ЯL REVERSINGLABS

TitaniumCloud
Reputation and Threat Intelligence Services

The Most Comprehensive Source for Reputation Data

ReversingLabs' TitaniumCloud Reputation Services is a powerful threat intelligence solution with up-to-date threat classification and rich context on over 18+ billion goodware and malware files. Alongside file reputation, the solution also identifies malicious network infrastructure. ReversingLabs operates independently of crowdsourced data collection, instead curating the acquisition of files from leading antivirus vendors and a range of malware and network threat intelligence sources and internal harvesting systems.

Every file sourced undergoes an analysis through the proprietary ReversingLabs' File Decomposition technology. This data, once refined, is integrated with additional dynamic and detection metrics, delivering industry-leading reputation consensus. ReversingLabs TitaniumCloud supports a powerful set of query and feed functions through REST APIs for automating threat identification, analysis, intelligence development, and hunting.

Key Features

Rich Reputation Information
accelerates threat analysis & response by quickly identifying known goodware & malware, or malicious network infrastructure.

Advanced Search in Milliseconds
enables malware analysts to research threats before they reach their organization.

Powerful Hashing Algorithms
identify a file's functional similarity to known malware, including APT and polymorphic attacks.

Targeted Feeds
allow customers to monitor attacks in the wild to prepare defenses & minimize impact.

Extensive APIs
enhance the effectiveness of existing security solutions and custom automated workflows.

Flexible Deployment Options
offer a cloud-based or on-premises appliance for air-gapped operations.
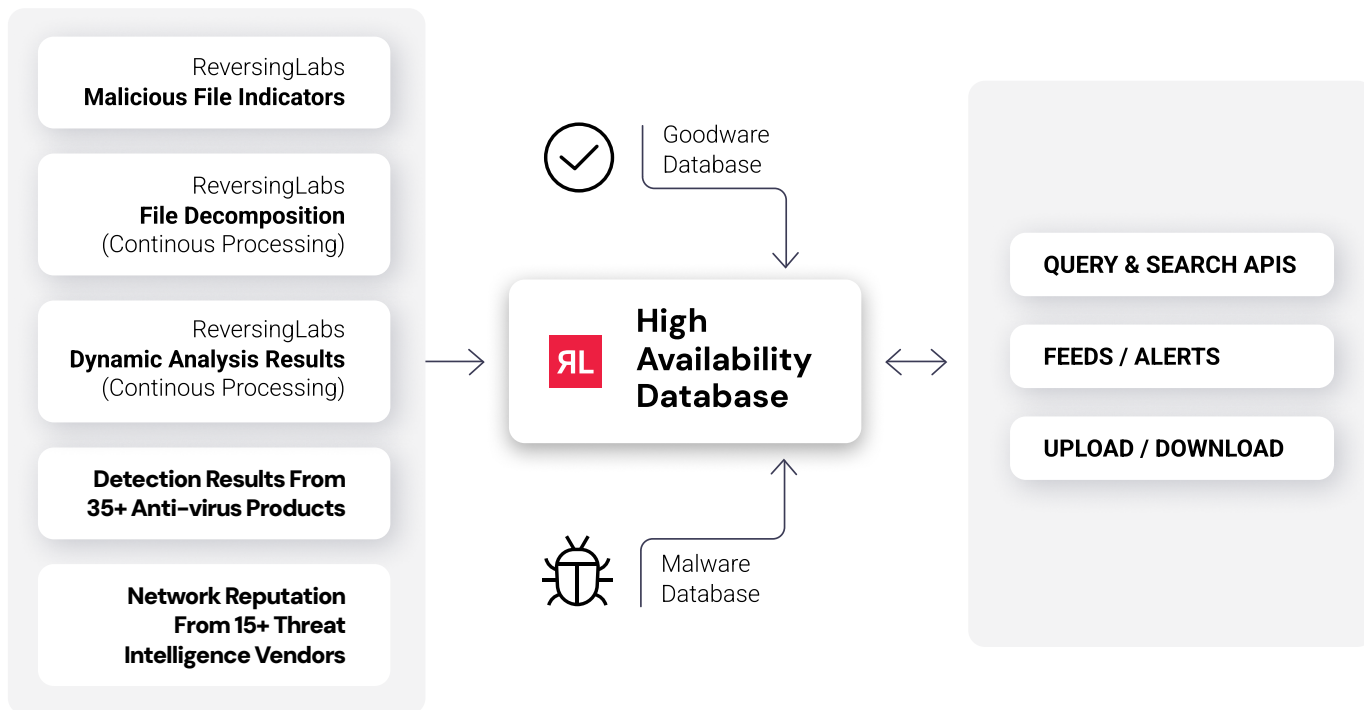
ReversingLabs API (RLAPI)
Bundles key APIs into a single offering to streamline purchase and deployment.

