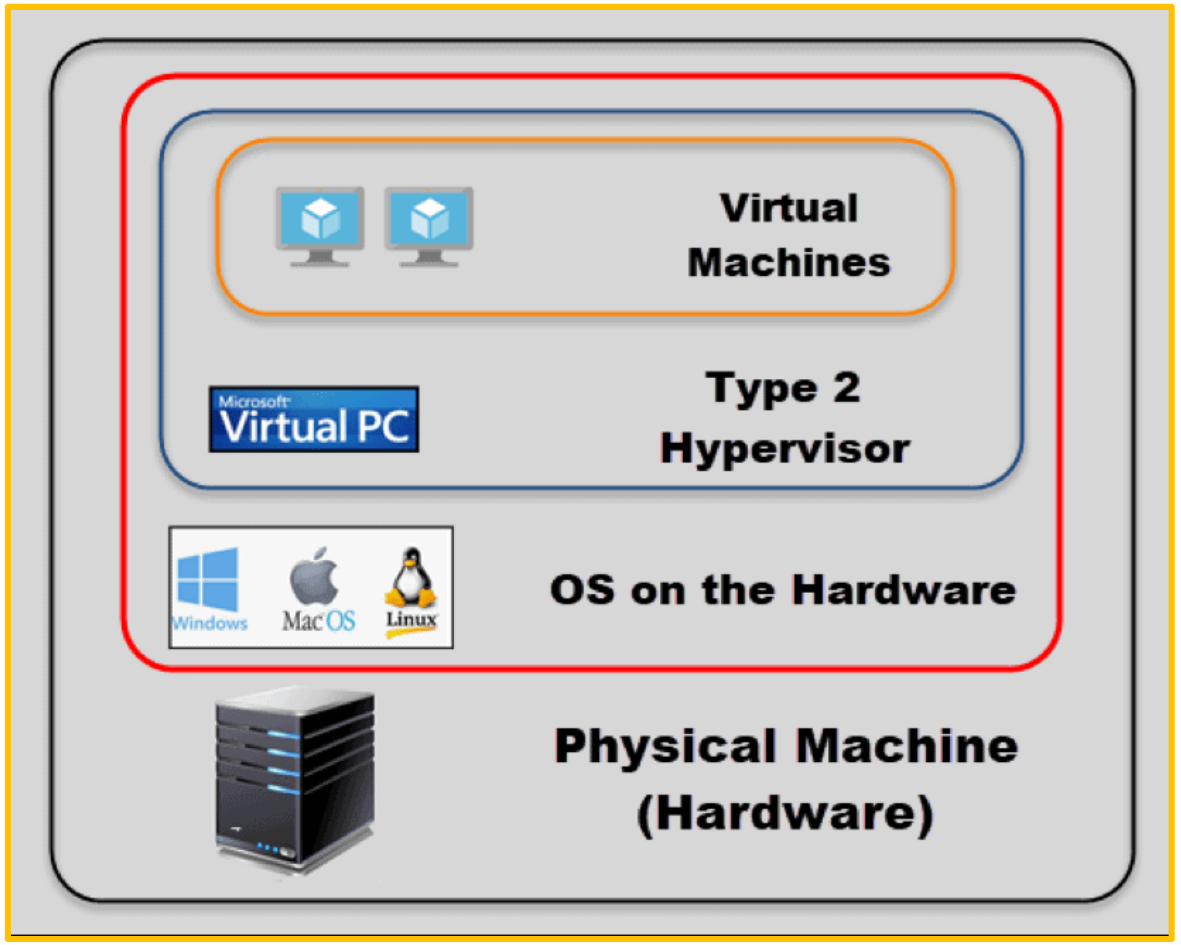
About Hypervisors (Types)

Type 2 Hypervisor

This type of hypervisor runs inside of an operating system of a physical host machine.

