Google Cloud | VIRUSTOTAL

VirusTotal Enterprise

Faster, more confident, more accurate and more cost-effective security operations

VirusTotal is the world's richest, most interlinked and closest to real-time crowdsourced malware corpus. By applying to it Google's planet-scale infrastructure and instant search capabilities, as well as VirusTotal home-grown innovations such as YARA, we have built the most actionable threat intelligence suite in the planet. To the extent that it has become a **necessary layer in any defense-in-depth security strategy, the "Google" of malware**. G2K companies and the largest governments on Earth use it every day to shed light into their security telemetry, unearth compromises and outsmart their adversaries.

Automate alert triage and false positive remediation

Leverage API and SIEM/SOAR integrations to programmatically confirm, prioritize or discard alerts with threat reputation for files, domains, IPs and URLs coming from over 70 security vendors, crowdsourced YARA rules, sandboxed dynamic analysis, SIGMA rules acting on detonation behavior, IDS detections on network traffic and a myriad of other security tools & datasets. Superior defense-in-depth.

Expedite and augment incident response

Explore VirusTotal's threat graph to understand the full attack chain and map out threat campaigns. Instantly pivot to related infrastructure and identify remediative and hunting IoCs to feed your SIEM and network perimeter defenses. Assess the impact to your organization.

Discover unknown threats, take preventive measures

Deploy generic hunting YARA rules and make use of anomalous pattern searches to surface malware flying under the security industry's radar. Eliminate blind spots in your existing security technologies by automatically feeding them IoCs coming from static dissection and dynamic analysis. Identify pre-operational campaign infrastructure and preventively block it. VirusTotal is the missing piece of your existing security investments.

Track adversaries and implement proactive defenses

Understand the global threat landscape and monitor the evolution of specific actors targeting your industry, shed light into their modus operandi and make data-driven infrastructure hardening decisions. Profile adversaries and conduct proactive TTP-based hunts, automatically generate detection rules that can be deployed in your EDR and other defensive layers to supercharge your security posture.

Benefits

- **Improve the efficiency of your security team**
- **Strengthen your security posture and lower risks**
- **Proactively identify threats and take action**

Unique visibility into threats

- **19 years of malicious observations, going back to 2004**
- **Enrichment for 3.7B+ 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**

See it in action

Google Cloud | VIRUSTOTAL

You are fighting global adversaries constrained by the narrow visibility of internal-only logs. There is a better way.

Today's adversaries are state-sponsored units and organized cybercrime groups. These threat actors operate globally, as a 8x5 full-time job, targeting you but also others. Still, you continue to counter these threats with just one piece of the puzzle, your network telemetry. Attacker footprints surface in VirusTotal thanks to community crowdsourcing. Unlike any other service, VirusTotal contextualizes your internal logs with real-time world-wide patterns, expanding your field of vision and making telemetry truly actionable.

Use cases by team ➤➤➤➤

VirusTotal Enterprise is an investigative exoskeleton that radically upskills your security organization, effortlessly from day zero

Security Automation team

- Automatic alert triage via API interaction or one-click integrations
- Security telemetry enrichment, continuously via feeds + API lookups
- Context-driven security orchestration, through your SOAR or custom via API

SOC/CERT

- True positive prioritization and false positive discarding
- Contextualization of alert observables & phishing investigations
- Incident campaign IoC identification for preventive & remediative actions

Incident Response team

- Root cause analysis and attack chain exploration
- Forensic analysis and breach containment
- IoC-driven SIEM threat hunting to understand breach breadth

Threat Intelligence team

- Discovery of unknown threats to complement existing defenses
- Campaign monitoring to preventively block malicious infrastructure
- Threat actor tracking for proactive TTP hunting & situational awareness

Malware Analysis team

- Automatic static & dynamic analysis to understand unknown files
- Download and dissect malware reported by the industry
- Classification and attribution via genetic analysis with n-gram searches

Anti-fraud team

- Identification of phishing campaigns & counterfeiting sites targeting your org
- Mitigation of banking and identity theft trojans against your company
- Interception and study of phishing kits and C2 panels for the above

