

T1000 File Reputation Appliance

On-Premises Access to Industry Leading TitaniumCloud Database

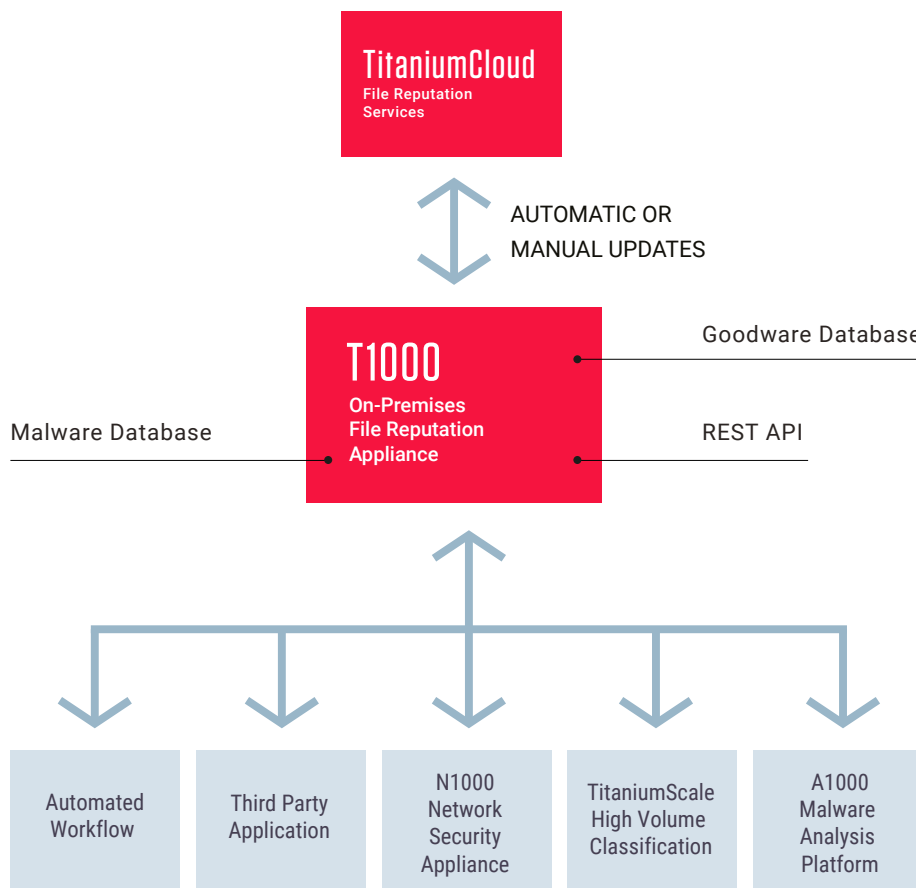
T1000 Benefits

- **Operate in Complete Privacy:** with a local replica of TitaniumCloud File Reputation data so no queries leave your site.
- **Stay Up-to-Date:** over 8 million data updates daily can be applied automatically in real-time over the Internet or manually for "air-gapped" situations.
- **Access the Right Level of Detail:** includes two data sets to support summary or detailed file intelligence requirements.

The T1000 File Reputation Appliance provides on-premises access to file reputation and threat information via a private, high-performance REST interface. The T1000 Appliance utilizes a local, up-to-date replica of data from the TitaniumCloud File Reputation database containing the industry's most comprehensive coverage with over 8 billion goodware and malware files. The T1000 database supports continuous updates over the Internet or manual updates for air-gapped operations.

T1000 Provides On-Premises File Reputation Data

The T1000 Appliance provides access to an on-premises, up-to-date copy of data from the industry's most comprehensive source for threat intelligence and reputation data on files - ReversingLabs TitaniumCloud. The T1000 can support use cases where file reputation lookup and malware presence queries require higher performance or privacy.



T1000 Data Sets

ReversingLabs' TitaniumCloud File Reputation Services is the industry's most comprehensive solution with up-to-date, threat classification and rich context on over 8 billion goodware and malware files. ReversingLabs does not depend on crowdsourced collection but instead curates the harvesting of files from multiple software vendors and diverse sources of malware intelligence. All files are processed using unique ReversingLabs File Decomposition (FD) technology to derive detailed context and input from over 40 anti-virus scanners providing industry reputation consensus. The T1000 File Reputation Appliance delivers on-premises access to two data sets for the files in the TitaniumCloud database: R1 for summary information and XG for detailed information.

T1000 Features

On-Premises File Reputation Access

- Local replication of TitaniumCloud File Reputation data for privacy or air-gapped operations.
- High-performance REST API for single or bulk file hash queries (same API as TitaniumCloud online).
- Two data sets support summary or detailed file intelligence requirements.
- Database updates automated via the Internet or manual for air gapped operations.

Integration

- Seamless integration with ReversingLabs solutions:
 - A1000 Advanced Malware Analysis Platform
 - N1000 Network Security Appliance
 - TitaniumScale Enterprise Scale File Analysis
- REST Web Services API to support custom automated workflows.

Data Set	R1	XG
MD5, SHA1, SHA256 Hashes		✓
File Size		✓
Threat Level	✓	✓
Threat Name	✓	✓
Anti-Virus Detection Percentage	✓	✓
Platform	✓	✓
Threat Type and Family Name	✓	✓
First Seen, Last Seen	✓	✓
Last Scanned		✓
Trust Factor	✓	✓
File Type		✓
Classification Result	✓	✓
Continual File Reputation Status Analysis	✓	✓
Anti-Virus Results by Vendor		✓
Source(s) of Sample's Origin		✓
Parent Packages of File Samples Origin		✓
PE Version Information & Static Analysis Data		✓
Full Certificate Chain and Validation		✓

TitaniumCloud File Reputation

- Over 8 billion unique file records, with up to 8 million malware and goodware updates daily.
- Every sample processed using unique ReversingLabs File Decomposition to extract all objects and uncover threat indicators.
- 3600 file formats identified.
- Over 360 file formats unpacked and analyzed including archives, installers, packers & compressors.
- Files processed using over 40 AV scanners for industry consensus.
- Malware samples continually reanalyzed for the most up-to-date file reputation status.

T1000 Appliance Packaging

- Hardware: 1U appliance
- Virtual: VMDK image
- Cloud: AWS AMI