Cognizant

Google Cloud Platform

GCP Security Services

May 18, 2020

Agenda - Master Class

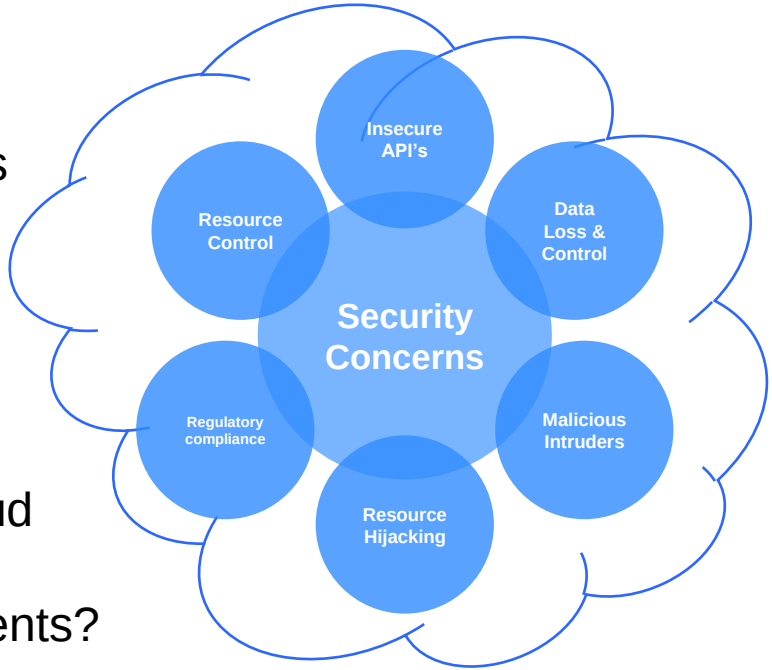
S.No.	Topic (Master Class)	Date	Day
1	Introduction to Google Cloud Platform	4-May	Mon
2	Introduction to Google Compute Services - GCE | GAE | GKE	6-May	Wed
3	Introduction to Google Storage - GCS | Bigtable | Big Query | Datastore	8-May	Fri
4	Introduction to Google Networking	11-May	Mon
5	Introduction to GCP Monitoring Services	13-May	Wed
6	**DEMO-I (2 Hours)**	15-May	Fri
7	**Introduction to GCP Security Services**	**18-May**	**Mon**
8	Introduction to Google Data & Serverless Services	20-May	Wed
9	Introduction to GCP DevOps Services	22-May	Fri
10	Introduction to Google API Services	26-May	Tue
11	Introduction to Google Anthos	27-May	Wed
12	**DEMO-II (2 Hours)**	29-May	Fri

Agenda

1. Security Threats/Concerns
2. Google Security Architecture
3. Google Security Services
4. Identity and Access Management
5. Key Management Service
6. Data Loss Prevention API
7. Cloud Security Scanner
8. Cloud Armor
9. Security Command Center
10. Responsibility, Best practices, Whitepaper, etc.
11. References

Some security concerns

- Organizations feel as if they have lost control
- Data Theft from Cloud applications by malicious intruders
- Provisioned Cloud applications are outside the control of IT team?
- Inability to monitor data in-transit to & from Cloud
- Who owns the regulatory/compliance requirements?



Cognizant

Google Security Architecture

Rely on a secure-by-design infrastructure with hardening, configuration management, and patch and vulnerability management.

Operational Security

- Intrusion Detection
- Reducing Insider Risk
- Safe Employee Devices & Credentials
- Safe Software Development

Internet Communication

- Google Front End
- DoS Protection

Storage Services

- Encryption at rest
- Deletion of Data

User Identity

- Authentication
- Login Abuse Protection

Service Deployment

- Access Management of End User Data
- Encryption of Inter-Service Communication
- Inter-Service Access Management
- Service Identity, Integrity, Isolation

Hardware Infrastructure

- Secure Boot Stack and Machine Identity
- Hardware Design and Provenance
- Security of Physical Premises

Two-Factor Authentication

Encryption By default

Reward Programs

Physical Security

Elliptic-Curve Cryptography

Data-Loss Prevention

600+ Security Professionals

https://cloud.google.com/security/infrastructure/design/

Cognizant

Google Security Services

Identity and Access Management

Smart Access Control

- Policies
- Roles

Key Management Service

Data Encryption

- Generate/ Rotate/Destroy
- CMEK
- CSEK

Data Loss Prevention API

Sensitive Data Masking

- Identification
- Classification
- Action

Cloud Security Scanner

Security Scanner for GAE

- XSS (cross-site scripting)
- Flash Injection
- Outdated Library

Cloud Armor

Protection Against DDoS attack

- Works with GLB*
- Whitelisting
- Flexible Rules
- Security Partners

Security Command Center

Monitoring Command Center

- Detect
- Prevent
- Respond

CMEK-customer-managed encryption keys
CSEK-customer-supplied encryption keys

*Global Load Balancer

Cognizant

Cloud Identity and Access Management (IAM)

