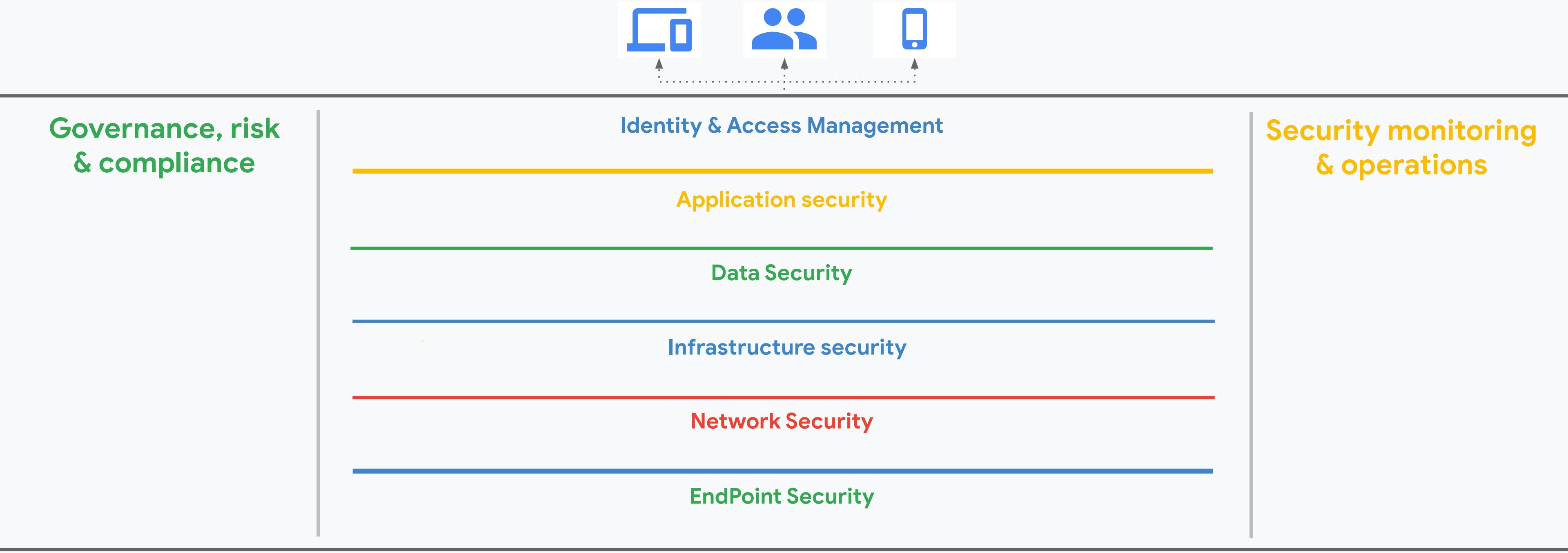
APPLICATION SECURITY ON GOOGLE CLOUD PLATFORM

Amitkumar Pandey
Customer Engineer
Infrastructure Modernisation Specialist
Google Cloud
LinkedIn
https://www.linkedin.com/in/amitkumarpandeyme/

Google Cloud’s Security Services



Governance, risk & compliance

Identity & Access Management

Application security

Data Security

Infrastructure security

Network Security

EndPoint Security

Security monitoring & operations

Google Cloud's Security Services

Governance, risk compliance

Third-party audits

International Certifications

Access Transparency

Access Approvals

Key Access Justifications

Cloud Storage Retention Policy

Cloud Audit Logging

&

Identity & Access Management

Cloud Identity IAM IAP Conditions Recommender Troubleshooter Validator

Application security

ReCaptcha Web Risk BeyondCorp Web Security Scanner Binary Authorization

Data Security

Encryption by Default CMK CSK HSM External Key Manager DLP API

Infrastructure security

Titan Shielded VM · GKE Binary Auth Confidential Computing Container Threat Detection

