

Name:- Aditya Ravindra Ghayal

Roll No:- 24

Topic :- Types of Security in AWS and Google Cloud Platform (GCP).

Subject:- Cloud Computing

Case Study: Types of Security in AWS and Google Cloud Platform (GCP)

1. Introduction

As organizations increasingly migrate to the cloud, **security** has become one of the most critical aspects of cloud computing. Two leading cloud service providers—**Amazon Web Services (AWS)** and **Google Cloud Platform (GCP)**—offer robust and comprehensive security architectures to protect data, applications, and infrastructure from cyber threats.

This case study explores how AWS and GCP implement different types of security measures, focusing on **data protection, network security, identity management, compliance, and operational security**.

2. Background

Both AWS and GCP operate on a **shared responsibility model**:

- **Cloud provider responsibility:** Security *of* the cloud (physical data centers, hardware, global infrastructure).
- **Customer responsibility:** Security *in* the cloud (user data, applications, and configurations).

This model ensures flexibility and accountability while maintaining high levels of protection for cloud-based assets.

3. Security Framework in AWS

a. Identity and Access Management (IAM)

- **AWS IAM** allows administrators to control who can access which resources.
- Features include **role-based access control (RBAC)**, **multi-factor authentication (MFA)**, and **temporary credentials**.
- Supports integration with external identity providers via **AWS Cognito** and **SAML 2.0**.

b. Network Security

- **Amazon Virtual Private Cloud (VPC)** enables customers to isolate network environments.
- **Security Groups** act as virtual firewalls controlling inbound and outbound traffic.
- **AWS Shield** and **AWS WAF (Web Application Firewall)** protect against DDoS and web attacks.

- **AWS GuardDuty** provides intelligent threat detection using machine learning.

c. Data Protection

- Data encryption is supported both **in transit (TLS/SSL)** and **at rest (AES-256)**.
- **AWS Key Management Service (KMS)** and **CloudHSM** manage encryption keys securely.
- **S3 Object Lock** prevents accidental or malicious deletion of data.

d. Monitoring and Compliance

- **AWS CloudTrail** logs all API activity for auditing and compliance.
- **AWS Config** tracks resource configurations and compliance status.
- AWS meets multiple international standards such as **ISO 27001**, **SOC 2**, **GDPR**, and **HIPAA**.

e. Application and Operational Security

- AWS provides **Amazon Inspector** for vulnerability management.
- **CodeGuru** helps developers identify security flaws during development.
- Continuous monitoring through **CloudWatch** ensures operational integrity.

4. Security Framework in Google Cloud Platform (GCP)

a. Identity and Access Management (IAM)

- GCP IAM defines **roles and permissions** at project and resource levels.
- Integrates with **Google Workspace** and **Cloud Identity** for centralized access control.
- Supports **OAuth 2.0**, **MFA**, and **federated identity management**.

b. Network Security

- **Virtual Private Cloud (VPC)** offers network segmentation and isolation.
- **Firewall rules** and **private service access** protect workloads from unauthorized access.
- **Google Cloud Armor** and **Cloud CDN** defend against DDoS attacks.
- **Traffic Director** manages secure service mesh and load balancing.

c. Data Protection

- Data is **automatically encrypted** at rest and in transit using **AES-256** encryption.
- **Cloud Key Management Service (KMS)** and **External Key Manager (EKM)** allow customers to manage or bring their own encryption keys (BYOK).

- **Confidential Computing** ensures data encryption even during processing, using **secure enclaves**.

d. Monitoring and Compliance

- **Cloud Audit Logs** provide transparency into administrative and user activity.
- **Security Command Center** offers a unified dashboard for risk management, threat detection, and compliance tracking.
- GCP maintains compliance with **ISO 27017**, **PCI DSS**, **FedRAMP**, and **GDPR**.

e. Application and Operational Security

- GCP employs **Binary Authorization** for verifying container integrity before deployment.
- **Container Analysis** scans images for known vulnerabilities.
- **Chronicle Security Operations** offers advanced threat detection using Google's AI.

5. Comparative Analysis: AWS vs GCP Security

Security Area	AWS Features	GCP Features	Remarks
Identity & Access Management	IAM, MFA, Cognito, STS	IAM, Cloud Identity, OAuth 2.0	Both offer granular role-based access control
Network Security	VPC, Shield, WAF, GuardDuty	VPC, Cloud Armor, Traffic Director	GCP focuses more on AI-driven traffic analysis
Data Protection	KMS, CloudHSM, S3 encryption	KMS, EKM, Confidential Computing	GCP adds encryption during processing
Monitoring & Compliance	CloudTrail, Config, Inspector	Security Command Center, Audit Logs	AWS has mature compliance tools; GCP integrates with AI
Operational Security	CloudWatch, CodeGuru, Inspector	Binary Authorization, Container Analysis	GCP leads in container and Kubernetes security

6. Case Study Example: Multi-Cloud Security Adoption

A multinational financial company migrated workloads to both AWS and GCP for redundancy and performance.

- **On AWS:** It used **GuardDuty** and **AWS WAF** to detect anomalies in customer transactions.
- **On GCP:** It implemented **Security Command Center** and **Confidential VM** for sensitive data analytics.

This **hybrid multi-cloud strategy** allowed the company to benefit from AWS's deep compliance ecosystem and GCP's advanced data encryption, achieving a robust and compliant multi-cloud security posture.

7. Benefits of Cloud Security

- **Scalability:** Security controls scale with workload demands.
- **Automation:** Continuous monitoring and response through AI and ML.
- **Compliance:** Built-in adherence to global security standards.
- **Visibility:** Centralized dashboards improve security governance.

8. Challenges

- **Configuration errors** remain a major risk for users.
- **Cost management** of security tools across multiple clouds.
- **Vendor lock-in** due to proprietary security services.
- **Complex identity management** in hybrid or multi-cloud environments.

9. Conclusion

AWS and GCP both provide end-to-end cloud security solutions covering identity, network, data, and application layers.

While AWS is known for its mature and extensive security ecosystem, GCP is recognized for AI-driven security analytics and confidential computing innovations.

Together, these platforms demonstrate how cloud security has evolved from basic protection to a strategic enabler of trust, compliance, and innovation in the digital era.