Google Cloud | VIRUSTOTAL

VirusTotal Augment OEM Program

Enrich your end-user offering with VirusTotal's superior threat context, power faster and more accurate response

Organizations are becoming increasingly concerned about missed threats due to lack of context. Machine learning, AI, UEBA, heuristics, generic detections, etc. are only magnifying the issue, both in terms of false positives and puzzling alerts. Moreover, your users are fighting threat actors that operate globally constrained by the narrow visibility of their internal-only logs. VT AUGMENT OEM expands your solution's threat visibility with crowdsourced reputation and insights from a network of hundreds of security vendors, thousands of security professionals and millions of monthly VirusTotal users.

Mitigate missed threats & false positives

Your users often miss serious breaches due to alert fatigue. Add a second opinion layer to IoCs seen in incidents with reputation from 100+ vendors and dozens of crowdsourced {YARA, Sigma, IDS} ruleset sources.

Power proactive & preventative defense

Your customers are often confronted with an unknown file/URL/IP/domain and asked to make sense of an attack. Without further context, it is virtually impossible to determine attribution, build effective defenses against other strains of the attack, or understand the impact in their organization. Empower your users to quickly build a picture of an incident, and then use the insights to neutralize other attacks.

Increase revenue and customer retention

Threat Intelligence is becoming indispensable for security leaders. Uplift your offering with real-time sightings coming from the industry's de-facto threat sharing hub. Generate a new revenue stream through upselling or disrupt the market with unrivaled off-the-shelf value.

Reduce in-house development time

Embed VirusTotal in your product with a radically simple widget - no complex API parsing, no template coding, no capacity planning. Always up-to-date with the latest VirusTotal features.

In a nutshell ➤➤ ➤

Compliant, easy, and actionable integration of VirusTotal in third-party solutions to gain unique visibility into threats.

- **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 intel sharing hub, used by organizations such us US Cyber Command**
- **Google planet-scale and instant search capabilities**

See it in action

Google Cloud | VIRUSTOTAL

Compliant, easy and actionable integration of VirusTotal in third-party security solutions

Your customers are demanding a single pane of glass experience from your product. Corporate cybersecurity stacks are increasingly complex: too many tools and services, information scattered across numerous databases, arduous stitching together of disparate sources, etc. Incident response and threat hunting have become a time consuming quest across multiple browser tabs. The experience is poor. VT AUGMENT OEM addresses the most popular demand coming from security analysts these days: incorporating VirusTotal's unrivaled context in their tools of choice.

Compliant

VT AUGMENT OEM is the only allowed vehicle to display VirusTotal data in third-party products besides end-user bring-your-own api key integrations.

VirusTotal is built on an ecosystem of contributors that has strict guidelines prohibiting the misuse of data by threat scanning organizations and banning the integration or exposure of VirusTotal data in third-party solutions or to end-users. Through the development of this OEM program, VirusTotal has created a technically-compliant licensing offering that allows organizations to leverage VirusTotal's raw data in a meaningful format that can be integrated in their existing solutions.

Easy

Minimal engineering. No API parsing, no HTML templates, no updates, no capacity planning required. Integrate in 3 hours and forget thereafter.

- REST JSON API
- Iframe widget
- Custom themes
- Open source Javascript library
- Updates seamlessly
- Scales automatically

