



Google Cloud Security Overview

March 2024



Trusted
Cloud
Platform



Frontline
Intelligence
& Expertise

Modern Security
Operations
&
Cloud Security
(CNAPP++)



+ Supercharging with AI

Address threats, toil, talent

Google: a Leader in IaaS Platform Native Security

Of the 8 vendors evaluated, Google Cloud scored the **highest rating in the strategy category**, and received the highest total number of 5 out of 5 scores across the Wave's current offering, strategy, and market presence criteria.

In the current offering category, Google Cloud received the **highest scores possible** in: data centers, security certifications, administrative IAM, hypervisor security, guest OS security, container security, and network security.

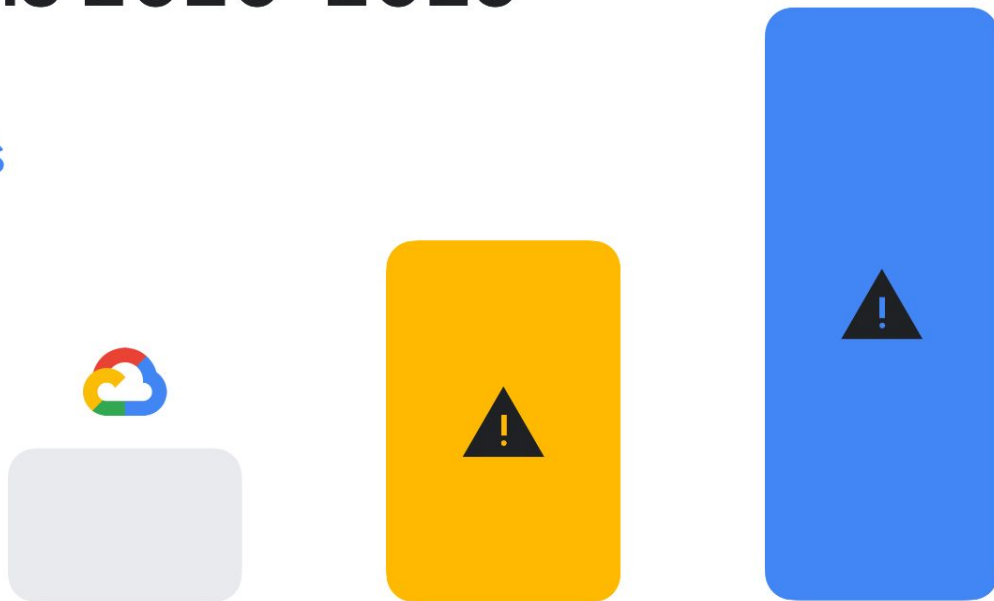
Google Cloud also received the **highest scores possible** in the strategy category criteria of: vision, market approach, planned enhancements, innovation, delivery model, and commercial model.



The Forrester Wave™: IaaS Platform Native Security Q2 2023. The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources.³ Opinions reflect judgment at the time and are subject to change.