In this case we have:

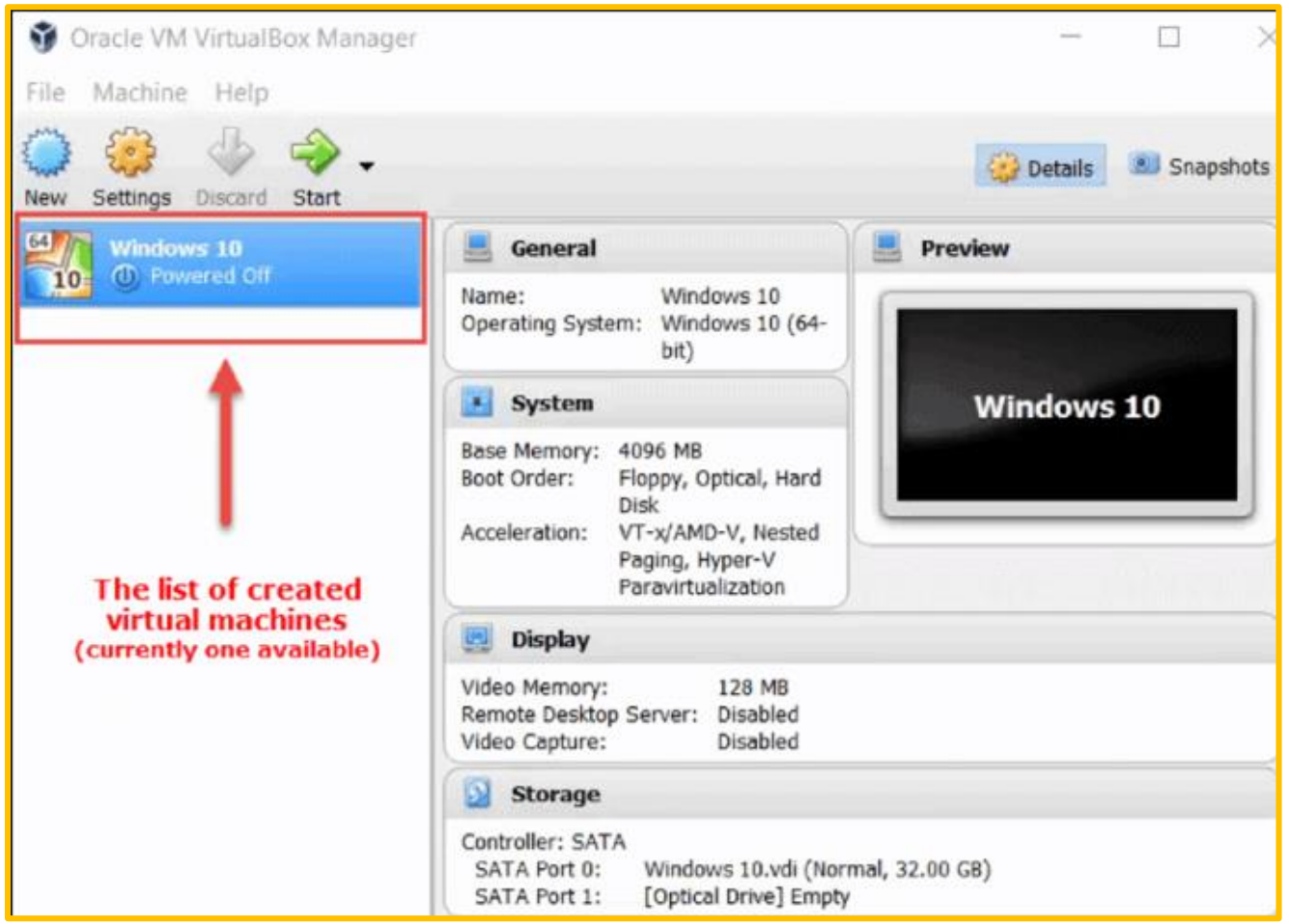
- A physical machine.
- An operating system installed on the hardware (Windows, Linux, macOS).
- A type 2 hypervisor software within that operating system.
- The actual instances of guest virtual machines.



About Hypervisors (Types)

Type 2 Hypervisor Vendors

- Oracle VM VirtualBox
- VMware Workstation Pro/VMware Fusion
- Windows Virtual PC
- Parallels Desktop



Q&A Session

1. What is a Hypervisor?
    a. Software Used for OS Virtualization
    b. Software which virtualizes hardware
    c. Software used for Storage Virtualization
    d. Software which allows physical hardware to be shared between VMs

2. What are some different usage of Virtualization?
    a. Virtual Memory
    b. Virtual Storage
    c. Virtual Network
    d. Virtual Machine

About Virtualization

In computing, virtualization refers to the act of creating a virtual (rather than actual) version of something, including **virtual computer hardware platforms, operating systems, storage devices, and computer network resources**