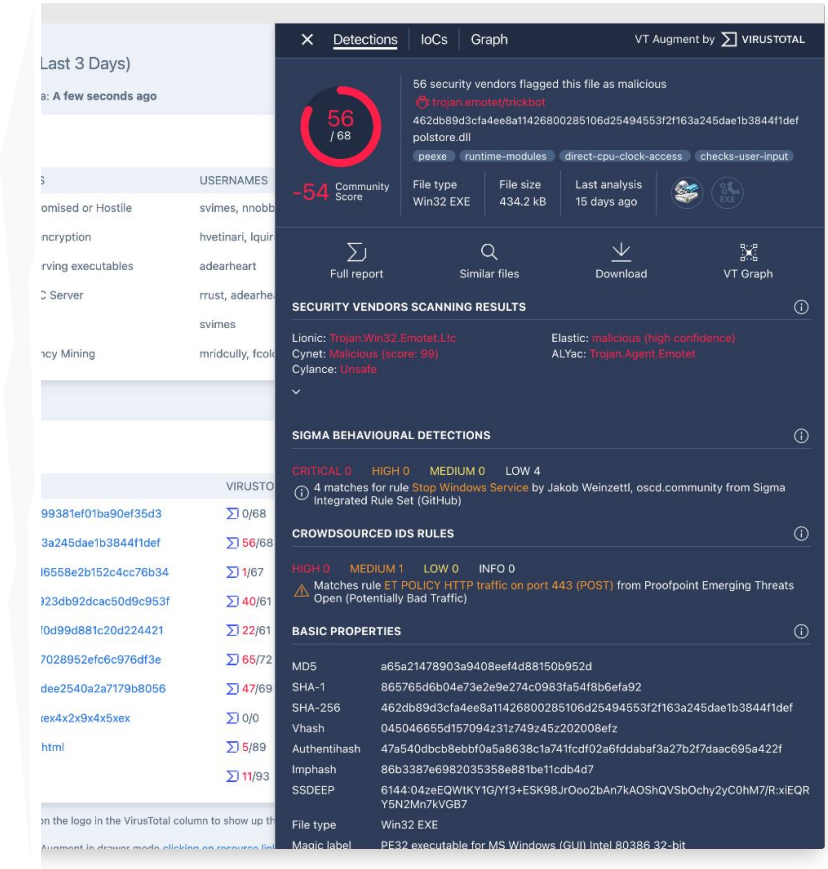
Actionable

Any observable, every detail, everywhere throughout your product. Context is not limited to a threat score but rather includes insights to power preventative security operations.

- Threat reputation by 100+ vendors
- Multi-angular {YARA, SIMGA, IDS} detection
- Related IoCs
- In-the-wild observations
- Interactive threat graph
- Whois lookups and geolocation
- Activity timelines and geo spread
- Provenance details
- Prevalence and popularity information

Google Cloud | VIRUSTOTAL

Superior context and threat visibility at and beyond your customers' network perimeter



Multi-kind characterization—Enrich files/hashes, domains, IP addresses and URLs.

Observable identification—Identifiers and characteristics allowing your customers to reference the threat and share it with other analysts (for example, file hashes, size, file type, similarity hashes).

Threat reputation—Maliciousness assessments coming from 70+ security vendors, including antivirus solutions, security companies, network blocklists, and more.

Multi-angular detection—Additional threat analysis coming from crowdsourced rule matches and community scoring (for example, YARA, Sigma, and IDS rules).

Security-relevant metadata—Includes software publisher information, identification of malicious macros in documents, popularity ranks for domains, domain content categorization, and more.

Related indicators of compromise (IOCs)—Examples of IOCs include network infrastructure distributing a malware file, servers acting as a command-and-control for a given threat, malicious URLs seen under a given domain, domains seen behind a given IP address, and more.

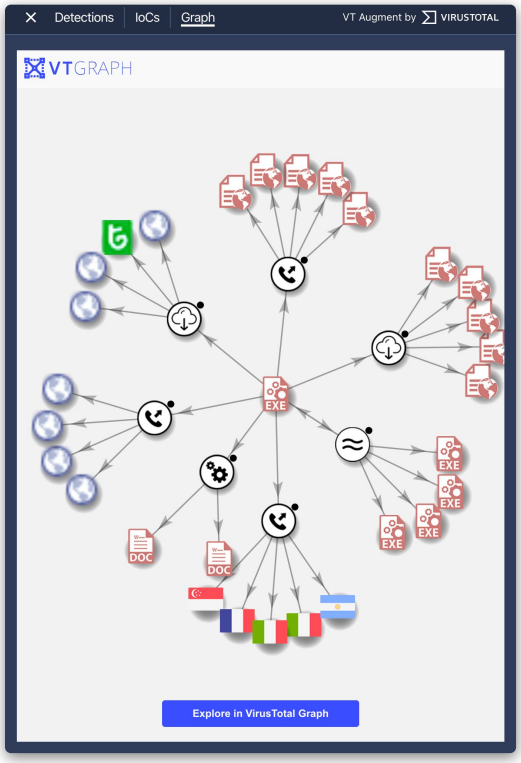
In-the-wild details—Geographical-spread and distribution details for threats, common attacker deception techniques, and more, through VirusTotal submission metadata.

Domain/IP Whois lookup—Registrar and registrant details for domains, as well as ownership and network range information for IP addresses.

Domain and server security-relevant metadata—HTTPS certificates for web servers, DNS resolution records, and web server HTTP headers.

Threat time spread—Key dates that enable your customers to understand when a given threat was first observed in-the-wild and how long it's been active.

Interactive threat graph—Graphical format that maps out entire threat campaigns by visualizing the relationships between IOCs.



Leave nothing unanswered

Given a hash in an alert, is there any second stage payload that your customers should be searching for in their environments?

