So you want to solve cloud security

Helping Carahsoft customers sleep better at night knowing their digital infrastructure is protected
Your Google Cloud Security Team

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

Casey Cesca
ReCaptcha Channel Manager
caseycraig@google.com
How to introduce security
Every customer cares about security, but it’s a daunting subject.

Security Command Center Premium
Protect your customer’s google cloud workloads by providing them insights to possible threats and vulnerabilities.

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

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

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

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....

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
Security is top of mind

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

—attempts were also behind notorious SolarWinds hack
—Microsoft says attacks are part of larger wave of activity

From the Apple scoop machine
Did you know which two tech icons Mark Gurman’s Power On newsletter?

The hackers behind the notorious SolarWinds hack 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.

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

“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.”
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.

Acquired 2022
SCC Premium
## High Level Points

<table>
<thead>
<tr>
<th>What is it?</th>
<th>The best view anyone can ever have of their GCP environment.</th>
</tr>
</thead>
</table>
| **What does it solve for?** | - 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)?
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
  - 0 new threats
  - 0 active vulnerabilities

- High Severity Findings
  - 0 new threats
  - 4 active vulnerabilities

- Medium Severity Findings
  - 0 new threats
  - 19 active vulnerabilities

- Low Severity Findings
  - 4 new threats
  - 17 active vulnerabilities

- Other Findings
  - 0 new threats
  - 0 active vulnerabilities

Active Vulnerabilities Over Time By Severity

40 active vulnerabilities over the last 7 days

New Threats Over Time

4 new threats over the last 7 days
The SCC Premium Sales Plays

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

- **We need it now!**
  - First Meeting
  - Managed Structured Trial
  - Confirm Technical Win

- **We are interested, convince us**
  - First Meeting
  - Confirm Technical Win

- **Not our first cloud, but we are green field on GCP**
  - First Meeting
  - Managed Structured Trial
  - Confirm Technical Win

Create Vector Case to generate Order Form
- Execute Order Form
- Provision Service
- Happy Customer!
## Security Command Center Pricing Tiers

<table>
<thead>
<tr>
<th>Tier</th>
<th>Price</th>
<th>Built-in services</th>
</tr>
</thead>
</table>
| 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 |

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.

<table>
<thead>
<tr>
<th>Type of Request</th>
<th>Subscription Pricing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without Commit</td>
<td>Greater of:</td>
</tr>
<tr>
<td></td>
<td>- $25,000 or</td>
</tr>
<tr>
<td></td>
<td>- 5% of the last 12 months of GCP Spend</td>
</tr>
<tr>
<td>With New or Existing Commit</td>
<td>Greatest of :</td>
</tr>
<tr>
<td></td>
<td>- $25,000 or</td>
</tr>
<tr>
<td></td>
<td>- 5% of Annual Commit or</td>
</tr>
<tr>
<td></td>
<td>- 5% of the last 12 months of GCP Spend,</td>
</tr>
</tbody>
</table>

**Common Pricing Scenarios:**
- Free Trials
- No GCP Commit
- Attach to a new Commit
- Add-on to existing Commit
- Renewals
- Multi-year Commits
- Partner pricing
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
### High Level Points

<table>
<thead>
<tr>
<th>What is it?</th>
<th>All security logs in one place, instantly searchable, greater than a year.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does it help?</td>
<td>● Visibility from across the <strong>entire enterprise</strong> - on-prem, multi-cloud</td>
</tr>
<tr>
<td></td>
<td>● Identify threats, their scope and reach, faster</td>
</tr>
<tr>
<td></td>
<td>● Lowers the time and cost of an investigation</td>
</tr>
<tr>
<td>When should I discuss it?</td>
<td>When the customer talks about their broader security environment.</td>
</tr>
<tr>
<td></td>
<td>You hear “SIEM” (security information event management) or “SOAR”</td>
</tr>
<tr>
<td></td>
<td>(security orchestration automation response)</td>
</tr>
<tr>
<td>How is this different than...</td>
<td>● SCCP is exclusively GCP-focused</td>
</tr>
<tr>
<td></td>
<td>● SIEMs (Splunk, IBM QRadar) do not have the same scale, speed, or pricing</td>
</tr>
<tr>
<td>SIEM Challenges</td>
<td>Chronicle Security Analytics</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Can’t scale</td>
<td>Cloud-native:</td>
</tr>
<tr>
<td>Legacy platforms were not built for</td>
<td>Operate at Google scale and speed</td>
</tr>
<tr>
<td>petabyte scale</td>
<td></td>
</tr>
<tr>
<td>Too expensive</td>
<td>Fixed Cost:</td>
</tr>
<tr>
<td>Ingestion based pricing forces</td>
<td>No penalty for analyzing everything ($45/employee)</td>
</tr>
<tr>
<td>customers to limit what is collected</td>
<td></td>
</tr>
<tr>
<td>and retained</td>
<td></td>
</tr>
<tr>
<td>Misses threats</td>
<td>Clear Signals:</td>
</tr>
<tr>
<td>Incomplete data, teams unable to see</td>
<td>Curated intel X enriched telemetry X YARA</td>
</tr>
<tr>
<td>relationships between malicious</td>
<td></td>
</tr>
<tr>
<td>indicators and events across time</td>
<td></td>
</tr>
</tbody>
</table>
Chronicle Architecture

