Visibility, prevention and detection on Google Cloud

Andy Chang
Senior Product Manager, Google Cloud Security
andychang@

Google Cloud

Agenda

- Overview Google Cloud Security
- Cloud Operations Suite (formerly Stackdriver)
- Cloud Security Command Center - Threat prevention, detection, response
- Q&A

Google Cloud

Enterprise CISO objectives

Protect your business and your customers - connect only the right people to the right data, for the right purpose each and every time.

Meet your audit and regulatory obligations

Evolve and innovate, be proactive to stay ahead of threats

Provide sufficient visibility and control to meet the requirements of your business

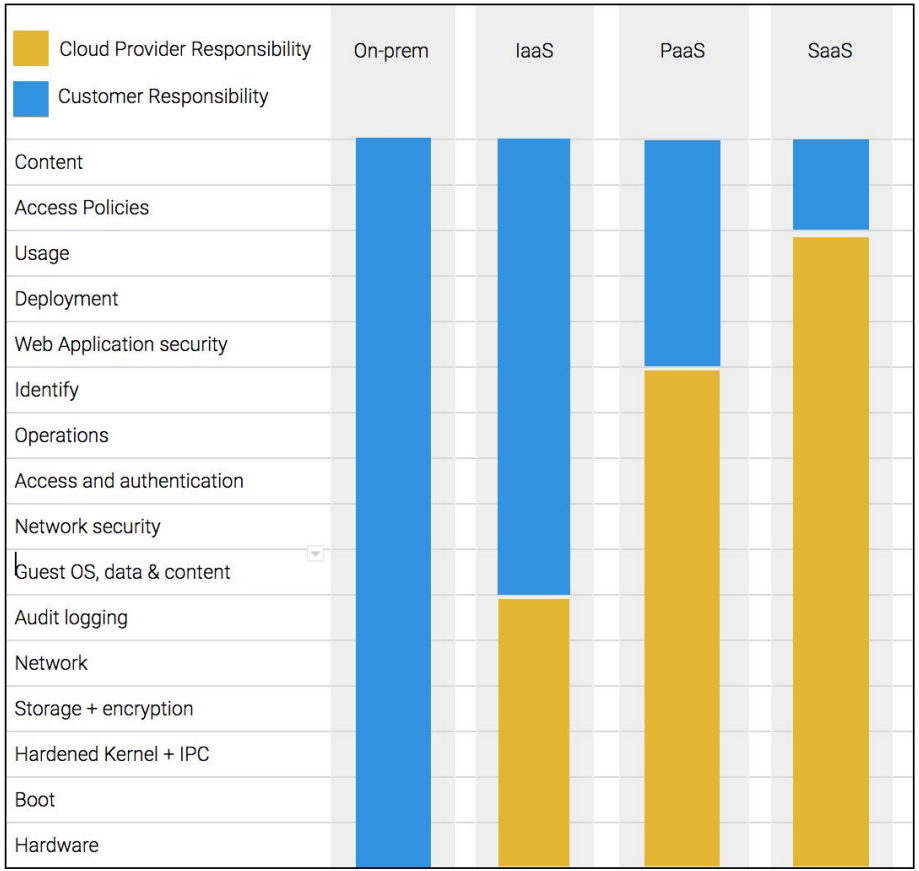
Understand and be empowered to execute your part of shared responsibility model

Google Cloud

Understanding Shared Responsibility

The **boundaries change** based on the services selected by the customer

Customers can use multiple classes of services **simultaneously**

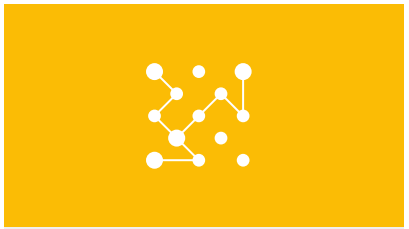


Google Cloud

Cloud security challenges

Lack of visibility and control

Inability to detect and respond to threats



Increase in complexity

Google Cloud

Google security principles

You determine and control what happens to your data

Defense ***in depth, at scale, by default***

Identity as the perimeter supported by hardware attestation and provenance

Move security policy, controls, enforcement and detection ***up the stack***

Transparency - reduce the unverifiable trust surface including

Customers have the **control** and **visibility** they need to help build secure apps and businesses in the cloud in an easy and effective way

Control & Visibility

Google Cloud

Leverage native built-in security

Control

Resource Hierarchy

Organization Policies

Curated IAM Roles Policy Intelligence

Encryption: Default/CMEK/EKM

VPC Service Controls

Shared VPC's

Binary Authorization

Access Approvals

BeyondCorp Remote Access

Control: top-down, logically central, globally distributed

Google Cloud

Leverage native built-in security

Visibility

Cloud Security Command Center

Cloud Operations Suite and Logging

Access Transparency/ Access Justifications Key Access Justifications

Cloud DLP API

Config Validator

Container Vuln Scanning

Chronicle

Third party review, validation & certifications

Google Cloud

Visibility: Cloud Operations Suite

Cloud Operations Suite provides **comprehensive observability** of Cloud Operations at scale for all **GCP customers**. It helps Developers and Operators efficiently run their workloads and keep their systems and applications fast and available

