REVERSINGLABS

Titanium Platform

ENTERPRISE PLATFORM FOR AUTOMATED MALWARE ANALYSIS

File Threat Inspection, Intelligence, and Insight at Scale

Challenges

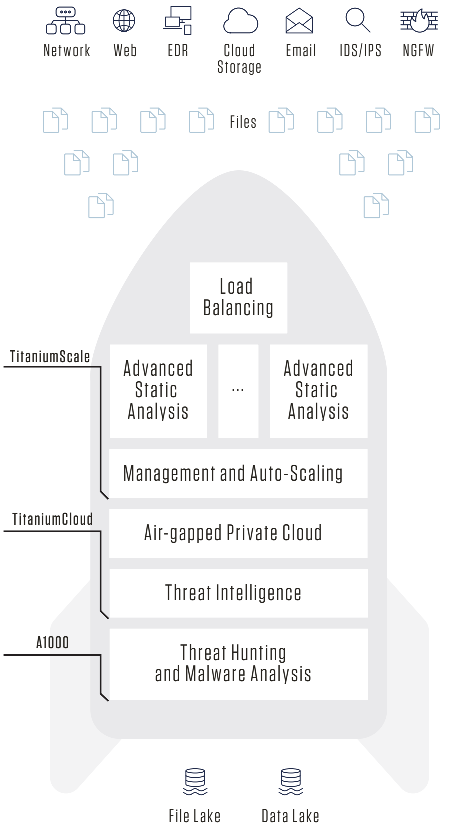
Files are at the heart of every modern organization, but files also represent the dominant cybersecurity threat, creating numerous challenges for enterprises attempting to analyze all files.

- **STABLE, MAINTAINED, INNOVATIVE**
  Multiple discrete security components, often designed for other purposes, can be internally assembled by organizations to analyze files for potential threats. However, these ad hoc solutions require resources to create, are often unstable, not commercially supported or maintained, and lack continuous innovation without dedicated development.
- **IT-APPROVED, USE ANYWHERE, MASSIVELY DEPLOYED**
  Creating solutions which meet IT compliance, can be deployed in private or public clouds or on-premises, and easily integrate into security ecosystems is particularly challenging. Ideally a platform enables simple insertion into any environment and has been validated by multiple enterprises, with massive deployments, across verticals and use-cases.
- **ANALYZE FORMATS IGNORED BY MODERN SOLUTIONS**
  Existing approaches have major limitations on file formats, malware obfuscation techniques, and speed of analysis, meaning many critical files are simply ignored. Solutions need to identify threats in all types of files (documents, application executables, backups/storage, multi-media, uploads, and business-specific formats) and provide customizable methods to search for file threats.

Solution

The Titanium Platform is an enterprise-grade solution which can be deployed in the public cloud, private cloud, or on-premises and solves these challenges with continuous innovation, support, and maintenance.

- **Identify Malware** Enterprises generate and process vast numbers of files from internal sources, customer uploads, and SaaS solution they operate. The Titanium Platform can inspect and identify malware files from any of these sources while protecting critical data with a range of enterprise privacy options including completely isolated private cloud or on-premises deployment.