Global File Reputation

ReversingLabs TitaniumCloud continuously processes goodware and malware files, providing early intelligence about attacks before they infiltrate customer infrastructures. This visibility of in-the-wild threats enables threat analysts and hunters to prepare for new attacks and quickly identify the threat levels of new files as they arrive. TitaniumCloud enables more effective and efficient file analysis, the development of better threat intelligence, and the implementation of proactive threat-hunting and incident response programs.
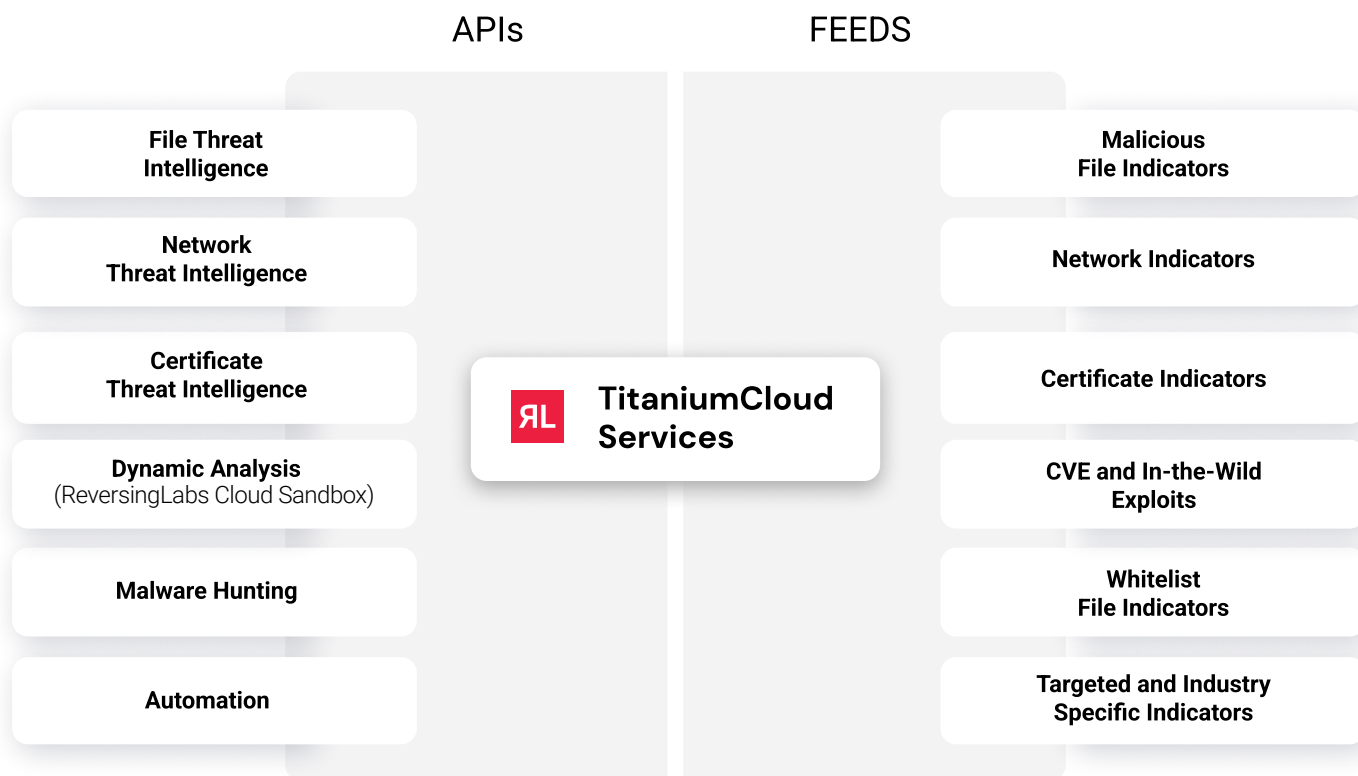
Secure and Private Goodware & Malware Repository

