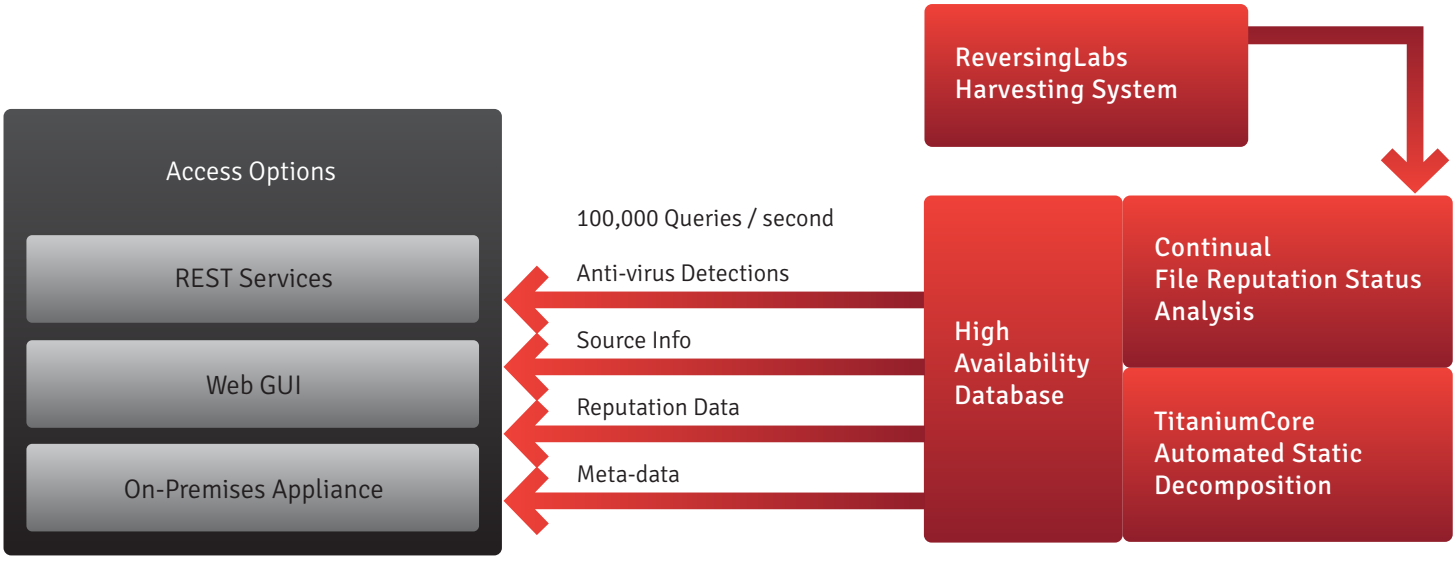
TitaniumCloud™

The Ultimate File Reputation Source



TitaniumCloud™ file reputation services provide the industry's most comprehensive source for threat intelligence and reputation data on files.

TitaniumCloud identifies files and provides rich information about their contents. Every sample is processed using the ReversingLabs TitaniumCoreTM Automated Static Analysis Decomposition engine to extract all contained objects and their internal Proactive Threat Indicators (PTIs). The samples are recursively unpacked, decompressed, decrypted and de-obfuscated. The proactive indicators extracted from the resulting components includes format, format validation, strings, sections and certificate chains. Malware samples are also continuously re-scanned providing historical detection information and their detection history is stored in the TitaniumCloud database.

Powerful query functions are accessed through a high performance REST Interface. **TitaniumCloud** uses a proprietary NoSQL database optimized to support advanced search and record updates across billions of file records in milliseconds.

FEATURES

Threat intelligence and reputation data on files
- XREF – 800+ million malware samples
- GREF – 1.7+ billion known goodware samples

Over 3000 threat indicators per file
- Indicators include file reputation, anti-virus detection history and detailed internal information
- File source information and trust factor for all goodware samples
- Historic anti-virus scan data and threat factors
- Malware repository re-scanned continuously for changes to detection information

Query services
- Search for files by hash or anti-virus detection name
- Bulk queries supports multi-file searches

Performance scales to meet stringent requirements
- Bulk queries supports multi-file searches

Performance scales to meet stringent requirements
- 8+ billion online queries per day capacity
- Optional on-premises appliance with database instance for low latency access and privacy

Sample downloads access for qualified customers

USE CASES

Forensics and High Volume Classification

- TitaniumCloud reduces wasted analysis time and assets by identifying new samples as known malware or goodware through an automated REST Web Services interface.

Incident Response and Triage

- TitaniumCloud makes analysts more productive by quickly identifying and providing information on known goodware and malware.
- Analysts can search for samples with the same anti-virus detection malware name for comparison to learn more about a threat.
- Analysts can search for similar samples using threat indicators, e.g., same section hash, embedded domain name.

RHA1

- Analysts can uncover similar hashes leveraging ReversingLabs Similarity Hashing Algorithm (RHA1)

Software Validation

- TitaniumCloud can identify malware and unknown components within an installation package.
- Analysts can proactively learn about false positive anti-virus detections on their company's software through alerts from TitaniumCloud.

OEM Solution

- Software and appliance vendors can integrate TitaniumCloud into their products to quickly identify known software.
- TitaniumCloud provides a REST interface that scales for high performance requirements.

TITANIUMCLOUD PLATFORMS

A1000 Malware Analysis Platform

The A1000, available as an online service or on-premises appliance, enables users to search TitaniumCloud for file information using a web GUI.

REST Web Services Over the Internet

Customer applications access TitaniumCloud REST Web Services API over the Internet. Results are returned in JSON or XML format.

On-premises T1000 Appliance

The T1000 Appliance provides high performance, low latency solution for high volume, automated applications. The appliance maintains a local copy of the TitaniumCloud File Reputation Service on a customer's premises which is updated in real-time over the Internet.

On-premises AT1000 Portable Incident Response Lab

The AT1000 plug and play appliance integrates with industry leading forensics solutions to significantly increase the speed and effectiveness of cyber investigations.

DATA SET OPTIONS

GREF

Access to information on over 1.4 billion known non-malicious files

XREF

Access to information on over 600 million known malicious files

Sample Access

Access to all files for qualified customers