Anti-abuse team

- Corporate infrastructure abuse detection & digital asset monitoring
- Brand impersonation detection - fake apps, online lures and others
- Scoring of IP addresses interacting with your services

Red team / Pentesting team

- Blackbox reconnaissance & passive fingerprinting
- Breach & attack simulation emulating adversary TTPs
- Security stack validation to identify blindspots and mistaken setups

Vulnerability Management team

- Vulnerability prioritization & smart risk-driven patching strategy
- In-the-wild vulnerability weaponization monitoring
- Threat landscape exploration from a vulnerability exploitation perspective

Most importantly, all of the above can be performed **collaboratively**. Modules like *VT GRAPH* allow ACL-driven investigation sharing, such that **multiple analysts from your organization or trusted circles** can cooperate to understand the full scope of an attack. Act faster and smarter by working together.

Google Cloud | VIRUSTOTAL

VirusTotal boosts your team's performance and radically increases the RoI for your existing security investments

As a CISO, C-Level or any other kind of business leader, you do not need more tools, feeds or services. What you truly need is more relevance and effectiveness coming from your existing staff and technical stack, it is your job to empower them. Most security intelligence vendors excel at creating media buzz around the latest fancy nation-state attack they have uncovered, usually completely irrelevant to your company. VirusTotal, rather, invests those dollars in the product itself, so that it is you the one that does not hit the headlines.

Outcomes for leaders

CISO challenges	Solving with VirusTotal
Alert fatigue & overload A Palo Alto Networks survey data shows that SOC analysts are only able to handle 14% of alerts generated by security tools	**Eradicate SOC analyst burnout** VirusTotal includes malicious + benign information, automate false positive discarding and true positive confirmation via API or integrations
Quality & speed of incident response Overloaded staff, disconnected IT systems, numerous sources and services leads to high reaction & remediation times	**Improved productivity through automation** Orchestrate & automate response via API, speed up decisions with unrivaled context & multi-angular characterization
Missed threats Threat feeds and most security technologies only block known bad. Despite increasing investments, breaches continue and attackers outpace defenders	**Proactiveness & prevention** VirusTotal equips your analysts with a swissknife to unearth threats unknown to the industry, and gives you unmatched context to up your security stack
Increasing & changing attack surface area Licensing of new technologies, SaaS products and the move to the cloud is introducing unprecedented entropy and heavily impeding monitoring	**Increased visibility & early warnings** VirusTotal allows you to enrich anything, everywhere. We are not tied to GCP observations or any other cloud or infrastructure
Finding and maintaining security talent There is a shortage of qualified security candidates, recruiting and retaining these is an endemic challenge. Keeping them up-to-date with threats is even harder.	**More performant and efficient staff** VirusTotal elevates your teams and upskills your juniors, such that L1 analysts can perform like advanced threat hunters
Budget constraints & understaffing Cybersecurity isn't top of mind at most organizations when budget line items are getting funded. These constraints also apply to headcount	**Consolidate/lower costs, do more with less** VirusTotal is the one-stop-shop for everything threat related, consolidate and automate repetitive tasks to do more with your existing staff
Proving value on security investments Existing technology metrics have little to no correlation with business success, and thus fail to make a positive impression on the board. Securing budget in subsequent cycles becomes challenge.	**Increased SIEM/SOAR return on investment** Take your technology stack to the next level with the richest threat intelligence suite. Radically improve value and easily generate performance metrics by reporting on blindspot coverage.

Google Cloud | VIRUSTOTAL

VirusTotal betters the promise that others fail to deliver

Cybersecurity teams currently license expensive threat feeds, TIPs or platforms that promise to extend your threat visibility but lack breadth and context. In the best case, you are consuming intelligence generated by a skilled team of 10 or 20 analysts, thus, your operations can only be as effective as their findings. This introduces latency and noise, as those threat might be irrelevant to your org. VirusTotal is the missing, and much needed, piece in your existing security investments - the crowdsourced lense.