Cognizant

Overview of IAM

- IAM provides fine-grained controls for managing access to resources
- Admins define...
  - Who (accounts/groups/domains)
  - Can do what (role)
  - To which resources (e.g. instances)

Owner

Invite members
Remove members
Can delete project
Includes Editor rights

Editor

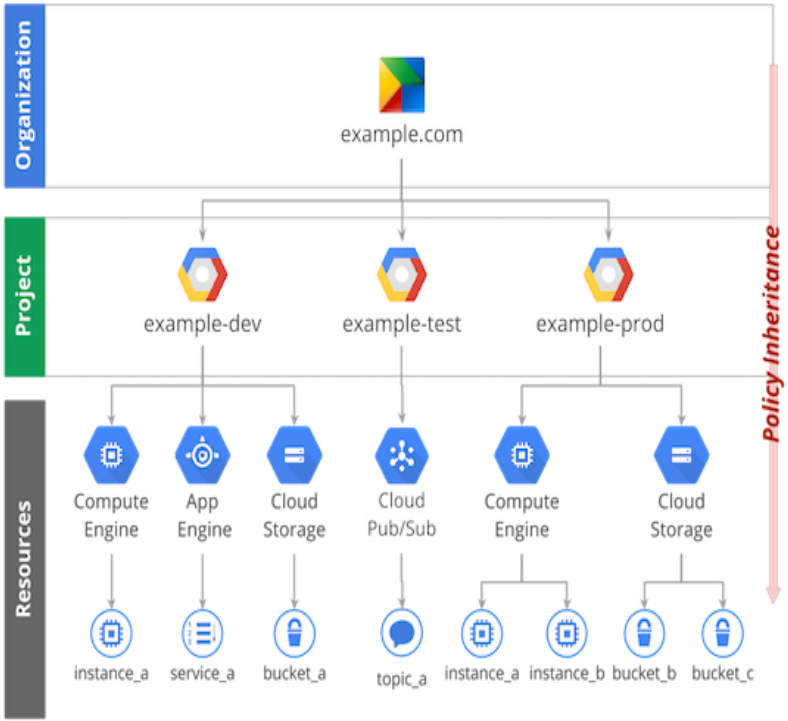
Deploy applications
Modify code
Configure services
Includes Viewer rights

Viewer

Read-only access

Billing administrator

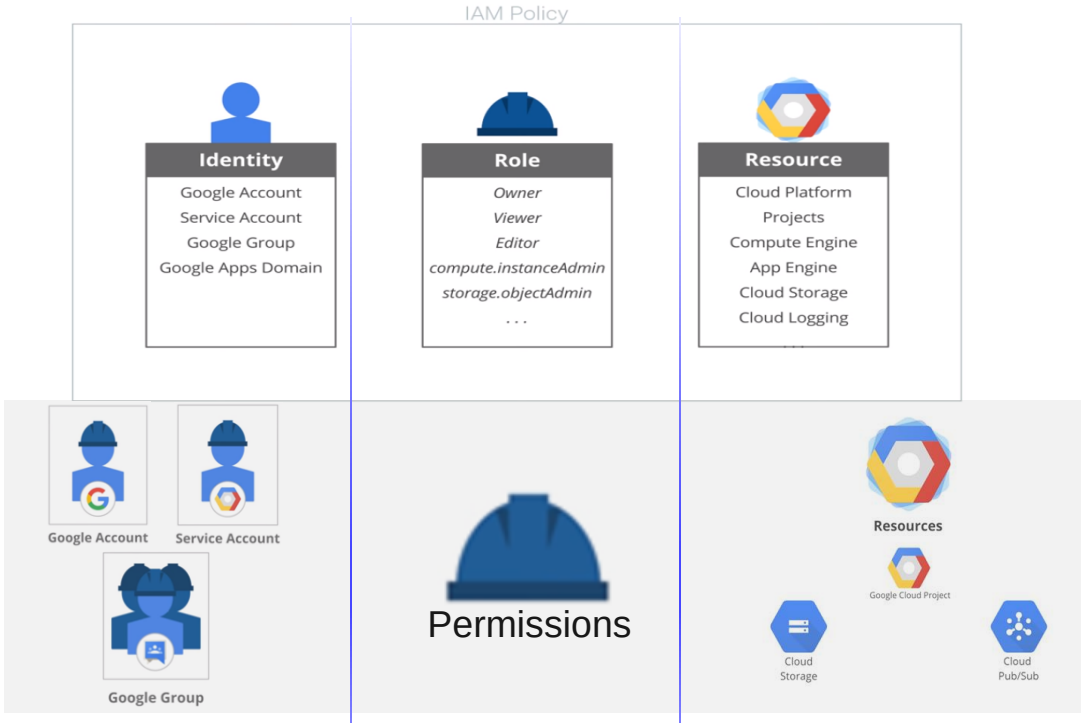
Manage billing
Add administrators
Remove administrators



