TitaniumScale Enterprise Scale File Analysis

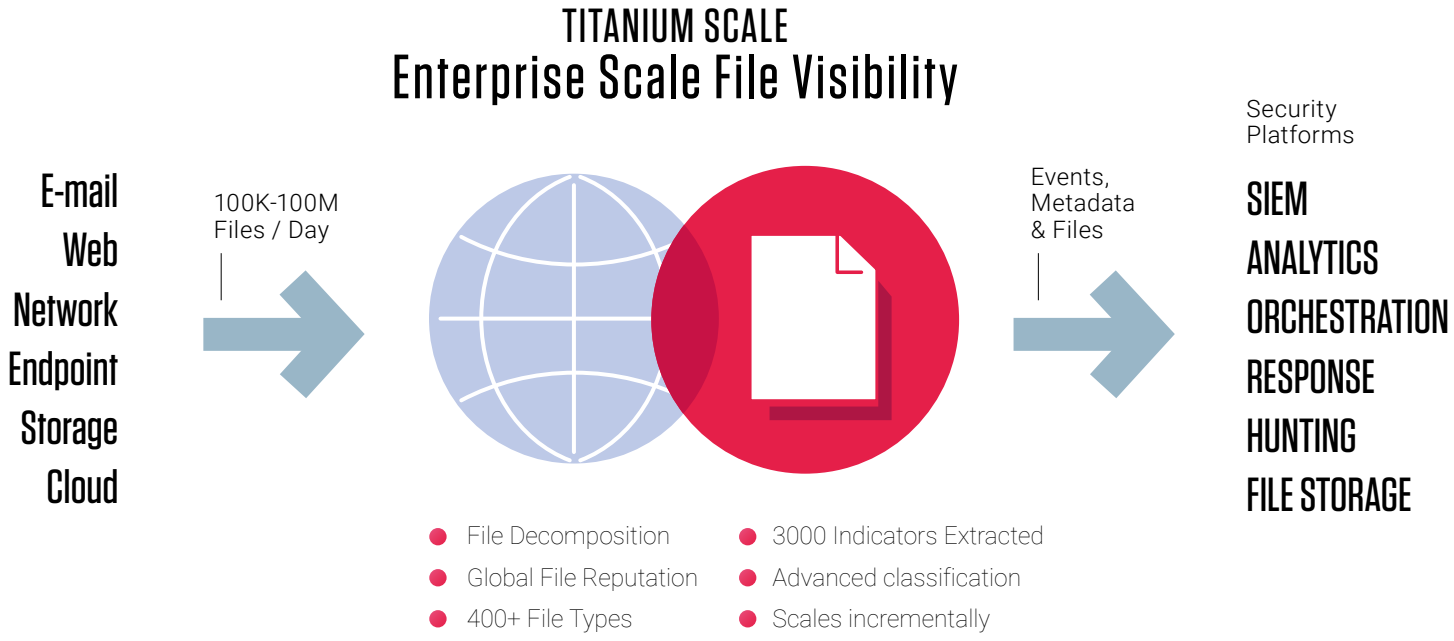
Comprehensive File Level Threat Classification and Visibility

