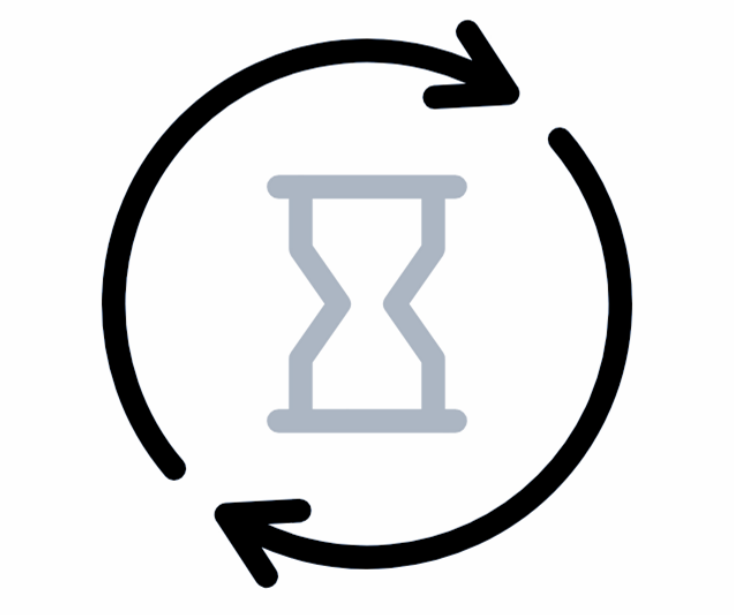
Introduction to Cloud

AGENDA

- Why Move to the Cloud
- Understanding Cloud Computing
- Cloud Infrastructure
- Cloud Security
- Cloud Cost Management

Let’s rollback in Time



The First Wave...

On-Prem

Hardware Defined Data Center (HDDC)

- *Storage*
- *Network Switches*
- *Racks*
- *Servers/machines/nodes*
- *Power Supply*
- *Cables*
- *PDU's*
- *Cooling System*
- *Security*
- *Operators/Staff/Maintenance*
- *Firewalls*
- *Routers*
- *and many more...*

Availability of Data Center and Resources

CAPEX (Upfront Cost)

Long waiting time (months to year)

Capacity planning challenge

Poor Resource Utilization (30% - 40%) - 1:1

No business focus

Availability, Reliability, and Fault Tolerance are organization's responsibility

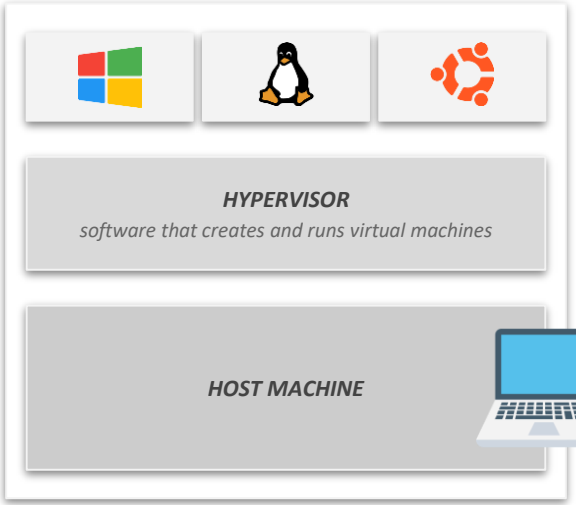
The Second Wave...

On-Prem

Hardware Defined Data Center (HDDC)

Virtualization

Software Defined Data Center (SDDC)



Resource Utilization becomes 1:N

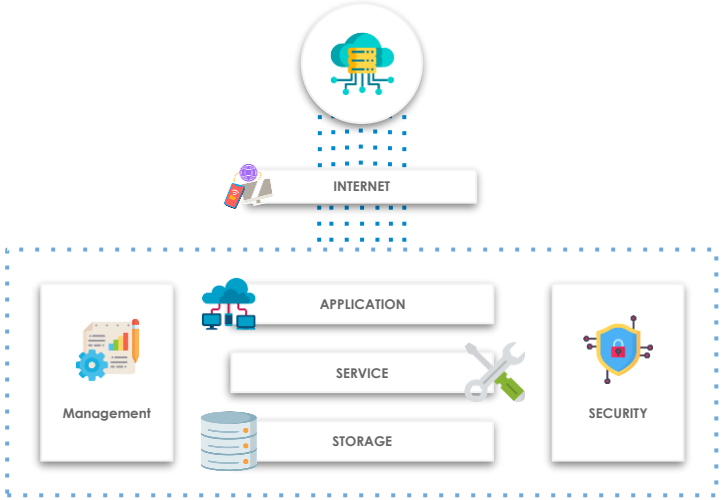
The Third Wave...