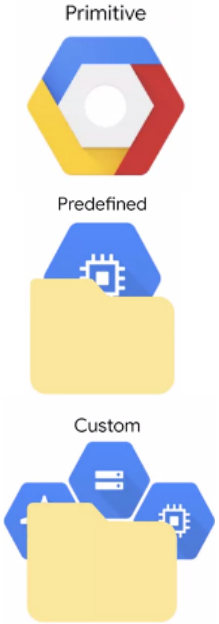
Note: A project can have multiple owners, editors, viewers and billing administrators

Cognizant

Components of IAM



Three types of IAM roles



On all resources in the project

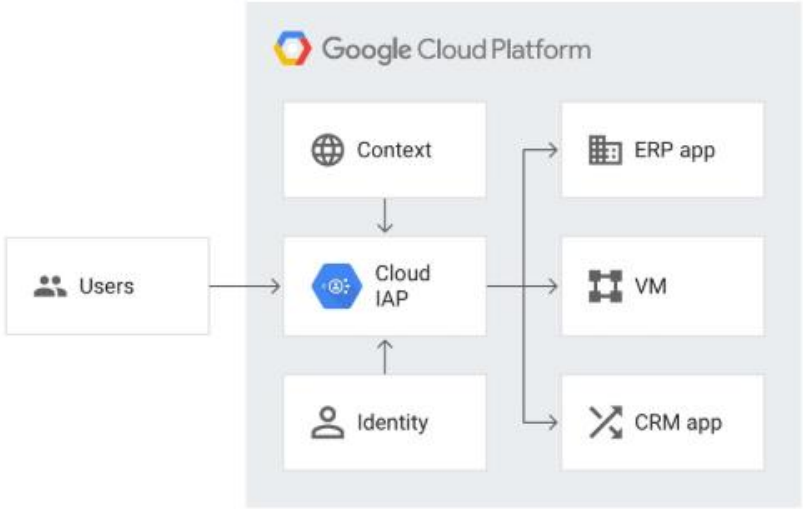
Granular level access on Specific resources in a project

Roles that you create to tailor permissions

Permissions are always with: ***service.resource.verb***
e.g. storage.bucket.create

Identity-Aware Proxy

- Cloud Identity-Aware Proxy (Cloud IAP) lets you manage access to applications running in App Engine standard environment, App Engine flexible environment, Compute Engine, and Kubernetes Engine
- **Identity-based access control:** Cloud IAP uses identity to protect access for applications deployed on GCP.
- **Saves admin time:** Faster to deploy than a VPN. Once deployed, Cloud IAP provides a single point of control for managing user access to web applications
- Free of charge
- **Saves end-user time:** Faster to sign into than a VPN. No VPN client login.
- **Deploys in minutes:** Let your developers focus on their application logic, while Cloud IAP takes care of authentication and authorization.



Cognizant

Service Accounts

A service account is a special kind of account used by an **application** or a **virtual machine (VM) instance**, not a person. Applications use service accounts to make authorized API calls.

- Identified by an **email** address:
  - 123456789-compute@project.gserviceaccount.com
- Three types of service accounts:
  - User-created (custom)
  - Built-in
    - Compute Engine and App Engine default SA's
  - Google APIs Service account
    - Runs internal Google process on your behalf

- Identity for application to authenticate
- Designed for non-human use
- Uses RSA Keys instead of passwords
- Cant access the web console

Key Management Service

Cognizant

Key Management Service

Cloud Key Management Service stores cryptographic keys in a hierarchical structure designed for useful and elegant access control management

It lets you manage cryptographic keys for your cloud services the same way you do on-premises

The levels in this hierarchy, from top to bottom, are:

- Project
- Location
- Key ring
- Key
- Key version

Cognizant

Key Management Service - Features

- Cryptographic key management
  - You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys
  - Cloud KMS is integrated with Cloud Identity and Access Management and Cloud Audit Logs
- Scalable, automated, fast
- Greater management over key use
- Easily encrypt and sign data
- Implement envelope encryption
  - Key hierarchy with a local data encryption key (DEK), protected by a key encryption key (KEK)
- Help satisfy compliance needs

