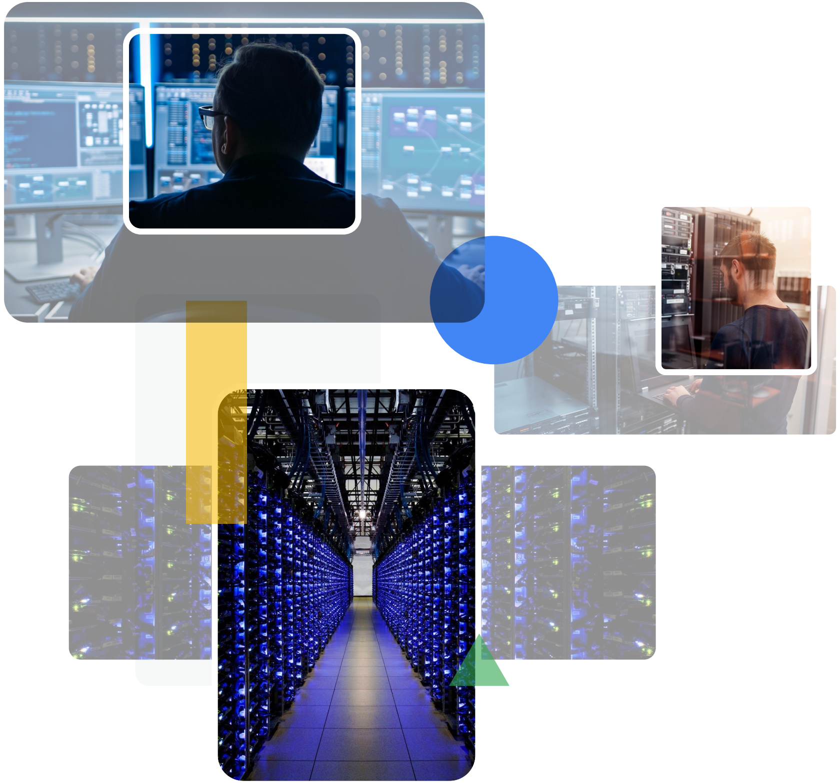
So you want to solve cloud security

Helping Carahsoft customers sleep better at night knowing their digital infrastructure is protected



Google Cloud

Your Google Cloud Security Team

Alex Popp
Security Partner Manager
alexpopp@google.com
650 999 1453

Casey Cesca
ReCaptcha Channel Manager
caseycraig@google.com

Agenda

1 How to introduce security your customers

2 Security Command Center Premium

3 Chronicle

4 ReCaptcha

5 BeyondCorp

6 Sales Plays

3:00p

How to introduce security

Every customer cares about security, but it's a daunting subject

3:05p

Security Command Center Premium

Protect your customer's google cloud workloads by providing them insights to possible threats and vulnerabilities.

3:20p

Chronicle

Improve your customers' security analysts productivity by leveraging the scale and speed of google inherent to our threat hunting platform.

4:00pm

ReCaptcha.

Protect your customer's web and mobile applications from bot attacks and fraud.

4:20pm

BeyondCorp

Customers asking about zero trust? Expand their security policies to the browser and ensure remote access to applications are continuously protected.

4:45pm

Sales Plays

Upsell your existing spending customers, or position the end to end platform early in the commit or recommit conversation

If you only have 5 minutes....

SUMMARY
SUMMARY
SUMMARY

Every customer cares about security, but it’s a daunting subject

- Organizations don’t have the talent in house, and can’t keep up with the increasing complexity of threats
- Main challenges: lack of visibility, inability to detect & deter external threats, mishandling of access policies

GCP is unique as a security vendor because we are in the best position to protect our cloud services:

- Cloud Posture Management: Security Command Center Premium
- Threat Detection: Chronicle
- Zero trust: Beyondcorp
- User & Fraud Protection: ReCaptcha

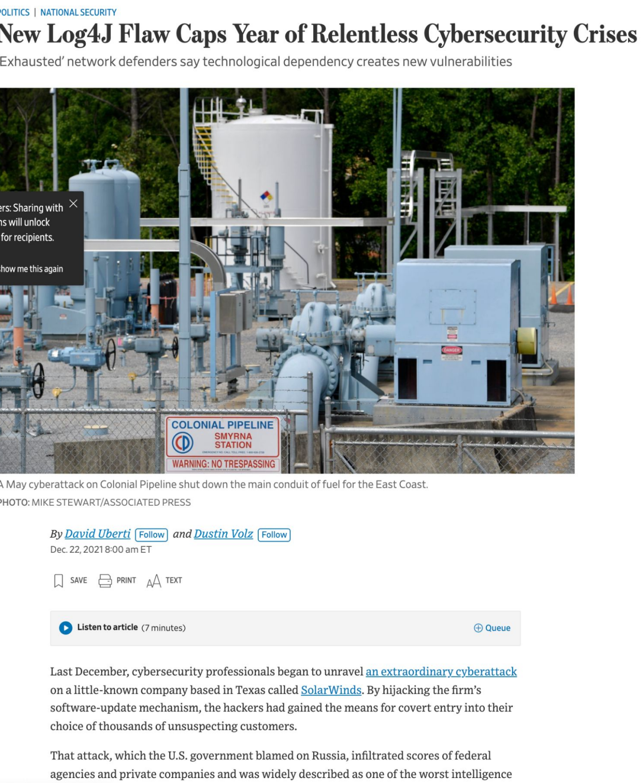
Sales process starts with the same personas you serviced for cloud migrations

- CIOs & CTOs (who champion cloud strategy) are both technical decision maker & economic buyers
- Next Steps: identify accounts, move forward in pre-sales efforts

How to introduce security to your customers

Google Cloud

Security is top of mind



OLITICS | NATIONAL SECURITY

New Log4J Flaw Caps Year of Relentless Cybersecurity Crises

Exhausted' network defenders say technological dependency creates new vulnerabilities

A May cyberattack on Colonial Pipeline shut down the main conduit of fuel for the East Coast.
PHOTO: MIKE STEWART/ASSOCIATED PRESS

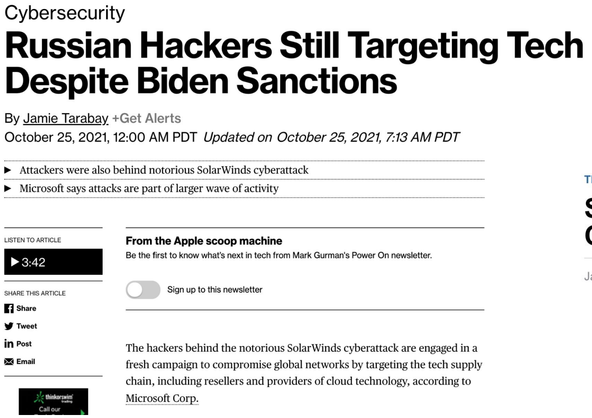
By *David Uberti* Follow and *Dustin Volz* Follow
Dec. 22, 2021 8:00 am ET

SAVE PRINT TEXT

Listen to article (7 minutes) Queue

Last December, cybersecurity professionals began to unravel an extraordinary cyberattack on a little-known company based in Texas called SolarWinds. By hijacking the firm's software-update mechanism, the hackers had gained the means for covert entry into their choice of thousands of unsuspecting customers.

That attack, which the U.S. government blamed on Russia, infiltrated scores of federal agencies and private companies and was widely described as one of the worst intelligence



Cybersecurity

Russian Hackers Still Targeting Tech Despite Biden Sanctions

By Jamie Tarabay +Get Alerts
October 25, 2021, 12:00 AM PDT *Updated on October 25, 2021, 7:13 AM PDT*

- Attackers were also behind notorious SolarWinds cyberattack
- Microsoft says attacks are part of larger wave of activity

LISTEN TO ARTICLE
▶ 3:42

SHARE THIS ARTICLE
Share
Tweet
Post
Email

From the Apple scoop machine
Be the first to know what's next in tech from Mark Gurman's Power On newsletter.