Network Security

Shared VPC VPC Firewalls Cloud Armor VPC Service Controls Packet Capture

EndPoint Security

ChromeOS Chrome Browser SafeBrowsing Device Management ChromeBook Pixel

Security monitoring operations

Ops Suite Logging,

Security Command Center

Incident Response Management

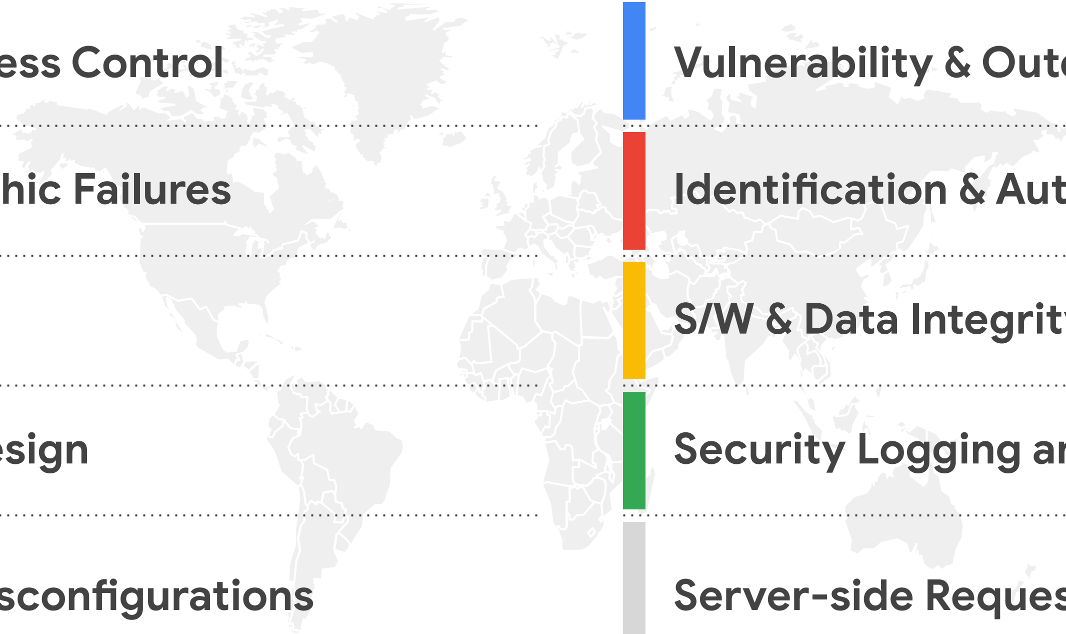
Security Health Analytics

Event Threat Detection

VirusTotal

Chronicle

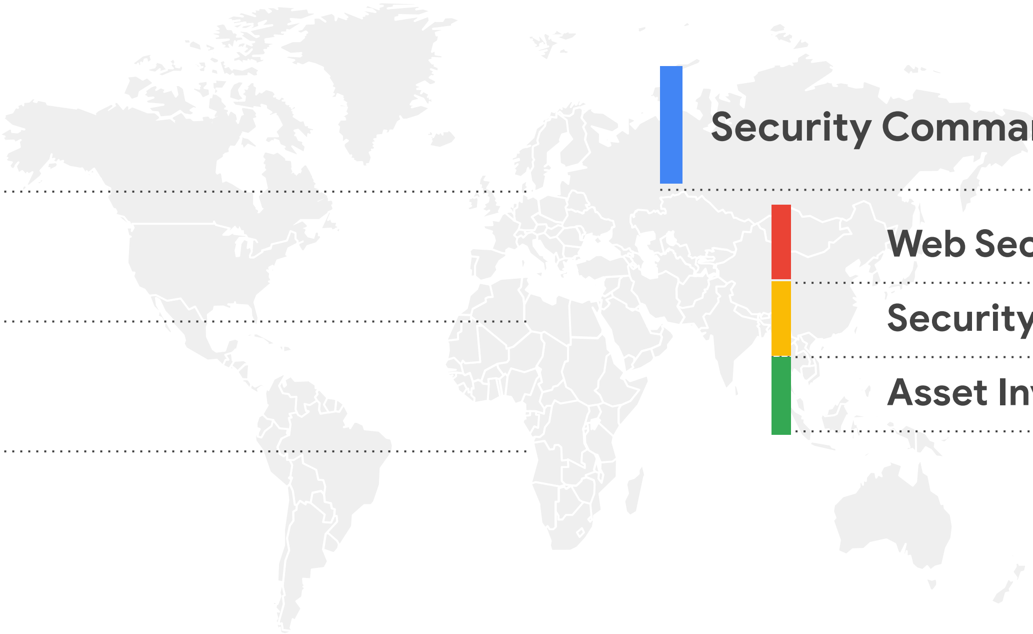
What is OWASP Top 10?



- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfigurations
- Vulnerability & Outdated Components
- Identification & Authentication Failures
- S/W & Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-side Request Forgery

Disclaimer: All of these slides are for representation and serves a view that is limited to just few services from GCP. This is for educational purpose only. Does not indicate the ultimate security practices.

GCP Services for OWASP Top 10



Cloud Armor

Apigee

reCaptcha

Security Command Centre

Web Security Scanner

Security Health Analytics

Asset Inventory

Disclaimer: All of these slides are for representation and serves a view that is limited to just few services from GCP. This is for educational purpose only. Does not indicate the ultimate security practices.

