ONE PAGE SUMMARY

IT & Software › Google Cloud Platform › GCP Security

Introduction to GCP Security

Master the essentials of GCP Security for cloud protection.

DEFINITION

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

KEY CONCEPTS

Identity and Access Management (IAM)

IAM controls who can access resources in GCP and what actions they can perform. It uses roles and permissions to manage user access.

Data Encryption

Data encryption protects sensitive information by converting it into a secure format. GCP provides encryption at rest and in transit to safeguard data.

Network Security

Network security involves protecting the network infrastructure from unauthorized access and attacks. GCP offers firewalls and Virtual Private Cloud (VPC) for secure networking.

Security Monitoring

Security monitoring involves continuously observing GCP resources for suspicious activities. Tools like Cloud Security Command Center help identify vulnerabilities and threats.

Compliance and Governance

Compliance ensures that GCP users adhere to legal and regulatory standards. GCP provides tools to help manage compliance and maintain governance.

EXAMPLES

→ Using IAM to grant specific access to developers.

→ Encrypting sensitive customer data before storage.

→ Setting up VPC to isolate resources from public access.

MEMORY TIPS

★ Think 'I AM Secure' to remember IAM.

★ Use 'Encrypt Everything' for data protection.

★ Remember 'Network is a Fortress' for network security.

COMMON MISTAKES

✗ Neglecting to regularly review IAM permissions.

✗ Forgetting to enable encryption for sensitive data.

✗ Overlooking security monitoring tools.

QUICK RECAP

GCP Security encompasses IAM, data encryption, network security, monitoring, and compliance. Understanding these concepts is crucial for protecting cloud resources effectively.