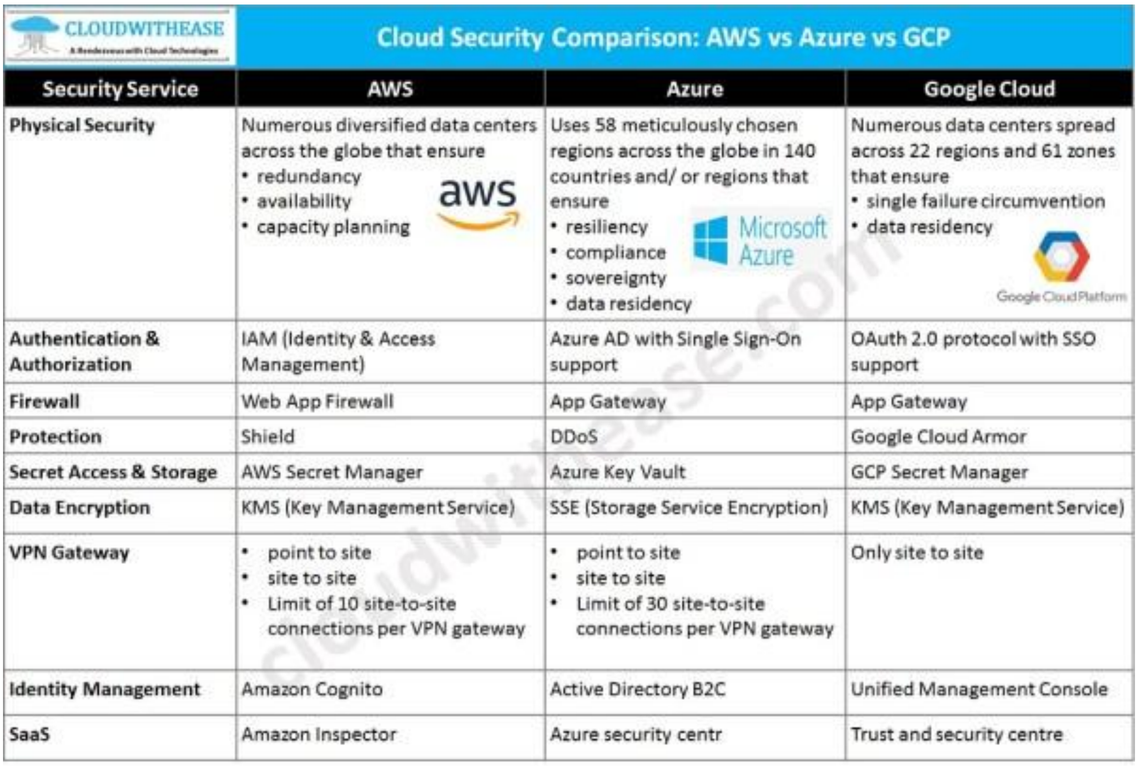
Day 4

“CLOUD SECURITY”

Evaluating Cloud Service Providers for Security:

The security maturity of the CSP should be evaluated based on:

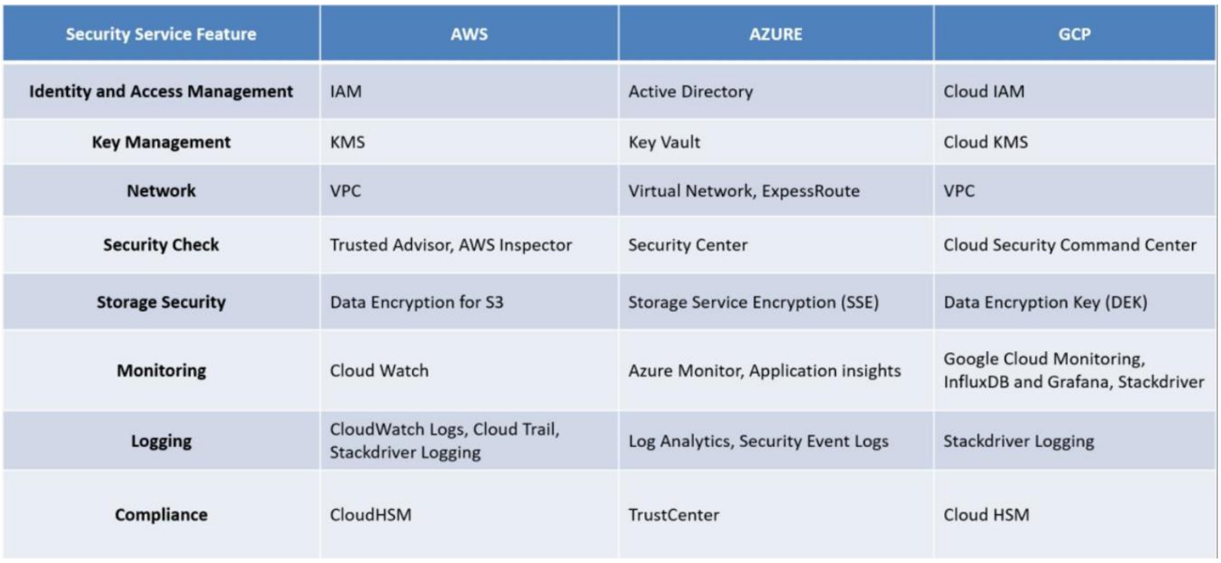
- Disclosure of security policies, compliance, and practices
- Disclosure when mandated
- Security architecture
- Security automation
- Governance and security responsibility



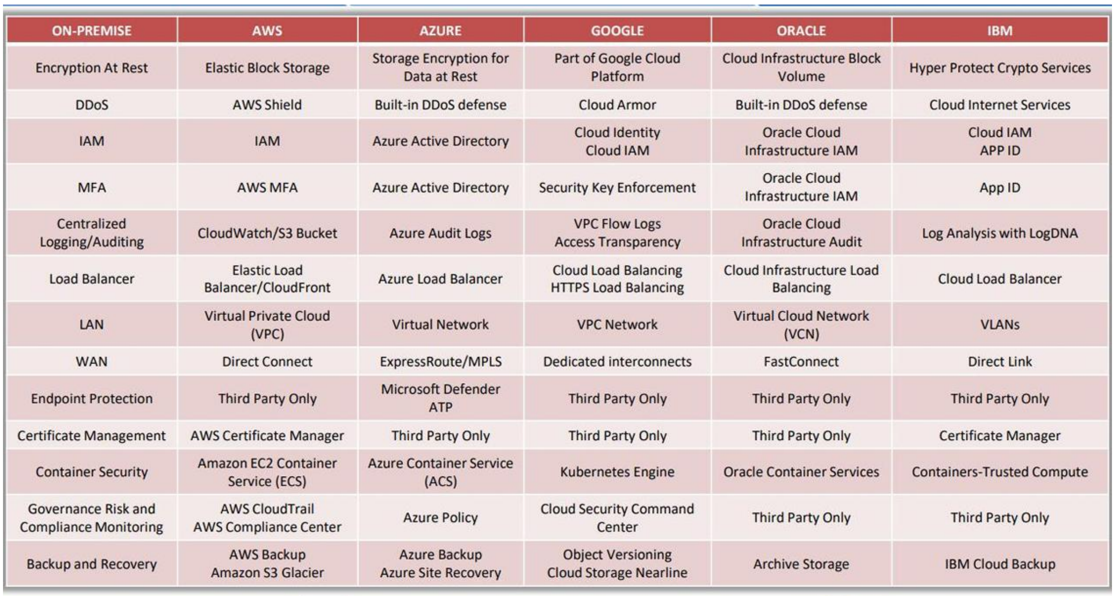
CLOUDWITHEASE A Rendezvous with Cloud Technologies

