

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, 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 performance.



VirusTotal OEM Advantages

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

Users of VirusTotal (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

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. The Google Cloud Security OEM program allows you to take advantage of the speed, scalability and analytics of the Chronicle platform when building an XDR platform, storing and analyzing large amounts of data or meeting the need to normalize multiple types of log data.

Easily store & utilize 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 find threats & anomalies instantly

Quickly analyze real-time activity plus if and how new threats may have appeared over the past year. Embed Chronicle within your UI so your customers can instantly detect, visualize and analyze more threat and anomaly details. Chronicle uses the power and speed of Google search combined with pre-built rules and customizable dashboards to deliver actionable results in seconds vs. hours or days.

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 use cases your customers need. Load and utilize all relevant data without scalability, security or storage concerns.

Uplift revenue, value & brand

Scale to 100's of petabytes on an unparalleled data infrastructure that assures performance and data security without compromise. Google Chronicle is a cloud-native platform built with the same components that power Google's global search. Capitalize on Google scale, credibility and branding to elevate your security solution's business.

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, delivers valuable data insight in seconds



Infinite scalability, able to ingest 100s of petabytes of security telemetry data and securely store for an extended period of time



Instant normalization, indexing, correlation and dashboarding, makes data available for immediate analysis



Automatically connects related activity data into a single data structure for each event for greater contextual understanding



Presents the whole picture with an identity graph to best understand and respond to unusual activity

Web Risk OEM Advantages

Detect phishing and malware URLs with the power of Google

Want to use the same technology as Gmail and Chrome to detect unsafe URLs? Upgrade your product's security to Google-level with an easy to use API.

Flexible OEM deployment options

Display detection results in your UI and attribute them to Google or simply use the technology behind the scenes

1 Billion URLs scanned daily

Let Google do the work for you. Google scans over one billion URLs everyday. Our crawlers never stop hunting for social engineering, unwanted software and malware URLs.

A live database, not a thread feed

Help your customers steer clear of verified unsafe URLs with a real-time updated blacklist. The Web Risk database is constantly updated to ensure that unsafe URLs are added as they come online, and benign URLs are removed once they are safe again.

1 to 3 million URLs on the blacklist

Increase your customers' web surfing and link safety by utilizing the world's largest database of blacklisted URLs. After scanning billions of URLs daily, our list of unsafe websites typically ranges from 1 to 3 million.

Protect against live attacks

Detect malicious attacks when they begin. Using proprietary signals, Google tracks which URLs are actively being used in attacks in real-time. Our mission is to detect URLs that are currently posing real threats to users and organizations, not dormant and stale URLs. With this focus, you are able to detect URLs that have the highest chance of actually making a negative impact on users and organizations and take action to block access.

Help control the world's largest firewall

Submit unsafe URLs to Google to have them blacklisted on 5 billion devices using our NEW Submission API. This product requires special approval. Reach out for more information.

Web Risk Highlights →

Upgrade to Google-level security with an easy to use API.



99%+ true positive detection rate



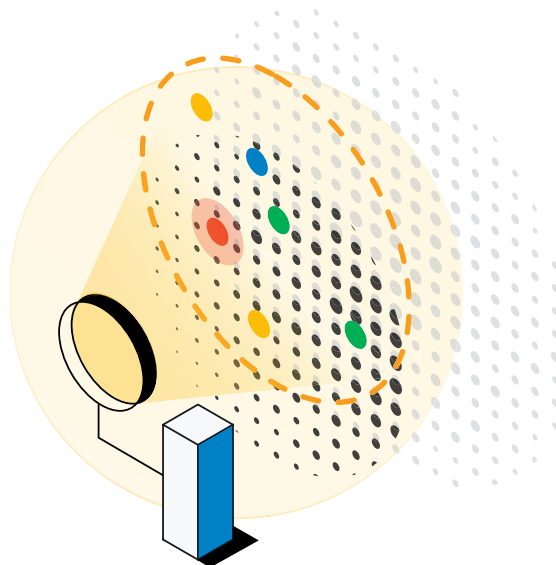
Privacy preserving option available using a URL hash-prefix



Built for hyperscale and available to scan billions of URLs everyday with 10 ms latency



Leverage our AI, ML, custom rules and human analysts to detect unsafe URLs



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

©2022 Google LLC. All rights reserved. Chronicle and VirusTotal were acquired by Google and operate under Google Cloud.