On-Prem
Hardware Defined Data Center (HDDC)

Virtualization
Software Defined Data Center (SDDC)

Cloud Computing
Pay as you go

- On Demand - Pay-as-you-go
- CAPEX to OPEX cost transition
- Capacity auto-scaling
- No waiting time
- Go global in minutes
- Business focused
- Highly Available, Reliable & Fault Tolerant



On-prem vs IaaS vs Serverless

On-Prem

(Buy a Car)

IaaS

(Rent a Car)

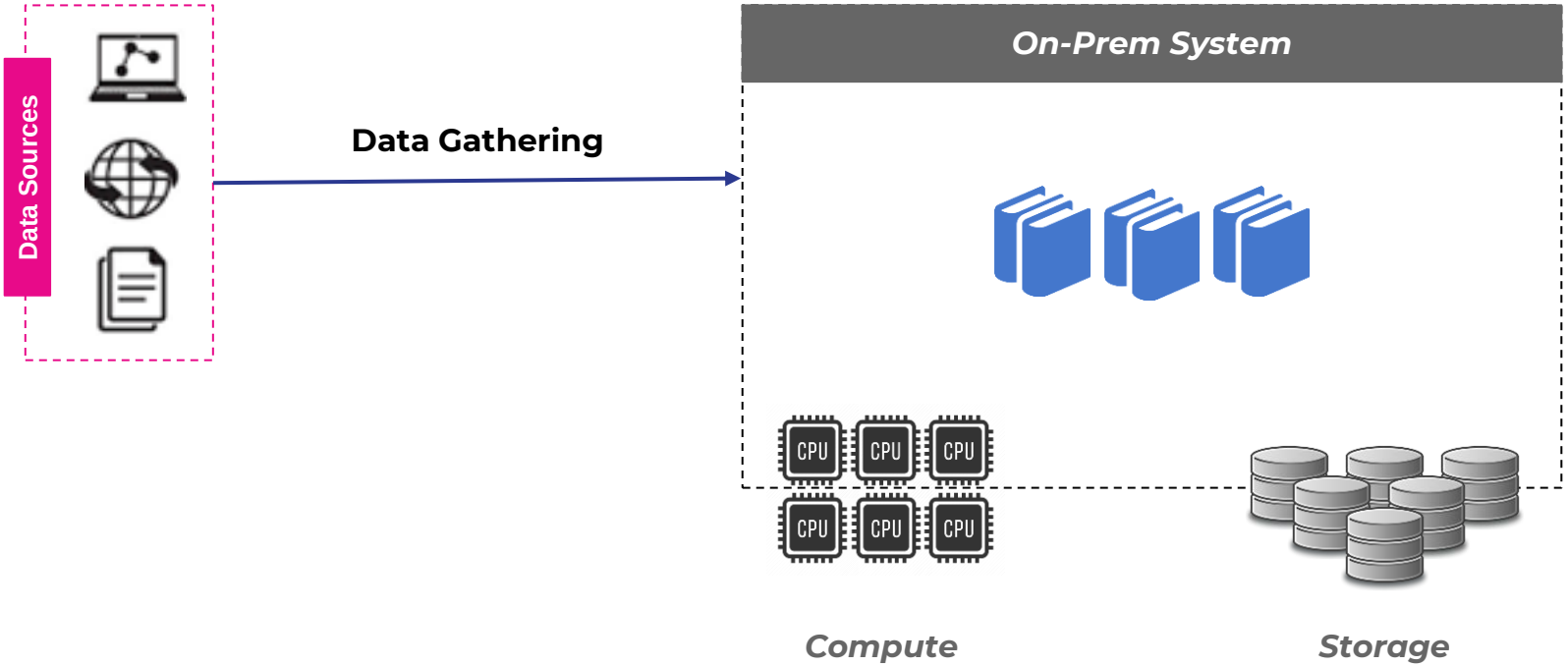
Serverless

(Pay-as-you-go)