Critical and high severity security vulnerabilities in cloud platforms 2020-2023

75%, 60% fewer than
other major providers

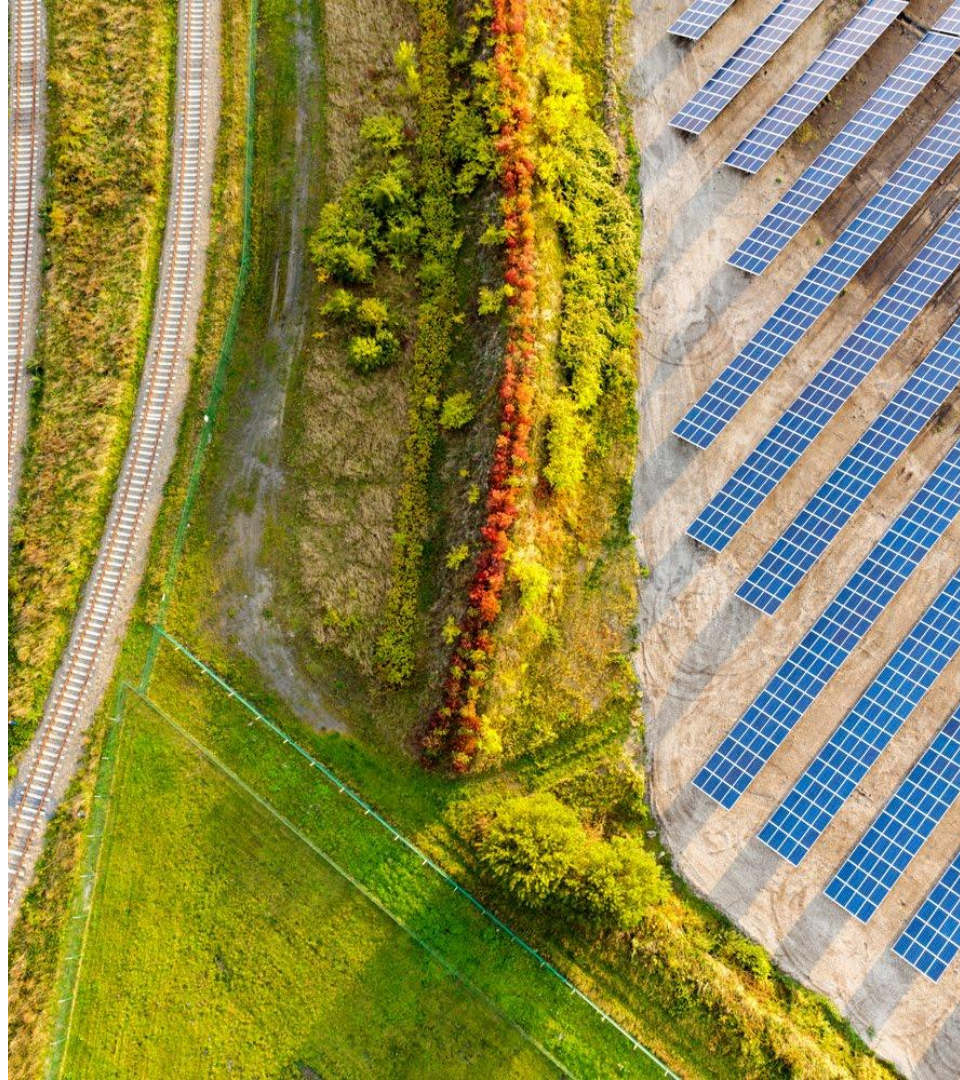


The Difficulties of Compliance

Keeping up with the world

Regulatory compliance needs to keep up with the pace of change in technology, geo-politics, and new security threats. Today customers face:

- Reactive responses to changes
- Shifting technology, processes, and procedures creates toil
- New approaches are difficult for regulators to accept








In 2020 Google Launched Assured Workloads

Confidently secure and configure sensitive workloads to support your compliance and security requirements in the cloud. Choose your security settings, and we'll put the necessary cloud controls in place.



Assured Workloads Behind the Scenes

Assured Workloads Layers Control into Existing Products and Services

	Data residency controls	<i>Data residency controls to remove global APIs and regionalize at rest, in process, and in transit operations.</i>
	Data access controls	<i>Data access paths are mapped and access controls are put in place to restrict based on the customers selected compliance.</i>
	Key Management	<i>Customers have the ability to manage their keys on or off Google Cloud to meet their security and compliance needs.</i>
	Access control and Access Transparency	<i>Administrative access to customer data and workloads is logged, audited, and permitted only under predefined support conditions</i>
	Service Usage Restrictions	<i>Restrict developers from using non-compliant products & services</i>




Controls Backed with Contractual Commitments and Transparency

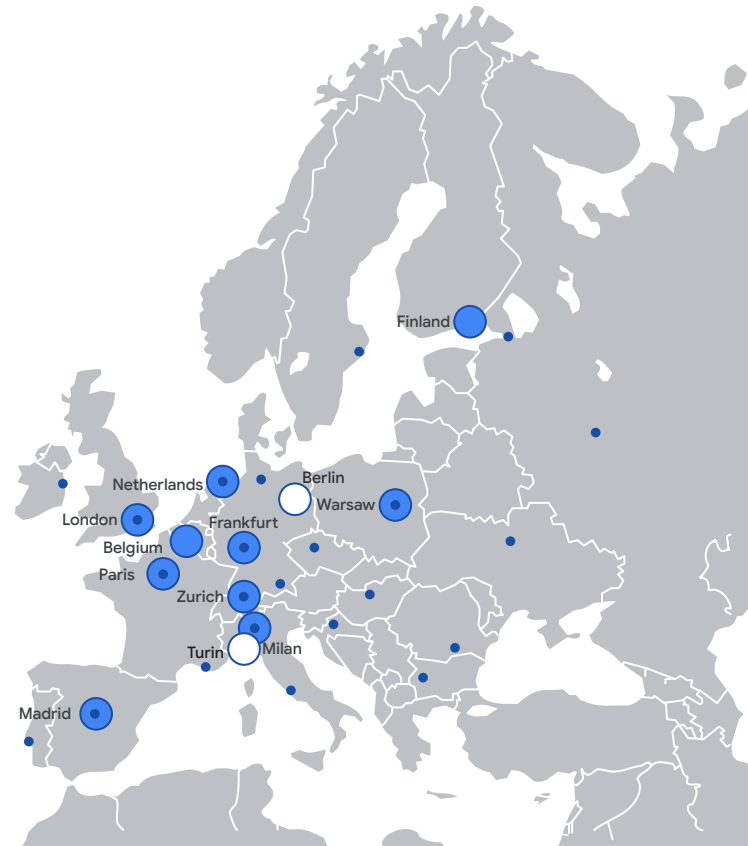
Data Residency ensures that customer data remains in a local region

Data residency

Control Function:

Customer data will be stored at rest in the selected Google Cloud region and restricted from moving outside of the region.

-  Current region with 3 zones
-  Future region with 3 zones
-  Edge point of presence



Assured Workloads Setting Precedent

- Granted provisional authority to operate by the Defense Information Systems Agency of the **US government for Impact Levels 4 and 5.**
- Regulators recognized personnel access controls, data residency, and encryption capabilities of the highest level could provide a more secure computing environment for sensitive data than a GovCloud.
- **Driving to meet the needs of all levels of EUCS**



Trusted
Cloud
Platform



Frontline
Intelligence
& Expertise

Modern Security
Operations
&
Cloud Security
(CNAPP++)