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

Specialized applications for investigation

Retain, analyze, and automate

Incident investigation

Threat hunting

Threat detection

Read APIs ⇒ 3rd party APIs

Telemetry Aggregation Platform

Private container

Network alerts
Endpoint directory
App/SaaS SaaS

Forwarder, Ingest APIs

3rd party data / APIs

Internal data / APIs

Proprietary signals

DNS resolutions
File hashes
Curated indicators

YourCorp

Google Cloud
Sales Plays

**New**
- All security telemetry

**Replace**
- SIEM logs
- High volume telemetry

**Augment**
- SIEM logs
- High volume telemetry

Google Cloud
What Makes Us Different

- **Intelligent data fusion**: Timelines and enriched data model for investigation and detection
- **Modern threat detection**: YARA-L for detecting modern malware-based threats
- **Continuous IoC Matching**: Continuous, retrospective analysis of telemetry vs. threat intelligence
- **Self-managed**: Unlimited scale-out without customer tuning, sizing, or management
- **Hunt at Google speed**: Subsecond searches against petabytes of data
- **Disruptive economics**: Full security telemetry retention, analysis at a fixed, predictable cost
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
White Glove Deployment
Expanded Search (Lucene)
Case Management integration
SOC Dashboards
Compliance Reporting
Advanced Rules Logic
SOC Ready Content Library

CNAP: Accelerate SIEM Modernization

Google Cloud
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

Telemetry Aggregation Platform

Read APIs ➔ 3rd party APIs

Private container

Network alerts
Endpoint directory
App/SaaS

Proprietary signals
DNS resolutions
File hashes
Curated indicators

Cyderes

Forwarder, Ingest APIs

3rd party data / APIs

Internal data / APIs

YourCorp

Homeland Security

avast

VirusTotal

Comprehensive SIEM Features

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

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

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

<table>
<thead>
<tr>
<th>What is it?</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does it help?</td>
<td>defend your company’s website or mobile application from bots, fraud, &amp; abuse. Super important in light of the fact that companies on average lose 8% of revenue to fraud</td>
</tr>
<tr>
<td>When should I discuss it?</td>
<td>Anytime you’re in contact with the team responsible for the customer experience for a B2C business (especially in retail, financial services, hospitality, healthcare)</td>
</tr>
<tr>
<td>How is this different than...</td>
<td>Only solution in market that detects and deters bots based on 14+ years worth of the broadest and deepest training data</td>
</tr>
<tr>
<td></td>
<td>Your customers are probably using version 1 or 2 of ReCaptcha and might be out of compliance - great excuse for an upsell conversation!</td>
</tr>
</tbody>
</table>
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
Evolution of reCAPTCHA

Version 1
Evolution of reCAPTCHA

Version 2
Evolution of reCAPTCHA

Version 3
# reCAPTCHA Versions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Enterprise</th>
<th>v3</th>
<th>v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Calls</td>
<td>Unlimited</td>
<td>1M calls / month</td>
<td>1M calls / month</td>
</tr>
<tr>
<td>Checkbox</td>
<td>Optional</td>
<td>Optional</td>
<td>X</td>
</tr>
<tr>
<td>Risk Score</td>
<td>11 scores</td>
<td>4 scores</td>
<td></td>
</tr>
<tr>
<td>ML Model Tuning</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GCP Terms &amp; Conditions</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile SDKs</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Verification (2FA)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Checkup</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What to listen for

- Customer has a log-in page. A bot defense solution is a must have
- Customers with heavy 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
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

<table>
<thead>
<tr>
<th>What is it?</th>
<th>Access controlled by user/device attributes, continuously evaluated.</th>
</tr>
</thead>
</table>
| 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 |
Internal web apps and VMs hosted on Google Cloud

Employees

Contractors

Partners

Internal web apps hosted on-premises

Internal web apps hosted on other clouds

Proxies & protects traffic from the internet

Enforces access policies based on identity & context

Cloud

Threat and data protection built-in to the Chrome browser

SaaS Applications

Endpoints

Cloud Network

Internal web apps hosted on-premises

Internal web apps and VMs hosted on Google Cloud

Internal web apps hosted on other clouds

SaaS Applications

Cloud

Endpoints

Cloud Network

Internal web apps hosted on-premises

Internal web apps and VMs hosted on Google Cloud

Internal web apps hosted on other clouds

SaaS Applications

Cloud
High-level architecture

User trust

Device trust

Global Front-End

DLP Rules

Access Rules

Enforcement Point

Malware Protection
Sensitive Data Protection
Phishing Protection

Apps & Resources

Internal Web Apps (Cloud & On-Premises)
SaaS Apps
GCP Services and APIs
VMs (TCP/RDP/SSH)

Device Rules
Geo Rules
3rd party rules

IDP
BYOD
Corp

User trust

Device trust

Time
Session Age
Location
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.

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