Security Command Center

Customer challenges

Challenge #1	Challenge #2	Challenge #3
Lack of visibility into all GCP assets across projects	Inability to detect vulnerabilities & threats	Lack of confidence that GCP infrastructure posture is compliant with major third party frameworks

What it solves for

Security Command Center Premium is a single pane of glass for your GCP infrastructure. It proactively monitors your cloud assets to detect vulnerabilities and threats.

- **Real time visibility**- Customers benefit from a holistic perspective on all their cloud assets (networking, databases, containers, etc)
- **Improve Security Posture Management**- Most ransomware attacks start due to simple misconfigurations of cloud assets. SCCP recommends secure policies and access management controls to deter against this.
- **Identify vulnerabilities and threats**- Detect events such as cryptomining, brute force SSH, injected libraries in containers at runtime. Provide remediation pathways.
- **Maintain compliance** - Ensure that your infrastructure follows guidelines of major third party frameworks, such as CIS 1.1, PCI DSS v3.2.1, NIST 800-53, ISO 27001

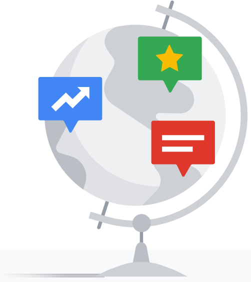
Differentiators & Competitive Landscape

Google visibility into Google assets	Other solutions will instrument agents or do 'API side scanning' to have visibility into assets
SCCP is instrumented at the hypervisor level - no other vendor has the same amount of visibility with the same latency as google.	They take snapshots, which have to be continually refreshed; and add bloatware to your cloud assets, which could impact performance.

How to get the conversation started?

- Do you want to proactively know if your GCP assets are misconfigured?
- How do you detect anomalous or malicious events across your GCP infrastructure?
- How do you provide regularly updated reports to fulfill your compliance requirements?

Chronicle



Customer challenges

Security Information and Event Management (SIEM) tools don’t scale	Legacy tools are expensive	Threats are too often missed because data cannot be searched quickly or correlated
Legacy platforms were not built for petabyte scale	Ingestion based pricing forces customers to limit what security telemetry is collected and retained	Teams unable to see relationships between malicious indicators and events across time because they have incomplete data

What it solves for

Chronicle is a global security telemetry platform for investigation and threat hunting, built on top of core Google infrastructure, and brings unmatched speed and scalability to analyze massive amounts of security telemetry.

- **Bring all your data**- Chronicle is built on google infrastructure and can handle petabytes of data.
- **Hunt at Google Speed**- Run complex queries across your petabytes of data and get results back in seconds, not hours. Enhance your security analyst productivity.
- **Intelligent and context aware event stitching -** Chronicle automatically correlated DHCP logs with devices and identitie then create timelines so security analysts see a complete and contextual representation of suspicious events.
- **Automatic twelve month lookback -** Store your security logs for longer, so as new vulnerabilities and threats become detected, look back to see if your organization has been compromised previously undetected.

Differentiators & Competitive Landscape

Scale	Data structure & rule authoring is simple	Price
Take advantage of one of the largest and most secure private networks in the world. Legacy vendors (Splunk, IBM QRadar) were built on - prem, not in the cloud.	Intelligent fusion of data sources reduces the burden on security analysts to clean the data, and frees them up to do what they do best: hunt for attackers.	Chronicle charges on a per seat model, rather than on data ingestion, encouraging customers to do more with data at significantly less the cost.

How to get the conversation started

- Are you having any issues scaling the amount of security telemetry available in your SIEM?
- How much do you spend on compute and storage to manage and run your SIEM?
- What is your mean time to detect threats? Mean time to resolve issues?
- How does your team proactively hunt for threats and attackers?

BeyondCorp Enterprise

Customer challenges

Challenge #1	Challenge #2	Challenge #3
In an increasingly hybrid work model, employers access to internal resources, but do so on unsecured devices and networks.	VPNs leave much to be desired for the employee experience (ie slow connection speeds, multiple reconnection attempts, etc)	Data exfiltration and phishing increasingly take advantage of employees default to trust; extending security controls to all apps and workflows is cumbersome

What it solves for

Beyondcorp is Google's approach to enabling remote access to web applications through Chrome browser, extending data and threat protection across all apps.

- **Zero trust access for web apps**- Enable employees to easily access web applications without the need of VPNs.
- **Mitigate data exfiltration risks** - Detect sensitive data in upload, download, and paste. Prevent downloads on unmanaged devices
- **Prevent Malware & Phishing**- Stop malware / ransomware, Prevent phishing attacks, Detect credential leakage.

Differentiators & Competitive Landscape

Agentless	Built on Google's Infrastructure	Price
No need to deploy an agent on the device or proxy traffic (think Zscaler, Palo Alto Networks, Ilumio). Policies are extend through Chrome and managed profiles.	Take advantage of 144 edge locations in over 200 countries and territories, capable of handling the largest DDoS attacks ever recorded.	$6/user is one of the most competitive price points in the market.

How to get the conversation started

- Are you looking at implementing a zero trust security strategy?
- How do you enable your employees to remotely and securely access internal applications?
- Is your current VPN solution providing for suboptimal and latent connections?

reCAPTCHA

Customer challenges

Bot Attacks	Top OWASP Attacks	Customer Satisfaction
84% of companies saw an increase in the number of bot attacks in 2021. **71%** of companies saw an increase in successful attacks **53 Days** of time spent on average fully resolving a bot attack	● Account Creation ● Credential Stuffing ● Skewing ● Carding ● Denial of Inventory ● Coupon/Gift Card Fraud	**Business Problem:** Preventing fraud and bot attacks without having the customers feel the friction. **Business Goal**: Protecting customers information while reducing customers complaints or abandoned purchases.

What it solves for

You may be familiar with reCAPTCHA, a free service that has been defending 6 million + sites for over ten years. reCAPTCHA Enterprise is built on the existing reCAPTCHA API with added features creating a comprehensive anti-fraud and bot mitigation solution.

- **Comprehensive** -Coverage for both web and applications using our Mobile App SDK (Android/iOS)
- **Customizable** - Increased customizability of risk algorithms to organizations and page-specific risk profiles. A feedback loop via the annotation API.
- **Insights of Attacks**- Reasons codes provided to describe threats such as AUTOMATION and UNEXPECTED-ENVIRONMENT
- **Password Leak Detection** - Conduct regular audits of user credentials (passwords) to ensure they haven't been leaked or breached

Differentiators & Competitive Landscape

Proven Results	Frictionless	Adaptive
6 million + websites protected including Pinterest, HBOMax, Etsy, Caribou Coffee and Adobe.	No challenges, no problem. Seamless fraud detection stops bots and automated attacks while approving valid users.	Continuous machine learning factors in every customer and bot interaction for the most accurate results in real-time.

How to get the conversation started

- What are the biggest challenges you are trying to protect against with a fraud/bot solution? (ex Account Takeovers, Credential Stuffing, Fraudulent activities, Scraping, etc)
- Are there specific workflows on your website you are worried about like Login/Checkout etc?
- Have you experienced any recent bot attacks that can be shared with us?