+ Supercharging with AI

Address threats, toil, talent

Applied curated + community-sourced threat intel

500+

threat intelligence analysts

1000+

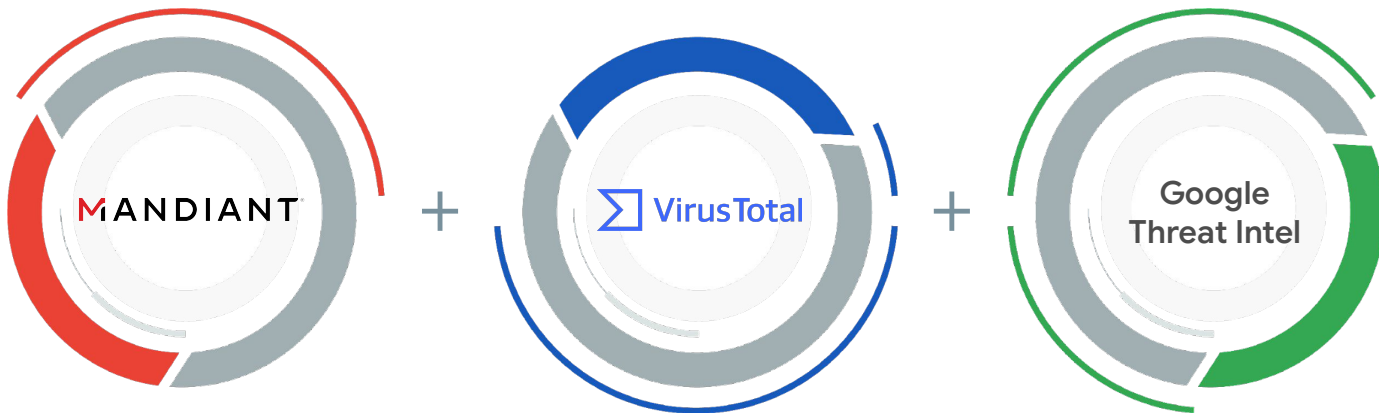
state-sponsored threat clusters tracked

2.4B+

files in VirusTotal dataset

40B+

Gmail files scanned daily

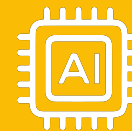


Google delivers
trustworthy,
relevant and
current threat
intelligence

**Broadest Threat
Visibility**

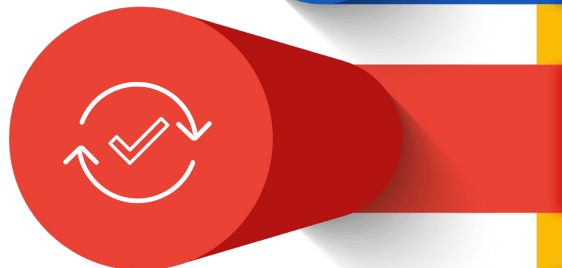
MANDIANT

VIRUSTOTAL



AI that just
works

**Trusted Threat
Intel Expertise**



**Next-Gen
Operationalization**



Mandiant Consulting Services

Our approach addresses business challenges and increases cyber resilience

Incident Response

Resolve incidents quickly and get back to business



Strategic Readiness

Improve capabilities against future compromise



Technical Assurance

Test controls and operations with real-world attacks



Cyber Defense Transformation

Develop and mature security posture with improved operations and capabilities



Bringing the power of Google and Mandiant to modernize security operations



Leading threat intelligence from the frontlines

Together, Google Cloud & Mandiant bring intel from the frontlines across GCTI, VirusTotal & 800+ Mandiant researchers in 26 countries



Bringing the power of Google Cloud + Mandiant to SecOps

Google Cloud Security Operations combined with Mandiant Advantage enables teams to detect, investigate & respond to cyber threats with speed, scale, expertise & intelligence



Access to expertise when you need it

Frontline expertise to help organizations transform their cyber defense to mitigate threats & reduce business risk - before, during and after an incident

Industry Threat Scores

2023 INDUSTRY CYBER THREAT SCORES

Frequency measures how often a given sector is perceived to be targeted.

Magnitude measures the severity of observed threats by considering factors including the proportion of observed targeted intrusions, notable threat actor tactics or sophistication, observed impact of incidents for the victim.

	FIN		IO/HACK		STATE		Weighted Score
	FREQ	MAG	FREQ	MAG	FREQ	MAG	
Governments							9.0
Financial Services							8.3
Technology							8.1
Legal & Professional Services							5.5
Media & Entertainment							5.4
Healthcare							5.4
Education							5.1
Manufacturing							5.1
Civil Society & Non-Profits							4.8
Telecommunications							4.6
Energy & Utilities							4.6
Oil & Gas							4.2
Construction & Engineering							4.1
Transportation							4.1
Retail							4.0
Aerospace & Defense							3.8
Chemicals & Materials							3.0
Hospitality							3.0
Pharmaceuticals							2.8
Insurance							2.5
Automotive							2.2



Industry Threat Scores Over the Last 4 Years

	2020	2021	2022	2023
Governments	5.8	7.8	8.6	9.0
Financial Services	6.1	5.9	5.9	6.3
Technology	4.3	5.6	5.8	6.1
Legal & Professional Services	4.6	4.6	3.3	5.5
Healthcare	3.2	3.9	5.1	5.4
Media & Entertainment	4.6	4.8	4.4	5.4
Manufacturing	5.6	5.2	5.2	5.1
Education	3.8	5.2	5.0	5.1
Civil Society & Non-Profits	3.2	4.2	5.0	4.8
Telecommunications	4.1	4.6	4.8	4.6
Energy & Utilities	5.0	4.9	3.6	4.6
Oil & Gas	4.2	3.9	3.6	4.2
Transportation	3.0	4.9	5.2	4.1
Construction & Engineering	3.5	3.9	3.4	4.1
Retail	4.2	4.3	4.0	4.0
Aerospace & Defense	3.4	3.8	3.8	3.8
Hospitality	4.2	2.6	3.0	3.0
Chemicals & Materials	2.7	2.7	2.9	3.0
Pharmaceuticals	2.9	4.1	3.5	2.8
Insurance		2.7	2.7	2.5
Automotive	2.7	3.0	3.0	2.2

