Google Cloud Security: KMS, Cloud Armor, and Security Command Center

This presentation explores Google Cloud's robust security offerings. We'll cover Key Management Service (KMS), Cloud Armor, and Security Command Center. Discover how to protect your cloud environment effectively.

T by The XYZ Company

Understanding Google Cloud Security Landscape

Shared Responsibility

Google secures the cloud infrastructure. You secure what you put in the cloud.

Multi-Layered Approach

Defense in depth: identity, network, data, and application security layers.

Compliance

Google Cloud meets many industry compliance standards and certifications.

Key Management Service (KMS): Securing Your Keys

1. ### Centralized Key Management

   Store, manage, and use cryptographic keys in one location.

2. ### Hardware Security Modules (HSMs)

   Option to use HSMs for added key protection and compliance.

3. ### Role-Based Access Control (RBAC)

   Control who can access and manage your cryptographic keys.

Cloud Armor: Web Application Firewall (WAF) & DDoS Protection

WAF

Protects web applications from common web exploits.

DDoS Protection

Mitigates distributed denial-of-service (DDoS) attacks.

Custom Rules

Create custom rules to address unique application threats.

Security Command Center: Centralized Security Management

1

Visibility

Gain insights into your security posture across Google Cloud.

2

Threat Detection

Detect threats and misconfigurations in real time.

3

Remediation

Get recommendations to remediate security issues quickly.

Use Case: Protecting a Web Application with KMS and Cloud Armor

1. **Encrypt Data**

   Use KMS to encrypt sensitive data stored in Cloud Storage.

2. **Deploy Cloud Armor**

   Deploy Cloud Armor in front of the web application.

3. **WAF Rules**

   Configure WAF rules to block common web attacks.

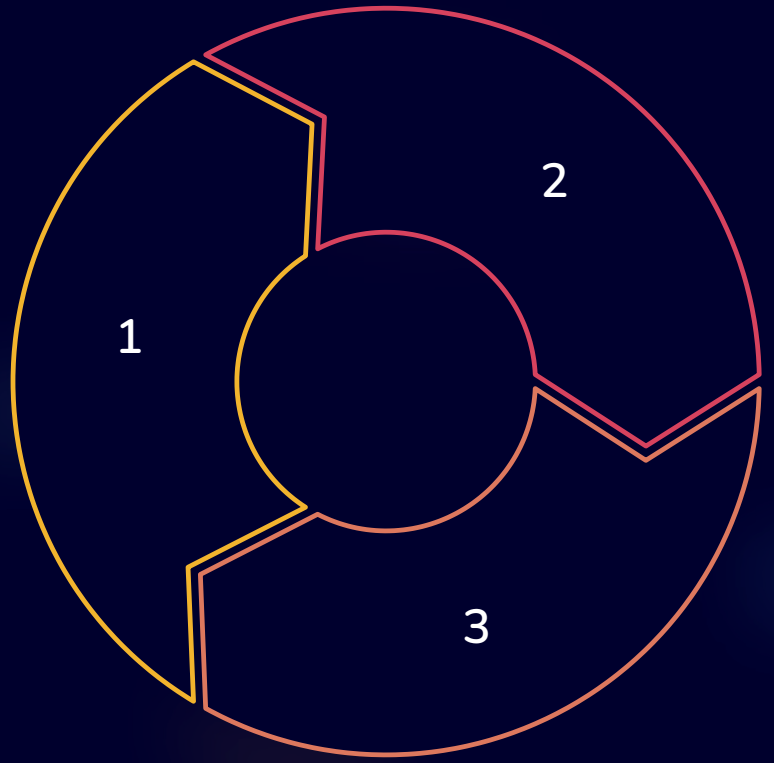
4. **Monitor & Alert**

   Monitor Cloud Armor logs and set up security alerts.

Integrating KMS, Cloud Armor, and Security Command Center for Enhanced Security

KMS

Encrypt sensitive data at rest and in transit.



Cloud Armor

Protect web applications from external threats.

Security Command Center

Monitor and manage overall security posture.

Best Practices and Next Steps for Google Cloud Security

Principle of Least Privilege

Grant users only the permissions they need.

Regular Security Audits

Conduct regular security audits to identify vulnerabilities.

Stay Updated

Keep your security tools and configurations up to date.