Data Loss Prevention API

Cognizant

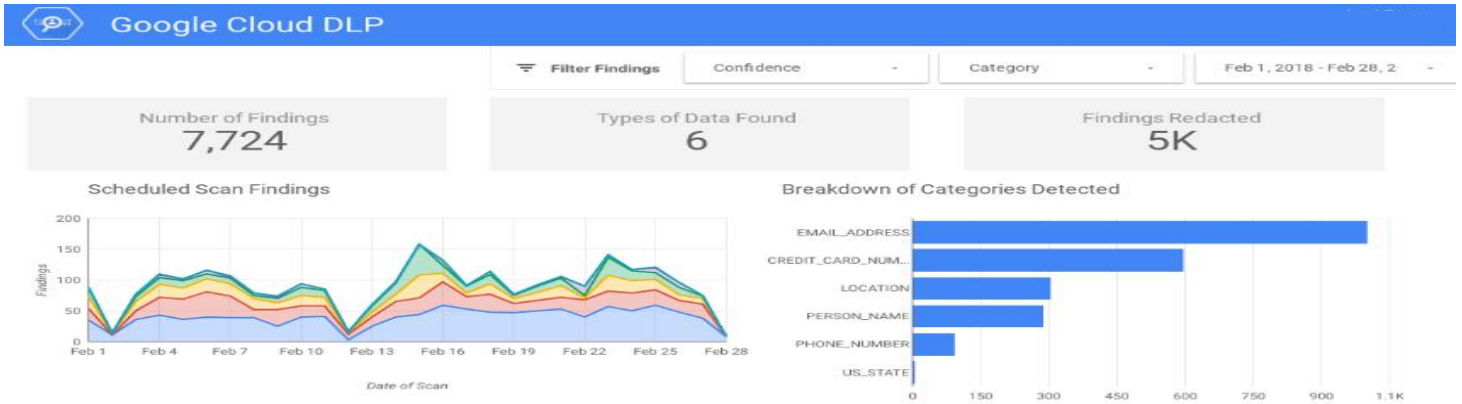
Data Loss Prevention API

DLP API provides programmatic access to a powerful sensitive data inspection, classification, and de-identification platform Wipe devices remotely

Capabilities:

- Flexible **Classification** of sensitive data like Personally Identifiable Information (PII)
- **De-ID**: Dynamic data masking, format-preserving encryption, transformation
- Re-Identification risk analysis (k-anonymity)
- Custom Dictionaries, Custom RegEx

Data Loss Prevention API - Features



- 70+ predefined information type (or "infoType") detectors and has an ability to define custom infoType detectors using dictionaries and regular expressions
- De-identification techniques including redaction, masking, format-preserving encryption, date-shifting, and more.
- The ability to detect sensitive data within streams of data, files in storage repositories such as Cloud Storage and BigQuery and even within images.
- Stream data from virtually anywhere
- Redact data from free text and structured data at the same time
- Measure re-identification risk with k-anonymity and l-diversity

Cognizant

Cloud Security Scanner

Cognizant

Cloud Web Security Scanner

Web security scanner for common vulnerabilities in

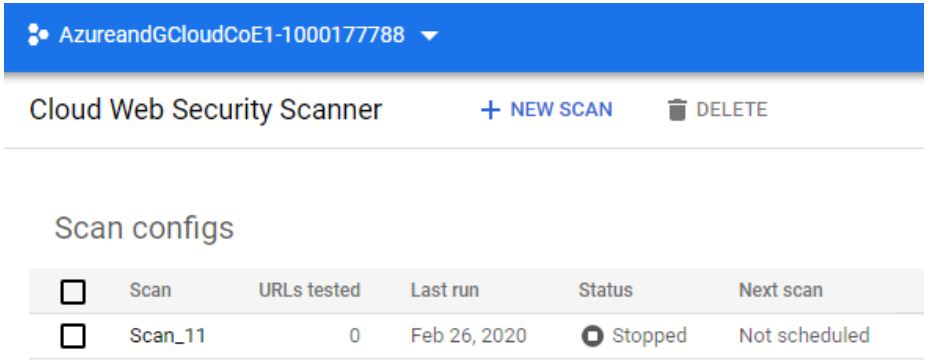
- App Engine
- Compute Engine
- Google Kubernetes Engine applications

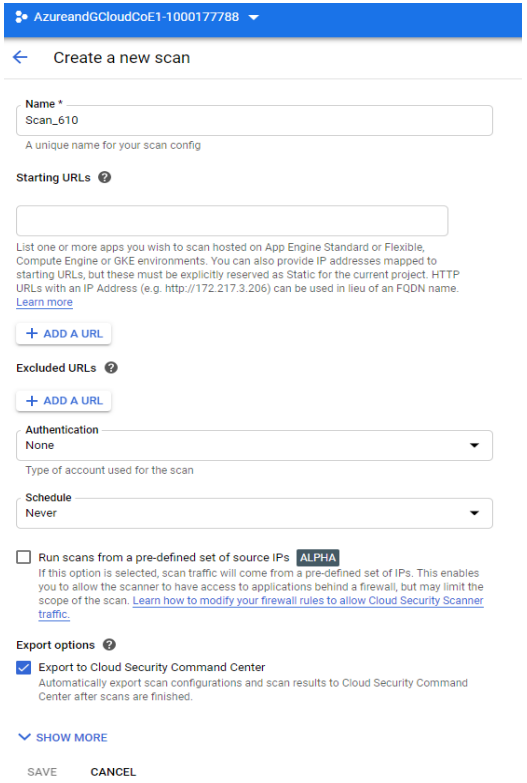
Automatically scan and detect the below vulnerabilities

- Cross-site scripting (XSS)
- Flash injection
- Mixed content (HTTP in HTTPS)
- The use of outdated/insecure libraries

Cloud Web Security Scanner

Application LB: http://34.102.197.245/SearchDB





Cloud Armor

Cognizant

Cloud Armor

Protect your services against denial of service and web attacks. It sits on the edge of Google's network, aids in blocking attacks to its services, and has IP whitelisting and blacklisting tools.