Cloud Security Comparison: AWS vs Azure vs GCP

Security Service	AWS	Azure	Google Cloud
Physical Security	Numerous diversified data centers across the globe that ensure • redundancy • availability • capacity planning	Uses 58 meticulously chosen regions across the globe in 140 countries and/ or regions that ensure • resiliency • compliance • sovereignty • data residency	Numerous data centers spread across 22 regions and 61 zones that ensure • single failure circumvention • data residency
Authentication & Authorization	IAM (Identity & Access Management)	Azure AD with Single Sign-On support	OAuth 2.0 protocol with SSO support
Firewall	Web App Firewall	App Gateway	App Gateway
Protection	Shield	DDoS	Google Cloud Armor
Secret Access & Storage	AWS Secret Manager	Azure Key Vault	GCP Secret Manager
Data Encryption	KMS (Key Management Service)	SSE (Storage Service Encryption)	KMS (Key Management Service)
VPN Gateway	• point to site • site to site • Limit of 10 site-to-site connections per VPN gateway	• point to site • site to site • Limit of 30 site-to-site connections per VPN gateway	Only site to site
Identity Management	Amazon Cognito	Active Directory B2C	Unified Management Console
SaaS	Amazon Inspector	Azure security centr	Trust and security centre



Security Service Feature	AWS	AZURE	GCP
Identity and Access Management	IAM	Active Directory	Cloud IAM
Key Management	KMS	Key Vault	Cloud KMS
Network	VPC	Virtual Network, ExpressRoute	VPC
Security Check	Trusted Advisor, AWS Inspector	Security Center	Cloud Security Command Center
Storage Security	Data Encryption for S3	Storage Service Encryption (SSE)	Data Encryption Key (DEK)
Monitoring	Cloud Watch	Azure Monitor, Application insights	Google Cloud Monitoring, InfluxDB and Grafana, Stackdriver
Logging	CloudWatch Logs, Cloud Trail, Stackdriver Logging	Log Analytics, Security Event Logs	Stackdriver Logging
Compliance	CloudHSM	TrustCenter	Cloud HSM



ON-PREMISE	AWS	AZURE	GOOGLE	ORACLE	IBM
Encryption At Rest	Elastic Block Storage	Storage Encryption for Data at Rest	Part of Google Cloud Platform	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services
DDoS	AWS Shield	Built-in DDoS defense	Cloud Armor	Built-in DDoS defense	Cloud Internet Services
IAM	IAM	Azure Active Directory	Cloud Identity Cloud IAM	Oracle Cloud Infrastructure IAM	Cloud IAM APP ID
MFA	AWS MFA	Azure Active Directory	Security Key Enforcement	Oracle Cloud Infrastructure IAM	App ID
Centralized Logging/Auditing	CloudWatch/S3 Bucket	Azure Audit Logs	VPC Flow Logs Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA
Load Balancer	Elastic Load Balancer/CloudFront	Azure Load Balancer	Cloud Load Balancing HTTPS Load Balancing	Cloud Infrastructure Load Balancing	Cloud Load Balancer
LAN	Virtual Private Cloud (VPC)	Virtual Network	VPC Network	Virtual Cloud Network (VCN)	VLANs
WAN	Direct Connect	ExpressRoute/MPLS	Dedicated interconnects	FastConnect	Direct Link
Endpoint Protection	Third Party Only	Microsoft Defender ATP	Third Party Only	Third Party Only	Third Party Only
Certificate Management	AWS Certificate Manager	Third Party Only	Third Party Only	Third Party Only	Certificate Manager
Container Security	Amazon EC2 Container Service (ECS)	Azure Container Service (ACS)	Kubernetes Engine	Oracle Container Services	Containers-Trusted Compute
Governance Risk and Compliance Monitoring	AWS CloudTrail AWS Compliance Center	Azure Policy	Cloud Security Command Center	Third Party Only	Third Party Only
Backup and Recovery	AWS Backup Amazon S3 Glacier	Azure Backup Azure Site Recovery	Object Versioning Cloud Storage Nearline	Archive Storage	IBM Cloud Backup

AWS Shared Responsibility Model:

- AWS Responsibilities (Security *of* the Cloud)

AWS is responsible for securing the infrastructure that runs all cloud services:

- Global Infrastructure: Data centers, physical servers, and network hardware.
- AWS Software: Tools for encryption, monitoring, and resource protection (e.g., AWS Shield, KMS).