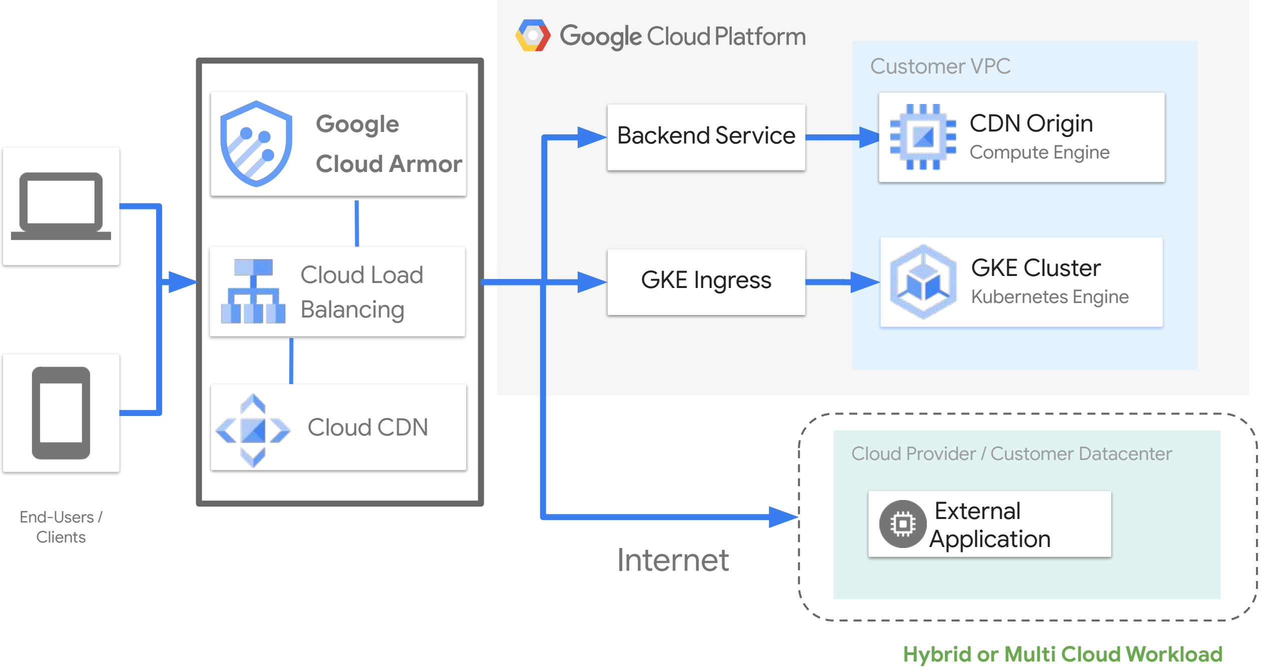
Cloud Armor

Mitigate infrastructure DDoS attacks TCP SYN floods, Amplification attacks, IP fragmentation attacks, protocol attacks, etc

Allow or block traffic based on IP, Geo, and custom match parameters

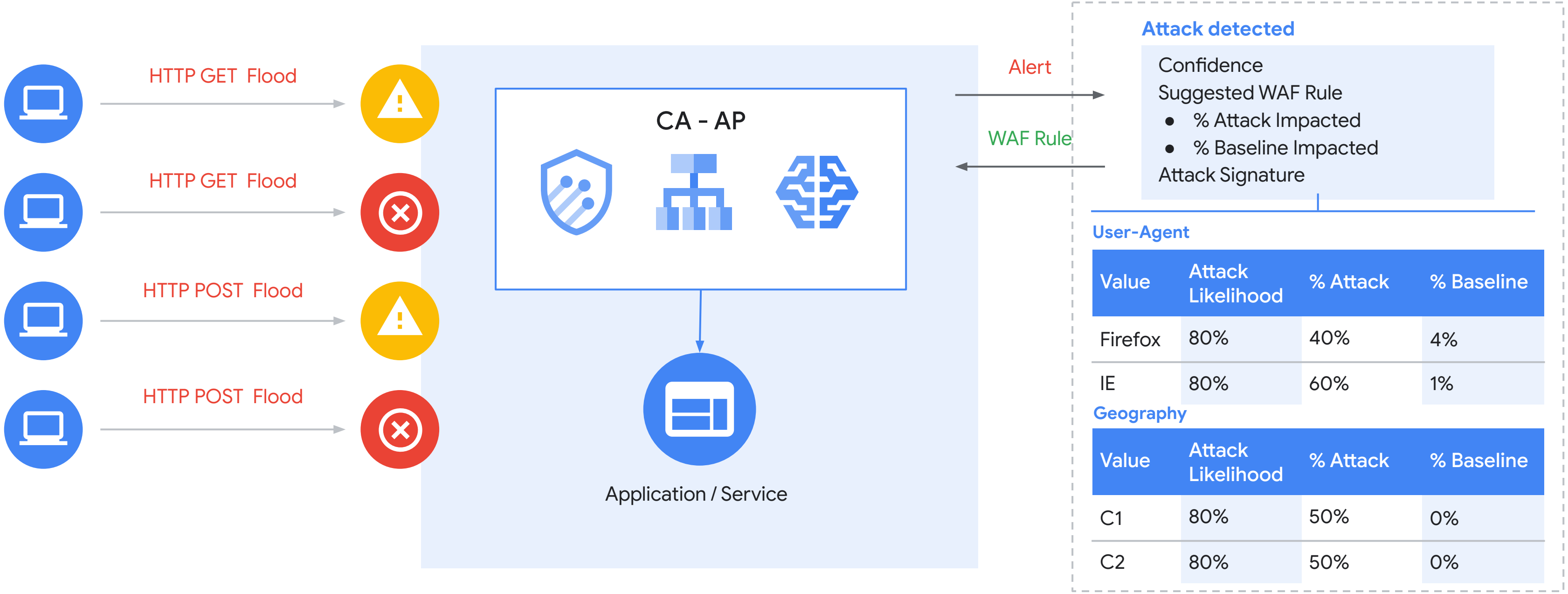
Defend against application layer attacks (SQLi, XSS, RCE, LCE, etc). Protect against **OWASP Top 10**