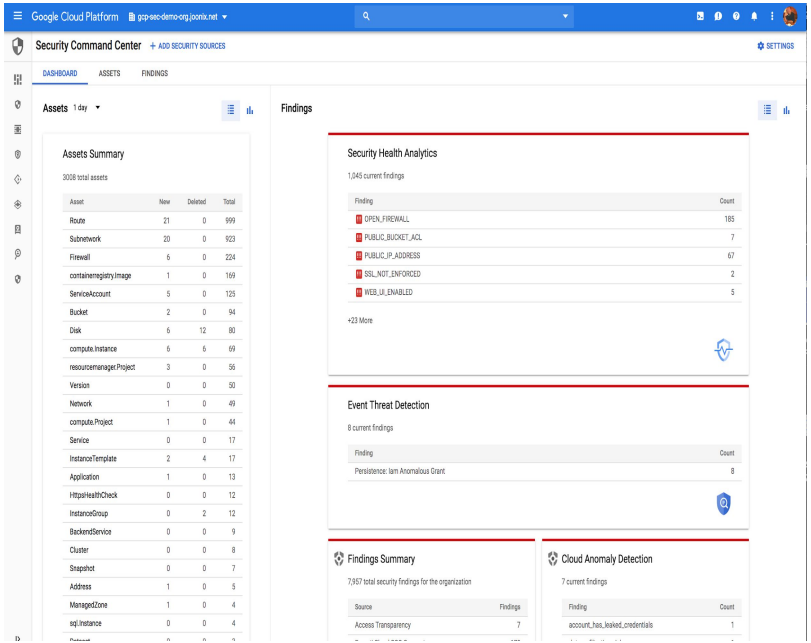
The best solution for GCP. Works on **every** GCP-managed environment

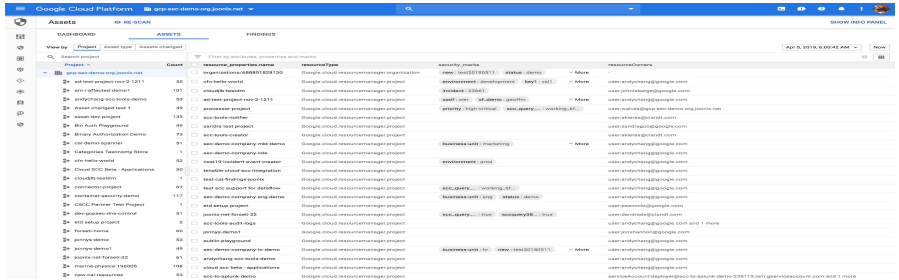
Observability of workloads running in Google Cloud, on prem and in other clouds through **Anthos**

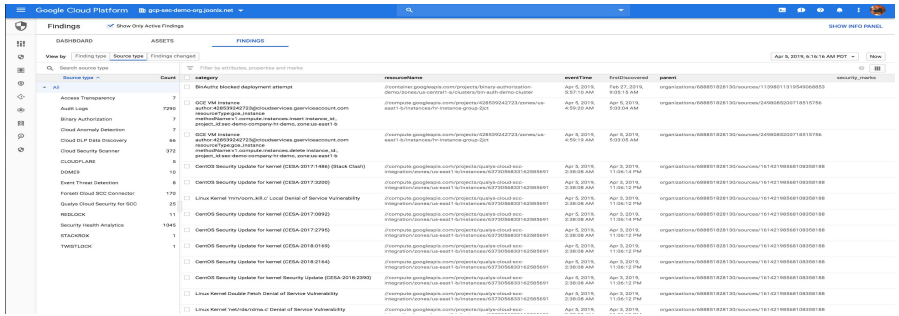
Set SREs up for success! Made for **scaling data analytics and greater automation** - this is what we at Google do best!

1. **Value Proposition**
2. **Differentiation Statement**
3. How our customers succeed

Visibility: Security Command Center - Premium & Std







Google Cloud

Cloud Operations Suite:

Capture events in your system

With Cloud Operations Suite you are able to

- **Collect** signals across GCP internal/external apps, platforms and services
- **Analyze** and visualize those signals
- Set up appropriate performance and availability **indicators**
- Use built-in observability to **troubleshoot** and improve your applications.
- **Automate** Ops using programmatic interfaces and out-of-the-box practices

1 Value Proposition

2 Differentiation Statement

3 **How our customers succeed**

Google Cloud

Customer use cases

- ➔ Can you help us **discover/map** our workloads?
- ➔ Can you **show us how** our cloud deployment is behaving?
- ➔ Can you tell us **when** we are broken?
- ➔ Can you help us **root cause, remediate, and resolve** issues?
- ➔ Can you help us **reduce** our cost?

