REVERSINGLABS

PRODUCT BRIEF

TitaniumCloud File Intelligence vs. VirusTotal

Security teams have a choice! ReversingLabs offers unequalled file intelligence with more total and more current data along with complete query/post privacy and enterprise class support. ReversingLabs also offers an option VirusTotal cannot – a complete onsite malware analysis solution that combines the industry's authoritative file intelligence database with an on-premises malware analysis and threat hunting platform. If your security team is tired of struggling with the limitations of VirusTotal, it is time to take a look at ReversingLabs.

- **3X more Malware & Goodware files**
- **Private, GDPR compliant service**
- **More flexible YARA hunting & retro-search**
- **Enterprise Class Support**

ReversingLabs

ReversingLabs' TitaniumCloud File Intelligence Service is the authoritative source for up-to-date intelligence on over 7 billion goodware and malware files. ReversingLabs does not depend on crowdsourced collection but instead curates the acquisition of files from extensive harvesting operations, software vendors and diverse malware sources.

TitaniumCloud processes every file using unique File Decomposition technology for definitive classification and meta data extraction. This information is then augmented with information from hundreds of security partners including next gen endpoint, intelligence, analytics, anti-virus and dynamic analysis vendors to provide industry reputation consensus. TitaniumCloud supports an extensive array of query, hunting, retro-search and YARA rules capabilities. TitaniumCloud also provides API intelligence feeds that can be delivered directly into your SOC tools.

TitaniumCloud is a private, secure and GDPR compliant file intelligence service designed for world-class enterprise security teams. The user controls the privacy of uploaded data, choosing to share the files, share only the results or share nothing. ReversingLabs is also an enterprise class security software company. We provide world-class support and account management. You can call us directly and talk to a real employee - 1.617.250.7518.

VirusTotal

As part of Chronicle, VirusTotal is a crowdsourced malware intelligence service that contains over 2 billion malware files, and has about a million files uploaded per day. VirusTotal includes query, hunting, search and YARA rules capabilities, and includes 66 antivirus scanners to provide industry consensus file reputation data. VirusTotal offers both a free and premium service based on query numbers and service types.

VirusTotal's crowdsourced model provides useful information, but it also puts your enterprise at risk. Any data loaded into VirusTotal is essentially public. That means files with PII, PHI and IP data cannot be investigated with VirusTotal. As an enterprise with sensitive data, you do not want the risk that the wrong files are uploaded. As a company that must be GDPR compliant, you cannot risk allowing any files to be loaded into VirusTotal. Finally, because anyone can access VirusTotal, cyber criminals are reported to use it to test their own malware code (1).

Chronicle is not a commercial enterprise-focused software company. You will not find a phone number on their contact site (only emails) or find a customer support site (2). And being part of the Chronicle behemoth, being flexible to meet customer needs is not in their DNA.

THE BOTTOM LINE: TitaniumCloud is not a crowdsourced service. It combines ReversingLabs research, curated file harvesting, and an expansive partner network sourcing malware from hundreds of leading security vendors, and not just anti-virus vendors, to provide intelligence on 3x more files than VirusTotal.

Capabilities Comparison: TitaniumCloud versus VirusTotal

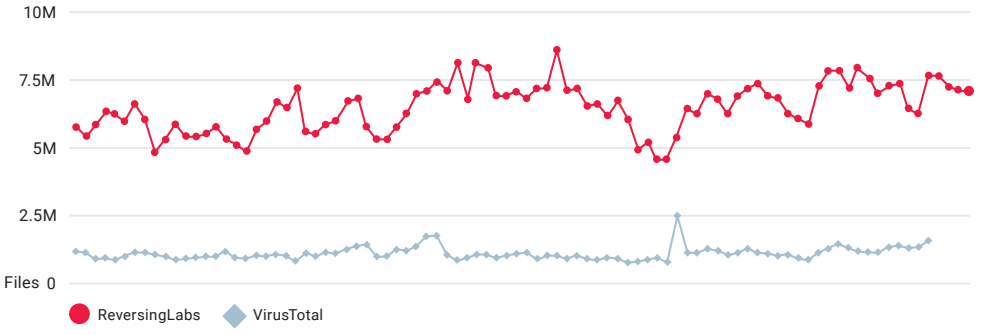
	TitaniumCloud	VirusTotal
Total Files	7 Billion	2 Billion
Daily files uploads	6 Million	1.5 Million
Private, GDPR Compliant, Protected Access	Yes	No
Specialized feeds and APIs	Yes – over 30	2
Uploaded file privacy with sharing option	Yes	No
File Types Supported	3500	125
Delete uploaded files	Yes	No
Primary malware research	Yes	No
Option for onsite database	Yes	No
Flexible YARA & Retro rules searches	Yes	Limited
Services	Automated File Unpacking, Queries, Uploads, Downloads, Alerts, Notifications, Multi-scanning	Queries, Uploads, Downloads, Alerts, Notifications, Multi-scanning