Trusted
Cloud
Platform



Frontline
Intelligence
& Expertise

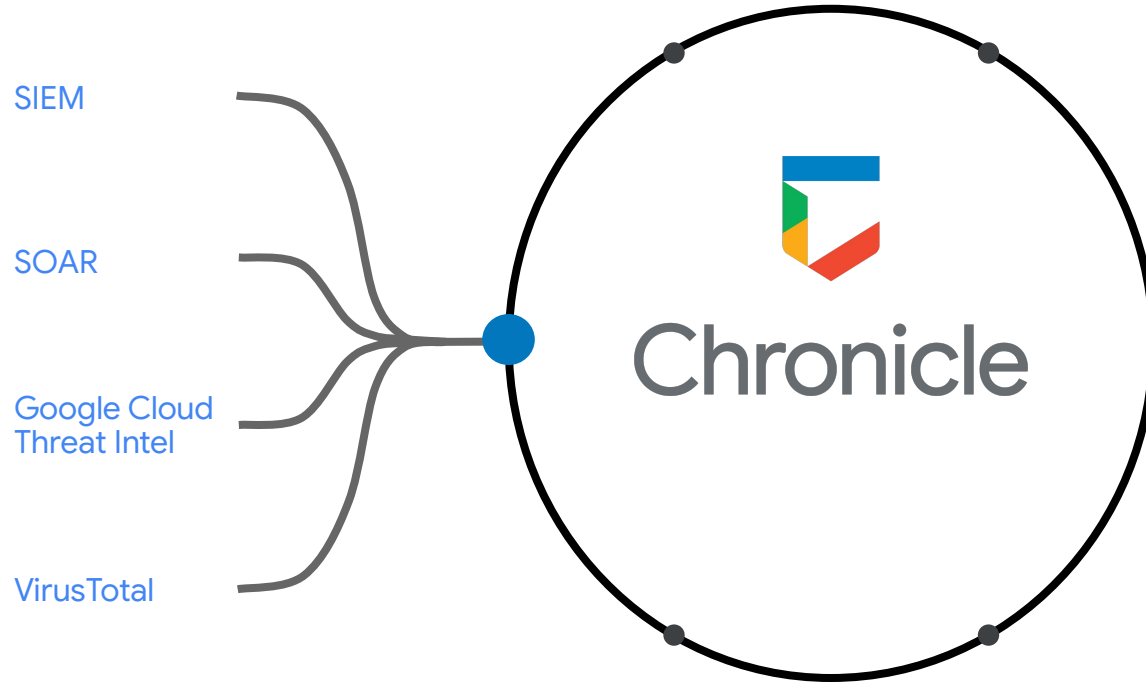
Modern Security
Operations
&
Cloud Security
(CNAPP++)



+ Supercharging with AI

Address threats, toil, talent

Google Cloud Security Operations



Bringing the power of Google and Mandiant to modernize security operations



The Chronicle Difference



Google Scale and Speed

Eliminate security blind spots by ingesting, normalizing, analyzing and searching all security telemetry at Google scale and speed

20x Faster searches

Source: Product documentation, August 2023



Applied Threat Intelligence

Proactively uncover and defend against **novel attacks** in near real-time without extensive custom engineering.

Curated outcomes apply Google's vast threat and exposure visibility to your unique environment.

20x More real-time detections

Source: Product documentation, August 2023



AI-Infused Productivity

Elevate your team's talent and productivity with a **unified platform** infused with generative AI and expert help when you need it before, during and after an incident.

10x Faster investigations

Source: Internal Google Testing, Aug 2023

Applied Threat Intelligence

Market-Leading
Threat Intelligence



Google Cloud

MANDIANT  VIRUSTOTAL

Applied to Your
Environment

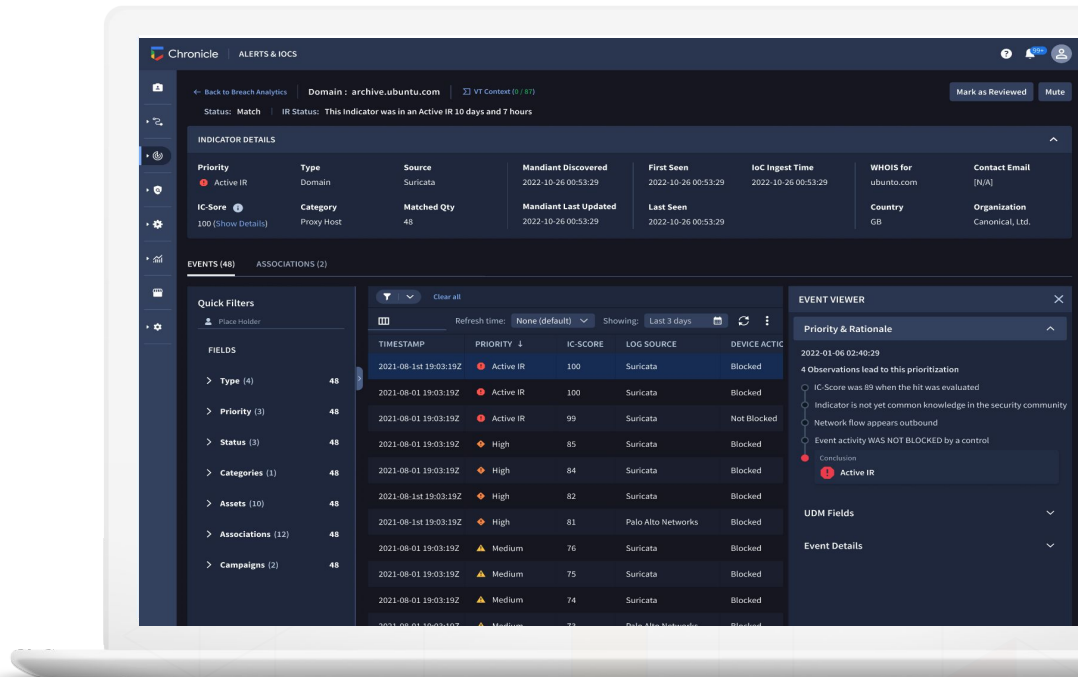
Turnkey
Actionable
Near real-time
“No patient 1”