Cloud Security Command Center:

Visibility, prevention, detection and response

Google Cloud

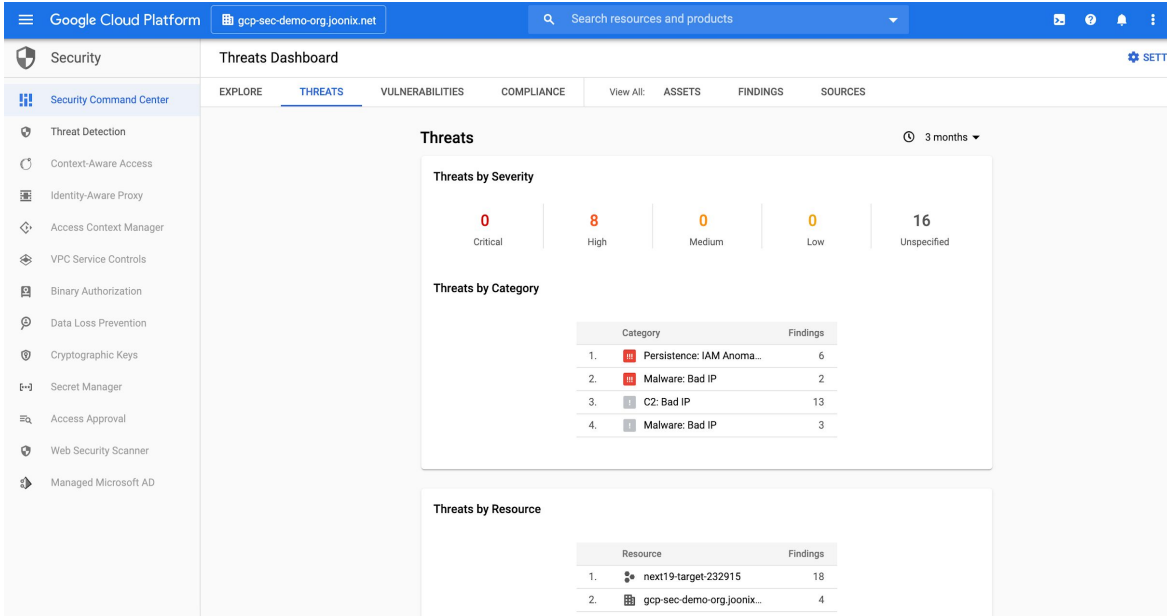
Manage and review your security posture from one place in Google Cloud

Security Command Center

Organizational level visibility, management, and control of your security posture

Prevent threats with vulnerability and misconfiguration detections

Detect and respond to active threats against your cloud assets



Google Cloud

Security Command Center

Premium

Advanced features for near-real-time prevention, detection, response and compliance

Paid Service

Standard

Security foundation - visibility w/ scans for key vulnerabilities and abuse

Free service

Google Cloud

Security Command Center Premium

Prevent threats

Web Security Scanner with managed scans

Security Health Analytics continuous compliance

Detect threats

Cloud Abuse Detection

Event Threat Detection

Container Threat Detection (Beta)