Try writing a YARA rule with keywords like company name/ username/ password/ etc. and watch sensitive and classified documents leaked into VirusTotal begin to appear.

(1) https://thehackernews.com/2017/08/fortune-1000-data-leak.html
https://www.wired.com/2014/09/how-hackers-use-virustotal/

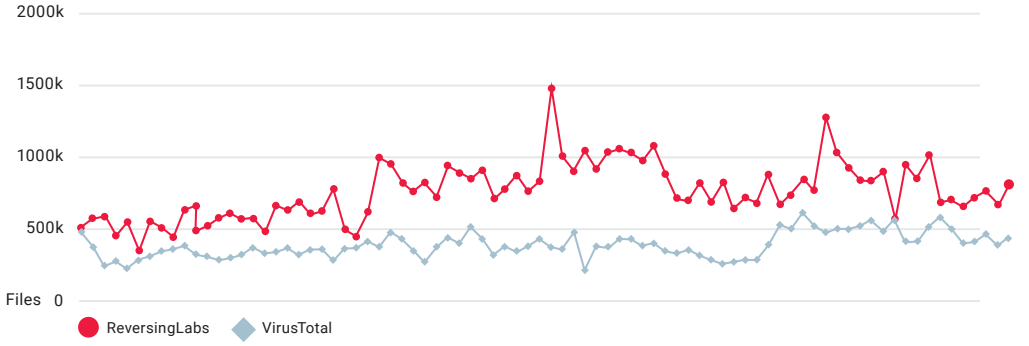
(2) https://chronicle.security/work-with-us/

Files Analyzed per Day



350%
More files analyzed daily

New Malware per Day



160%
More new malware analyzed daily

TitaniumCloud Features

Reputation Database with 3X More Data

- Over 7 billion unique file records with data classification, adding up to 8 million malware and goodware updates daily
- Every sample is processed using automated static analysis to extract all objects and uncover threat indicators
- 3500 file formats identified
- Over 350 family types unpacked and analyzed including archives, installers, packers and compressors
- Historic detection information from more than 45 AV scanners for industry consensus showing changes over time
- Malware samples continually reanalyzed for the most up-to-date file reputation status

Flexible Query, Hunt and Retro-Search

- High-performance online query processing
- Functional similarity hash queries to identify new threats and find similar malware
- Advanced search and hunting by file context and threat indicators
- Alerting on threat level changes for subscribed files
- Integrated YARA/SNORT Rules Engine

Private and Secure File Intelligence Service

- Absolute control over privacy and sharing of uploaded files
- Achieve GDPR and other privacy regulation compliance
- Retrieve files uploaded in error
- Choose what threat metadata that is shared
- Optional ReversingLabs A1000 adds global analysis without requiring files to leave your network.