Seamlessly applied to your environment

Auto-enrich every event with the latest threat intelligence from Google to eliminate blind spots

Focus on the most critical threats with **ML-based prioritization** that combines threat insights with your unique environment

Near real-time notifications of potential **active breach threats** from Mandiant's frontline investigations



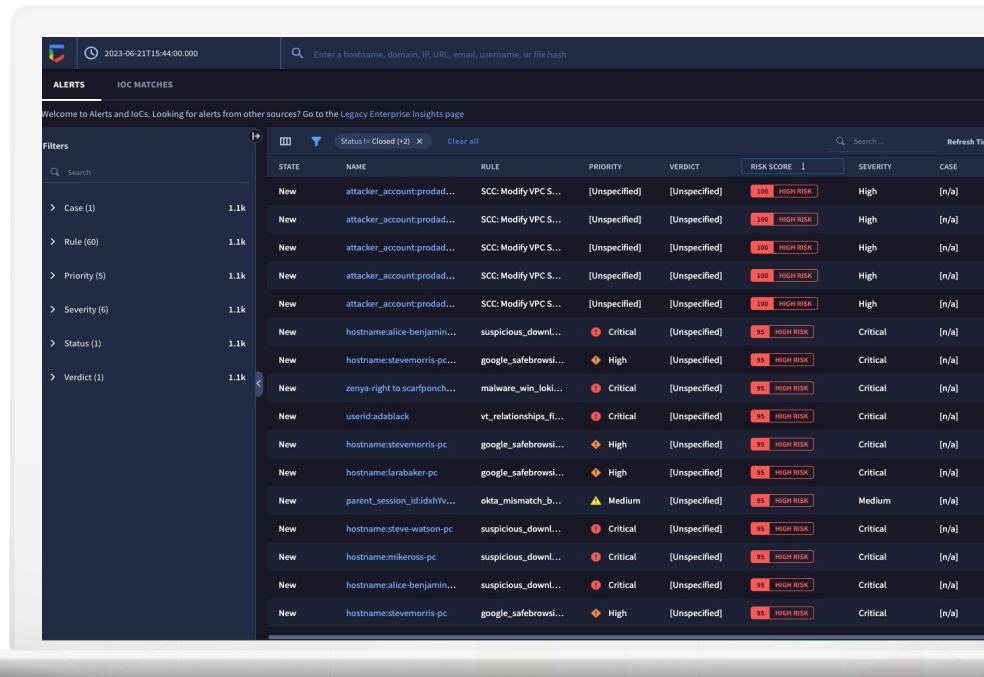
Detect threats with confidence

Leverage **curated detections** by Google to detect the latest threats and **map** them to MITRE ATT&CK

Simplify detection authoring with YARA-L to **build custom content**

Receive early warning signals of potential threats with seamless matching of active breach intelligence from Mandiant investigations

Identify potentially exploitable entry points accessible to attackers with attack surface management (ASM) integrations



Investigate with insights at your fingertips

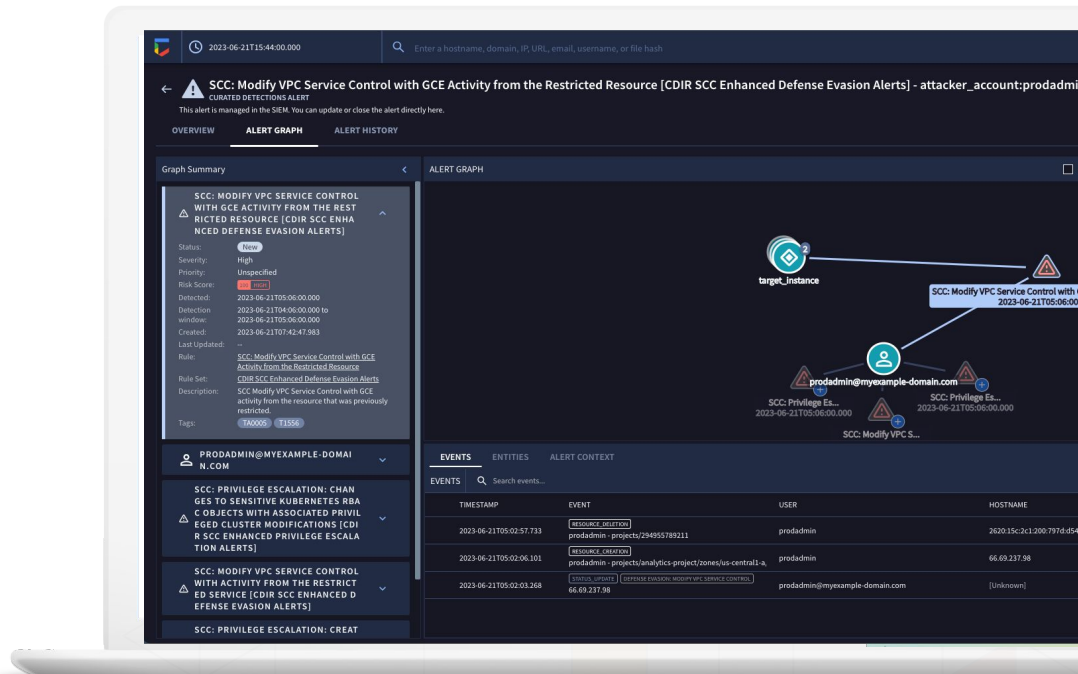
Analyze real time activity with investigation views, visualizations, threat intel insights, and user aliasing