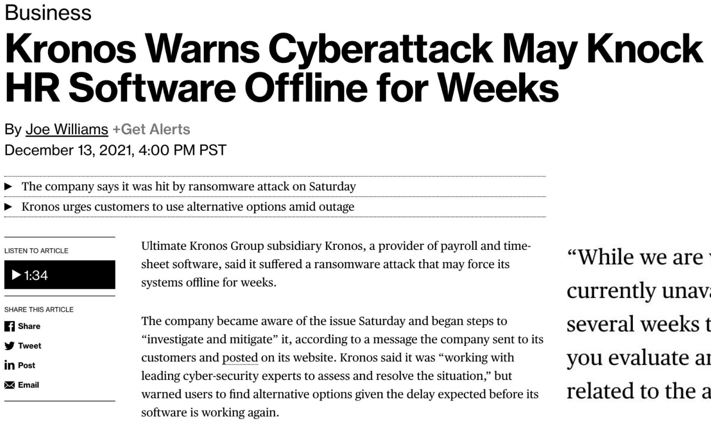
Sign up to this newsletter

The hackers behind the notorious SolarWinds cyberattack are engaged in a fresh campaign to compromise global networks by targeting the tech supply chain, including resellers and providers of cloud technology, according to Microsoft Corp.

TECHNOLOGY | Commodities | News Wire | Company News Oct 25, 2021

SolarWinds Hackers Targeting Tech Supply Chain, Microsoft Says

Jamie Tarabay, Bloomberg News



Business

Kronos Warns Cyberattack May Knock HR Software Offline for Weeks

By Joe Williams +Get Alerts
December 13, 2021, 4:00 PM PST

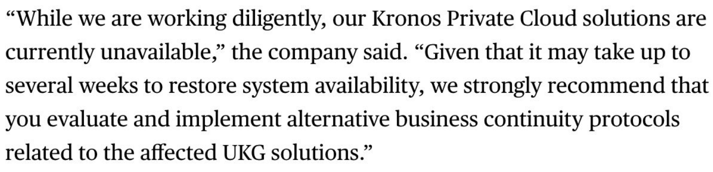
- The company says it was hit by ransomware attack on Saturday
- Kronos urges customers to use alternative options amid outage

LISTEN TO ARTICLE
▶ 1:34

SHARE THIS ARTICLE
Share
Tweet
Post
Email

Ultimate Kronos Group subsidiary Kronos, a provider of payroll and time-sheet software, said it suffered a ransomware attack that may force its systems offline for weeks.

The company became aware of the issue Saturday and began steps to "investigate and mitigate" it, according to a message the company sent to its customers and posted on its website. Kronos said it was "working with leading cyber-security experts to assess and resolve the situation," but warned users to find alternative options given the delay expected before its software is working again.



"While we are working diligently, our Kronos Private Cloud solutions are currently unavailable," the company said. "Given that it may take up to several weeks to restore system availability, we strongly recommend that you evaluate and implement alternative business continuity protocols related to the affected UKG solutions."

Google Cloud

Market Context: Exponential Increase in attack vectors & malicious third parties

Work from home / hybrid policy means traditional approach of security is dead

↓

Uptick in identity theft, fraudy, network compromised

New types/never been seen before methods, tactics, hacker behaviors

↓

increase in number and complexity of cyber threats

Explosion of security data & logs that need to be parsed, indexed, and readable by analyst teams

↓

Difficult to detect threats as close to real time as possible (and respond to them!)

How to introduce security to your customers?

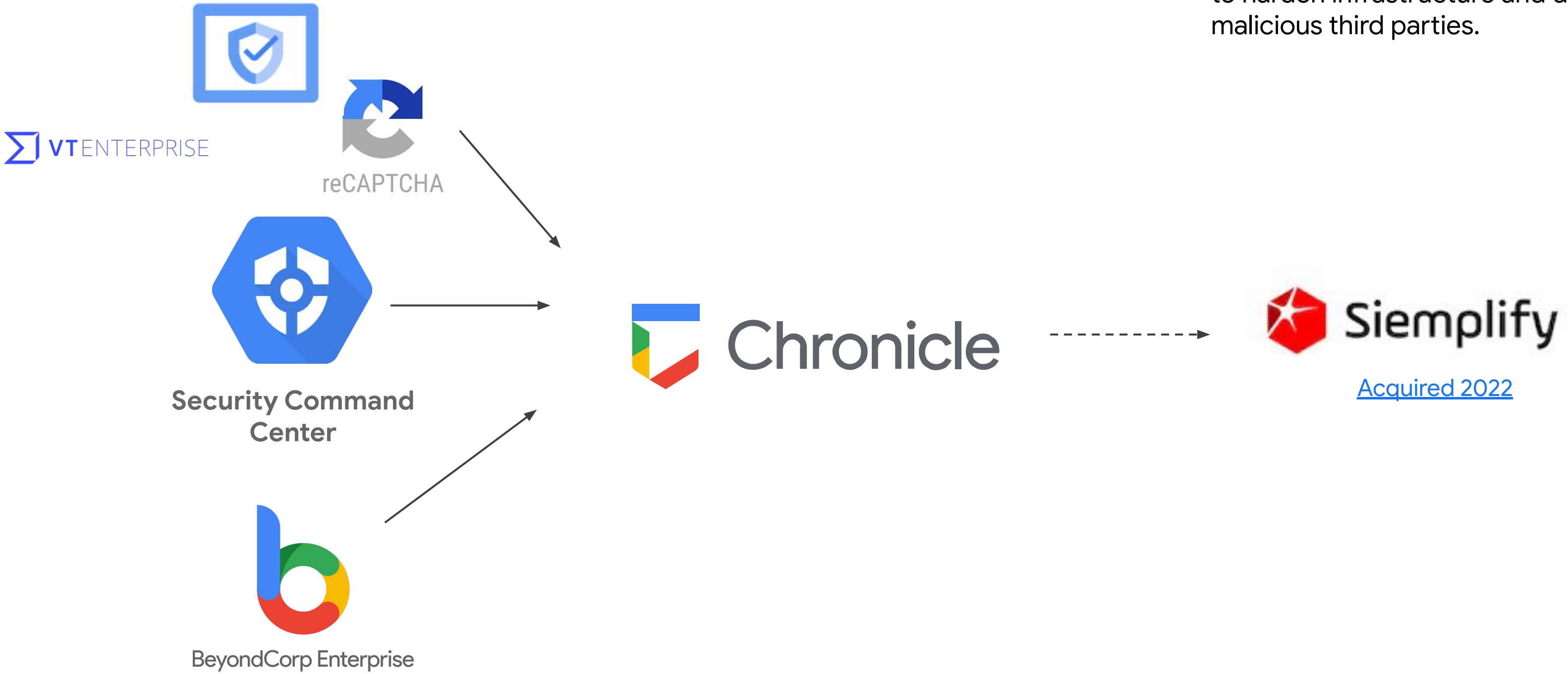
- How do you maintain **real-time visibility into your cloud workloads**?
- How do you **maintain compliance** with third party frameworks?
- How do you **manage your cloud's security posture**?
- How do you **enable your employees & contractors to remotely & securely connect** to internal apps?
- How do you **hunt & respond to attacks** against your **digital infrastructure (multi/mono/hybrid cloud)**?
- How do you **protect your website and/or mobile apps** from bots and fraud?

Google Security Portfolio

Capture user, infrastructure, security telemetry...

...Proactively detect and hunt threats...

... and automate + orchestrate response playbooks to harden infrastructure and defend from malicious third parties.



VTENTERPRISE

reCAPTCHA

Security Command Center

BeyondCorp Enterprise

Chronicle

Siemplify

[Acquired 2022]

SCC Premium

High Level Points

What is it?

The best view anyone can ever have of their GCP environment.

What does it solve fr?

- Track your assets and their use
- Detect vulnerabilities
- Identify threats
- Keep compliant
- Will help customers save money (stolen credentials -> stolen resources, breaches -> lawsuit/fines)

Differentiator

No other product on the market has the level of depth and visibility of GCP because it is instrumented at hypervisor level

When should I discuss it?

