Google Cloud

Google Cloud Security OEM Program

Time to value

Enhance your solutions with immediate, rich insight from massive volumes of security telemetry and global threat intelligence data.

Sales Growth

Collaborate with Google Cloud Security sales, co-brand your marketing and be in Google Cloud Marketplace and/or VirusTotal's Integration Portal.

Superior Technology

Enable customers to rapidly detect, prioritize, analyze and respond to real threats with technology built to ensure scalability and preformance.

Chronicle OEM Advantages

Massively scale and easily analyze security data to meet your customers' needs now and in the future

Accelerate your business and focus your engineering on your unique value by building your solution on top of Chronicle. Purpose-built on core Google infrastructure, Chronicle can ingest massive amounts of telemetry data, normalize it, index it, correlate it to known threats, and make it available for analysis in seconds. Also leverage Chronicle to automate security workflows and manage cases to streamline your customers' threat response processes. The Google Cloud Security OEM program allows you to take advantage of the speed, scalability and smarts of the Chronicle platform to: realize an XDR vision; store, enrich and analyze massive amounts of security data; and/or meet the need to normalize multiple types of relevant log data.

Easily store and analyze security data at global scale

Continuously ingest, normalize, index, correlate and store massive amounts of security telemetry and alert data from unlimited sources at Google speed and scale. Securely keep a year's worth of data in a private container for your customers to leverage for deeper investigations and compliance reporting.

Proactively detect, hunt for and respond to threats

Detect and analyze real-time activity plus if and how new threats may have appeared over the past year. Chronicle gives you the power of Google search speed, automatic data correlation and enrichment, a pre-built detection rule engine and integrated threat feeds so you can deliver actionable results in seconds vs. hours or days. You can also add capabilities to automatically respond to threats with orchestrated workflows triggered by contextual details for the right response.

Focus your engineering where you need it

Take advantage of Chronicle as your global-scale, secure, data intelligence backbone so your engineers can focus more on the security use cases your customers need. Capitalize on all relevant data without scalability, security or storage concerns.

Uplift revenue, value & brand

Scale to 100's of petabytes on an unparalleled architecture that assures performance and data security without compromise. Google Chronicle is a cloud-native platform built on the same infrastructure that powers Google's global search. Using the power of Google scale, speed and smarts can help elevate your security solution's viability.

Chronicle Highlights →

Embed the power of Google Chronicle scale, speed and smarts to elevate your solutions's value by using the highest level of actionable intelligence.

- Built on the power and speed of Google search and includes integrated threat intelligence to , deliver valuable security insight in seconds
- Infinite scalability to ingest and store for a year or more petabytes of security data, all available for immediate search and analysis
- Automatic normalization, indexing and correlation enables rich contextual analysis and actions
- Automatically connects related entities and activity into a single data structure for each event for greater contextual understanding
- Orchestrate automated security workflows to drive context-aware threat response actions and manage incident cases

VirusTotal OEM Advantages

Enrich your offering with VirusTotal's superior context to streamline threat detection, investigation and response

Users of Virus Total (VT), the world's largest and most trusted threat intelligence hub, are acutely aware of the value and necessity of leveraging VirusTotal's rich threat context to accelerate the investigation and response of critical threats in their environments. The VirusTotal OEM program enables your organization to enhance your customers' user experiences by compliantly displaying VirusTotal results directly within your solution's user interface (UI). Through the use of an easily embedded widget and a single API call, your security solution can now display VirusTotal threat detection ratios and drill down on malicious detections in a customizable i-frame that displays results directly from VirusTotal.

Enhance your product & customer experience

Prevent your users from missing serious breaches due to alert fatigue. Add a second opinion layer to IoCs seen in incidents with insight from 100+ vendors and dozens of crowdsourced {YARA, Sigma, IDS} ruleset sources, all while keeping your users within your UI.

Minimal engineering efforts & customizable layout

Embed VirusTotal in your product with a radically simple widget - no complex API parsing, no template coding, no capacity planning. Always be up-to-date with the latest VirusTotal features and threat intelligence without update requirements from your product.

Simple pricing & unlimited API lookups

Take advantage of unlimited API lookups for your full user base with our simplified, all you can consume, pricing model. This unique pricing model also allows your solution to leverage VirusTotal's OEM functionality in the way that makes the most sense for your business model. This can include monetization of a new offering or augmentation of existing offerings.

Uplift your brand & marketing momentum

Differentiate by co-branding with VirusTotal as part of your marketing campaigns. As part of the OEM program you will also be featured in VirusTotal's public and open integrations portal with a page entirely dedicated to your solution. Get exposure to 3M+ highly qualified monthly users that can influence the decision to buy your solution.

VirusTotal Highlights →

Compliant, easy, and actionable embedding of VirusTotal in third-party solutions to gain unique visibility into threats. Why leverage VirusTotal?

- 18 years of malicious observations, going back to 2004
- Enrichment for 3B+ files, 50B+ considering compressed bundles
- 2M file + 6M URL scans / day with 70+ antiviruses and 15+ sandboxes
- Contributions by 3M+ monthly users coming from 232 countries
- Industry de-facto threat intelligence sharing hub, used by thousands of organizations such as US Cyber Command
- Google planet-scale and instant search capabilities

Web Risk OEM Advantages

Detect and block unsafe URLs with the power of Google

Upgrade your product's web security to Google-level with easy to use Web Risk APIs to protect your customers from unsafe web pages/URLs. Enhance your product with the same technology used by Gmail, Chrome and Android to detect and block access to URLs used for phishing and malware.

Block access to unsafe URLs using Google's global ecosystem

Prevent phishing with a world-wide warning. When you submit a suspected unsafe URL using the Web Risk Submission API, Google will confirm if it is unsafe and automatically warn users on 5 billion+ devices when they attempt to visit that site.

Rapidly respond. Phishing happens fast so speed matters. We understand this and aim to have all of your URL submissions that are confirmed unsafe blocked in under an hour.

Detect malicious URLs at Google scale

Choose your display option. Send your customers' URL visits to Google and display the detection results in your product's user interface - URL safety status and what its malicious purpose is if unsafe. Attribute the results to Google or not, or simply use them in the background to improve your product's security.

Protect against live attacks. Using proprietary signals, Google knows when URLs are actively used in phishing and malware attacks so have the highest chance of harm. Confidently use detection results to trigger actions that protect your customers' environments.

Scan billions of URLs daily. Take advantage of Google's global scale hunting for unsafe URLs while you focus on protecting your customers.

Stay continuously current. The Web Risk database is continuously updated to ensure unsafe URLs are added as they come online, and benign URLs are removed once confirmed safe. Web Risk's database of unsafe websites/URLs, typically ranges from 1 to 3 million.

Web Risk Highlights →

Upgrade to Google-level URL security with easy to use APIs.

- >99% true positive detection rate
- Built for hyperscale scanning billions of URLs daily with 10 ms latency
- Unsafe URLs are quickly blocked for all your customers' users and majority of web users globally
- World's largest real-time database of unsafe URLs, typically ranging from 1 to 3 million
- Google's AI, ML, custom rules and human analysts continuously detect unsafe URLs for you
- Privacy preserving option available using a URL hash-prefix

Visit goo.gle/cloud-security-oem or contact GCS-OEM@google.com to learn more.