Respond to threats

Notifications Pub/Sub for alerting

Cloud Functions library to take automated actions

Google Cloud

Security Command Center Standard

Prevent threats

Web Security Scanner

Security Health Analytics scanning high severity vulnerabilities

Detect threats

Cloud Abuse Detection

Respond to threats

Notifications Pub/Sub for alerting

Cloud Functions library to take automated actions

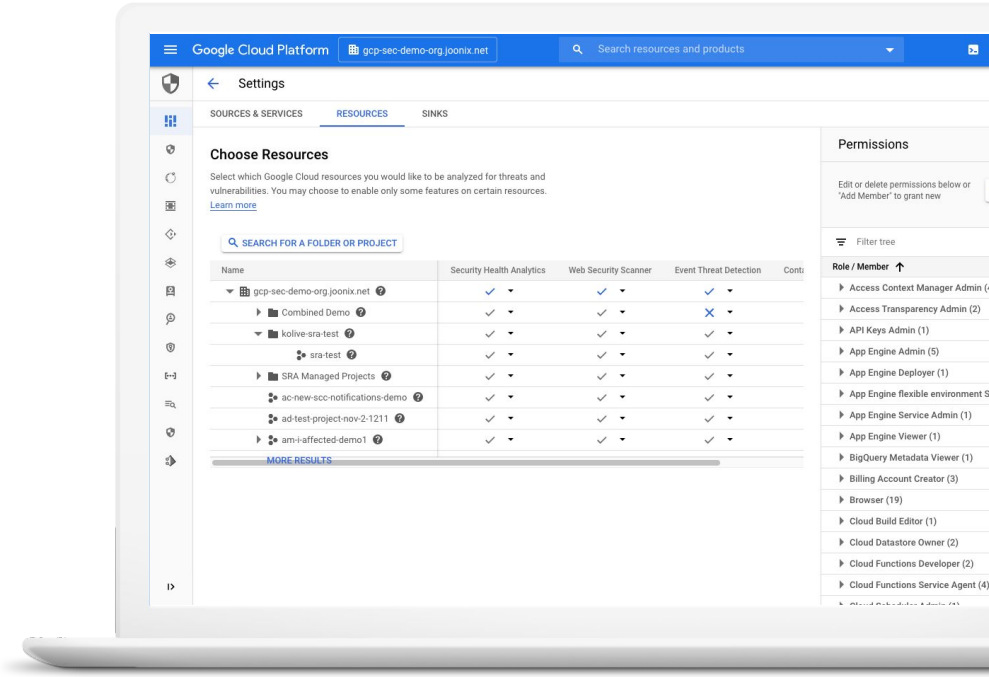
Google Cloud

Organization onboarding and configuration

- **Organization level configuration and onboarding**: Control threat and vulnerability detection from the top of your hierarchy for current and future projects. Protection for new resources happens immediately, without security team toil

- **Common IAM roles:** Curated IAM roles with necessary permissions to operate across findings providers

- **Common UI and API**: Consistent set of gcloud commands to manage all threat prevention and detection

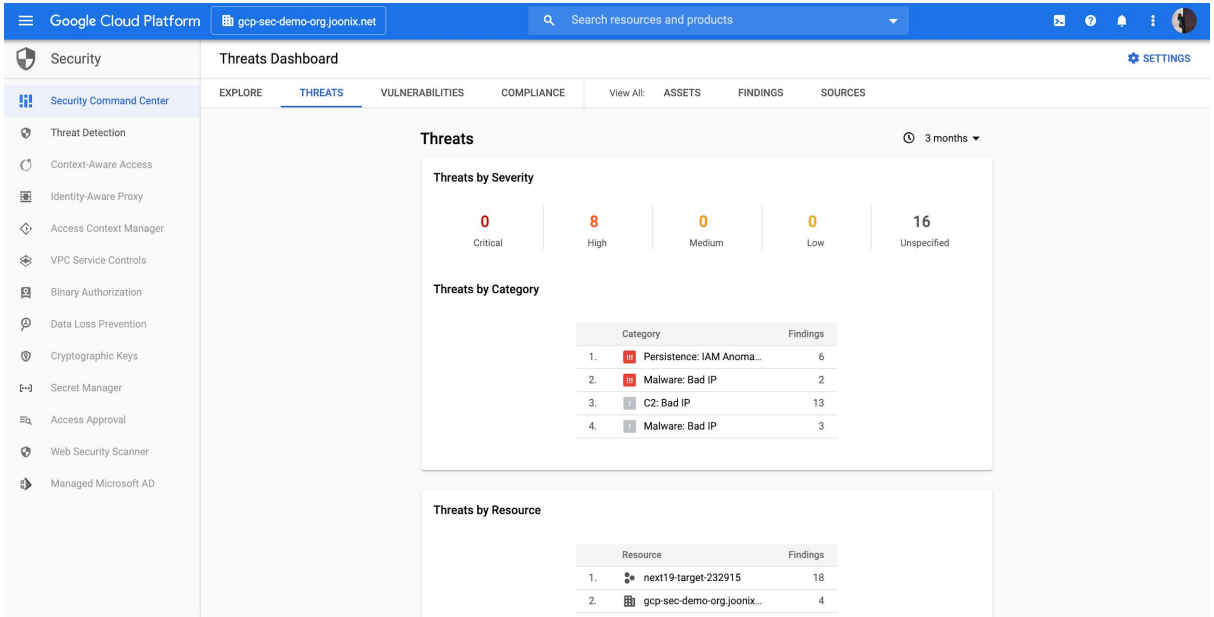


Google Cloud

Security Command Center Dashboards

Built in monitoring and visibility:

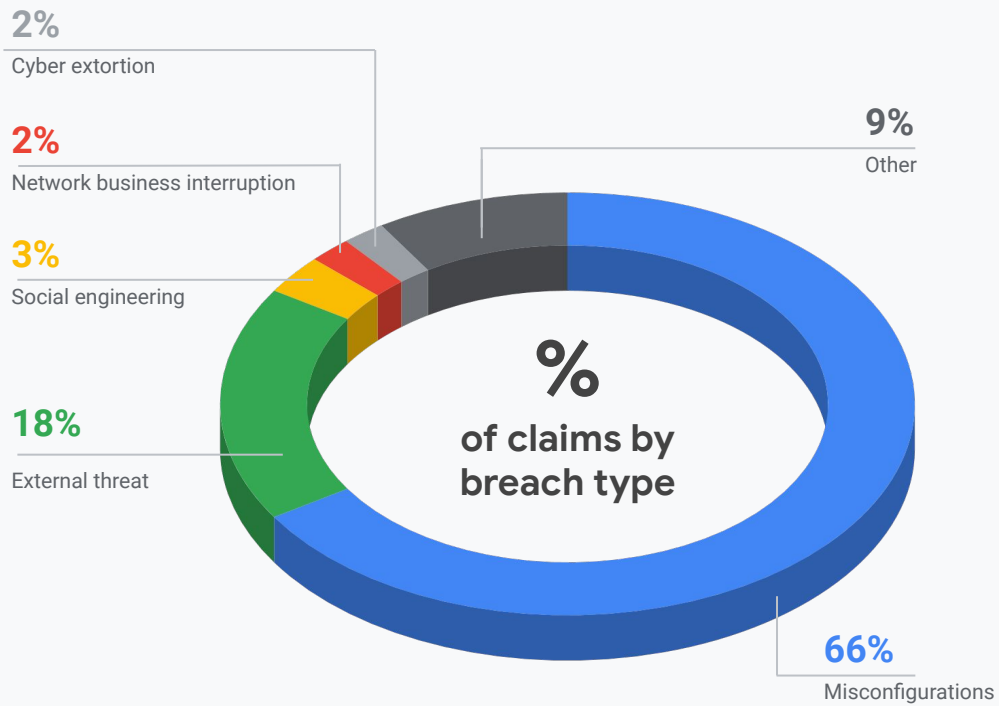
- Threat Dashboard
- Vulnerability Dashboard
- Compliance Dashboard
- Source Dashboard
- Asset inventory
- Findings Inventory



Google Cloud

Prevent threats

Misconfiguration are the largest cause of breaches!

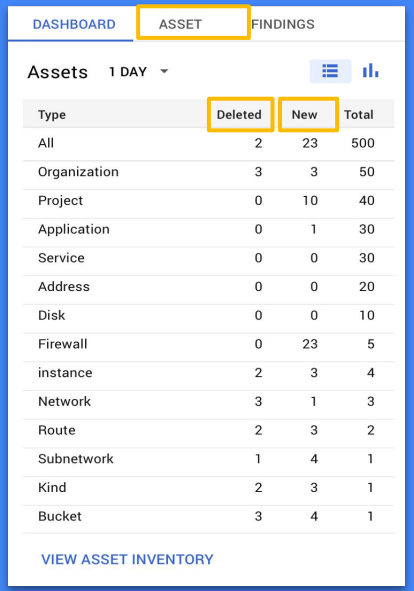


Google Cloud

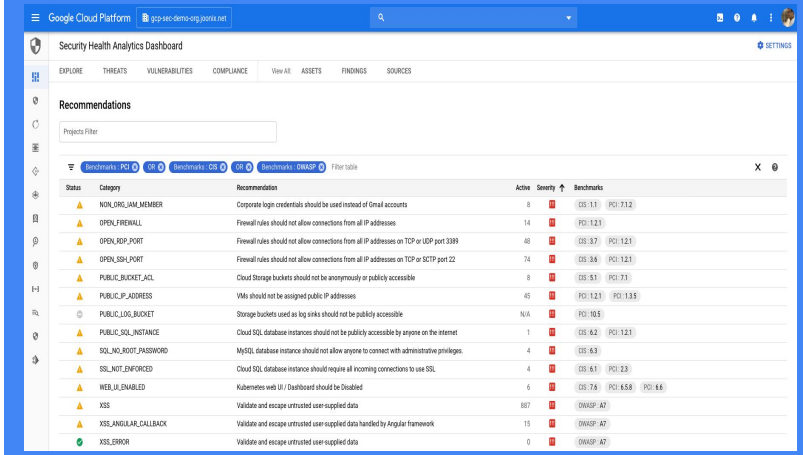
Prevent threats and meet compliance requirements with visibility and control over GCP data and resources

- Take inventory of your cloud assets
- View Google Cloud Platform resources and partner solutions
- Identify misconfigurations, vulnerabilities and compliance violations and reduce your exposure to threats