Enterprise-grade DDoS defense

Google Cloud Armor works with the Global HTTP(S) Load Balancer to provide built-in defenses against Layer 3 and Layer 4 infrastructure DDoS attacks.

Mitigate OWASP Top 10 risks**

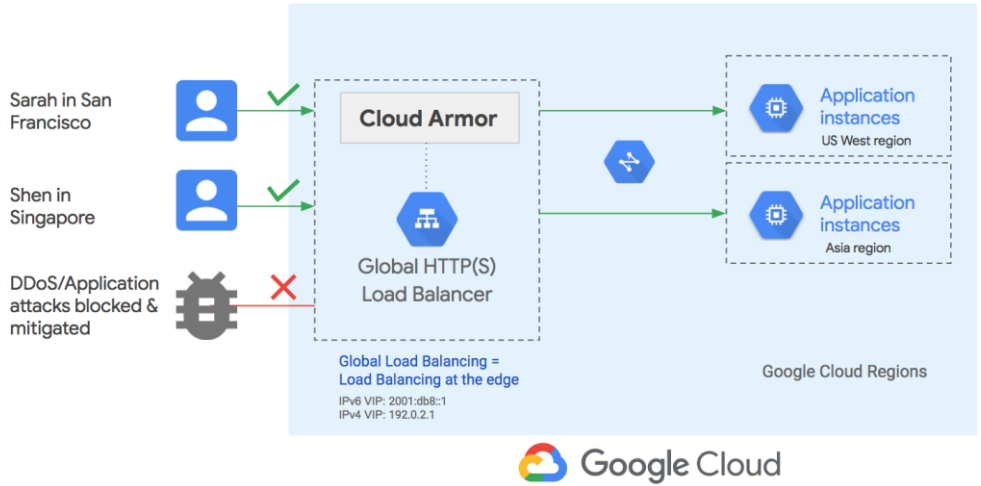
Google Cloud Armor offers a flexible rules language to help you customize your defenses and mitigate multi-vector attacks

The service is built on three pillars:

- Policy framework
- Rich rules language
- Global enforcement infrastructure.

**OWASP(Open Web Application Security Project)-Read More

Cloud Armor Features

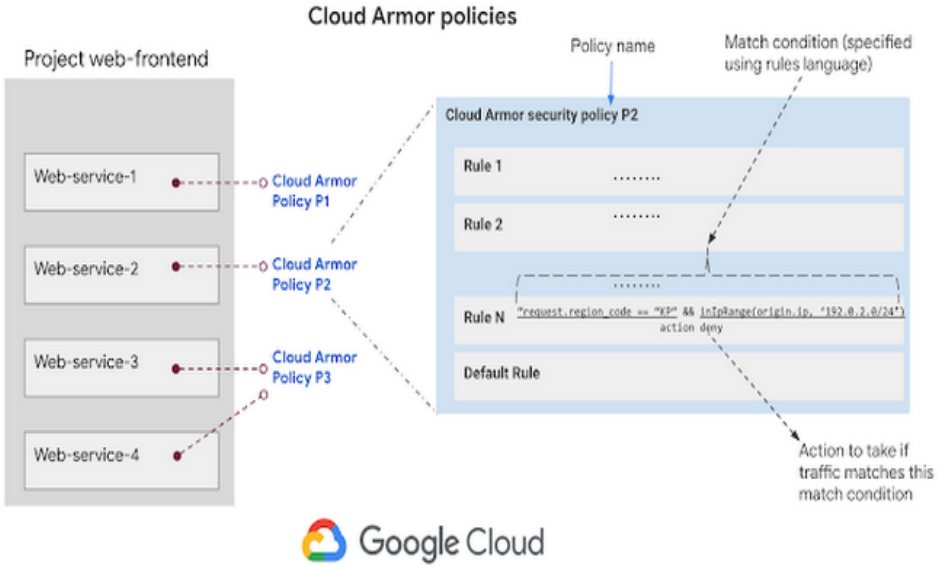


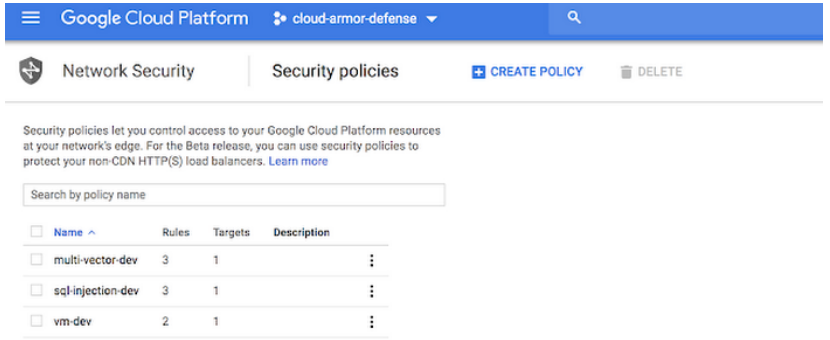
- Defend your services against infrastructure DDoS attacks via HTTP(S) load balancing
- Configure security policies, specify rules and order of evaluation for these rules
- Allow, Block, Preview and Log Traffic
- Deploy IP whitelists and blacklists for both IPv4 and IPv6 traffic
- Create custom rules using a rich rules language to match traffic based on any combination of Layer 3 and HTTP(S) request parameters and allow or block this traffic
- Enable geolocation-based control, and application-aware defense for SQL Injection (SQLi) and Cross-site Scripting (XSS) attacks

Cognizant

Cloud Armor Security Policy Framework

Cloud Armor configuration is driven by security policies. To deploy Cloud Armor, you must create a security policy, add rules, and then attach this policy to one or more HTTP(S) load balancing backend services.