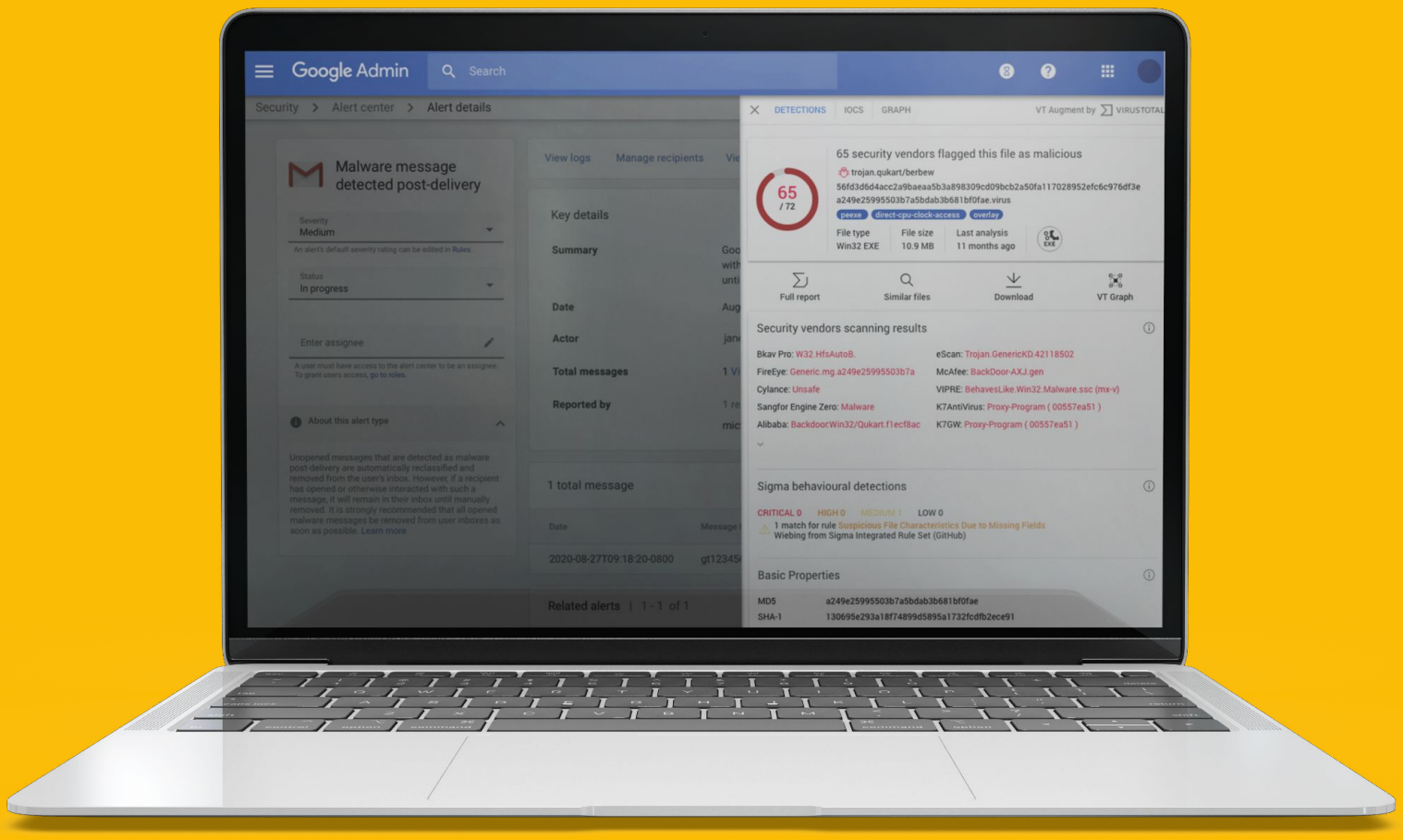
What's the C2 infrastructure tied to a given hash? Has it shown up in your customer network logs?

Given a domain flagged by your solution, is it a flagrant false positive based on its popularity and malicious observations recorded by VirusTotal?

Given an IP address in one of your alerts, has it been seen serving malware? If so, which hashes? Have those been seen across your customer's fleet of machines?

Once you have revealed a compromise, is it a well known threat to the industry? i.e. is it widely detected? Is it rather a targeted attack?

Google Cloud | VIRUSTOTAL



VirusTotal Augment OEM

Insightful, Differentiated, Profitable

It has never been easier to integrate elite crowdsourced threat intelligence in your product

Read success story