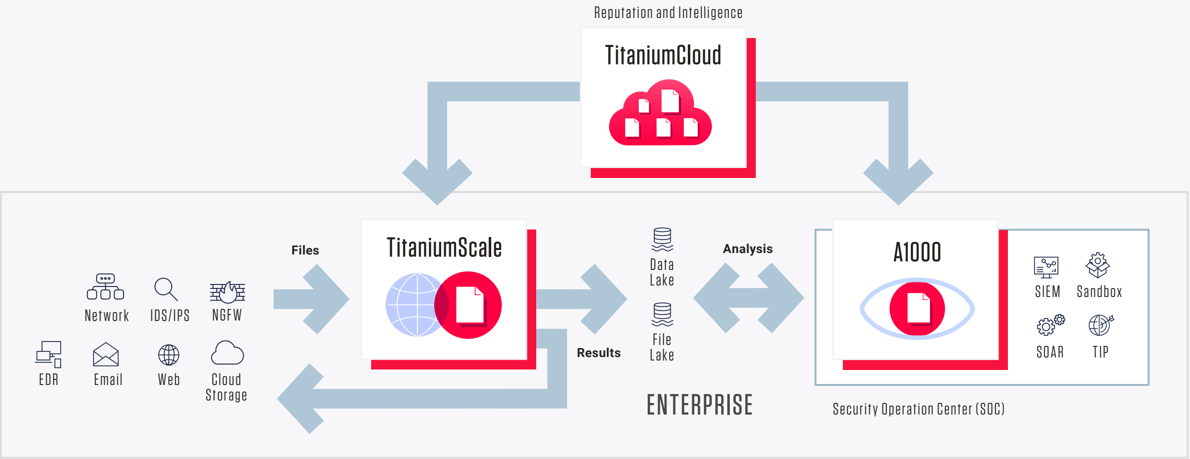


- **One Platform to Analyze 4,000+ Formats** At the core of the platform is a proprietary engine which analyzes more than 4000+ unique file formats at unparalleled depth. Further, the platform offers customizable rules, enabling one platform for analysis across all use-cases. Inspection is at millisecond speeds and minimal latency, providing security for even challenging real-time applications and use-cases.
- **Massive Scale, Explainable Verdicts** The architecture can scale horizontally to meet any need, with individual existing customers analyzing 10s of billions of files per year. Further the world's largest database of 10+ billion classified files provides unique intelligence, and the machine learning engine generates analysis with hundreds of explainable indicators for analysts to quickly identify and isolate file threats.

.005 sec to analyze — Enterprise-Grade — 100's of indicators

Product Components

To deliver solutions for a range of use-cases, the Titanium Platform consists of three major products, which can be purchased in several solution packages.



TitaniumScale Elastic File Analysis

TitaniumScale enables an organization to privately analyze large volumes of files in real-time to create relevant data for advanced analytics platforms to support threat correlation, hunting, and response. TitaniumScale ingests files from multiple sources, leverages file reputation and intelligence to generate malware results on all files for SOC teams.

TitaniumCloud Threat Intelligence

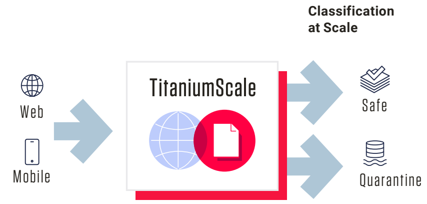
TitaniumCloud is a threat intelligence solution providing up-to-date file reputation services, threat classification and rich context on over 10 billion goodware and malware files. Hosted in the cloud, TitaniumCloud provides the most comprehensive file reputation and intelligence available on the market for use in file analysis and threat investigation.

A1000 Threat Hunting Portal

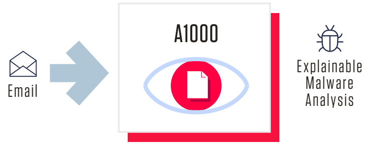
The A1000 is a malware analysis platform which supports advanced hunting and investigations through high-speed automated static analysis. As a key SOC tool, the A1000 supports visualization, APIs for automation, malware search, YARA rule matching, and integration with other tools in the security ecosystem.

Typical Use-Cases

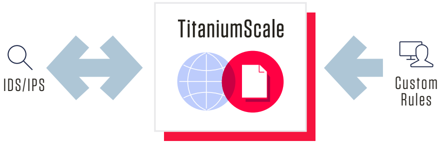
The Titanium Platform enables enterprises to privately analyze files on any scale, to leverage intelligence and reputation based on the largest private file repository, and to enable threat investigation and rapid action. The architecture is very flexible, and the products can be deployed individually or together to address a wide range of deployment examples.



- ***Web and Mobile Uploads:*** Numerous organizations are adopting web and mobile technology to simplify operations and develop new applications. In many scenarios large numbers of files are uploaded by employees or customers via the user application. To maintain security posture, TitaniumScale can be used to inspect all these files for threats and classify the files as safe to forward or as malicious to quarantine. The solution can be deployed in the public or private cloud and scale to millions of files per hour.



- ***Custom Protection for Email:*** Every organization employs email, and attached, embedded, and linked files present one of the largest threat vectors. Sophisticated attackers develop strategies tuned to specific organizations, which require custom protection. The A1000 can interface directly with email systems to identify threats based on custom, enterprise-specific, detection rules. The platform enables rapid investigation of detected threats and human-readable results based on explainable machine learning.



- ***Network File Visibility:*** Enterprises deploy numerous components, such as IDS/IPS and NGFW, to monitor network traffic. Integration with TitaniumScale enables every file traversing the network to be scanned using threat analysis or even custom enterprise rules. When a file threat is identified, TitaniumScale can respond with results back to the network platform for next steps, such as blocking in real time.