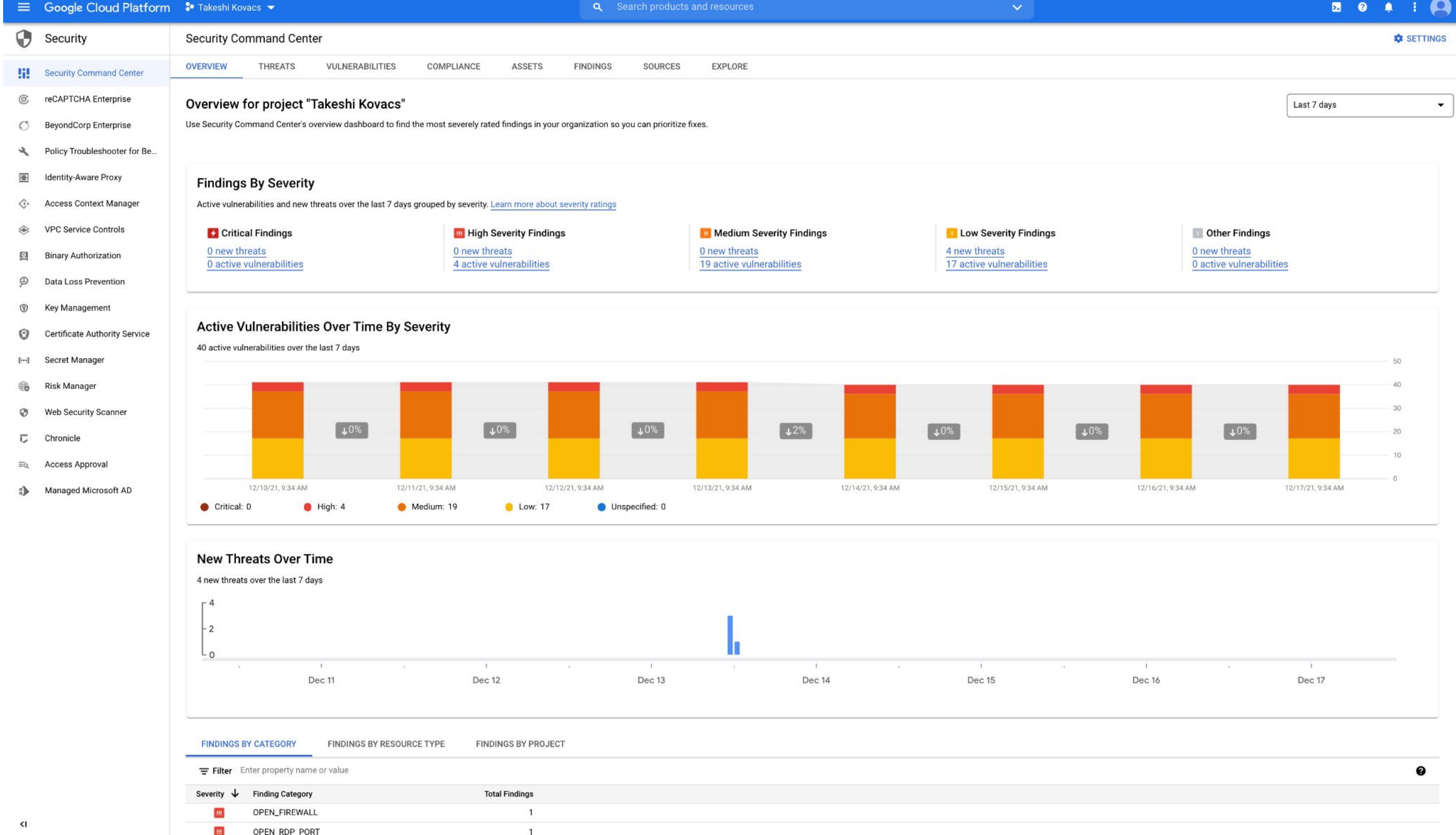
Early! The bigger their GCP footprint the more they'll appreciate it.

What is the value over Standard Edition?

- Event Threat Detection
- Web Security Scanner
- Container Threat Detection

Questions to listen to

- How do I track my assets?
- I’m currently dumping my logs into Big Query.
- What lets me see whether permissions have changed / are too broad?
- Where am I vulnerable?
- What’s under attack?
- How do I tighten my security footprint?
- Can I generate compliance reports?
- I need a single pane of glass for my GCP security!
- How do I access security telemetry for my Security Operations Center (SOC)?



Security Command Center

Overview for project "Takeshi Kovacs"

Use Security Command Center's overview dashboard to find the most severely rated findings in your organization so you can prioritize fixes.

Findings By Severity

Active vulnerabilities and new threats over the last 7 days grouped by severity. Learn more about severity ratings

Critical Findings	High Severity Findings	Medium Severity Findings	Low Severity Findings	Other Findings
0 new threats	0 new threats	0 new threats	4 new threats	0 new threats
0 active vulnerabilities	4 active vulnerabilities	19 active vulnerabilities	17 active vulnerabilities	0 active vulnerabilities

Active Vulnerabilities Over Time By Severity

40 active vulnerabilities over the last 7 days

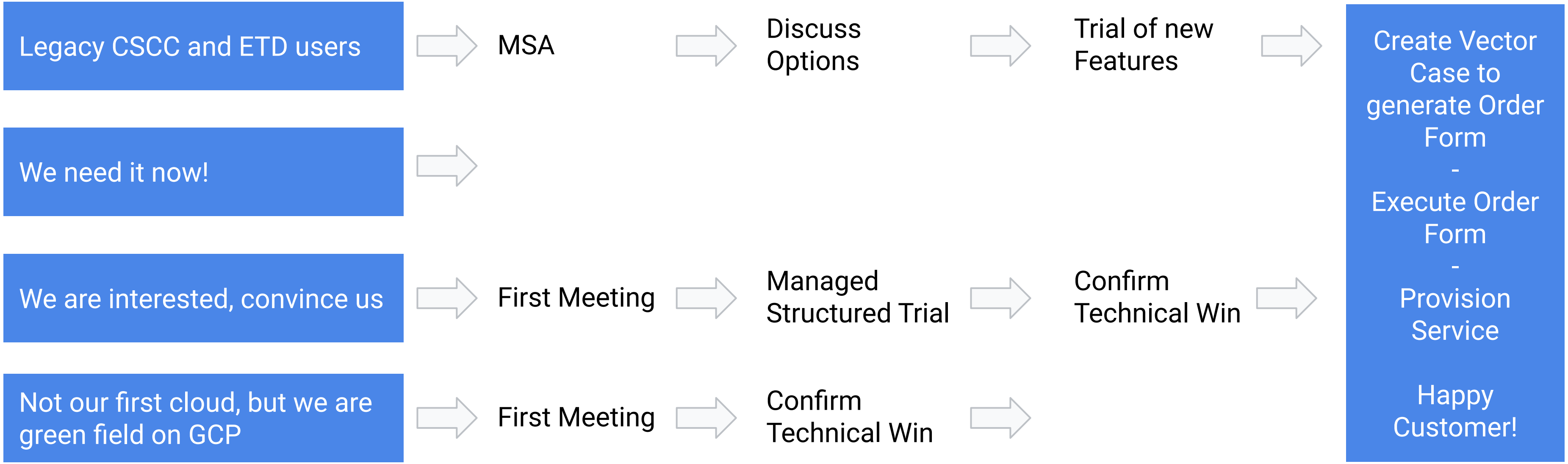
● Critical: 0 ● High: 4 ● Medium: 19 ● Low: 17 ● Unspecified: 0

New Threats Over Time

4 new threats over the last 7 days

Severity ↓	Finding Category	Total Findings
!!!	OPEN_FIREWALL	1
!!!	OPEN_RDP_PORT	1

The SCC Premium Sales Plays



Legacy CSCC and ETD users → MSA → Discuss Options → Trial of new Features →

We need it now! →

We are interested, convince us → First Meeting → Managed Structured Trial → Confirm Technical Win →

Not our first cloud, but we are green field on GCP → First Meeting → Confirm Technical Win →

Create Vector Case to generate Order Form
-
Execute Order Form
-
Provision Service

Happy Customer!

Security Command Center Pricing Tiers

Tier	Price	Built-in services
Standard	Free	- Security Health Analytics (SHA) - Limited functionality - Web Security Scanner (WSS) - Unmanaged
Premium	A fixed price Annual Subscription based on 5% of GCP spend. No overages, No true-ups just a fixed fee charged monthly.	- Everything in standard plus: - Security Health Analytics (SHA) - Full functionality - **Web Security Scanner (WSS) - Managed** - **Compliance Reporting** - **Event Threat Detection (ETD)** - **Container Threat Detection (KTD)** - **Export to Chronicle**

Google Cloud

During a customer conversation, show them this page.

Security Command Center Premium Pricing

SCC Premium can only be bought as a fixed price annual subscription with a minimum term of 1 year. It is priced at the Org level not the project.