On-prem vs IaaS vs Serverless

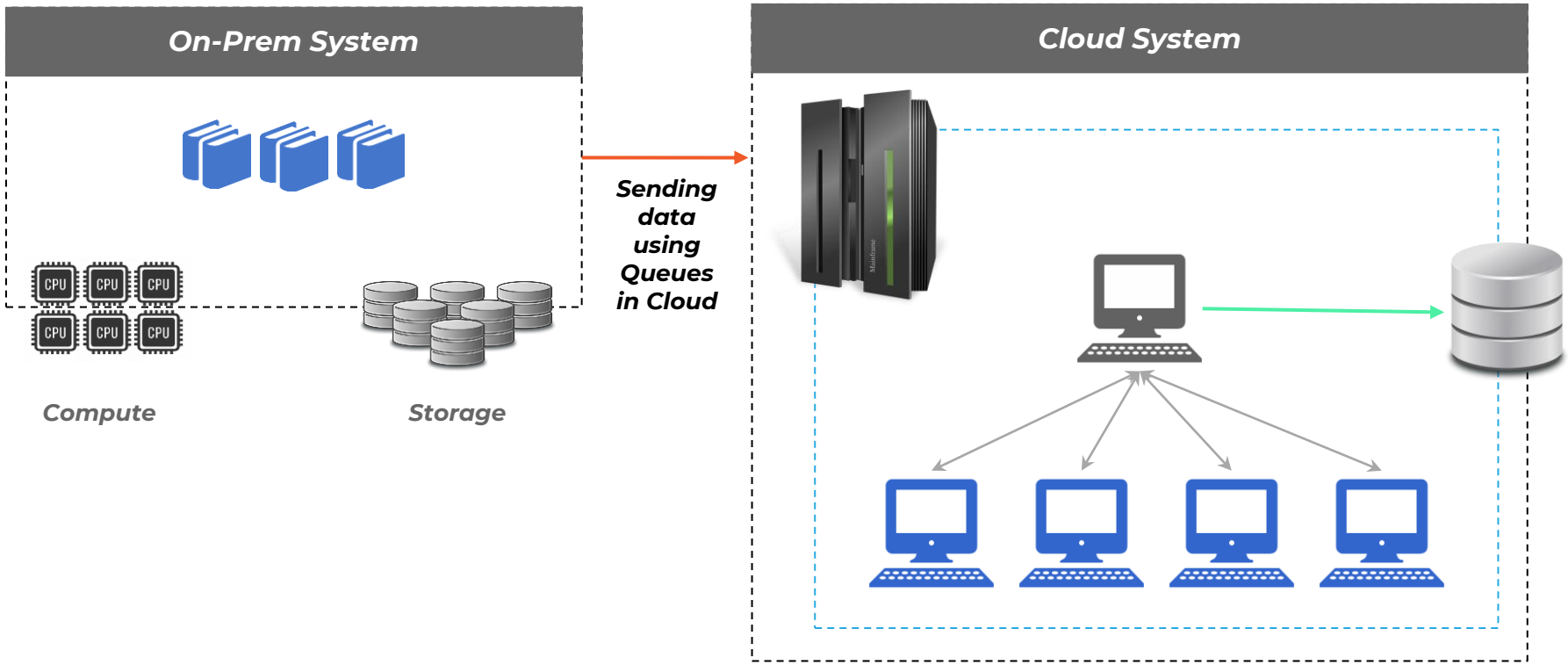
Private Network	Cloud Computing	
On-Prem	**IaaS**	**Serverless**
Servers that are physically located on the company's premises	It is pay-as-you-go service for on demand basic computation, storage, and networking resources	Apps are launched only as needed as an event triggers app code to run
We are fully responsible for all aspects of security	Helps us to reduce maintenance of on-premises data centres	Enables developers to build applications faster by eliminating the need for them to manage infrastructure
Need specialists for maintenance	Each resource is offered as a separate service component and we only pay for resource we use	Serverless is typically used as a synonym for *Function-as-a-Service*
Complete control over data, and based on traffic flow, it may be less expensive	Save money on hardware costs and gain real-time business insights	We only pay for compute resources when we run our code

Processing Data on On-Prem



For better performance, either increase the number of Servers or we can increase the number of CPUs & Storage in servers

Processing Data On Cloud

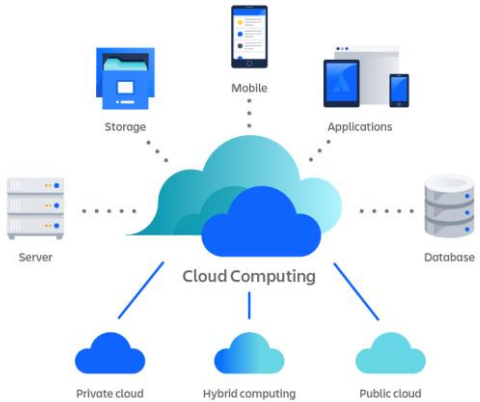


For better performance, we can either increase the number of devices or we can increase the no. of CPUs & Storage

What is Cloud Computing?

What is Cloud Computing?

Cloud computing refers to the on-demand availability of computer system resources, particularly data storage and computational power, without the user having to manage them directly. Functions in large clouds are frequently dispersed across numerous locations, each of which is a data centre.



Source: Atlassian

What is Cloud Computing?

" It is a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies. Public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization. Using public cloud services generates the types of economies of scale and sharing of resources that can reduce costs and increase choices of technologies."

Various types of Cloud Computing

PUBLIC CLOUD

(Provide resources which are over the internet)

PRIVATE CLOUD

(Provide resource which are available to an organization)

HYBRID CLOUD

(Mixes at least one private cloud to one or more public clouds)

Various Cloud Models

SaaS

(Software-as-a-Service)

IaaS

(Infrastructure-as-a-Service)