Queries via REST Web Services APIs

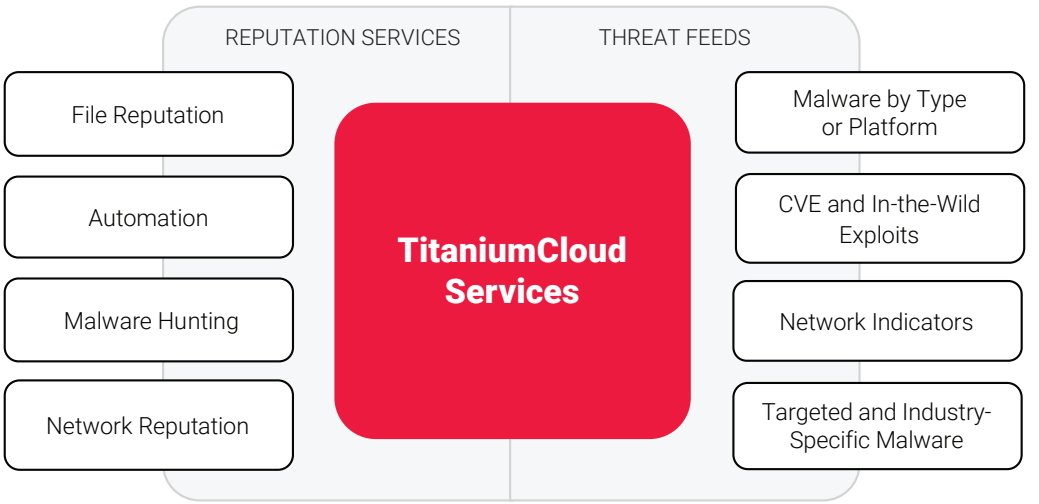
- Powerful query and feed functions
- REST API for automated analysis process integration
- File reputation information via single and bulk hash queries
- Extensive feeds for the latest malware for specific threats, e.g. file types, threat types, industry, CVE, URI

Delivery Options

- Online Cloud-based service with web GUI
- On-premises T1000 File Reputation Appliance

TitaniumCloud APIs and Feeds

TitaniumCloud REST APIs provide access to an array of services in the form of file intelligence and threat feeds. Among the more than 50 APIs included are file reputation, file analysis, malware hunting, and network information. These also include daily feeds of malware targeting Linux or MacOS devices, newly detected exploits, IPs and domains extracted from known malware, and threats targeting specific industry sectors (e.g. Financial Services, Healthcare, Retail).



With its superior total file counts and accuracy, curated file harvesting, expansive partner network and enterprise-class privacy, TitaniumCloud is the right file intelligence solution for security teams that are serious about early malware detection and response. ReversingLabs goes beyond what VirusTotal can offer by combining our authoritative File Intelligence Service with our A1000 onsite malware analysis platform. A complete, automated reverse engineering and malware hunting platform focused not just on global malware intelligence, but also on the unknown files and malware living within your enterprise.