Type of Request	Subscription Pricing
Without Commit	Greater of: - $25,000 or - 5% of the last 12 months of GCP Spend
With New or Existing Commit	Greatest of : - $25,000 or - 5% of Annual Commit or - 5% of the last 12 months of GCP Spend,

Common Pricing Scenarios:

- Free Trials
- No GCP Commit
- Attach to a new Commit
- Add-on to existing Commit
- Renewals
- Multi-year Commits
- Partner pricing

Google Cloud

Questions you can ask

Do you want to proactively know if something is misconfigured that can be exploited?

Do you know about threats present or targeting your environment?

Are you required to provide ongoing reports to fulfill your compliance requirements?

Get paid on qualified SCCP opportunities!

○ Qualified Opportunities > =$25K: $150 Google gift card *(max. of $600/person)*

○ Choice of redemption at Google Merchandise Store or Google Store

SCCP Upsell SPIFF Form - fill out after customer has seen a demo and agreed to PoC

Chronicle

High Level Points

What is it?	All security logs in one place, instantly searchable, greater than a year.
How does it help?	● Visibility from across the **entire enterprise** - on-prem, multi-cloud ● Identify threats, their scope and reach, faster ● Lowers the time and cost of an investigation
When should I discuss it?	When the customer talks about their broader security environment. You hear “SIEM” (security information event management) or “SOAR” (security orchestration automation response)
How is this different than...	● SCCP is exclusively GCP-focused ● SIEMs (Splunk, IBM QRadar) do not have the same scale, speed, or pricing

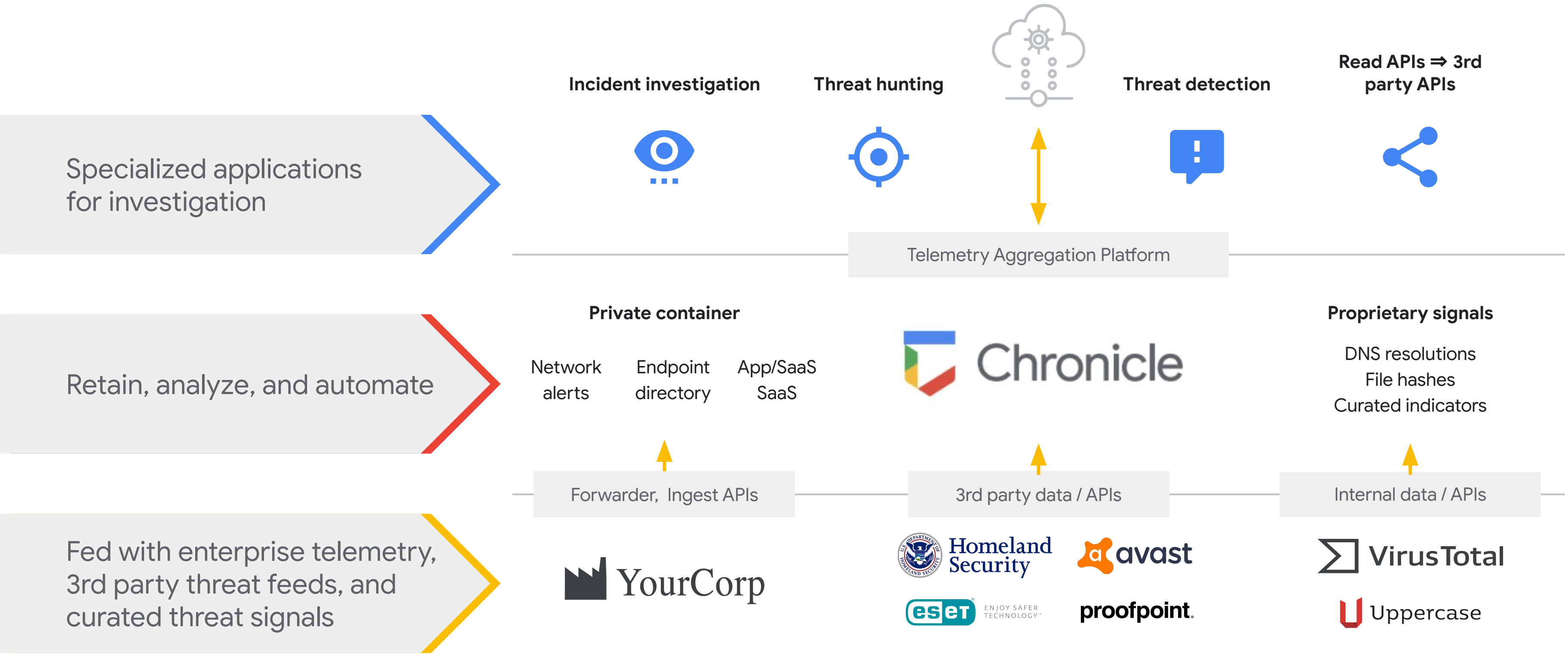
Chronicle

What Problem does it solve for? Security Data Overload

SIEM Challenges	Chronicle Security Analytics
Can’t scale Legacy platforms were not built for petabyte scale	**Cloud-native:** Operate at Google scale and speed
Too expensive Ingestion based pricing forces customers to limit what is collected and retained	**Fixed Cost:** No penalty for analyzing everything ($45/employee)
Misses threats Incomplete data, teams unable to see relationships between malicious indicators and events across time	**Clear Signals:** Curated intel X enriched telemetry X YARA

Chronicle

Chronicle Architecture



Specialized applications for investigation

Retain, analyze, and automate

Fed with enterprise telemetry, 3rd party threat feeds, and curated threat signals

Incident investigation

Threat hunting

Threat detection

Read APIs ⇒ 3rd party APIs

Telemetry Aggregation Platform

Private container

Network alerts

Endpoint directory

App/SaaS SaaS

Chronicle

Proprietary signals

DNS resolutions
File hashes
Curated indicators

Forwarder, Ingest APIs

3rd party data / APIs

Internal data / APIs

YourCorp

Homeland Security

avast

eset ENJOY SAFER TECHNOLOGY

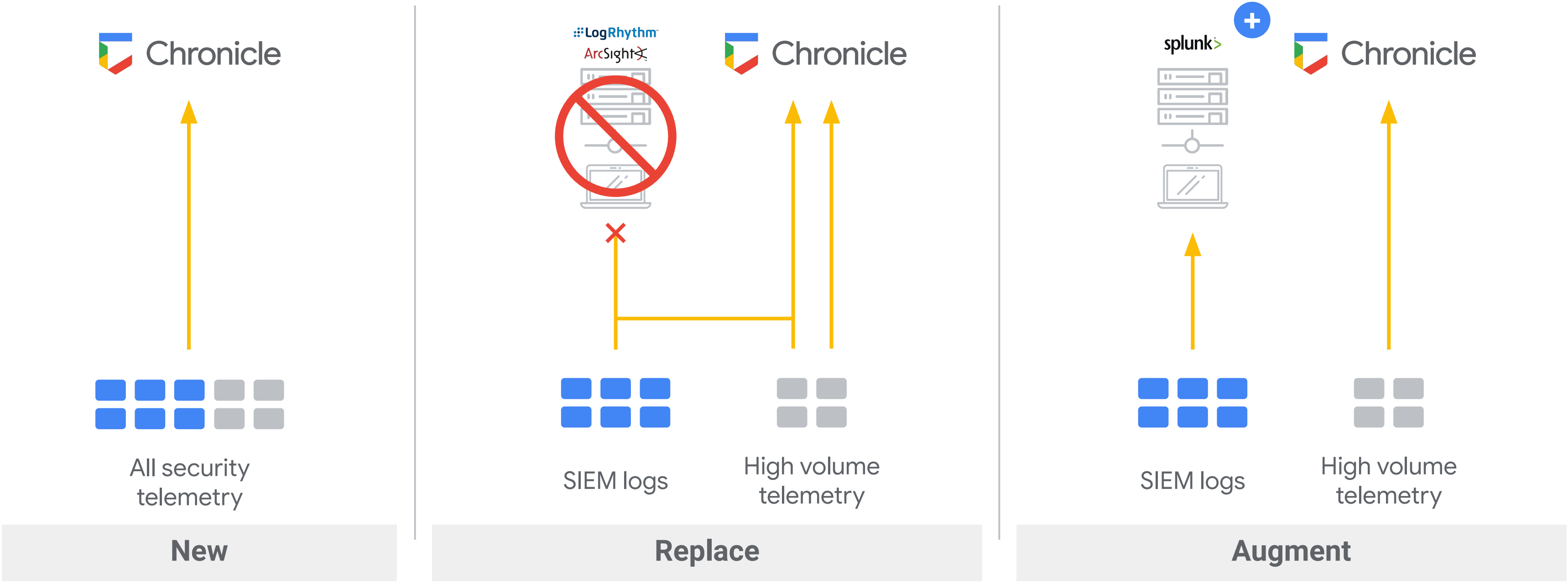
proofpoint.