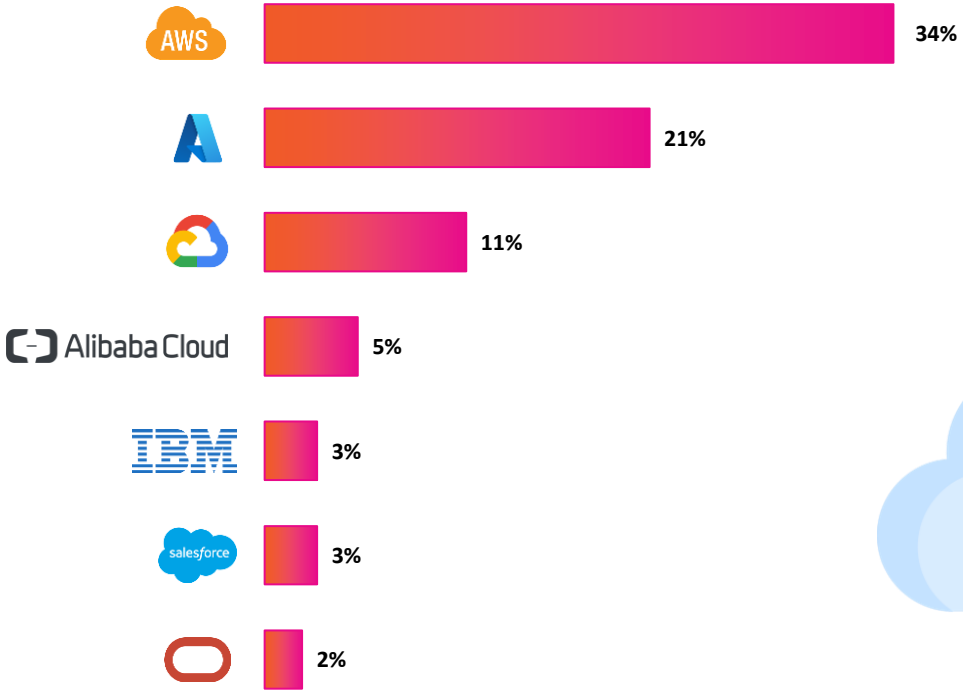
PaaS

(Platform-as-a-Service)

Why do we need Cloud Computing?

Amazon, Microsoft, & Google Dominate Cloud Market

As per statista, worldwide market share of leading cloud infrastructure service providers in Q3 2022