Telemetry: Decisions logged to Cloud Logging and Monitoring dashboard



Cloud Armor Adaptive Protection

ML based L7 DDoS detection and protection



Attack detected

Confidence
Suggested WAF Rule

- % Attack Impacted
- % Baseline Impacted

Attack Signature

User-Agent

Value	Attack Likelihood	% Attack	% Baseline
Firefox	80%	40%	4%
IE	80%	60%	1%

Geography

Value	Attack Likelihood	% Attack	% Baseline
C1	80%	50%	0%
C2	80%	50%	0%

Learn Baseline → Detect Attack → Suggest Rule → Mitigate

Cloud Armor - DDOS Protection

We handle the largest DDOS Attacks

Example:

- 2017 : 2.54 Tbps bandwidth consumption
- 2020 : 6M HTTPS requests per second

Cloud Armor

OWASP Top 10 Coverage

Broken Access Control
CSRF Attack

Cryptographic Failures
Sensitive Endpoints

Injection
Core Rule Set

Insecure Design

Security Misconfigurations
Block Access to insecure endpoints

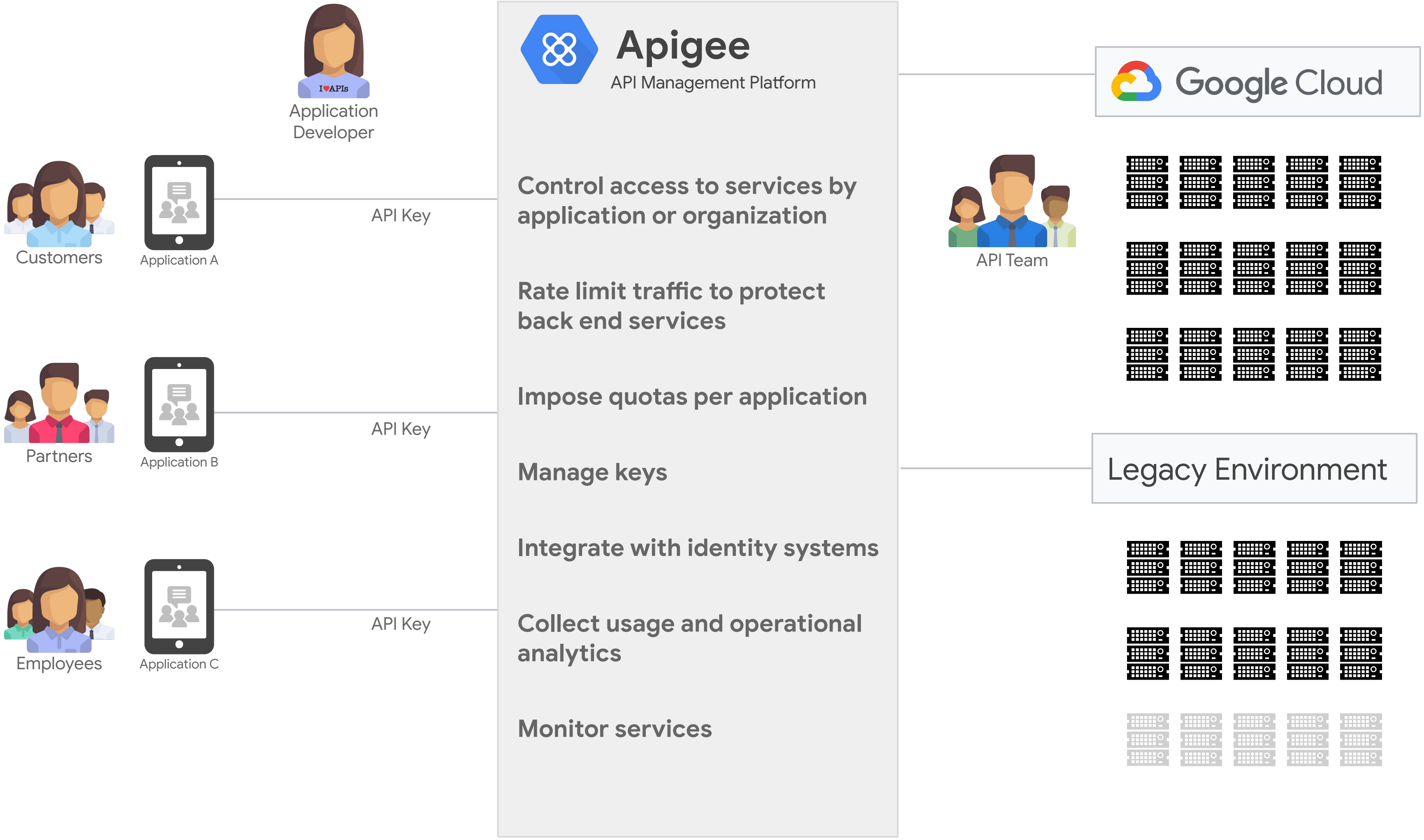
Vulnerability & Outdated Components
Block common attack