VirusTotal

Uppercase

Google Cloud

Sales Plays


Chronicle
All security telemetry
New
LogRhythm
ArcSight
Chronicle
SIEM logs
High volume telemetry
Replace
splunk>
Chronicle
SIEM logs
High volume telemetry
Augment

Chronicle

What Makes Us Different

Intelligent data fusion

Timelines and enriched data model for investigation and detection

Continuous IoC Matching

Continuous, retrospective analysis of telemetry vs. threat intelligence

Hunt at Google speed

Subsecond searches against petabytes of data

Modern threat detection

YARA-L for detecting modern malware-based threats

Self-managed

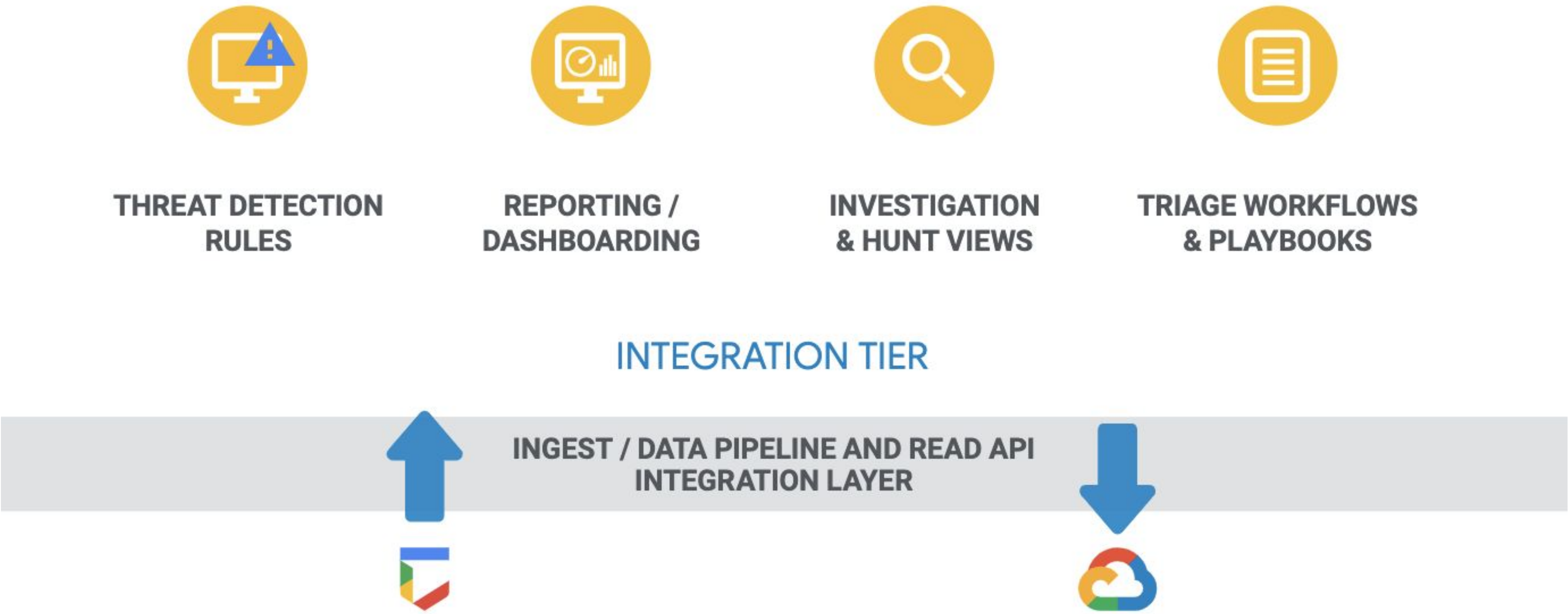
Unlimited scale-out without customer tuning, sizing, or management

Disruptive economics

Full security telemetry retention, analysis at a fixed, predictable cost

Google Cloud

CYDERES CNAP (CLOUD NATIVE ANALYTICS PLATFORM)



THREAT DETECTION RULES

REPORTING / DASHBOARDING

INVESTIGATION & HUNT VIEWS

TRIAGE WORKFLOWS & PLAYBOOKS

INTEGRATION TIER

INGEST / DATA PIPELINE AND READ API INTEGRATION LAYER

SECURITY DATA LAKE TIER

Unified Security Data Model; Data Forwarder Framework; Base Parser Library; High Performance Ingest and Read APIs; YARA-L Detection Engine; Curated Hunt/ Investigate Analyst Views

CLOUD INFRASTRUCTURE TIER

Scale, Performance, Availability, Trust & Compliance

CYDERES CNAP: Accelerate SIEM Modernization

White Glove Deployment

Expanded Search (Lucene)

Case Management integration

SOC Dashboards

Compliance Reporting

Advanced Rules Logic

SOC Ready Content Library

Google Cloud

Chronicle

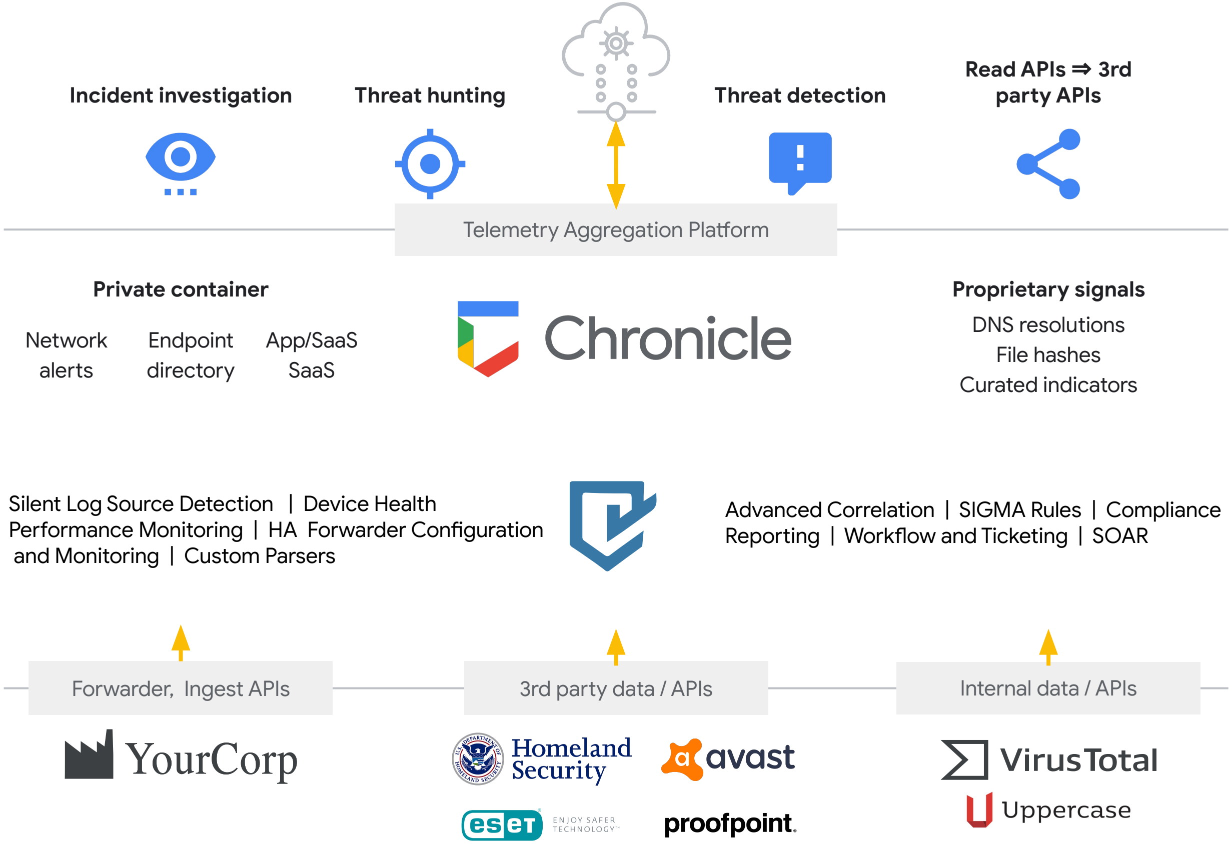
Cyderes CNAP Architecture

Specialized applications for investigation

Retain, analyze, and automate

Comprehensive SIEM Features (Cyderes)