Cloud Infrastructure Service revenues

In the 12 months ended September

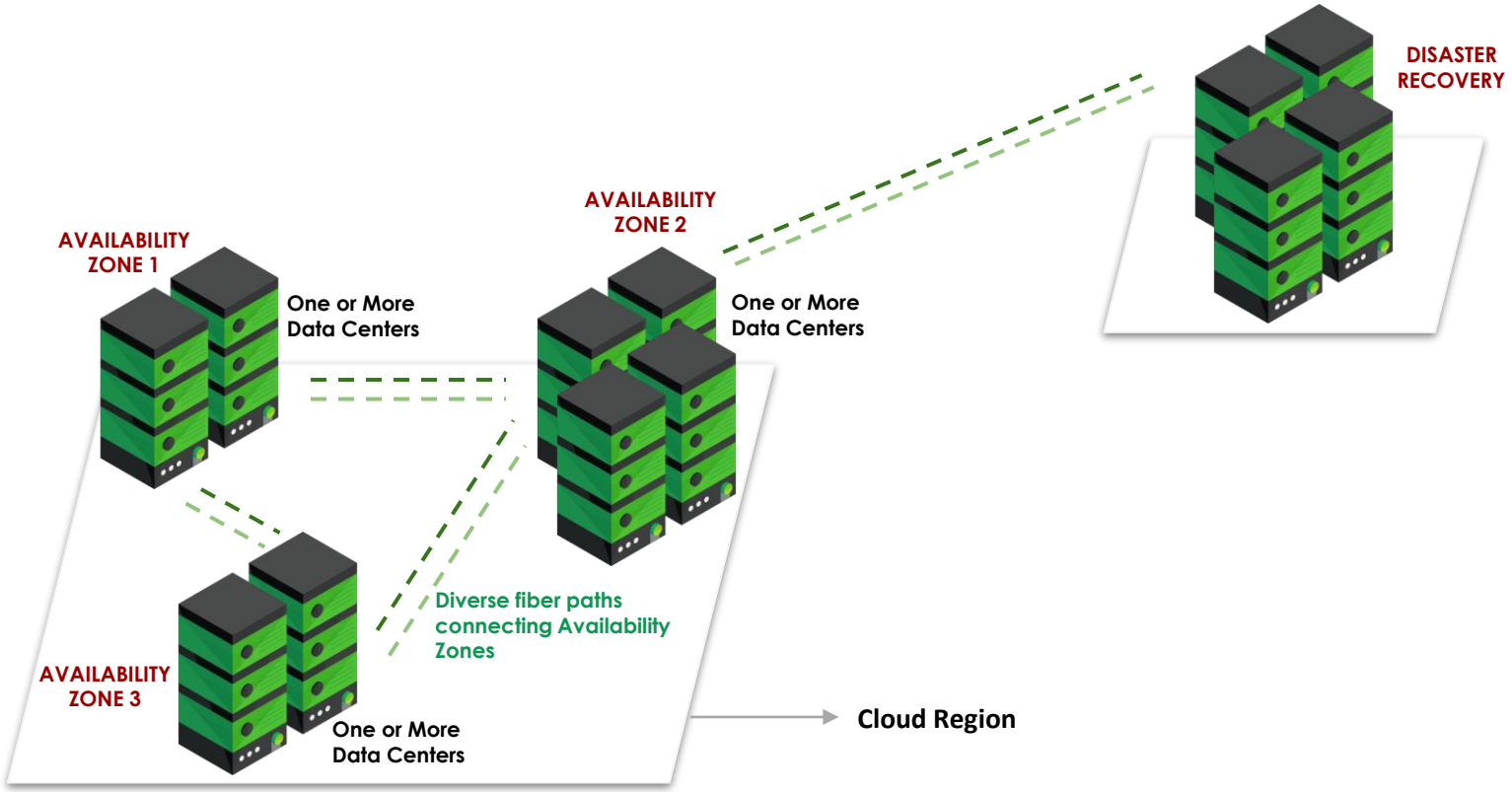
2022 were

$217 BILLION

Why AWS or Azure or GCP?

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services

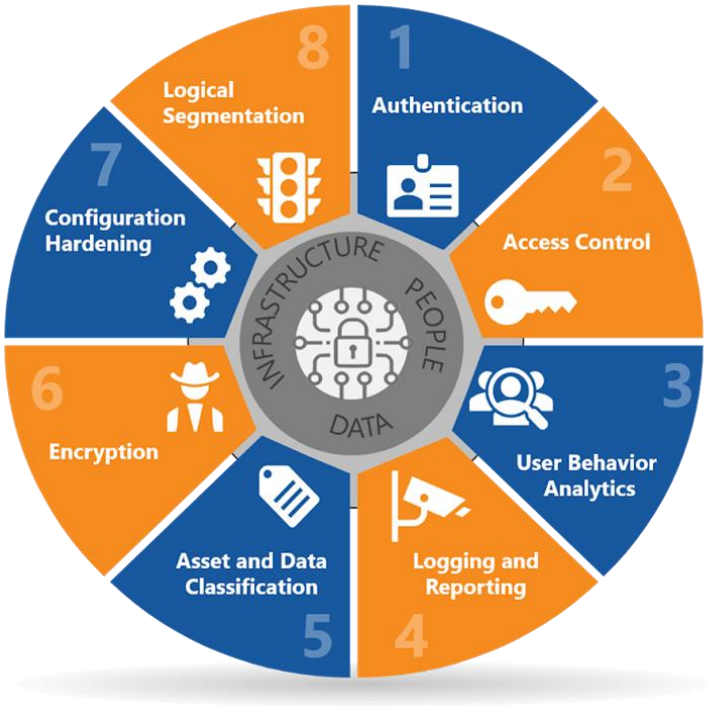
Cloud Physical Architecture



Cloud Security

PLURALSIGHT

Cloud Security



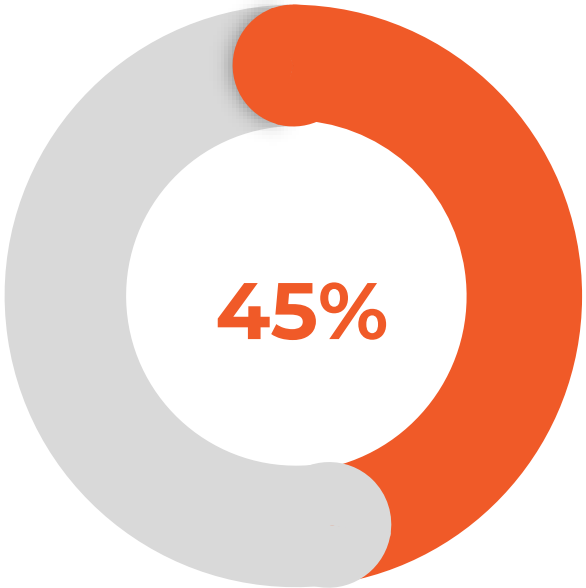
1	▪ Multi Factor Authentication ▪ Zero Trust Model	▪ IAM Policy ▪ Conditional Access
2	▪ Access Control ▪ Awareness Training	▪ IAM Roles and groups ▪ Information classification & protection
3	▪ Protective Technologies ▪ Detection process	▪ Audit Reports ▪ Regular patch management
4	▪ Governance ▪ Risk Management Strategy	▪ Anomalies and Events ▪ Threat Detection
5	▪ Assets Management ▪ Business Environment	▪ Risk Assessment ▪ Continues monitoring and alerts
6	▪ Encrypted Volumes ▪ Key management System	▪ Encryption for VPN ▪ Proxy, NAT Gateways, Load Balancers
7	▪ Threat prevention ▪ Risk and compliance	▪ OS hardening ▪ Regular Security updates
8	▪ Segregated network with unique routing ▪ Environment Segmentations	▪ NOC and SOC Segmentations ▪ Firewall and DMZ

Why we need cloud security?