Investigate with **full context at your fingertips** including anomalous assets and domain prevalence and more

“Google search” petabytes of data at lightning speed

Manage, prioritize and assign work with unique threat-centric case management

Seamlessly pivot between cases, alerts, entities and detections with a unified experience across the entire TDIR workflow

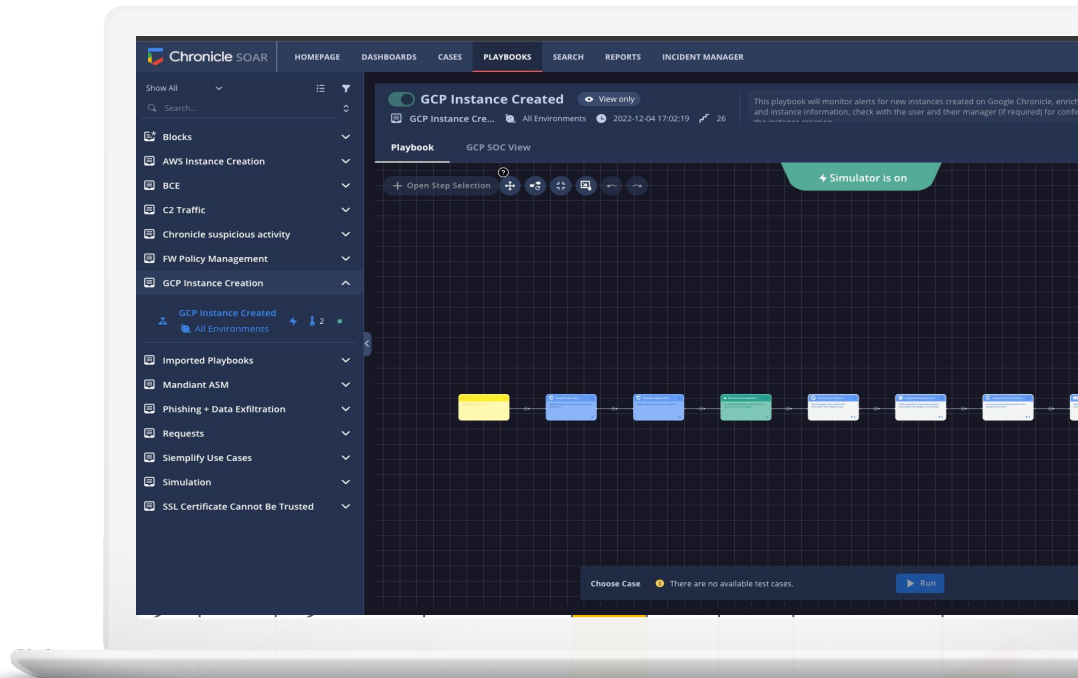


Respond with speed and precision

Drive consistency in your response and automate repetitive tasks with a full-featured intuitive playbook builder and 300+ integrations

Easily collaborate on every case with fellow analysts, service providers, and other stakeholders

Respond to incidents with stakeholders inside and outside the SOC (legal, PR, HR) in a secure “war-room”

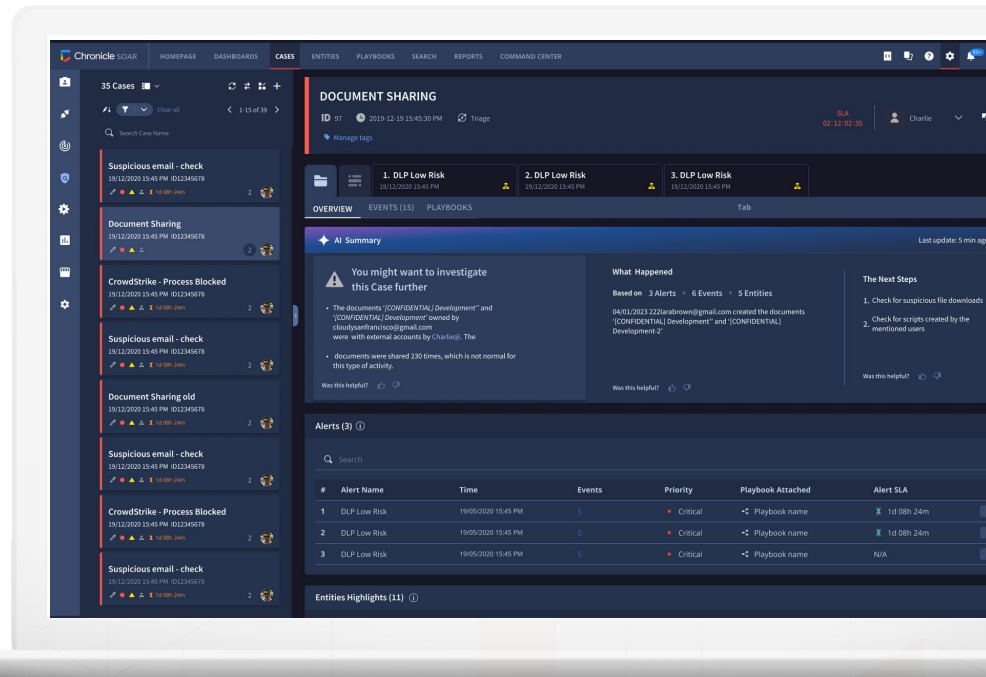


Supercharge productivity with Duet AI

Natural language search your data, iterate and drill down. Duet AI generates underlying queries and presents full mapped syntax.