Google Cloud

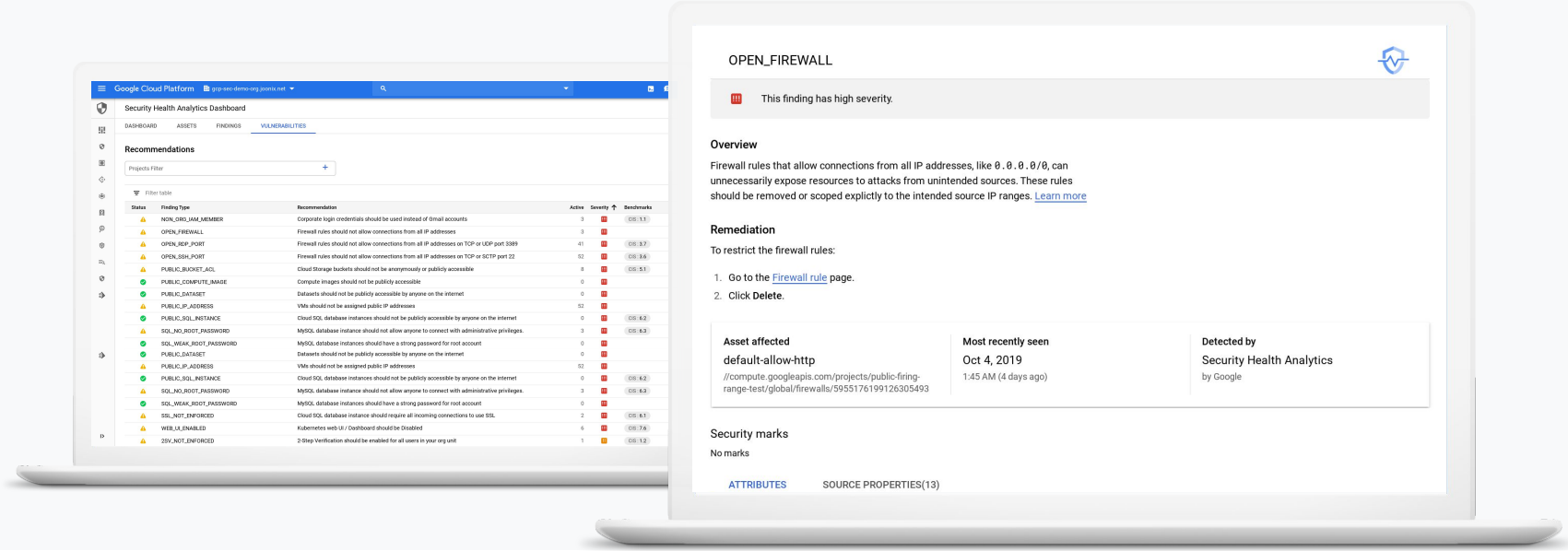


Type	Deleted	New	Total
All	2	23	500
Organization	3	3	50
Project	0	10	40
Application	0	1	30
Service	0	0	30
Address	0	0	20
Disk	0	0	10
Firewall	0	23	5
instance	2	3	4
Network	3	1	3
Route	2	3	2
Subnetwork	1	4	1
Kind	2	3	1
Bucket	3	4	1



Security Health Analytics

Analytics dashboard helps you to view security misconfigurations by severity, CIS Benchmark, or project -- and take action.



Google Cloud

Security Health Analytics Compliance

Standards

- CIS GCP Foundation 1.0
- PCI
- ISO 27001
- NIST 800-53
- More to come...

Dashboard

- Standard specific
- Filterable by resource hierarchy

Reporting

- Standard specific
- Filterable by resource hierarchy
- Exportable to .csv

Security Health Analytics examples of misconfiguration and compliance violations detected

Storage

- Publicly exposed buckets
- 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
- Stackdriver monitoring for Kubernetes clusters not enabled
- VPC Flow logs disabled

VM Instances

- IP forwarding enabled
- SSH and access misconfigurations

GKE Clusters

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

CIS Benchmarks

- Monitoring against the CIS GCP Foundation benchmark
- Certified for CIS Benchmarks 1.0, with more certifications to come

Google Cloud

How Security Health Analytics works in 3 steps

Leverages built-in GCP configurations checks for assets

Processes configurations and monitors for violations

Misconfigurations with actionable recommendations are surfaced in the Vulnerabilities dashboard

Google Cloud

Web application vulnerabilities

Detected by Web Security Scanner for web apps built on Google Cloud Platform

Cross-site scripting

- XSS Callback
- XSS Angular Callback
- XSS Error

Vulnerable resources

- Accessible GIT repository
- Accessible SVN repository
- Insecure library
- Clear text password
- Rosetta flash

Misconfigurations

- Mixed content
- Invalid headers
- Invalid content type
- Misspelled Security Header Name
- Mismatching Security Header Values

Google Cloud

How Web Security Scanner works in 3 steps

Create a scan configuration, telling the scanner where your web app is and where it's not allowed to go.

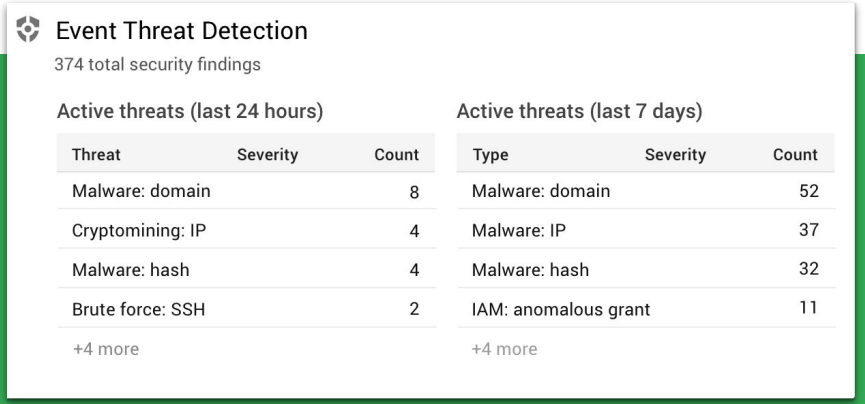
Scans run on the schedule you configure, navigate through your website and attempt to find real vulnerabilities.