Cloud computing is being used for more than two decades. Still, several businesses find security as a challenge to handle.

- Almost, everyone is on cloud
- It’s a shared responsibility
- For many its still new, so much to explore
- Multi tenancy make resource prone to attacks
- Cloud providers are not omnipotent
- Data security is a big concern
- and many more …

Exploited Vulnerabilities are preventable



have experienced one or more of these three types of exploits

- *Zero-day exploits that take advantage of OS/app vulnerabilities unknown to the victim*
- *Exploits that take advantage of known vulnerabilities in unpatched applications*
- *Exploits that take advantage of known vulnerabilities in unpatched OS versions*

Most Crucial aspects of Cloud Security

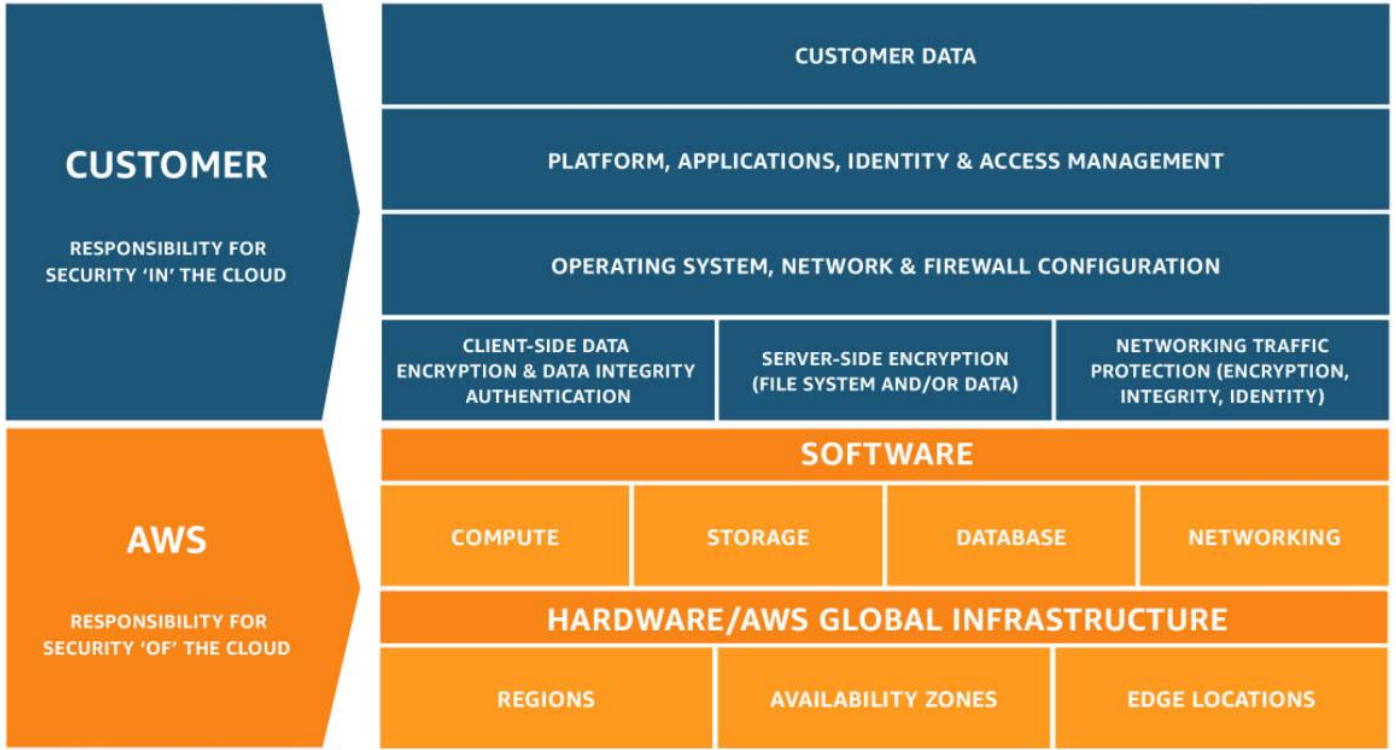
Security in the cloud consists of 4 areas:

- Data Protection
- Infrastructure Protection
- Privilege Management
- Detective Controls