Fed with enterprise telemetry, 3rd party threat feeds, and curated threat signals



Incident investigation

Threat hunting

Threat detection

Read APIs ⇒ 3rd party APIs

Telemetry Aggregation Platform

Private container

Network alerts

Endpoint directory

App/SaaS SaaS

Chronicle

Proprietary signals

DNS resolutions

File hashes

Curated indicators

Silent Log Source Detection | Device Health Performance Monitoring | HA Forwarder Configuration and Monitoring | Custom Parsers

Advanced Correlation | SIGMA Rules | Compliance Reporting | Workflow and Ticketing | SOAR

Forwarder, Ingest APIs

YourCorp

3rd party data / APIs

Homeland Security

avast

eset ENJOY SAFER TECHNOLOGY

proofpoint.

Internal data / APIs

VirusTotal

Uppercase

Google Cloud

Questions to ask

How does your team proactively hunt for threats that could affect your digital infrastructure?

How do you protect your software supply chain?

Does your team use a SIEM like Splunk or IBM QRadar?

If so, are you running into issues scaling the amount of data , and is the solution you are using more expensive the more data you use?

ReCaptcha

High Level Points

What is it?	reCAPTCHA Enterprise is an online fraud detection platform that is installed on the mobile/web client of a company to detect fraudulent, spam or abusive client activity.
How does it help?	defend your company's website or mobile application from bots, fraud, & abuse. Super important in light of the fact that companies on average lose 8% of revenue to fraud
When should I discuss it?	Anytime you're in contact with the team responsible for thec customer experience for a B2C business (especially in retail, financial services, hospitality, healthcare)
How is this different than...	Only solution in market that detects and deters bots based on 14+ years worth of the broadest and deepest training data Your customers are probably using version 1 or 2 of ReCaptcha and might be out of compliance - great excuse for an upsell conversation!

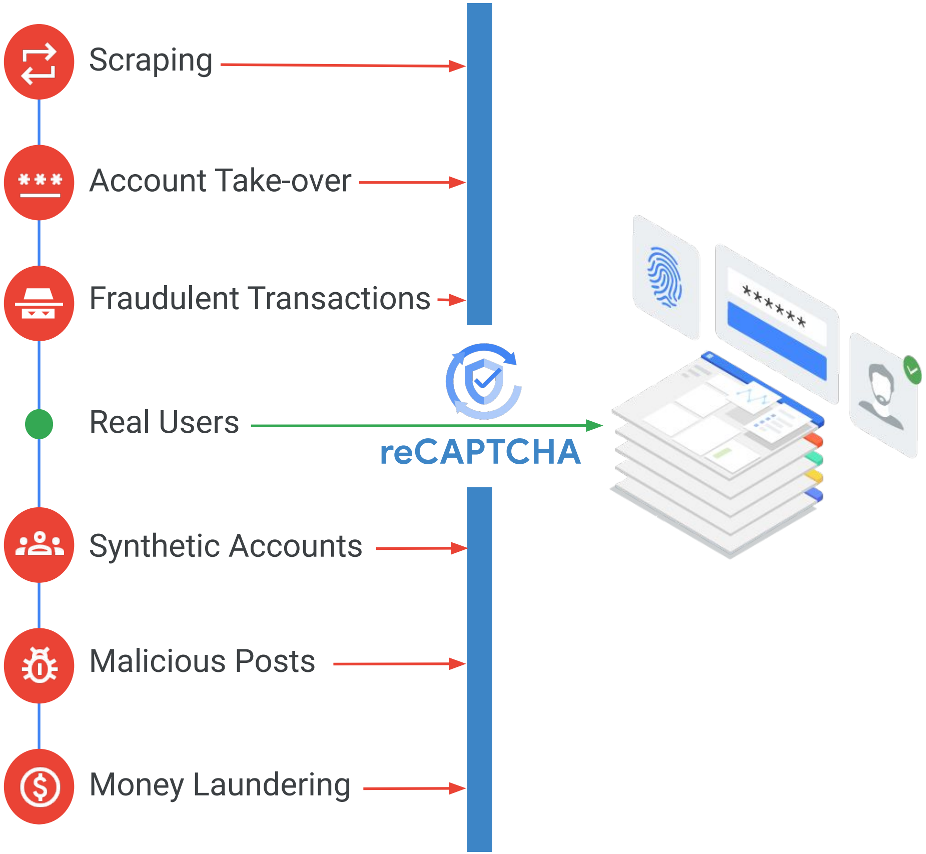
Evolving web security threats

⚠	Fraud	**8%** of online business revenue lost to fraud and account hijacking
⚠	Credential Stuffing	**30 Billion** attempted logins with stolen credentials in 2018
⚠	Fraudulent Logins	**29%** of all breaches involve the use of stolen credentials
⚠	Account Take Over	**300%** increase since 2017

reCAPTCHA Enterprise

Bot Detection Solution

Defend your business from bots, fraud, and automated abuse



Google Cloud

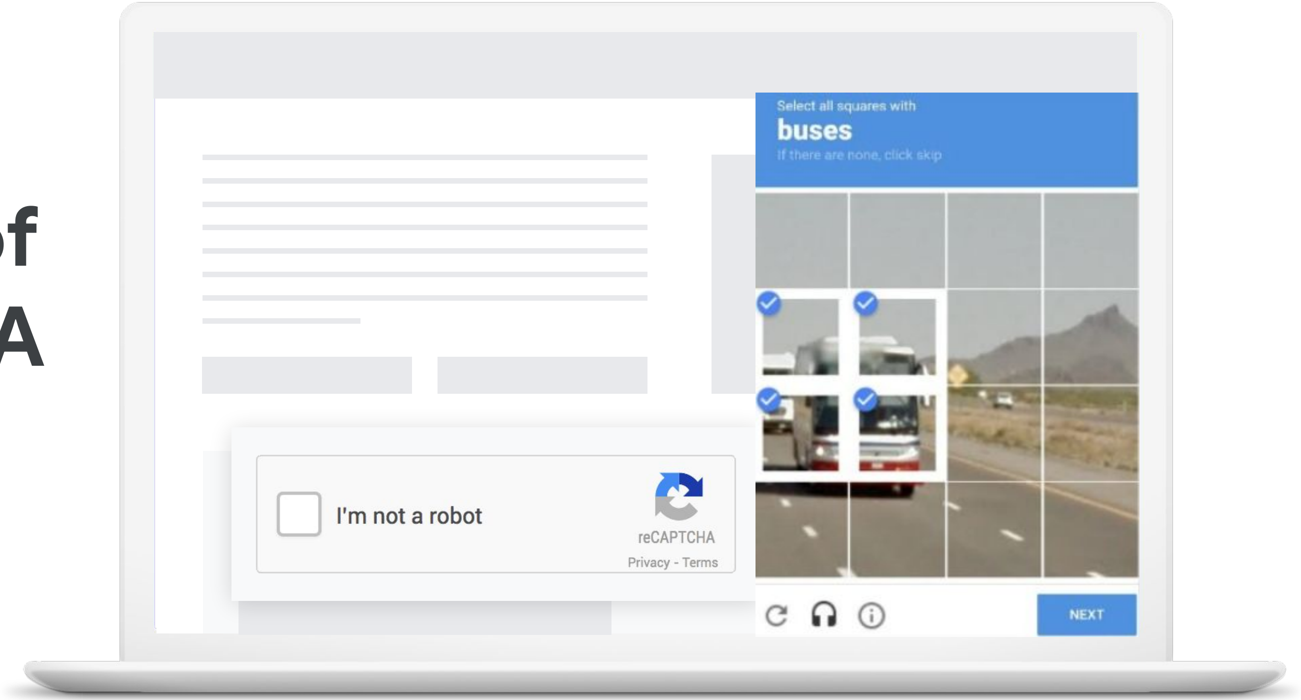
Evolution of reCAPTCHA

Version 1

sclt
..was here
Type the two words:
reCAPTCHA™
stop spam.
read books.