Investigate more efficiently with **AI-generated summaries** of what's happening in cases, along with recommendations on how to respond.

[COMING SOON] Interact with Chronicle using a **context-aware AI-powered chat**, including the ability to create detections and playbooks.



CNAPP- where we've been

SCC 2023 Strategic Deliveries



GCP First Detection

Leverage specialized GCP telemetry to perform centralized correlation and analytics for GCP threats, misconfigs & vulnerabilities

Leverage Mandiant to create a more complete GCP protection offering



Intelligent Risk Scoring

System level risk is scored and can be evaluated

Creating detailed level workload/asset risk scoring that combines finding signals & entities

Advance RPP success



Security Governance

Create capabilities for the management of the security lifecycle

Leverage core GCP componentry

Integrate with existing Customer practices



Platform Scale

Ensure the platform meets customers' growing scale, resilience, performance, usability and GCP horizontal needs

Raising the Bar on GCP Threat Detection

Better Signals

- Network Fabric Logs
- Agentless Disk Snapshots
- CloudRun Fabric Events
- GKE eBPF



Raising the Bar on GCP Threat Detection

Better Threat Intelligence

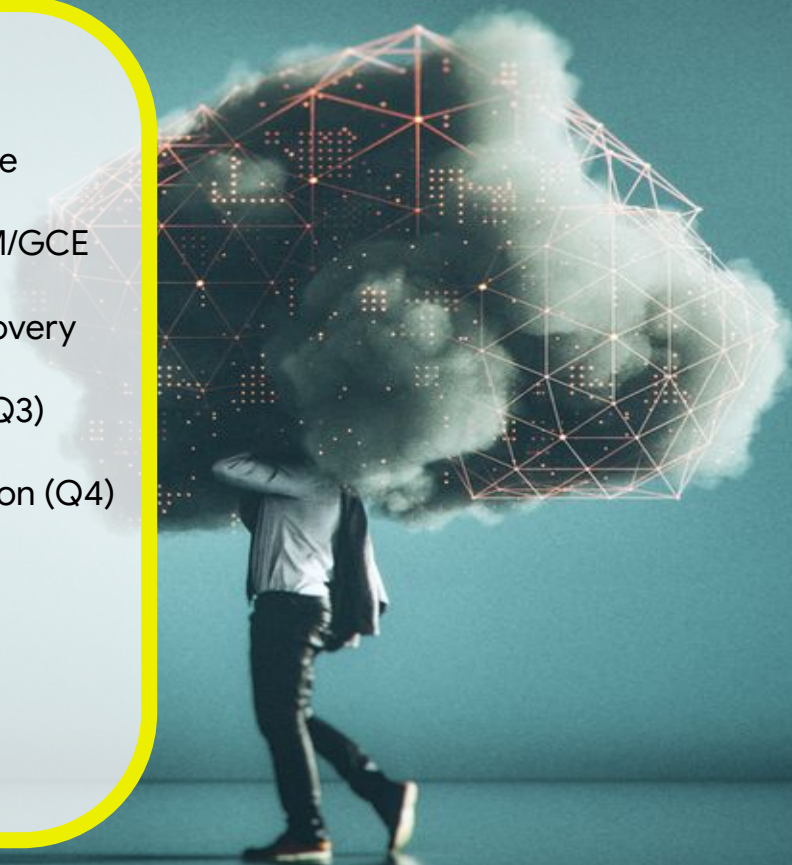
- Mandiant Threat Intel
- Mandiant YARA Rules
- GCTI Brokerage + YARA-L
- Scaled Honeypots
- GKE Security Research



Raising the Bar on GCP Threat Detection

Better Detection

- Service & IAM Account Compromise
- Custom ETD Modules–Network/IAM/GCE
- Google Cloud Backup Disaster Recovery
- Cloud IDS & GKE Security Posture (Q3)
- Zero-log Mandiant Malware Detection (Q4)
- CloudRun ETD (Q4)
- CloudRun KTD (Q2 24)
- New GKE ETD & KTD Detections



Risk as the Lens of Cloud Security



Model Generation

A graph model of your Google Cloud environment is automatically generated based on environment data