Key Features

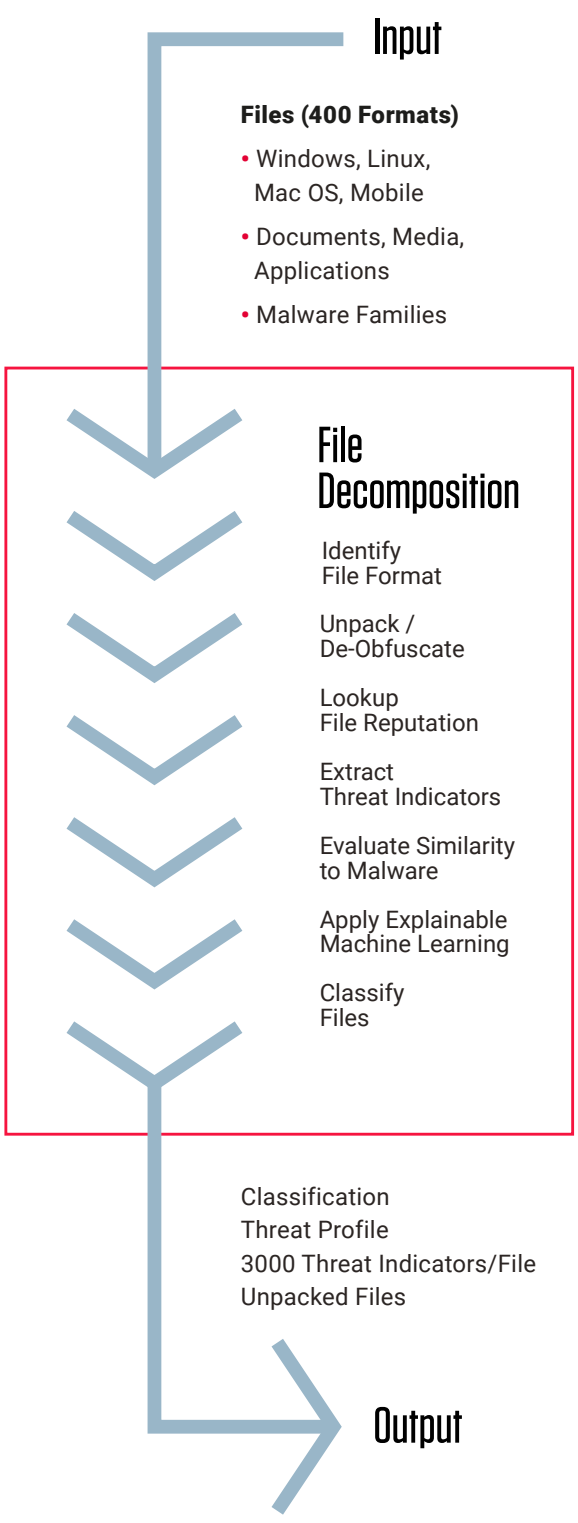
- **Real-time, deep inspection of files** scalable to millions of files per day without execution.
- **Broad coverage** identifying 4000+ file formats and unpacking of 400+ file formats.
- **Files sourced from a variety of inputs** via automated submission from ReversingLabs and third-party products.
- **Customer supplied YARA rule matching.**
- **Extracted file profiles are searchable** by content or context of the file.
- **Infrastructure scales incrementally** to meet customer volume and/or capacity requirements.
- **Programmable infrastructure** supports threat identification, analytics, hunting, and software verification.
- **Seamless integration for automated operations** with SIEM, analytics, and file collection.

TitaniumScale enables an organization to profile and classify large volumes of files in real-time to create relevant data for advanced analytics platforms to support threat correlation, hunting and response. Conventional malware products focus on detecting malware while treating unknown files as good, essentially overlooking them. As the amount of malware that evades detection grows, the need to profile, track and correlate undetected files becomes imperative to limit the impact of incidents and breaches. This intelligence data helps close the visibility gap between malware detection and tedious and expensive post-breach reconstruction.

TitaniumScale helps enterprises form a comprehensive assessment of millions of files from web traffic, email, file transfers, endpoints and storage. The solution uses unique ReversingLabs File Decomposition technology to extract detailed metadata, add global reputation context and classify threats. TitaniumScale automatically acquires files by integrating with solutions installed in the enterprise security infrastructure, including email gateways, intrusion detections systems, firewalls and other devices. The results feed into industry leading SIEM, orchestration and analytics platforms to provide visibility and data to analytics tools, support advance hunting strategies and enable advanced policy enforcement.



TitaniumScale Use Cases
File Classification - Close the malware visibility gap with near real-time file inspection and classification.
Accelerate Response - Find threats in existing files by searching by their attributes.
Custom Classification - Implement targeted malware identification at enterprise scale using YARA rules.
Validate Applications – Check installations and update packages before deployment.



File Decomposition

TitaniumScale derives extensive internal, reputation and classification information from files and can export that intelligence to SIEM, advanced analytics and big data platforms. It utilizes ReversingLabs' unique File Decomposition technology to derive detailed internal indicators and critical context from every file in real-time. File Decomposition utilizes automated static analysis to process files from diverse platforms, applications and malware toolkits providing results in milliseconds. The system recursively unpacks files, looks up the reputation of every child file, checks for functional similarity to known malware, extracts thousands of indicators and classifies the files for threat level and severity. The result is a full characterization of each file for use by SIEM and analytics platforms in responding to current and past events.