Product Architecture

The Titanium Platform consists of three different products, TitaniumScale, TitaniumCloud, and A1000, which can be used together or independently. Embedded in each product is TitaniumCore Technology, which provides the fastest and most comprehensive automated static analysis and explainable machine learning engine to classify unknown malware.

TitaniumCloud Threat Intelligence

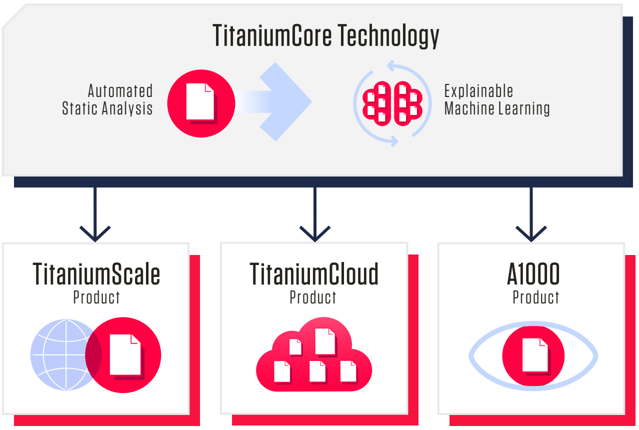
TitaniumCloud is Software-as-a-Service (SaaS) hosted in the ReversingLabs cloud.

- ***File collection:*** Billions of files are harvested on the Internet, from partners, and uploaded by customers.
- ***Repository analysis:*** The TitaniumCore engine is used to unpack, analyze, and classify files.
- ***Reputation and threat feeds:*** Numerous APIs are available to retrieve information on files and threats.

TitaniumScale Elastic File Analysis

The TitaniumScale solution can be deployed on-premises or in the private or public cloud with complete enterprise data privacy. The architecture scales, so as analysis needs grow, components can be added seamlessly. It consists of several elements which can be deployed flexibly and across geographies.

- ***Connectors:*** APIs pass files and data in and out of TitaniumScale or the A1000. Connectors provide integration with a wide range of external systems such as e-mail, EDR, NGFW, IDS/IPS, file systems, cloud storage, sandboxes, SIEM, SOAR, and TIPS using standard protocols such as REST, SMTP, and ICAP.
- ***Hub:*** Hubs load balance files across the worker file analysis engines. Multiple hubs can provide scaling and redundancy.