FUNCTIONALLY SIMILAR MALWARE WITH CLICKABLE LINK TO PIVOT

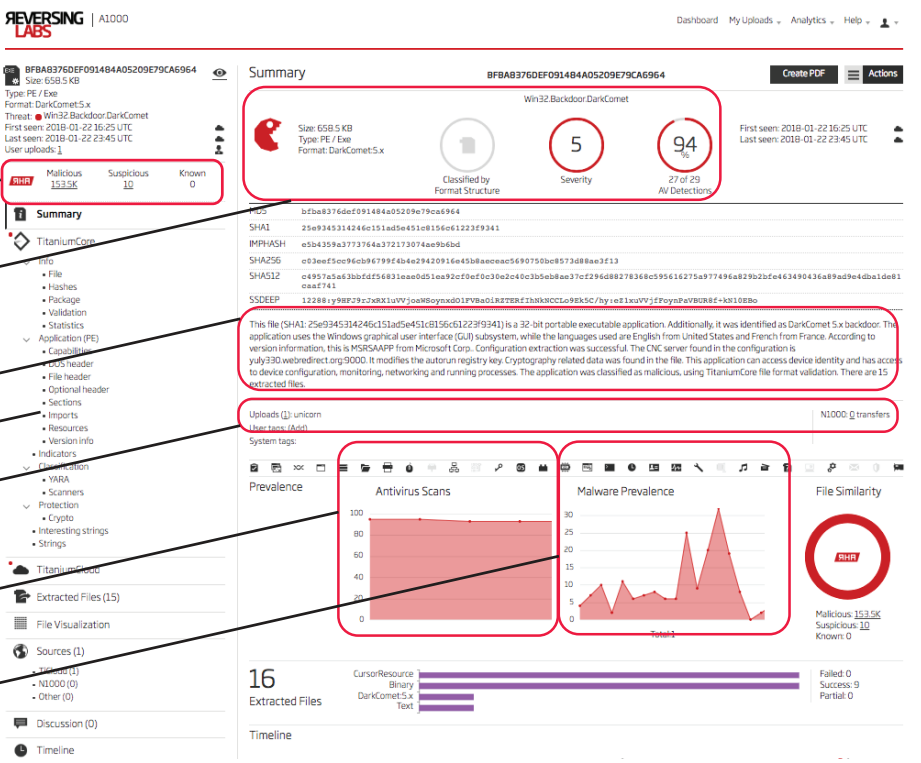
THREAT NAME, LEVEL, & SEVERITY

FILE CHARACTERISTICS AND INDICATORS IN PLAIN ENGLISH

STATIC BEHAVIORS

HISTORIC A/V DETECTION

PREVALENCE OVER TIME



The A1000 Summary Page shows threat levels based on TitaniumCloud File Reputation, Automated Static Analysis, and ReversingLabs' Hashing Algorithm (RHA) which correlates file content to functionally similar known malware.

PERMISSIONS: TAMPERS WITH OR REQUIRES PERMISSION

FILE: ACCESSES FILES IN AN UNUSUAL WAY

EXECUTION: CREATES OTHER PROCESSES OR STARTS OTHER APPLICATIONS

NETWORK: CONTAINS URLS

REGISTRY: ACCESSES REGISTRY AND CONFIGURATION FILES IN AN UNUSUAL WAY

EVASION: TRIES TO EVADE COMMON DEBUGGERS, SANDBOXES/ANALYSIS TOOLS

The A1000 Threat Indicators Page includes plain English details and descriptions of analytic and activity-based indicators of attack.

Add the Power of the ReversingLabs A1000 Malware Analysis Platform

For security teams that want to significantly upgrade their inhouse malware analysis and hunting capabilities, ReversingLabs offers the A1000 Malware Analysis Platform. The A1000 delivers automated file decomposition and static malware analysis as well as targeted malware hunting without ever sending files off-site. It is fully integrated with the TitaniumCloud File Intelligence service. The A1000 includes threat and context visualization, APIs for integration with automated workflows, a dedicated database for malware search, global and local YARA rules matching, as well as integration with 3rd party sandbox tools.

When your security team discovers an unknown piece of malware or a variant unknown to AV scanners, the A1000 empowers your team to take control. The A1000 processes all files locally providing critical on-time information. All unknown files are automatically unpacked and analyzed without files leaving the premises unless explicitly instructed to do so. The results are presented with summary and in-depth analyses. YARA rules can be written to search out similar files or upgrade defenses when a new threat is identified. Newly discovered threats are checked against TitaniumCloud's records for malware family similarity to surface new or polymorphic malware. YARA rules can also be tested against TitaniumCloud samples for result accuracy.

A1000 Benefits

- **Definitive File Analysis:**
  extracts internal indicators and assigns threat levels in milliseconds.
- **Extensive Format Coverage:**
  includes PE, ELF, MachO, Dex, .NET, Java, JS, documents, firmware, and business apps.
- **Rich Context Visualizations:**
  view context, intent and severity to determine further action.
- **Integrated YARA Rules Engine:**
  utilize custom rules to search out new and advanced malware across local and global file collections.
- **Onsite Private File Analysis:**
  files not shared publicly so files and results never leave your site.
- **Centralized Content Repository:**
  securely store local files of interest for collaborative search, analysis and hunting.
- **Automated Workflow Integration:**
  powerful REST APIs integrate with existing workflows and processes.

When security teams cannot risk letting the bad guys know their defense posture. When data is just too valuable to lose. When compromise is not an option, ReversingLabs offers a superior solution to VirusTotal as it's designed and supported for enterprise security teams. Unequalled file intelligence, comprehensive private query and feed services, and a complete onsite malware analysis and hunting solution provide the tools security teams need to detect malware earlier, respond faster and stop the damage caused by advanced malware attacks.

REVERSINGLABS
+1.617.250.7518
sales@reversinglabs.com