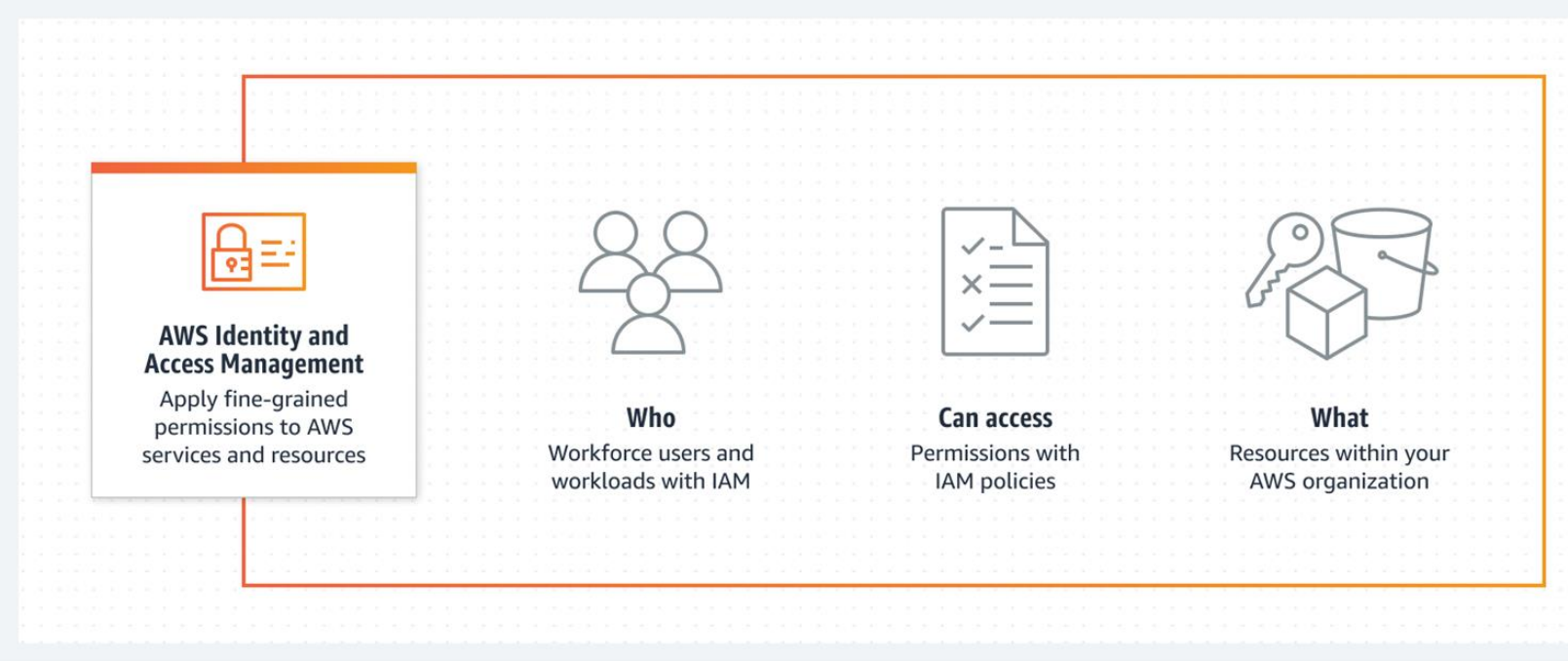
Cloud Security Dissection

- It’s a shared responsibility
- IAM: Principle of Least Privilege
- Network Security
- Application Security
- Data Security
- Logging and Monitoring
- Cloud Security Automation