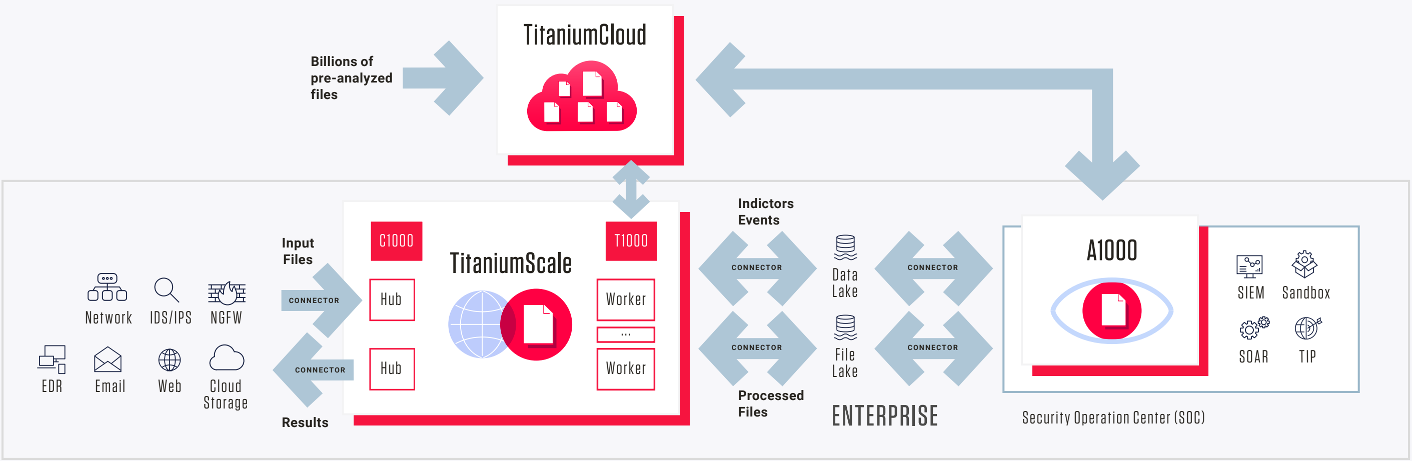


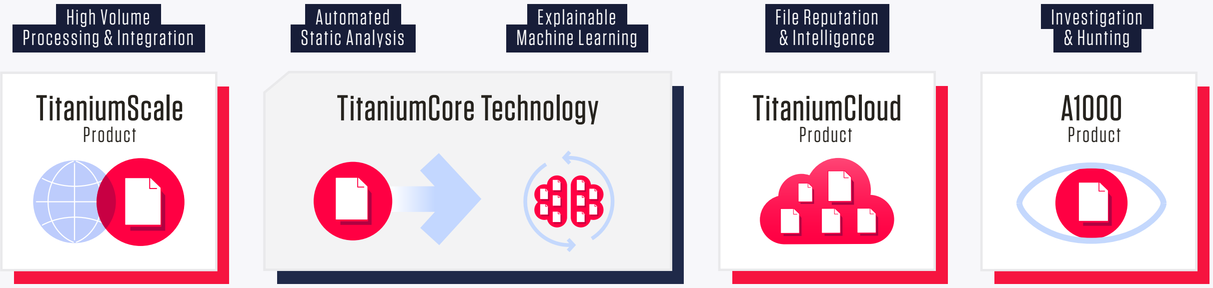
- ***Worker:*** Embedded TitaniumCore Technology and TitaniumCloud file reputation and threat intelligence data are used to analyze files. Workers output events, indicators, and metadata to systems for further analysis and can direct files to storage based on classification.
- ***C1000:*** In the solution management is centralized for configuration and synchronization of polices.
- ***T1000:*** An optional component maintains a local copy of file reputation and intelligence information from TitaniumCloud, to enable Internet-isolated private cloud.

A1000 Threat Hunting Portal

The A1000 can be acquired as SaaS or deployed on virtual or physical servers, on-premises or in the public or private cloud.

- ***Connectors:*** APIs enable passing of files and data between the A1000 and any IT or security system.
- ***File analysis:*** TitaniumCore Technology and TitaniumCloud feeds are employed for analysis.
- ***GUI:*** A web interface enables visualization, search, advanced hunting, and YARA configuration.
- ***APIs:*** Automated custom external workflows are possible through APIs to the portal.





High Volume Processing & Integration — TitaniumScale Product

Automated Static Analysis / Explainable Machine Learning — TitaniumCore Technology

File Reputation & Intelligence — TitaniumCloud Product

Investigation & Hunting — A1000 Product

Platform Features

The Titanium Platform provides high-speed detection through static analysis, accurate threat detection leveraging the largest malware repository in the industry, and explainable and transparent results with thousands of indicators. The platform is designed for enterprise privacy, with numerous options to optionally limit sharing of business-critical files. The platform is designed to integrate with the broader IT and security ecosystem and can provide new capabilities in several key areas.

High Volume Processing & Integration [TitaniumScale]

- ***Runtime:*** Real-time, deep inspection of files from web traffic, email, file transfers, endpoints, or storage, while scaling to 100 million files per day without dynamic execution.
- ***APIs:*** 50+ APIs and feeds automate processing, analysis and threat status information gathering.
- ***Connectors:*** Connectors integrate to email, EDR, Network Security, SIEM, and SOAR platforms using standard protocols such as REST, SMTP, and ICAP.

Automated Static Analysis [TitaniumScale, Titanium-Cloud and A1000 enabled by TitaniumCore Technology]

- ***Formats:*** 4000 file formats with over 400 file formats unpacked and analyzed including archives, installers, packers, and compressors.
- ***Decomposition:*** Automated Static Analysis decomposes files without execution within milliseconds.
- ***Indicators:*** Threat indicators generated for every sample and extracted from all objects.
- ***Classification:*** 5 levels of classification including known, unknown, suspicious, malicious, and good.
- ***Compared:*** Functional similarity to known malware using ReversingLabs Hashing Algorithm.

Explainable Machine Learning (ML) [TitaniumScale, TitaniumCloud and A1000 enabled by TitaniumCore Technology]

- ***Human-Readable Indicators:*** Generates human readable descriptions across 12,000+ file indicators within malware code and metadata properties.
- ***Verifiable Classification:*** Provides visual tags to explain which indicators have contributed to final classification verdicts, thus supplying the "how" a decision was made.
- ***Full Transparency:*** Exposes the logic and most significant contributions behind each classification, and why each of these indicators had been triggered.
- ***MITRE ATT&CK Support:*** Links indicators to respective MITRE ATT&CK framework categories, helping SOC analysts understand the type of threat they are dealing with and its impact to the organization.