Evolution of reCAPTCHA

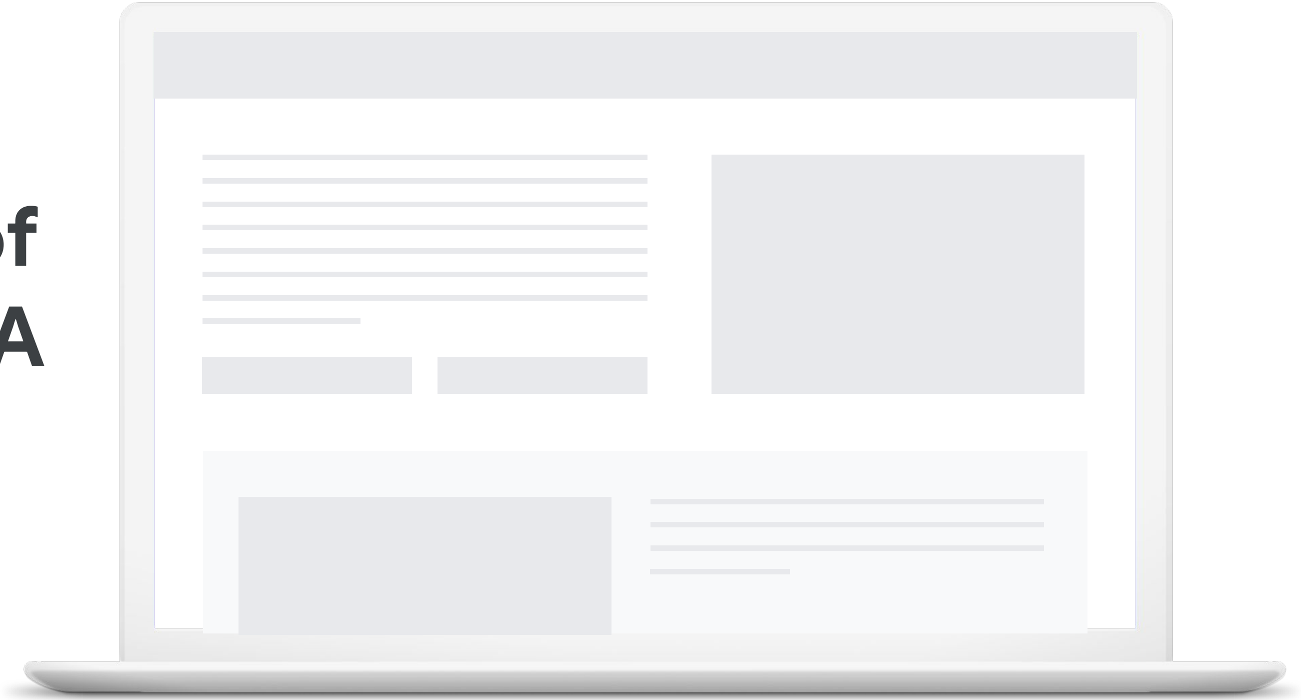
Version 2



Google Cloud

Evolution of reCAPTCHA

Version 3



Google Cloud

reCAPTCHA Versions

	Enterprise	v3	v2
API Calls	Unlimited	1M calls / month	1M calls / month
Checkbox	Optional	Optional	X
Risk Score	11 scores	4 scores	■
ML Model Tuning	X	■	■
SLA	X	■	■
GCP Terms & Conditions	X	■	■
Support	X	■	■
Mobile SDKs	X	■	■
Account Verification (2FA)	X	■	■
Password Checkup	X	■	■

What to listen for

- Customer has a **log-in page**. A bot defense solution is a must have
- Customers with h**eavy iOs/Android app traffic** (ie mobile-first businesses)
- Customer has a problem with **account takeovers**, **credential takeovers,** or **account hijacking**
- Customer is seeing **unexplained traffic spikes** to sensitive pages such as Login, Forgot Password, Add Credit Card
- Customer is seeking **fake account creations**
- Customer is seeing large amounts of credit card verifications per user
- Customer is experiencing highly desirable products **sold out extremely quickly**.

Target Stakeholders

Fraud = Champion

Biz = Budget

App = Implementor

Fraud

Fraud Team

Abuse Team (accounts/payments)

Security & Risk Leaders (CISO, CRO)

Biz

Product Director

C-Suite (CTO, CIO, CMO)

Procurement Office

Business Development Director

App

Site Ops Leader

Web & Mobile Developers

Identity Team (Web & App)

Questions to ask

Are you using version 1 or 2 of Captcha?

How much traffic do your web and mobile clients see per month?

What does the user experience look like? What pages do users interact with before check out?

Are you aware of any recent bot attacks or credential stuffing recently?

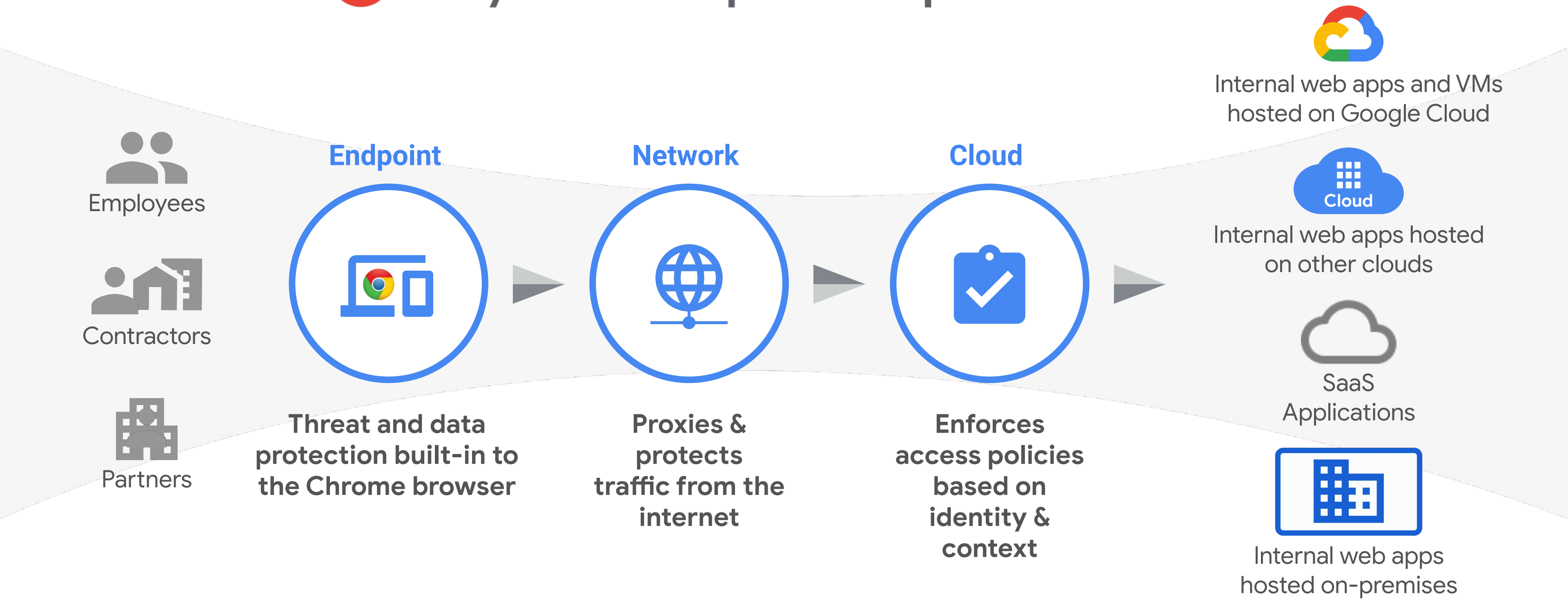
How do you go about detecting synthetic accounts, false posts on your website, and scraping from third parties?