- Customer Responsibilities (Security *in* the Cloud)

Customers must secure everything they run or store in AWS, including:

- Customer Data: Protection of data in transit and at rest.
- Platform & Applications: Securing OS, middleware, runtime, and IAM configurations.
- Encryption: Managing encryption keys and file system protection.
- Network Traffic: Ensuring secure transmission and firewall setup.
- Service Communication: Routing/zoning of internal application data.

- Shared Responsibilities:

Task	**AWS Responsibility**	**Customer Responsibility**
Patch Management	Underlying infrastructure	Guest OS & apps
Config Management	Physical hosts, networking devices	OS, databases, and application configs
IT Controls	Data center, facilities, infrastructure setup	Control implementation within the services
Training	AWS employee training	Customer staff training

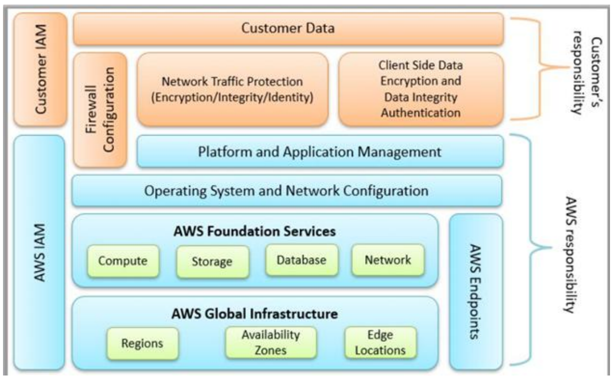
AWS Three Shared Responsibility Model:

Those three are:

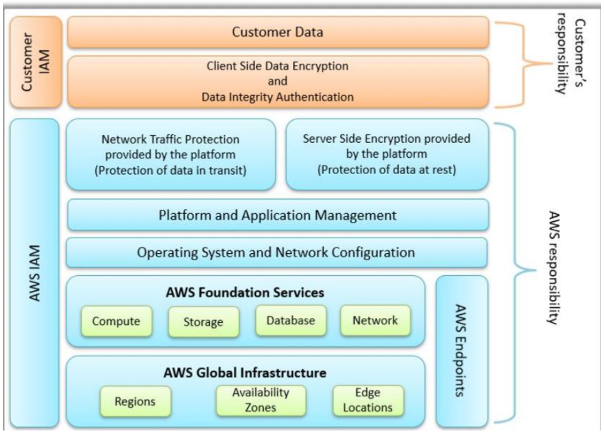
- Shared Responsibility Model for Infrastructure Services
- Shared Responsibility Model for Container Services
- Shared Responsibility Model for Abstract Services

Infrastructure Services security: Service provider involves securing the hardware, software, networking and other facilities that are responsible to run the cloud services. While customer should be responsible for client-side data encryption, server-side data encryption, network traffic protection, security of OS and managing IAM.

Container services security:


Customer IAM
Customer Data
Firewall Configuration
Network Traffic Protection (Encryption/Integrity/Identity)
Client Side Data Encryption and Data Integrity Authentication
Customer's responsibility
Platform and Application Management
Operating System and Network Configuration
AWS IAM
AWS Foundation Services
Compute
Storage
Database
Network
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS Endpoints
AWS responsibility

Abstract services:


Customer IAM
Customer Data
Client Side Data Encryption and Data Integrity Authentication
Customer's responsibility
Network Traffic Protection provided by the platform (Protection of data in transit)
Server Side Encryption provided by the platform (Protection of data at rest)
Platform and Application Management
Operating System and Network Configuration
AWS IAM
AWS Foundation Services
Compute
Storage
Database
Network
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS Endpoints
AWS responsibility

--The End--