Features

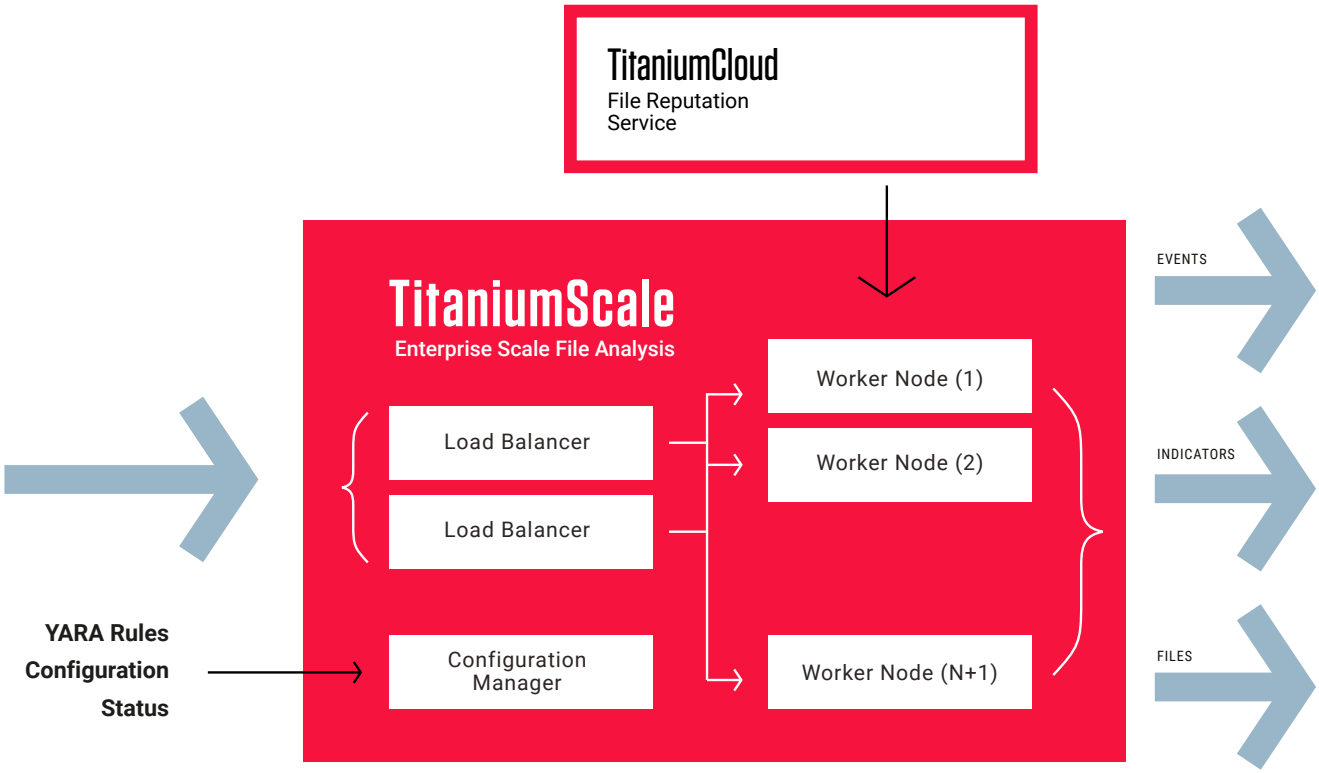
- **Speed:**
  Files cataloged in millisecond to support real-time, high-volume processing.
- **Coverage:**
  Over 400 file formats processed, and 4000 file formats identified from diverse platforms, applications and malware families.
- **Depth:**
  Recursive unpacking and extraction of 3000+ indicators per file.
- **Reputation:**
  Files checked against the industry's most comprehensive database base of goodware and malware.
- **Classification:**
  Files classified by advanced rules engine that supports ReversingLabs or customer supplied YARA rules.

Scalable Architecture

TitaniumScale uses a flexible cluster architecture that scales incrementally to support distributed or centralized file processing across physical and cloud environments. The cluster scales file processing capacity from 100K up to 100M files per day by adding worker nodes.

