ONE PAGE SUMMARY

IT & Software › Google Cloud Platform › GCP Security

Introduction to GCP Security

Master the essentials of Google Cloud Platform Security.

DEFINITION

GCP Security encompasses the tools and practices to protect data and applications in Google Cloud. It ensures confidentiality, integrity, and availability of resources in the cloud environment.

KEY CONCEPTS

Identity and Access Management

IAM controls who can access resources in GCP and what actions they can perform.

Data Encryption

Data is encrypted both at rest and in transit to protect sensitive information from unauthorized access.

Network Security

GCP provides firewalls and Virtual Private Cloud (VPC) to secure network traffic and isolate resources.

Compliance and Governance

GCP adheres to various compliance standards, ensuring that services meet legal and regulatory requirements.

Security Monitoring

Tools like Cloud Security Command Center help monitor and respond to security threats in real-time.

EXAMPLES

→ Setting IAM roles for team members based on their job functions.

→ Using encryption keys to secure sensitive customer data.

→ Implementing firewall rules to restrict access to specific IP addresses.

MEMORY TIPS

★ Think 'I AM' for Identity and Access Management.

★ Remember 'Encrypt Everything' to emphasize data protection.

★ Visualize a fortress for Network Security to recall protective measures.

COMMON MISTAKES

✗ Neglecting to regularly review IAM permissions.

✗ Assuming data is secure without encryption.

✗ Overlooking compliance requirements during deployment.

QUICK RECAP

GCP Security is vital for protecting cloud resources through IAM, encryption, and network security. Always monitor compliance and security measures to safeguard your applications and data.