Why VirusTotal? ➤➤➤➤

Community crowdsourcing ›› Unrivaled context

VirusTotal operates a free public website that is used by **millions of home and corporate users every month**. We are **not constrained to sightings in our own install base** and thus we have become the richest and freshest threat corpus.

Multi-kind characterization ›› Enrich everything

We offer in-depth characterization of files, hashes, domains, IPs and URLs, adding context to all observables found in your logs and allowing you to pivot over any of these kinds. Any file type, all threats. No need to license numerous products, **VirusTotal is your one-stop shop for everything Threat Intelligence related**.

Multi-angular detection ›› Miss nothing

VirusTotal aggregates a myriad **of orthogonal mechanisms to flag maliciousness**: 70+ antivirus solutions, behaviour verdicts coming from over 15 home-grown + 3rd-party sandboxes, crowdsourced YARA rules matching, SIGMA rules acting on detonation event traces, IDS rules acting on dynamic analysis network communications, static dissection of macros... The ultimate defense-in-depth enrichment platform.

Allow lists information ›› Eradicate alert fatigue

We excel at finding bad but also at discarding false positive alerts. **VirusTotal is also the largest aggregator of datasets to understand if an observable is benign**: Microsoft Clean File Metadata Feed (CFMDF), *trusted source project*, NSRL hashes, *VT Monitor software*, file signature information, tagging of files that appear in download sites (e.g. uptodown), domain popularity ranks, etc.

Partnerships ›› Stand on the shoulders of giants

Hundreds of **world-leading security vendors** across the globe have partnered with us to build the largest multi-scanner and threat sharing platform in the planet.

World-wide real-time telemetry ›› Know your enemy

Submissions by **2M+ distinct monthly users coming from over 232 countries**. This gives us unique visibility to understand geographical spread of threats, activity timelines, first seen dates, threat actor lures, in-the-wild patterns, etc.

Volume & history ›› Leave nothing unanswered

The threat corpus is composed of **over 3B files, more than 50B if we were to consider bundles**. 5B URLs growing at a rate of 6M analyses/day. 10B passive DNS records and growing. All these **sightings go back to 2004, unlike no other service,** and give you **unprecedented retrospective visibility** into threat actor campaigns and their evolution.

Interconnections & graph ›› Superior understanding

Parent-child relationships are created between all of the aforementioned IoCs. When confronted with an unknown file we can tell you all the URLs from which it gets downloaded, any emails in which it was seen as an attachment, etc. All of these links are explorable with *VT GRAPH*.

The home of YARA ›› Outsmart adversaries

VirusTotal **originally created and continues to advance *YARA***, the de-facto standard for campaign monitoring and threat actor tracking. Its capabilities when acting on VirusTotal's live flux are unparalleled, as you can even match *detonation traces* or automatically generate optimal rules.

Google planet-scale ›› Faster operations

VirusTotal is a Google Cloud team, building on the very same **planet-scale and instant search infrastructure** that powers Google's most popular services. As an example, our n-gram search index is 5PB in size and allows you to search for strings and random file binary patterns at sub-second speeds. Only Google has the computing resources required to power these kind of use cases.

Industry backbone ›› One-click integrations

VirusTotal has become and industry de-facto standard, no other solution has **plugins for almost any 3rd-party security technology** that you might be using. We take SIEM, SOAR, EDR, IDS, etc. to the next level, effortlessly.

Smooth & Simple ›› No expertise required

We have the *most exhaustively documented API* in the market and have **democratized the most complex of tasks**, e.g. automatic YARA rule generation. You do not want a solution that requires engineers to operationalize it, VirusTotal frees up resources so that your team can focus on protecting the organization, not on technical impediments.

Google Cloud | VIRUSTOTAL

Solutions that any team can use to defend like only the most advanced organizations can

Security analysts and incident responders are often confronted with files/URLs/domains/IPs for which they know nothing. Without further context, it is virtually impossible to make sense of an attack, determine attribution, build effective defenses against other strains, or understand the impact of a given threat to your organization. Through API and web based interaction with the VirusTotal corpus, corporate security teams can quickly build a picture of an incident, and then use the information to better protect against it and other attacks.