Beyondcorp

High level points

What is it?	Access controlled by user/device attributes, continuously evaluated.
What does it solve for?	● Employees want to connect to internal applications and resources without any latency, but security teams want to make sure they are protected ● Keep sensitive content protected even while widely available
When should I discuss it?	Your customers widely use Chrome, Workspace People mention “Zero Trust” or ask about Identity/Access
How is this different than…	● Identity Providers establish you can log in, but don’t evaluate that it’s safe to let you do so. ● Other Zero Trust solutions heavily depend on agents and hard-to-manage reverse proxies to work

BeyondCorp Enterprise



Employees

Contractors

Partners

Endpoint

Threat and data protection built-in to the Chrome browser

Network

Proxies & protects traffic from the internet

Cloud

Enforces access policies based on identity & context

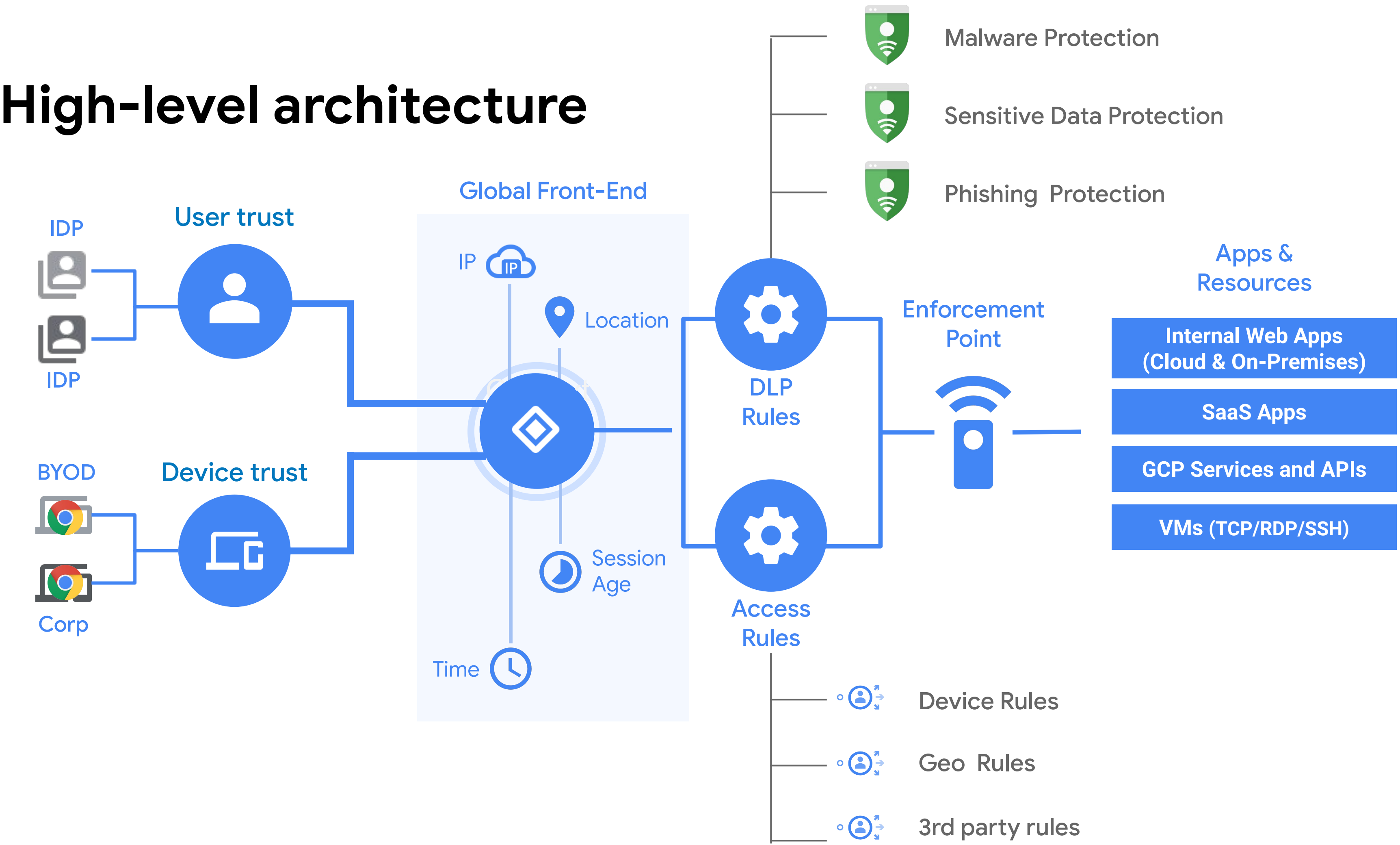
Internal web apps and VMs hosted on Google Cloud

Internal web apps hosted on other clouds

SaaS Applications

Internal web apps hosted on-premises

High-level architecture



Differentiators: Agentless, Google Network, Price

Endpoint

- Agentless support for Chrome endpoints (2B users)

Network

- 144 edge locations in over 200 countries and territories
- Proven to absorb the largest DDoS attacks (2.5 TB/sec)

Cloud

- Planet-scale identity management service
- Verifiable platform security, from chips to apps

$6 / user!

What to listen for

- We want a Zero Trust solution
- We have a lot of remote people / our people are all over the place
- We use a lot of contractors
- I want to enable our people to work from anywhere!
- I wish I could control how people access sensitive information!
- I’m looking for a DLP solution
- I’m worried about security at the edge
- I want to cut back on our VPN usage

Questions to ask

How do you enable your employees to remotely and securely access internal applications?

Is your current VPN solution providing for suboptimal and latent connections?

Are you looking at implementing a zero trust security strategy?

Sales Plays & Next Steps

Upsell & Greenfield Campaigns

Chronicle

Ask cloud champion for intro to CISO to learn more about threat hunting strategy -> demo of Chronicle / CNAP -> PoC -> contract through partner who delivers Managed Security Services or works through cyderes

BeyondCorp Enterprise

Ask cloud champion if they have a ‘zero trust’ strategy, discuss with person who manages security policies for remote access -> PoC -> order from GCP → resell to customer

Security Command Center

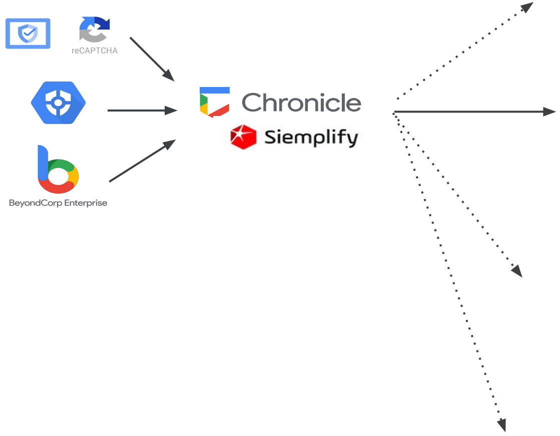
GCP Customer (non committed or commit) → upsell SCCP to cloud champion, ask to bring in security team → do trial → close 12 month contract

reCAPTCHA

Google Cloud Customer o w/ReCaptcha potential → discuss with application development team → kick off ReCaptcha pay-as-you-go -> contract

C level conversation re: Google security platform

CISO or head of security is solidifying more power at the C-level, and acts as a peer to the CIO/CTO for their cloud projects. Position the end to end platform.



Chief Information Officer	Oversight of all infotech and ´digital transformation´ projects	Under pressure to reassure board of directors that security posture is able to handle modern threats Unable to measure effectivity of security programs
Chief Information Security Officer	Senior information decision/policy maker; measures & reports on internal/external risk, compliance & performance	Not enough visibility across the estate Reactive to cyber threats vs being proactive Managing too many security tools but not getting the ROI they need to see
CFO	Financial planning, implementation, oversight	High costs associated with managing multiple cyber tools that overlap in functionality with low ROI
Security Operation Center (SOC) Leader	Leads the cybersecurity center of excellence	Improving on OKRs including MTTR, MTTD, etc
Security Architect	Individual contributor in SOC responsible for detecting and hunting threats	Frustrated by user experience of SIEM tools, latency in running queries (slows down ability to hunt threats)

Let’s go serve some customers!

(1) Identify your customers that have **$1 million+ ACV/yearly spend OR upcoming QBRs OR use SCC Standard**

(2) Qualify what security initiatives are top of mind

(3) Ask your customer’s cloud initiative leader is open to a discussion with security technical specialists

(4) Touch base with your google security partner team to strategize

(5) Set up meetings -> PoC -> deals deals deals

Casey Cesca
ReCaptcha Channel Manager
caseycraig@google.com

Alex Popp
Security Partner Manager
alexpopp@google.com
650 999 1453