Cognizant

Cloud Armor Rules Language

Language for specifying rules and creating match conditions

- Based on Common Expressions Language (a.k.a. CEL)
- Supports a subset of CEL expressions + Cloud Armor-specific attributes

Attributes

Attributes represent information from an incoming request, such as the origin IP address or the requested URL path.

Field	Type	Field description
origin.ip	string	The source IP address of the request.
request.headers	map	A string to string map of the HTTP request headers. If a header contains multiple values, the value in this map would be a comma-separated string of all of the values of the header. The keys in this map are all lowercase. Only the first 16kb of each header value is available for inspection. Any header value over 16kb is truncated per GCLB specifications.
request.method	string	The HTTP request method, such as `GET`, `POST`.
request.path	string	The requested HTTP URL path.
request.scheme	string	The HTTP URL scheme such as `http`, `https`. Values for this attribute are all lowercase.
request.query	string	The HTTP URL query in the format of `name1=value&name2=value2`, as it appears in the first line of the HTTP request. No decoding is performed.
origin.region_code	string	The Unicode country code that is associated with the origin IP, such as "US". For more information, see unicode_region_subtag in the Unicode Technical Standard.

Preconfigured rule examples

The following expression uses the `xss-stable` preconfigured rule to mitigate XSS attacks:

```
evaluatePreconfiguredExpr('xss-stable')
```

The following expression uses all the expressions from the `xss-stable` preconfigured rule except for member IDs `981136` and `981138`:

```
evaluatePreconfiguredExpr('xss-stable', ['owasp-crs-v020901-id981136-xss',
'owasp-crs-v020901-id981138-xss'])
```

Source

Cognizant

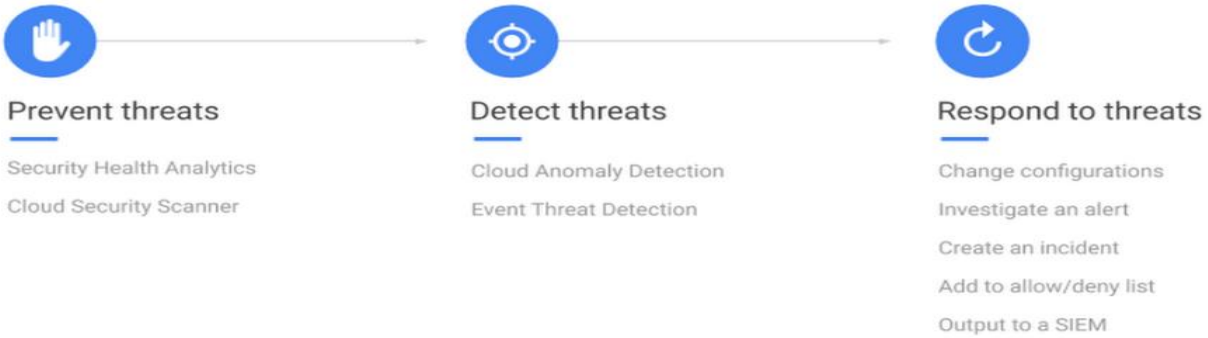
Security Command Center

Cognizant

Security Command Center

Security Command Center is the canonical security and risk database for Google Cloud.

- Gain centralized visibility and control with built-in cyber risk management
- Improve your vulnerability management
- Report on and maintain compliance
- Detect threats targeting your Google Cloud assets



Cognizant

Security Command Center - Features

❑ Security Health Analytics

- Publicly exposed assets, like Buckets, SQL Instances, Datasets, and VMs.
- Misconfigured firewalls, like Open Firewalls and Overly Permissive Firewalls.
- Insecure Cloud IAM configurations.