Service components

VT INTELLIGENCE

The "Google" of malware. Unparalleled context for individual threat observables found in your investigations. Allows you to pivot to similar or related artifacts to surface additional IoCs. Indexes antivirus labels, static properties (e.g. office macros), binary contents (n-grams), sandbox detonation reports, network traces, provenance information, whois lookups, SSL certificates, popularity ranks, etc. and makes it instantly searchable with *over 100 search modifiers*. Download matching files for further scrutiny offline.

VT GRAPH

Explore the VirusTotal threat corpus visually and map out attacker campaigns. Discover commonalities and symptomatic patterns with just one click. Share and collaborate on investigations, export connection graphs into executive reports. Follow investigation leads automatically via intelligent expansion playbooks.

VT HUNTING

Deploy YARA rules and apply them to the live flux of incoming files, review notifications or ingest them programmatically. Run YARA rules back in time over the historical corpus. Automatically generate optimal YARA rules for a group of files, perform sub-second searches across the historical threat corpus. Download matches via web interface or programmatically for offline study and complementary analysis.

VT API

Perform all of the above tasks programmatically, automate workflows with the VirusTotal dataset. Programmatic enrichment of alerts, e.g. SIEM real-time event contextualization. Any kind of threat observable (hashes, domains, IPs, URLs, SSL certificates, etc.).

Technical highlights

- **Understand what an unknown file does through sandbox tracing**
- **Learn about any malicious activity that was historically tied to an IP or domain**
- **Instantly pivot to similar artifacts, find additional IoCs and feed defenses**
- **Search for relevant malware targeting your org / industry**
- **Automatically create YARA rules, one-click export into your EDR**
- **Match community uploads with YARA and reveal attacker TTPs**
- **Programmatically check domains, IPs, files, hashes and URLs**
- **Copy & Paste your API key into your SIEM/SOAR and instantly enrich**

VT FEEDS

Live stream of absolutely all analysis reports for files, domains, IPs and URLs processed by VirusTotal. Perform live enrichment of SIEM logs for retrospective threat hunting. Create an on-premise dataset replica for highly sensitive investigations or use in regulated or air-gapped environments. Stream into data analytics solutions for automated IoC generation via aggregations and groupings. Download all uploaded files for analysis in specialised systems and sandboxes, or to apply YARA rules offline.

Google Cloud | VIRUSTOTAL

Plug your operations into the largest collaborative cybersecurity effort in the planet

VirusTotal's vision is to make breaches insignificant by consolidating as the leading threat intelligence sharing hub, orchestrating global threat response across world-wide distributed security teams. Our data is so comprehensive and unique that Google itself decided to acquire VirusTotal back in 2012, that's how world leading malware fighting met planet-scale technology to give good the advantage.

The VirusTotal advantage

The path to stronger and more affordable cybersecurity starts here

Cybercrime damages	Experienced at least one breach	Security alerts per day	Cybersecurity workforce gap
$6T	55%	15K+	3M+
A constantly evolving threat landscape	Increasingly sophisticated attacks	Alert fatigue & repetitive tasks	Talent is difficult to find & maintain
$5M+ Savings	**10X Threat visibility**	**70% Faster resolution**	**<1 min Complex tasks**
Prevents theft, reputation damage, fines and penalties	Live monitoring of threat landscape via YARA	Automate alert triage & leverage community insights	Instantly upskill your team, e.g. L1 analysts creating YARA rules in <1 min

19 YEARS Observations going back to 2004

3B+ files
50B+ considering compressed bundles

1B+ Sandbox reports

2M Analyses per day

232 COUNTRIES submitting files

3M+ MONTHLY USERS Generating Intel

6B+ URLs
6M+ URL analyses per day

5B+ Domains

170B+ pDNS Resolutions

45/71
70+ Antivirus
90+ URL blocklists
15+ Sandboxes
100K+ Crowdsourced YARA, SIGMA, IDS rules