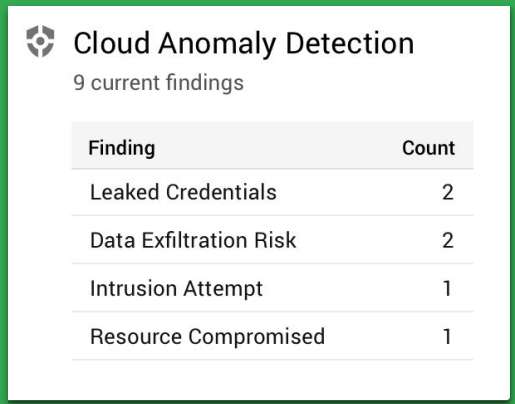
Vulnerabilities are reported in Cloud Security Command Center for review.

Google Cloud

Detect and respond to threats targeting your GCP assets

- Detect compromised machines and other anomalous activity
- Industry-leading threat intelligence surfaces suspicious activity within Stackdriver security logs
- Take action on security risks

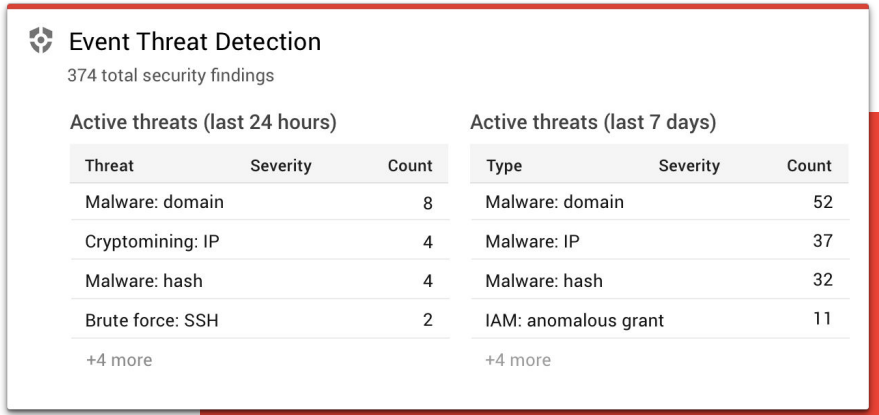




Google Cloud

Event Threat Detection

- Inspired by how Google protects itself
- Powered by industry-leading threat intelligence
- Near real-time detection against platform, network, and compute logs



Google Cloud

Event Threat Detection Current

Malware

Cryptomining

Phishing

IAM abuse

Outgoing DDoS attacks

Bruteforce

Leaked credentials

Hijacked accounts

Compromised machines

Google Cloud

How Event Threat Detection works in 3 steps

- Cloud Audit Logs
- VPC Flow logs
- Cloud DNS logs
- syslog via fluentd

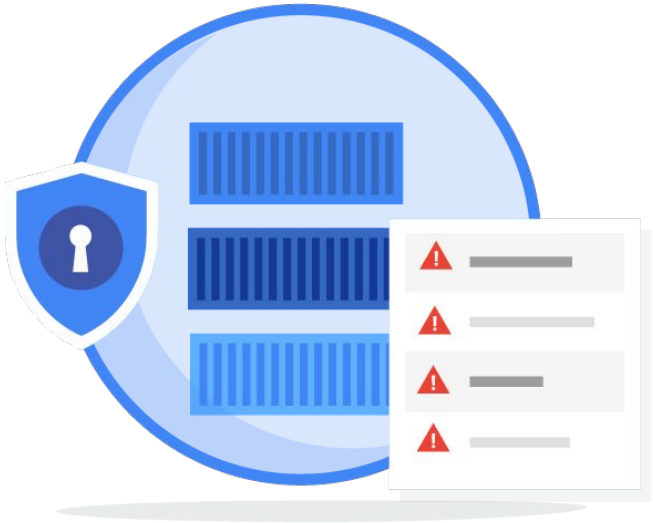
Processes logs using Detection Logic + Google Threat Intelligence

Remediate findings in **Security Command Center** using **Cloud Pub/Sub** and **Cloud Functions**