ReversingLabs TitaniumCloud maintains customer privacy with a secure query, file submission service, and data store.

TitaniumCloud Threat Intelligence APIs and Indicator Feeds

ReversingLabs TitaniumCloud provides over 50 Reputation Services, Threat Feeds, and Search/Query APIs that automate processing, analysis and threat status information gathering.

APIs

FEEDS

File Threat Intelligence

Network Threat Intelligence

Certificate Threat Intelligence

Dynamic Analysis (ReversingLabs Cloud Sandbox)

Malware Hunting

Automation

TitaniumCloud Services

Malicious File Indicators

Network Indicators

Certificate Indicators

CVE and In-the-Wild Exploits

Whitelist File Indicators

Targeted and Industry Specific Indicators

TRUST DELIVERED

TitaniumCloud Features

TitaniumCloud Database for File and Network Reputation Data

- Over 18+ billion unique file records with reputation data, analyzing up to 16 million malware and goodware files daily.
- 15+ network threat intelligence sources continuously consulted for the network infrastructure inspection.
- High-performance online query processing.

Delivery Options

- Online: Cloud-based service.
- On-Premises: T1000 File Reputation Appliance.
- Deployment in air gapped environments.

Targeted Reputation Feeds

- Malware samples continually reanalyzed for the most up-to-date file reputation status.

Queries via REST Web Services APIs

- Powerful query and feed functions.
- REST API for automated analysis process integration.
- File and Network reputation information via single and bulk hash queries.
- Functional similarity hash queries for identifying new and polymorphic threats.
- Control over privacy and sharing of uploaded files.
- Advanced search and hunting by file context and threat indicators.
- Alerting on classification and threat-level changes for subscribed files.
- File uploads and downloads.
- URL, Domain and IP Address Threat Intelligence.

Detailed File Reputation Information

- Every sample is processed using unique ReversingLabs File Decomposition to extract all objects and uncover threat indicators.
- Over 4,000 identifiable file formats.
- Over 400 file formats unpacked and analyzed, including archives, installers, packers & compressors.
- Historical detection information from over 35 anti-virus scanners for industry consensus shows changes.

Dynamic Analysis (ReversingLabs Cloud Sandbox)

- Delivers dynamic analysis reports or allows users to submit files and URLs for "detonation" within a virtual sandbox environment to generate a report.

About ReversingLabs

ReversingLabs is the leader of applied threat intelligence, protecting software development and powering advanced security solutions for the most advanced cybersecurity companies and Fortune 500 enterprises. The ReversingLabs Titanium Platform powers the software supply chain security and threat intelligence solutions essential to advancing enterprise cybersecurity maturity globally. ReversingLabs delivers trusted and actionable data, keeping enterprises informed, ahead of the threats, and ready to take on the challenges of tomorrow's attack surface.

Get started!

Improve your detection efficacy with a powerful threat intelligence solution with up–to–date threat classification

REQUEST A DEMO

reversinglabs.com

RL REVERSINGLABS

Worldwide Sales +1.617.250.7518
sales@reversinglabs.com