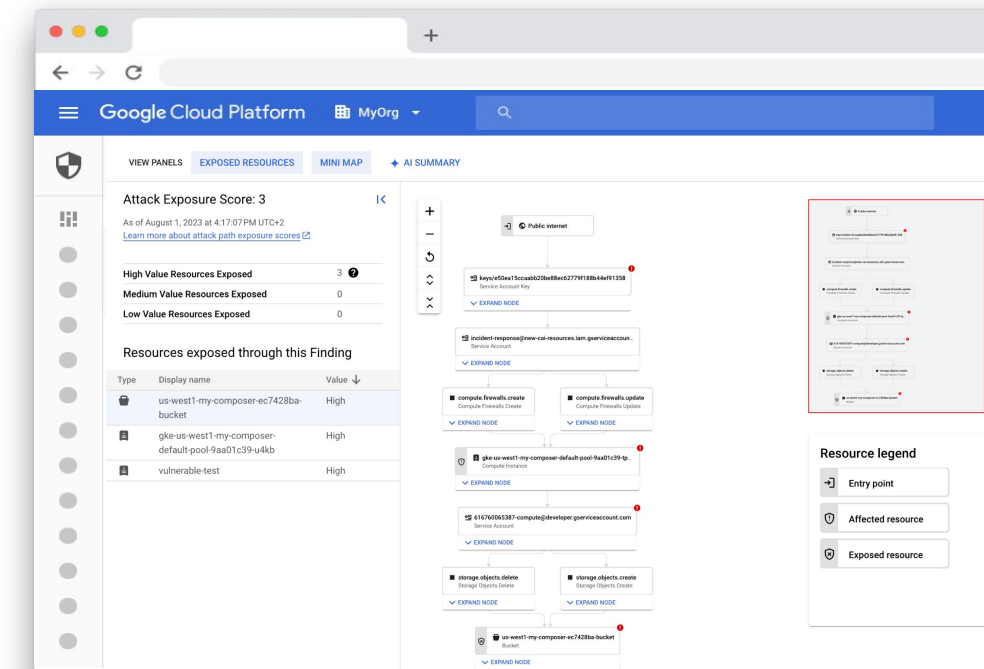
Attack Path Simulation

Automatic attack path simulations are performed on possible combinations of actions and attacks



Exposures and Mitigations

Insights on attack exposure scores, attack paths to your valuable resources, and key mitigation actions





CNAPP

Proactive, runtime
protection

Next horizon market for
Cloud Security

SecOps

Defensive Detection &
Response

First horizon market for
Cloud Security

Where we're going: Not Your Grandma's SCC

In 2024 SCC will be a comprehensive, multi-Cloud
CNAPP product.

We are leveraging the breadth of functionality we
have in Google Cloud Security: SIEM, SOAR,
Attack Surface Management, Policy Intelligence,
Mandiant TI and more...



One More Thing



Democratize
security with
AI.



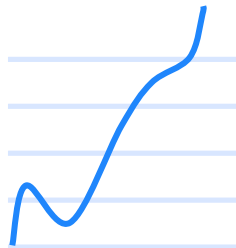
Top 3 Security Challenges over the last decade

GROWING

threats



Unabated Increase
(especially w/
LLMs)



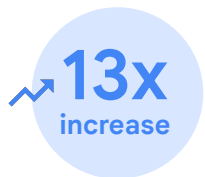
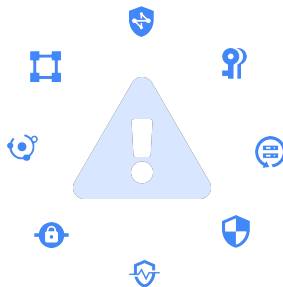
781 data breaches in
2012 totaling \$146M.
6,000 last year
totaling \$6T. ² ♦

ENDLESS

toil



Endless toil
make things
secure



2,000 cybersecurity
companies in 2012 to
26,000 today. ¹ ♦

LACKING

talent



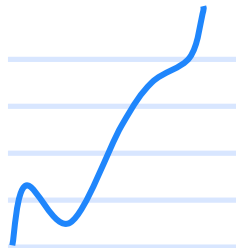
Dearth of
experts



Up from 1.5M unfilled
cybersecurity jobs in
2012 to 3.5 million
today. ³ ♦

What If ...

GROWING threats

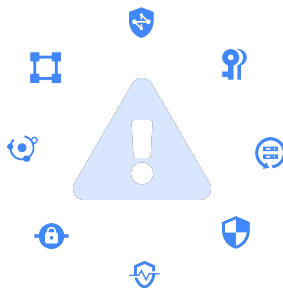


On a Novel Threat, combine
World-class TI +AI

**Quickly
identify &
prevent Patient
Ones**



ENDLESS toil



If code can be
generated, why not
also generate the
security controls?

**Systems
secure
themselves**



LACKING talent



Can any developer or IT person
become a security specialist with
a “Security AI Assistant”

**Democratize
Security
Expertise**

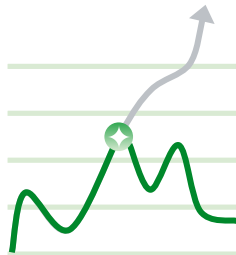


Delivering Step-function Outcomes with AI Innovations + World-Class TI

STOPPED threats



Quickly
identify &
prevent
Patient Ones



LESS toil



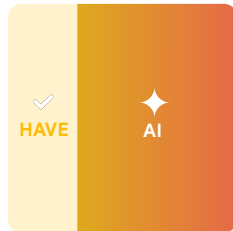
Systems
secure
themselves



SCALED talent



Democratize
Security
Expertise



AI-powered remediation with Frontline Threat Intel



Insights

Event	Correlation	Insight
1 Traffic Spike	192.168.1.1	More than 2,000,000 request
2 Brute force	Texas	More than 700 bad scores fr

Auto generated security controls, policies and configs

```
$ yarn pretty-quick
```

Novices become experts

ATTACK PATH SUMMARY



AI capabilities to tackle primary security challenges

Threats



VirusTotal Code Insight

Democratize malware analysis and flag unknown threats



Breach Analytics for Chronicle

Automatically find bad actors using novel techniques before you become the next victim

Toil



Assured Open Source

Leverage AI to be first to find critical vulnerabilities and malicious code submissions



Duet AI in Mandiant Threat Intelligence

Expedite risk assessment & operationalization of threat profile

Talent



Duet AI in SecOps

Put investigation expertise in the hands of every user to uncover threats at lightning speed



Duet AI in Security Command Center

Expedite risk assessment & improve customer defenses

Our Unique Security AI Platform + Apps Approach





Thank you.