File Reputation & Intelligence [TitaniumCloud]

- ***Goodware/Malware:*** 10 billion files stored for goodware and malware search queries, with 8 million updates daily for the most up-to-date file reputation status.
- ***AV Detection:*** Historical results from 40+ Anti-Virus Vendors combined with dynamic detection yields industry reputation consensus while showing changes over time.
- ***Files:*** Over 400 packed file formats processed, and 4000 file formats identified from diverse platforms, applications, and malware families.
- ***Privacy:*** Single source of global file reputation data - private, not publicly crowdsourced.

Investigation & Hunting [A1000]

- ***Persona UI:*** Threat intelligence, analysis and hunting teams use as a primary workbench for deep file analysis, accelerating investigations and response activities.
- ***Search & Hunt:*** 500+ search expressions with support for Boolean operators and auto-completion.
- ***YARA Rules:*** ReversingLabs or customer supplied YARA rules classify files by advanced rules engine, with support of up to 250 rules per ruleset for retro-hunting.

Ecosystem Integration

Organizations employ a wide range of security products, and the Titanium Platform is designed for simple insertion by supporting many platforms, connectors, and integrations to a wide range of systems.

CLOUD DEPLOYMENT

The platform can be deployed on virtually any public cloud, including AWS, Azure, GCP, Oracle, and IBM Cloud. Hybrid or private cloud deployments in either virtualized or bare metal configuration are possible. Completely private solutions enable enterprise privacy for sensitive files.

EDR

Endpoint Detection and Response (EDR) solutions integrate with the Titanium Platform through direct configuration or connector installation. TitaniumCloud file reputation can enhance EDR decisions or the EDR can forward files to an A1000 for hunting and investigation.

SIEM

Security Information and Event Management (SIEM) solutions integrate with the platform through plug-and-play applications, connectors, or output files. Titanium Platform reports and metadata can then be correlated with other events for full contextual analysis.

SOAR

Security Orchestration, Automation and Response (SOAR) solutions can employ playbooks leveraging APIs to the platform for automated response or to trigger additional investigation.

TIP

Many Threat Intelligence Platforms (TIPs) natively integrate TitaniumCloud file reputation and intelligence with simple configuration to provide authoritative results.

SANDBOX

Several sandbox solutions for dynamic analysis are integrated into the A1000 platform. During investigations, a file can be automatically sent to one or several sandboxes for additional analysis.

File shares

The Titanium Platform includes connectors to directly connect to major file shares for several use-cases.

- ***SMB and NFS:*** The connector can employ either the Server Message Block (SMB) or Network File System (NFS) protocol to interface with file shares to index, retrieve for analysis, and move files based on results.
- ***S3 Compatible:*** The connector employs AWS Simple Storage Service (S3) APIs to retrieve files for analysis and upload results. This provides compatibility with AWS, GCP, Oracle Cloud, IBM Cloud, and Dell ECS.
- ***Azure Data Lake:*** The connector employs Azure Data Lake APIs to retrieve files for analysis and upload results.

Email

The platform supports numerous e-mail platforms with several connectors.

- ***Microsoft Exchange:*** The connector creates an "Abuse" folder on a Microsoft Exchange Server or Exchange Online/O365. Using APIs, email in the Abuse folder is processed by the platform and then placed into good or malicious sub-folders based on analysis results.
- ***SMTP Relay – Simple Mail Transfer Protocol:*** The connector acts as an SMTP relay e-mail receiver for incoming and outgoing e-mail for solutions such as Gmail. The platform scans each e-mail and injects classification results into the mail header.

IDS/IPS, NGFW, and Gateways

Intrusion systems, Next-Generation Firewalls, and Secure Web Gateways can query the platform for analysis.

- ***ICAP – Internet Content Adaption Protocol:*** The platform supports an ICAP request to scan a file and returns the analysis result and detailed information to the query platform for policy-based actions.
- ***S3 Compatible:*** The platform supports S3 APIs, which several solutions employ to transfer files.
- ***REST:*** The REST API of the platform enables integration with several solutions.

Representative Ecosystem

Cloud	aws	Azure
EDR	TANIUM.	Carbon Black.
IDS/IPS	corelight	BROADCOM
SIEM/SOAR	splunk>	IBM
TIP	ANOMALI	ThreatConnect
Sandbox	FIREEYE	JOESecurity