Identification & Auth Failures
Control anomalous access from Region/IP

S/W & Data Integrity Failures
Restrict access to trusted sources and avoid RCE

Security Logging and Monitoring Failures
Monitor traffic anomalies

Server-side Request Forgery
CRS , LFI and RFI rule set



Apigee

API Management Platform

Control access to services by application or organization

Rate limit traffic to protect back end services

Impose quotas per application

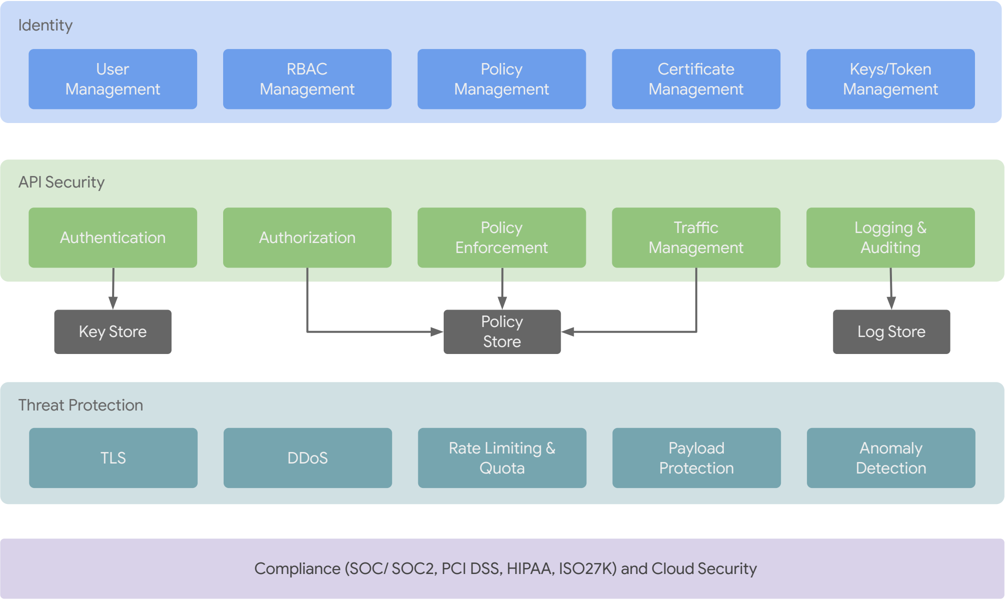
Manage keys

Integrate with identity systems

Collect usage and operational analytics

Monitor services

Use Apigee to Standardize Security



- **Holistic Security** Apigee implements a layered approach to it security to solidify our commitment to providing the most secure platform across every aspect

- **Identity** Properly manage developers, user, roles and permissions across your API program to effectively control who has access to what.

- **API Security** Implement modern and secure patterns with authentication, authorization with OAuth, API key, SAML and JWT policies along with the right level of audit and logging of the transactions

- **Threat Protection** Reduce your threat surface and protect yourself against common attacks such as SQL injection, DDoS and attacks using out of the box rate limit and threat protections

- **Compliance** Trust that the platform exceeds your compliance requirement with our numerous certifications across ISO27k, HIPPA, PCI and SOC reports.

Google Cloud

Apigee

OWASP Top 10 Coverage

Broken Access Control
SSO and RBAC

Cryptographic Failures
Mask and encrypt sensitive data at edge

Injection
Input validation mechanism to avoid injection

Insecure Design
SSO, RBAC, input validation

Security Misconfigurations
Reusable group of policies and resources : SharedFlow

Vulnerability & Outdated Components

Identification & Auth Failures
API Key, OAUTH2, JWT

S/W & Data Integrity Failures

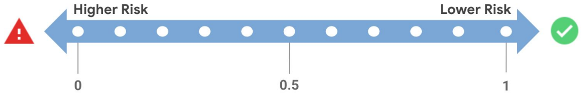
Security Logging and Monitoring Failures
Detailed monitoring for each API

Server-side Request Forgery
XML and JSON threat protection policy

reCAPTCHA Enterprise

Protect from Bad Bots

A piece of software that interacts with a website in an automated fashion to cause harm.



