Google Cloud | VIRUSTOTAL

VirusTotal Private Scanning

Get a second opinion on suspicious files, automatically extract IoCs and assess impact to your org

See files through the eyes of VirusTotal without uploading them to the main threat corpus, in a non-shareable fashion. Security teams are often confronted with an unknown file and asked to (1) understand if it is malicious, (2) 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 of a given threat in your organization. Private scanning bridges the gap and generates insights to neutralize threats.

Crowdsourced detection via orthogonal techniques & technologies.

Maliciousness flags based on static, behavioural, network and similarity analysis leveraging crowdsourced {YARA, Sigma, IDS} rules and community + proprietary clustering algorithms.

In-depth automated malware analysis with multi-platform sandboxes.

Dynamic analysis in {Windows, OS X, Linux, Android} to dissect process, filesystem, registry, synchronization, memory, network and other execution activity. Extracts IoCs and MITRE ATT&CK TTPs for advanced hunting in your environment.

Static dissection flagging suspicious attributes and capabilities.

File signature analysis, document macro extraction, module imports, permission requests, EXIF metadata, etc. to unearth unknown badness flying under the radar.

Similarity analysis for malware family, campaign and adversary context.

Uncover ties with other files and network locations in the open VirusTotal threat corpus without exposing your submissions to other VirusTotal users. Pivot and surface connected IoCs.

Key Benefits

- Flag known & unknown threats
- Full attack lifecycle visibility
- Maximize SOC & IR team efficiency
- Automations with extensive API
- Scales seamlessly - no devops, no setup, no engineering

Unique visibility into threats

- Comprehensive good/bad flags and more confidence
- Detailed behaviour report, including anti-VM + MITRE ATT&CK
- IoCs for containment, remediation and blast radius identification

Get a demo

Google Cloud | VIRUSTOTAL

Privacy Preserving?

VirusTotal private scanning provides an alternative for customers who want to use VirusTotal´s capabilities but cannot or don't feel comfortable sharing certain files with the rest of the VirusTotal community.

Uploaded files go through a similar process as any other file submitted to standard VirusTotal, being processed by a myriad of static and dynamic analysis microservices.

The main difference being that the files are not published in VT ENTERPRISE, are not downloadable by other users, and that antivirus verdicts will not be available for those files.

Massively validated

The world's largest crowdsourced threat intelligence community (www.virustotal.com) is powered by the very same building blocks as VT Private Scanning - used by 3M+ users a month and analyzing 2M+ files per day.

Fully cloud based, scales seamlessly, no setup, no admin.

Automatic malware analysis in the cloud with superior threat intelligence contextualization

API and web interaction

Immediate time to value with intuitive and insightful web interface. Easy-to-use REST API for integration with SIEMs, SOARs, TIPs, etc.

Command-line client tool

Automate from day 1, minimal coding required. Concise console summaries for fast, confident and accurate decisions and next-steps.

Broad file support

EXEs, DLLs, Documents, PDFs, DMGs, Mach-Os, ELFs, etc. Dynamic analysis for any file type supported by Windows, Linux, OS X and Android.

Multi-angular hybrid analysis

Static, dynamic, memory and network analysis. Automatic correlation with known bad in VirusTotal's main threat corpus.

Downloadable analysis artifacts

PCAP, Windows EVTX and memory dump available for offline study. Self-contained exhaustive HTML report for easy sharing with team and other collaborators.

Superior context & analysis

Contextualization of related IoCs (IPs, domains, URLs, hashes) with VirusTotal's market leading threat intelligence dataset. Links with known campaigns and actors.

Anti-evasion technology

Vast coverage for the most common anti-sandboxing techniques. User behaviour emulation. Multiple distinct sandboxes for the same platforms to fight cloaking.

Automatic malware config extraction

Decoders and decryptors for the most prevalent malware families. Unearth CnCs, payload download URLs, dropzones, etc. even when not seen during execution.