Shared Responsibility

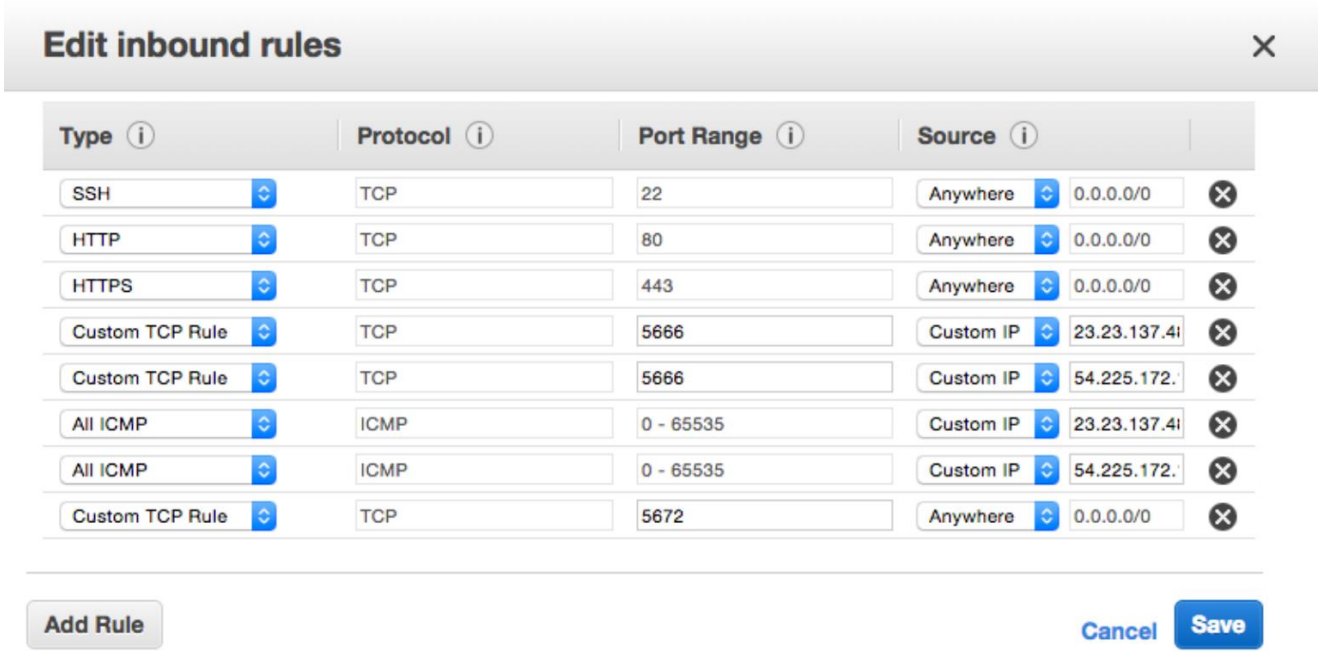


AWS Identity and Access Management



AWS security group

A ***security group*** acts as a virtual firewall that controls the traffic for one or more instances.



AWS security group

Inbound						
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows inbound SSH traffic from your home network's public IPv4 address range (over the Internet gateway).
130	RDP	TCP	3389	192.0.2.0/24	ALLOW	Allows inbound RDP traffic to the web servers from your home network's public IPv4 address range (over the Internet gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows inbound return IPv4 traffic from the Internet (that is, for requests that originate in the subnet). This range is an example only. For more information about how to select the appropriate ephemeral port range, see Ephemeral Ports.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Data Protection

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption

You request Amazon S3 to encrypt your object before saving it on disks at its data centers and decrypt it for you as you download these objects

You can encrypt data at client-side and upload the encrypted data to Amazon S3 - encryption/decryption are handled by client

Logging

- Whom to give log access
- What to log
- Where to store
- Log duration
- Secured cloud logging service - Sumo Logic, Alert Logic
- Cloudtrail, Cloudwatch, VPC flow logs in AWS

Cloud Cost Management

Cloud Cost Management

- Cloud Cost Management is the process of optimizing and controlling cloud expenses.
- It ensures efficient utilization of cloud resources while minimizing unnecessary spending.

Key Objectives

Identify cost-saving opportunities without compromising performance

Set and monitor budgets to prevent unexpected expenses

Gain clear insights into cloud usage and expenditure

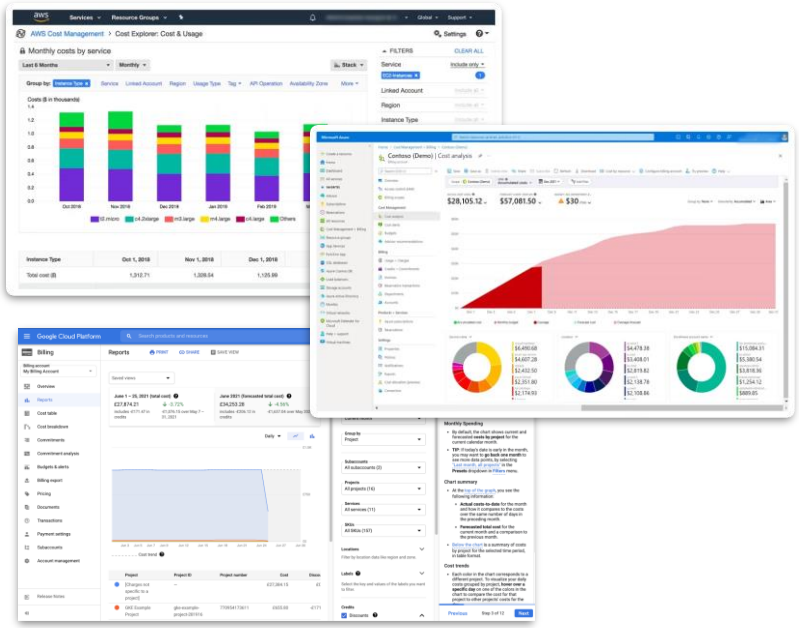
Implement policies to manage resource allocation effectively

Cost Optimization Strategies

Right-Sizing	Reserved Instances	Spot Instances
Match cloud resources to actual workload requirements	Leverage discounted pricing by committing to long-term usage	Utilize spare capacity at significantly reduced costs
Identify and eliminate over-provisioned instances	Ideal for stable and predictable workloads	Suitable for fault-tolerant, non-critical workloads

Cloud Cost Monitoring Tools

- AWS Cost Explorer
- Azure Cost Management + Billing
- Google Cloud Billing
- Third-Party Solutions



Case Study: Foursquare

FOURSQUARE

Foursquare Checks-In to 53% Cost Savings with AWS

Foursquare is a technology company that informs business decisions through a deep understanding of location intelligence. The company's mobile apps, Foursquare and Swarm, are used monthly by more than 50 million people who have left more than 87 million tips and checked in more than 10 billion times.

"Using AWS helps us scale up as our data grows, and as the complexity of our queries increases. And we can spin up nodes dynamically whenever we need them, whether we're launching a new feature or increasing capacity."

Jon Hoffman

Software Engineer, Fourquare

Questions