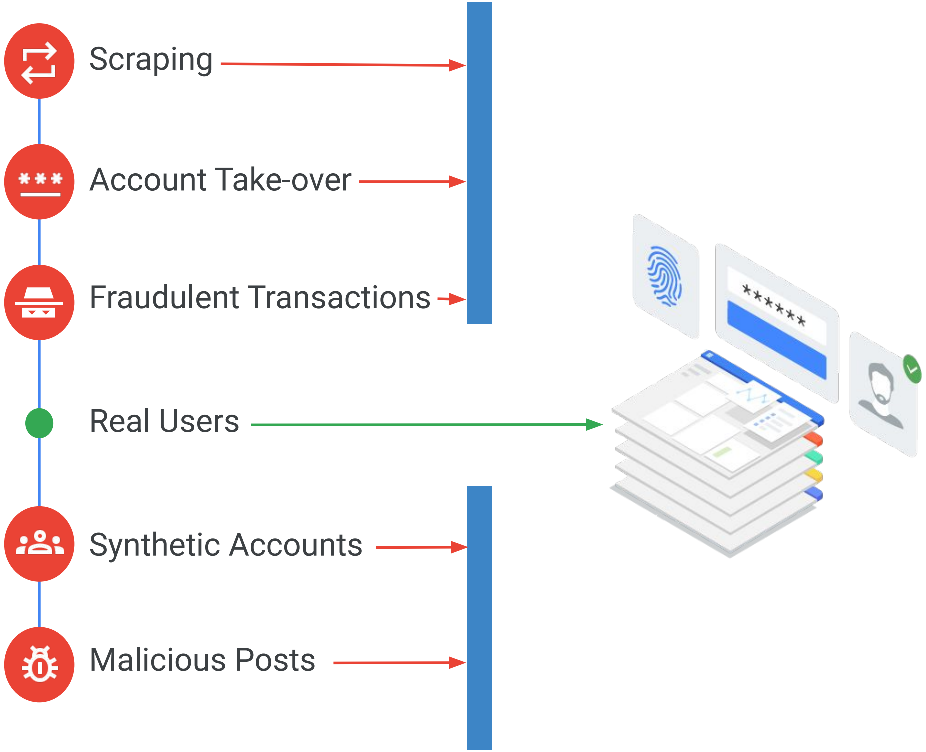
AUTOMATION

UNEXPECTED_ENVIRONMENT

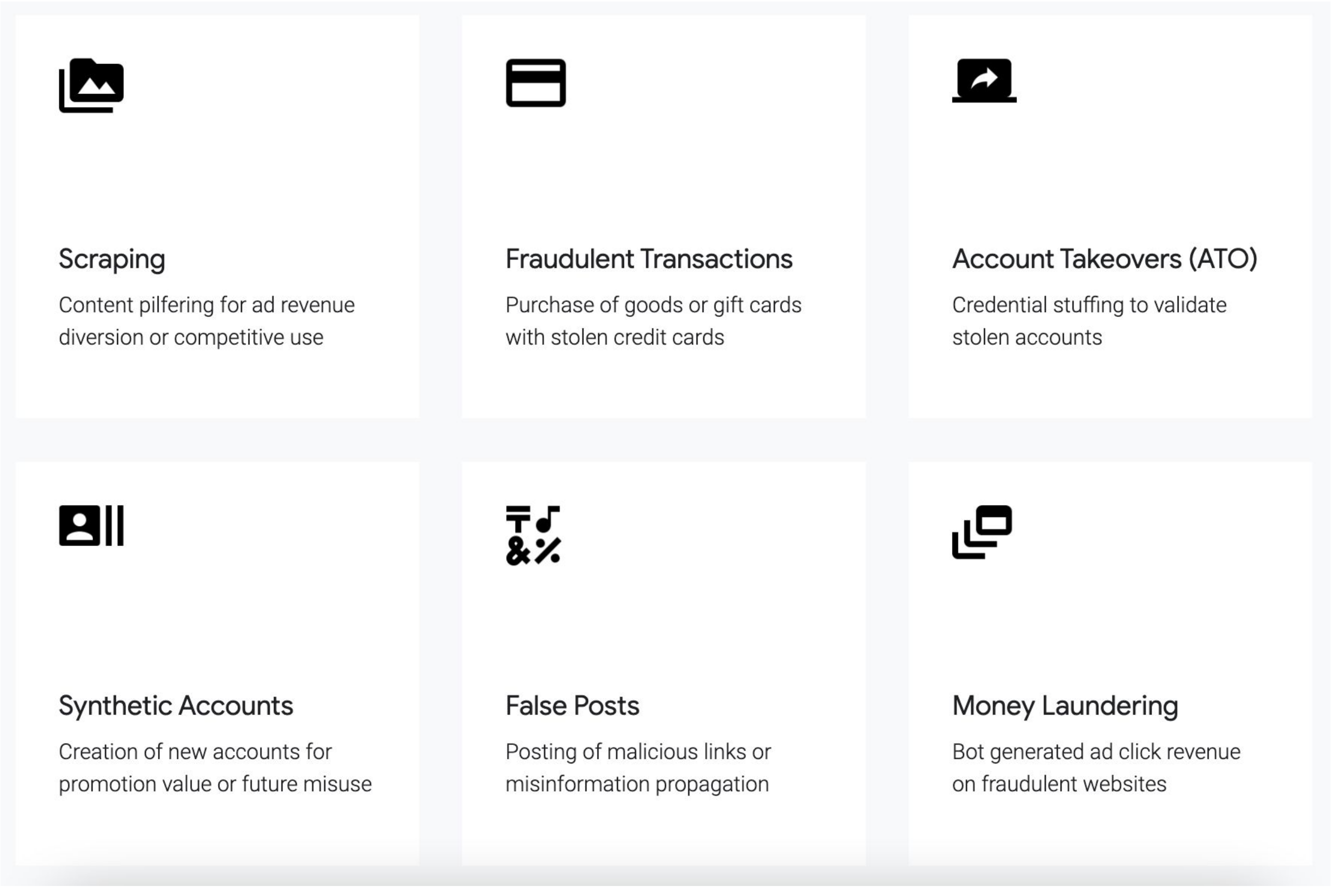
TOO_MUCH_TRAFFIC

UNEXPECTED_USAGE_PATTERNS

LOW_CONFIDENCE_SCORE



reCAPTCHA Enterprise



Scraping

Content pilfering for ad revenue diversion or competitive use

Fraudulent Transactions

Purchase of goods or gift cards with stolen credit cards

Account Takeovers (ATO)