Google Cloud

Container Threat Detection Beta detects common threats against containers

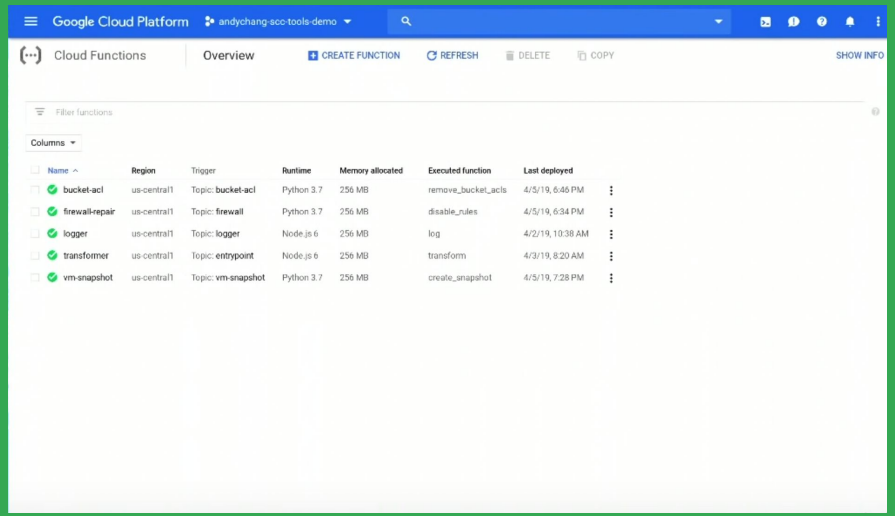
- Kernel-level detection for top attacker techniques
  - Execution of added binaries
  - Execution of new library linking
  - Opening shells to the Internet
- Integrations with
  - Cloud Security Command Center
  - GKE for one-click deployment
- Kernel integrations available in COS
- Managed daemonset deployment



Google Cloud

Alert and respond to threats targeting your Google Cloud Platform resources

- Define a query that generates a Cloud Pub/Sub event
- Build or leverage existing Cloud Functions on GitHub to take specific actions on Cloud Pub/Sub events

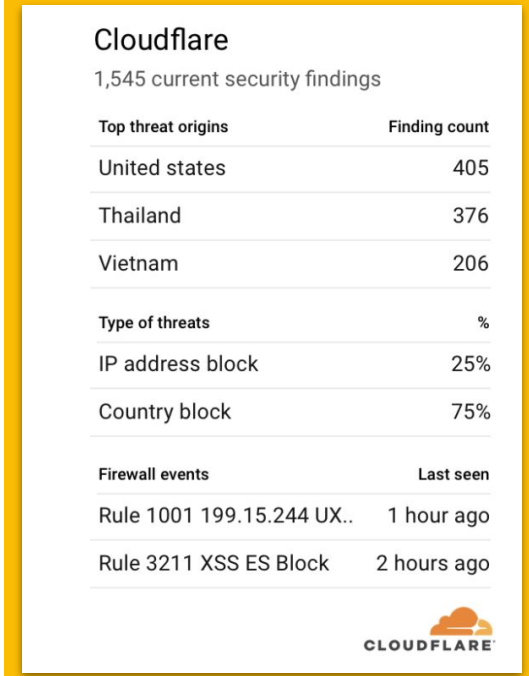


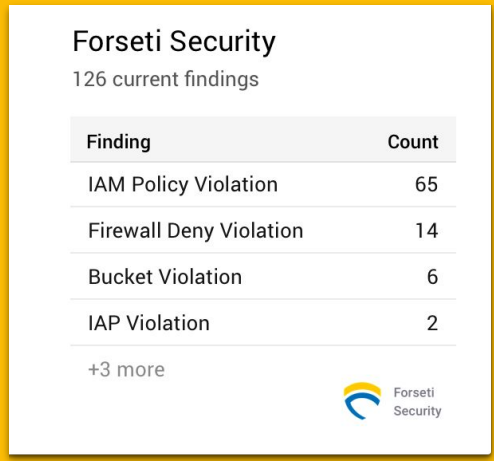
Google Cloud

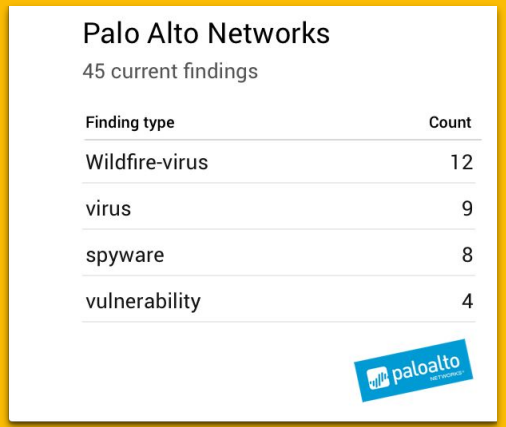
Integrate with your heterogenous, multi-platform environment

- Leverage the Command Center REST API or console to access assets and findings and easily integrate with existing systems
- Export findings to your SIEM
- Take advantage of existing partner solutions you're using on-premises and use them in Google Cloud

Google Cloud







SCC supports findings from Google security products and partner security products

Google


Binary Authorization


Cloud DLP API


Cloud Security Scanner


Forseti


Google Anomaly Detection


Event Threat Detection


Security Health Analytics


Cloud Armor

Partners

Google Cloud

Cloud Security Command Center is the cloud security posture management tool for Google Cloud Platform that helps you prevent, detect, and respond to threats.

Google Cloud

Thank you

Google Cloud