❑ Event Threat Detection

- Monitors your organization's Cloud Logging stream and consumes logs to detect Malware, Cryptomining, outgoing DoS etc.,

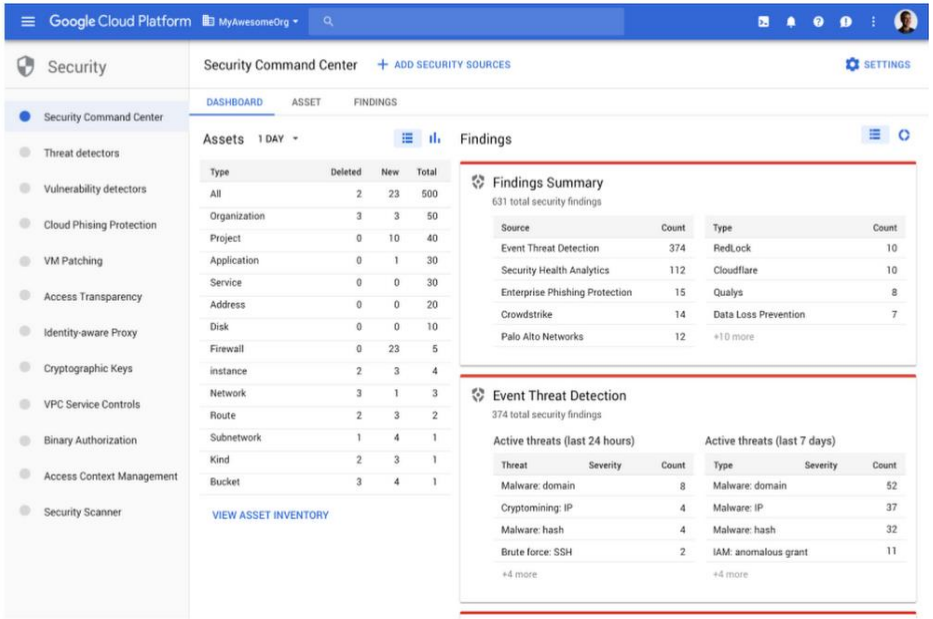
❑ Container Threat Detection

- detects the container runtime attacks e.g. Suspicious binary, Suspicious library, Reverse shell

❑ Web Security Scan

- Scans security vulnerabilities

Security Command Center



Security Health Analytics

2,868 current findings

Finding	Count
OPEN_FIREWALL	184
PUBLIC_BUCKET_ACL	7
PUBLIC_IP_ADDRESS	67
SSL_NOT_ENFORCED	2
WEB_UI_ENABLED	5

+21 More

Event Threat Detection

374 total security findings

Active threats (last 24 hours)

Threat	Severity	Count
Malware: domain		8
Cryptomining: IP		4
Malware: hash		4
Brute force: SSH		2
+4 more		

Active threats (last 7 days)

Type	Severity	Count
Malware: domain		52
Malware: IP		37
Malware: hash		32
IAM: anomalous grant		11
+4 more		

Cognizant

Security - Responsibility, Best Practices, etc.

Cognizant

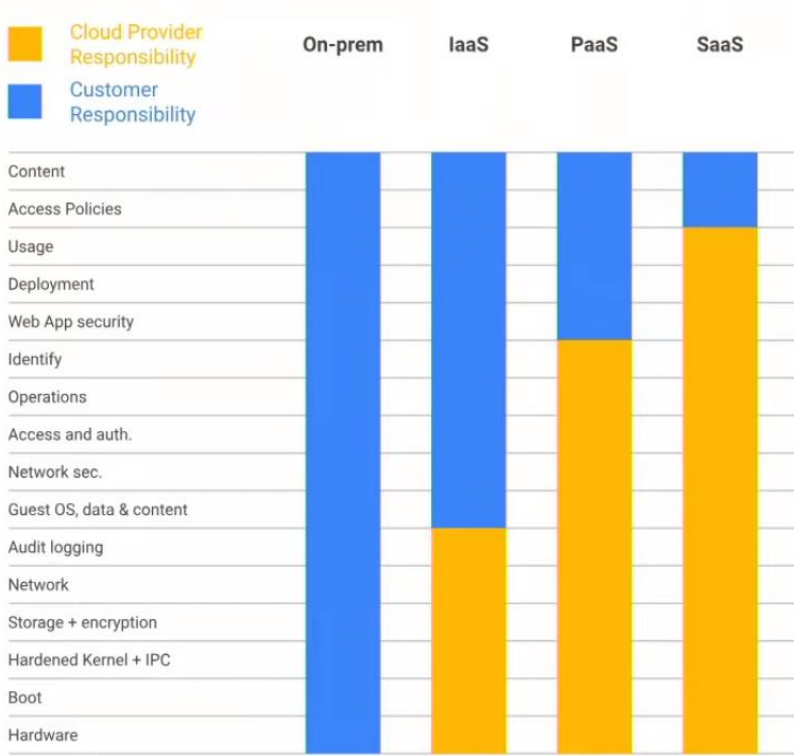
Security Collaboration

Security is a Shared responsibility.