Credential stuffing to validate stolen accounts

Synthetic Accounts

Creation of new accounts for promotion value or future misuse

False Posts

Posting of malicious links or misinformation propagation

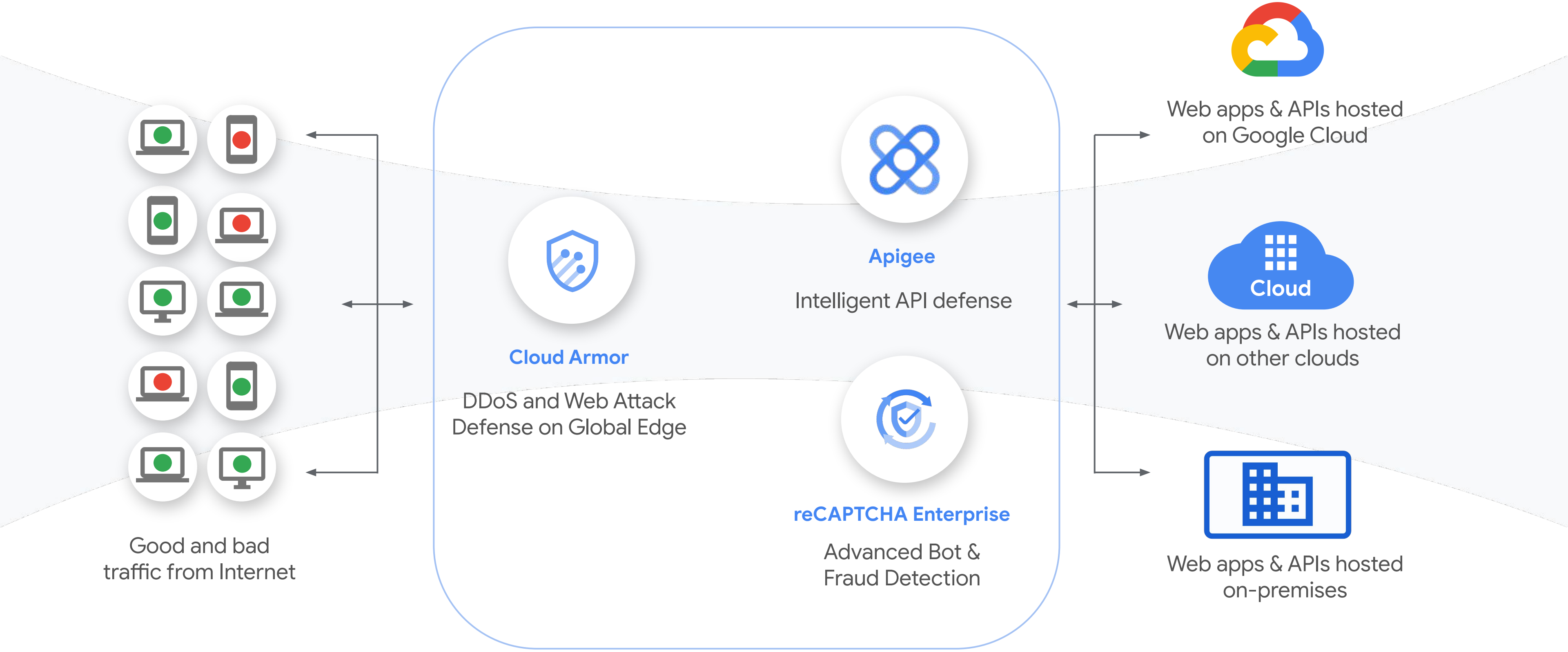
Money Laundering

Bot generated ad click revenue on fraudulent websites reCAPTCHA Enterprise

OWASP Top 10 Coverage

Broken Access Control	Vulnerability & Outdated Components
Cryptographic Failures	Identification & Authentication Failures
Injection	S/W & Data Integrity Failures
Insecure Design	Security Logging and Monitoring Failures
Security Misconfigurations	Server-side Request Forgery

