**Day 4**



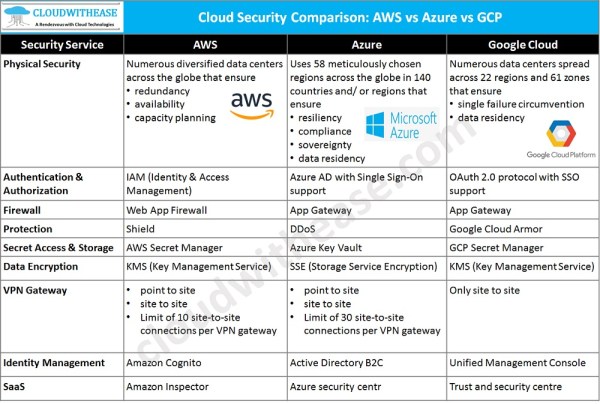


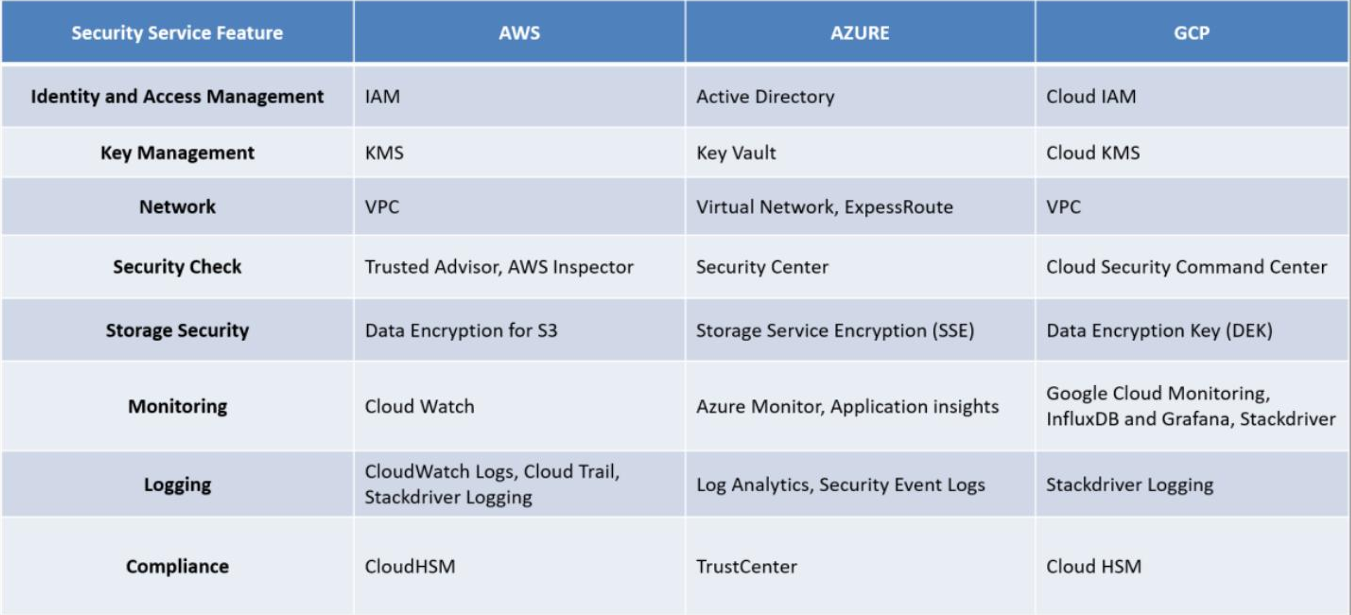
**“CLOUD SECURITY”**

**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







**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 |

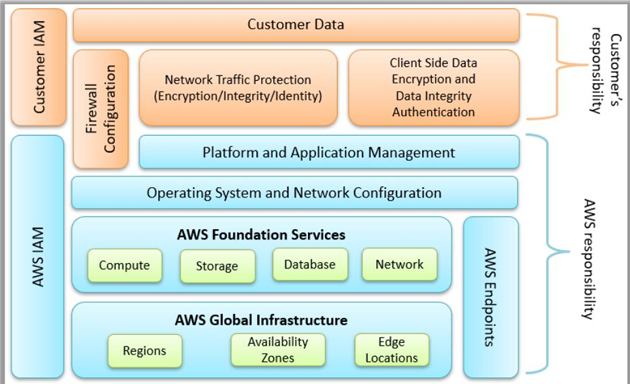
**AWS Three Shared Responsibility Model:**

Those three are:

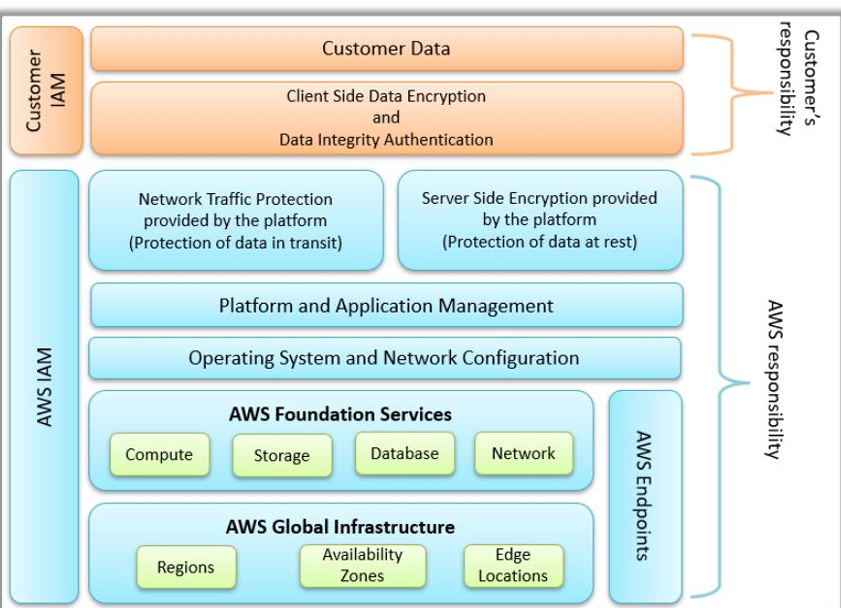
* Shared Responsibility Model for Infrastructure Services
* Shared Responsibility Model for Container Services
* Shared Responsibility Model for Abstract Services

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:



Abstract services:



--The End--