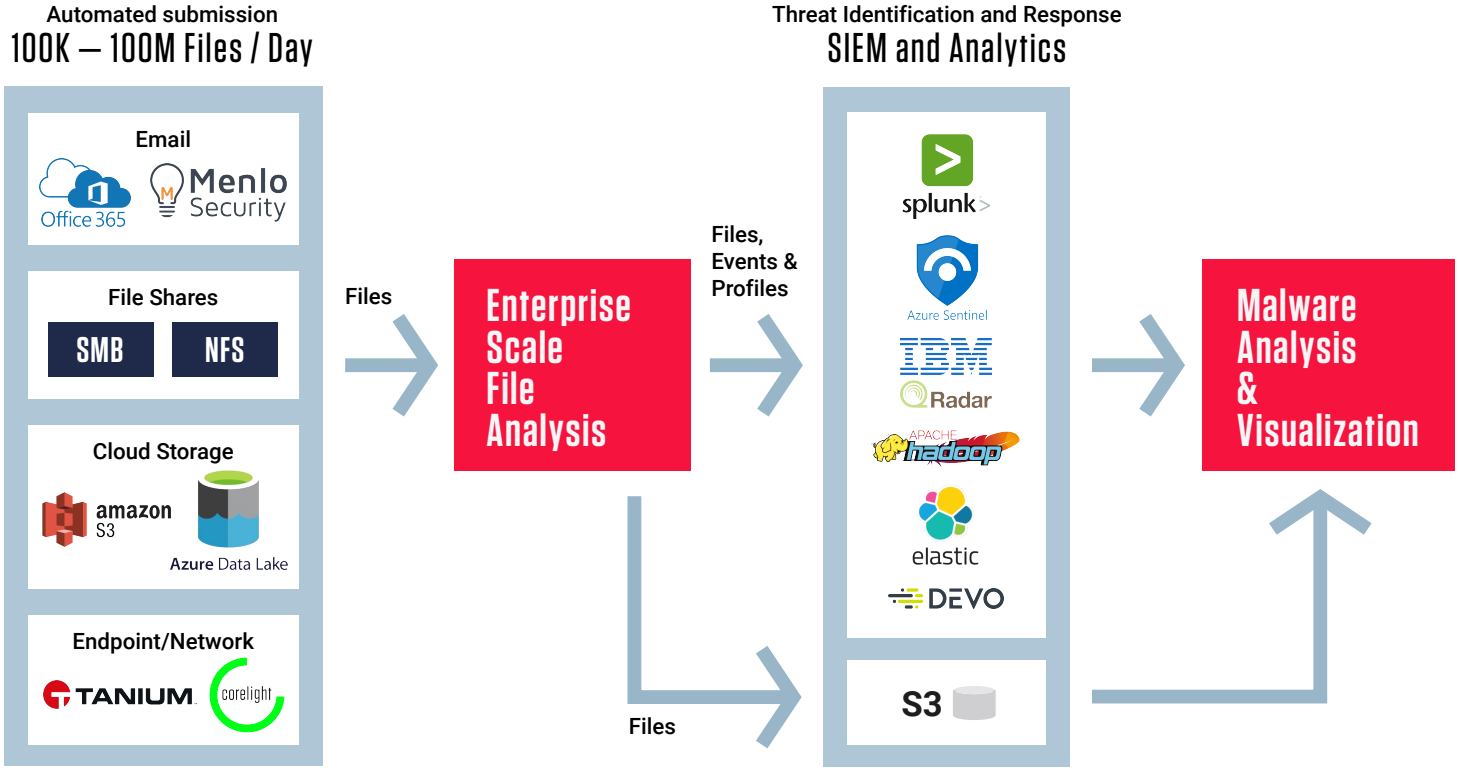
TitaniumScale consists of:

- **Worker Nodes:**
  A cluster of physical or virtual servers that perform the actual file assessment and support N+1 redundancy.
- **Load Balancer Hubs:**
  A server (and optional redundant server) that directs files to Worker Nodes for processing.
- **Control Manager:**
  A server that manages configuration (i.e. YARA rules, whitelists) and monitors status across the TitaniumScale cluster.
- **TitaniumCloud File Reputation:**
  A service available as a cloud-based resource or on-site appliance that identifies and provides information on known goodware and malware.



Example Implementation

A large financial institution uses TitaniumScale to derive detailed file profile and classification information at scale. The company feeds the resulting intelligence to its analytics platforms to identify threats and respond quickly to incidents. Industry leading security products deployed in 20 data centers extract files from email, web and file transfer traffic and automatically submit them to distributed TitaniumScale clusters. Each derived profile includes an URL pointing to a copy of the file so that it is available for further analysis. ReversingLabs A1000 Malware Analysis Workbench provides access to detailed analysis and visualization of these files. As a result, the customer accelerates the identification, correlation and resolution of threats that evade their traditional malware detection technologies.



REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com