Apigee + Cloud Armor + reCaptcha



Good and bad traffic from Internet

Cloud Armor

DDoS and Web Attack Defense on Global Edge

Apigee

Intelligent API defense

reCAPTCHA Enterprise

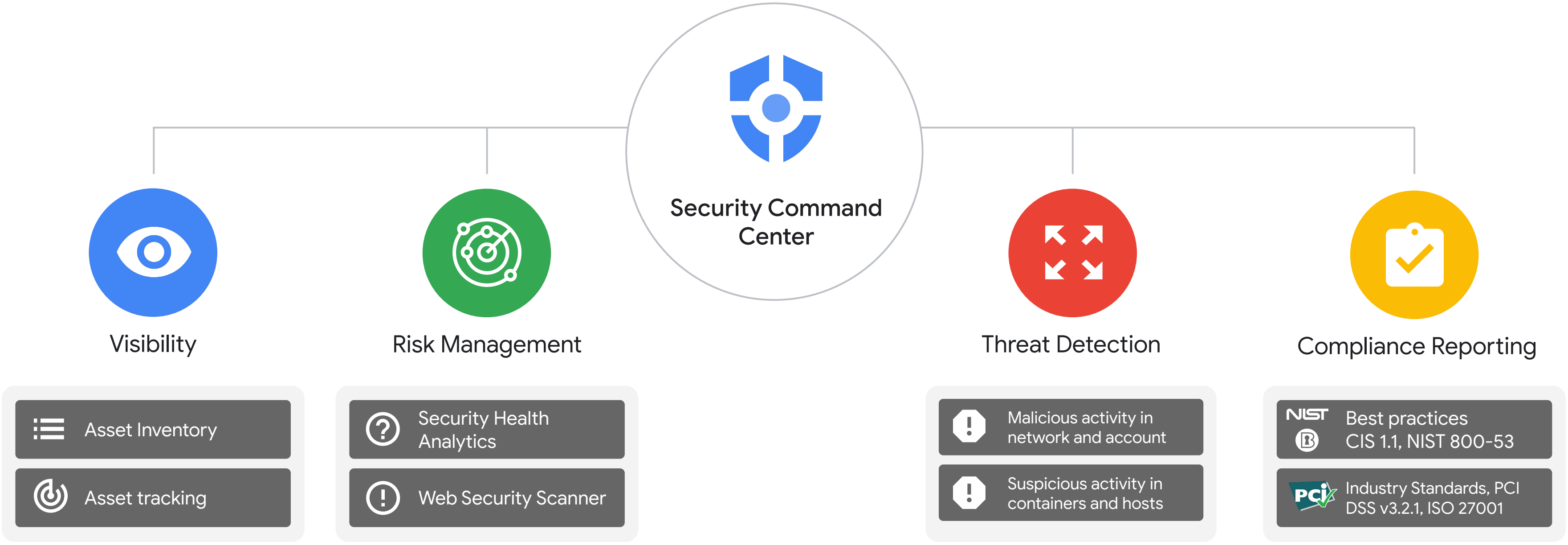
Advanced Bot & Fraud Detection

Web apps & APIs hosted on Google Cloud

Web apps & APIs hosted on other clouds

Web apps & APIs hosted on-premises

Security Command Center: Cloud-native protection



Security Command Center

Visibility

- Asset Inventory
- Asset tracking

Risk Management

- Security Health Analytics
- Web Security Scanner

Threat Detection

- Malicious activity in network and account
- Suspicious activity in containers and hosts

Compliance Reporting

- Best practices CIS 1.1, NIST 800-53
- Industry Standards, PCI DSS v3.2.1, ISO 27001

Visibility: Cloud Asset Inventory

Gain centralized visibility and control over your Google Cloud data and resources.

- Complete view into your Google Cloud resources and their policies
- Near real-time visibility into exactly what changed in your asset history and respond to the most pressing issues first
- Deep analytic query capabilities for historical investigation
- Receive notifications about findings associated with your critical assets and and take action

CryptoKey
CryptoKeyVersion
Bucket
TargetVpnGateway

UrlMap
Version
VpnTunnel
Network

Node
NodePool
Organization
Pod

Policy
Disk
Firewall
Folder

Application
Compute Instance

Risk management: Security Health Analytics

Continuous assessment of Google Cloud infrastructure for misconfigurations and vulnerabilities.

Storage

- Publicly exposed buckets
- Storage resources missing CMEK
- Use of legacy bucket ACLs

Networking

- Overly permissive firewall rules
- Use of default and/or legacy networks
- Subnetworks that do not use private access to Google APIs

Logging/ Monitoring

- Monitoring disabled
- Storage buckets with logging disabled
- Cloud Monitoring for Kubernetes clusters not enabled
- VPC Flow logs disabled

Identity

- Overprovisioned admin accounts
- Permission grants outside your org
- Insufficient separation of duties

VM Instances

- IP forwarding enabled
- Broad service account or API access enabled
- SSL & SSH misconfigurations

GKE Clusters

- Private cluster disabled
- Network policy disabled
- Primary authorized network disabled
- IP alias disabled
- Legacy authorization enabled

Risk management: Web Security Scanner

Continuous assessment of web applications on Google Cloud.

One-click coverage

- Turn on managed scans to automatically discover public web apps running on GKE/Compute Engine/App Engine
- Schedules weekly scans and detects changes and new apps

Detect key application vulnerabilities

- Detect 11+ categories of vulnerabilities, from XSS to app misconfigurations, including vulnerabilities from the OWASP Top 10
- Assess and triage security posture in unified Security Command Center dashboards

Security Command Centre

OWASP Top 10 Coverage

Broken Access Control	Vulnerability & Outdated Components
Cryptographic Failures	Identification & Authentication Failures
Injection	S/W & Data Integrity Failures
Insecure Design	Security Logging and Monitoring Failures
Security Misconfigurations	Server-side Request Forgery

Indicates alerting and monitoring capabilities

Thank you!

Until we meet again ...

What impact will Scattered Cloud Syndrome have on your Cloud Security?