*"Security **of the** cloud & security **in the** cloud"*

- Google is responsible for managing its Infrastructure security
- You (customer) are responsible for securing your data

The boundaries change based on the Services selected by the customer

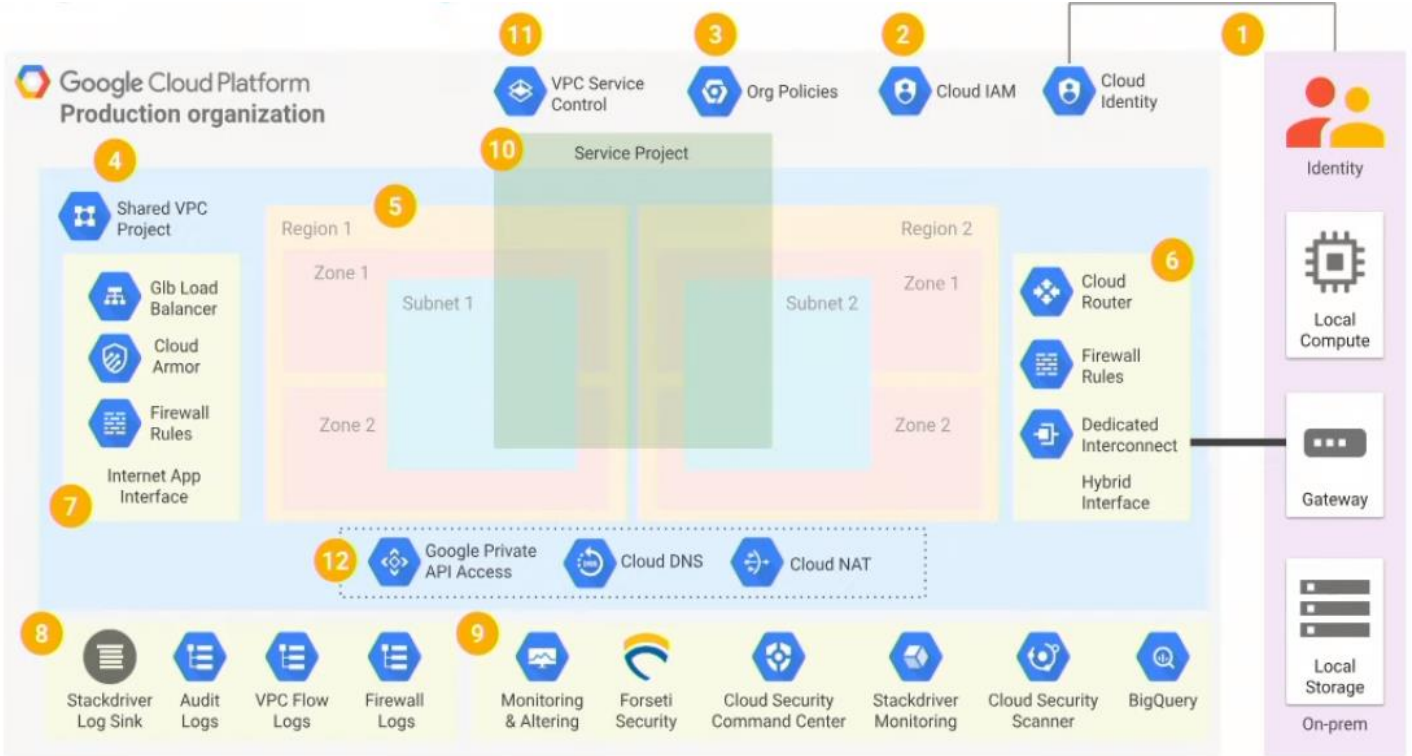


Read More

Cognizant

Secure Google Cloud Services

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Stackdriver Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. Create a service project to host workloads
11. Create security perimeter with VPC-SC
12. Access GCP services and the Internet through private IP



Read More

Cognizant

Governance | Risk | Compliance | Certifications

Global

ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
SOC 1
SOC 2
SOC 3
PCI DSS
CSA STAR
MPAA
Independent Security Evaluators Audit

Americas

USA

HIPAA
HiTrust
FedRAMP
FIPS 140-2
COPPA
FERPA
NIST 800-53
NIST 800-171
NIST 800-34
Sarbanes- Oxley
SEC Rule 17a-4(f)
CFTC Rule 1.31(c)-(d)
FINRA Rule 4511(c)
HECVAT
DISA IL2
CCPA

Canada

Personal Information & Electronic Documents Act

Argentina

Personal Data Protection Law

Europe, Middle East & Africa

Europe

GDPR
EU Model Contract Clauses
Privacy Shield
TISAX
EBA Guidelines

Germany

BSI C5

Switzerland

FINMA

France

HDS

Spain

Esquema Nacional de Seguridad

South Africa

POPI

UK

NCSC Cloud Security Principles
NHS IG Toolkit

Asia Pacific

Australia

Australian Privacy Principles
Australian Prudential Regulatory Authority Standards
IRAP

Japan

FISC
My Number Act

Singapore

MTCS Tier 3
OSPAR
MAS Guidelines
ABS Guide

As on Dec 2019

Icons made by Freepik from www.flaticon.com

https://cloud.google.com/security/overview/whitepaper
https://cloud.google.com/security/compliance/

Read More

References

https://cloud.google.com/security/products

https://cloud.google.com/iam

https://cloud.google.com/armor

https://cloud.google.com/kms

https://cloud.google.com/iap

https://cloud.google.com/security-command-center

https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

https://cloud.google.com/security/compliance

Thank You

Krishna Prasad

krishnaprasad.madhurakavi@cognizant.com

Cognizant