

Hosted TitaniumScale

Enterprise Scale File Analysis from the Cloud

Comprehensive File Threat Classification and Visibility

Key Solution Highlights

ENTERPRISE-LEVEL FILE PROCESSING POWER

without the need for dedicated maintenance resources

REAL-TIME, DEEP FILE INSPECTION

Inspects and classify multi-gigabyte files in milliseconds to support high-volume processing

BROAD COVERAGE

to identify 4800+ file formats and to unpack 400+ file formats

AUTOMATED INGRESS AND EGRESS

Analysis of AWS S3 buckets and output actions based on file classification

DETAILED REPORT METADATA

Rich file analysis with hundreds of IOCs

SOC2 COMPLIANT INFRASTRUCTURE

Isolated per customer to ensure enterprise-level security and seamless performance

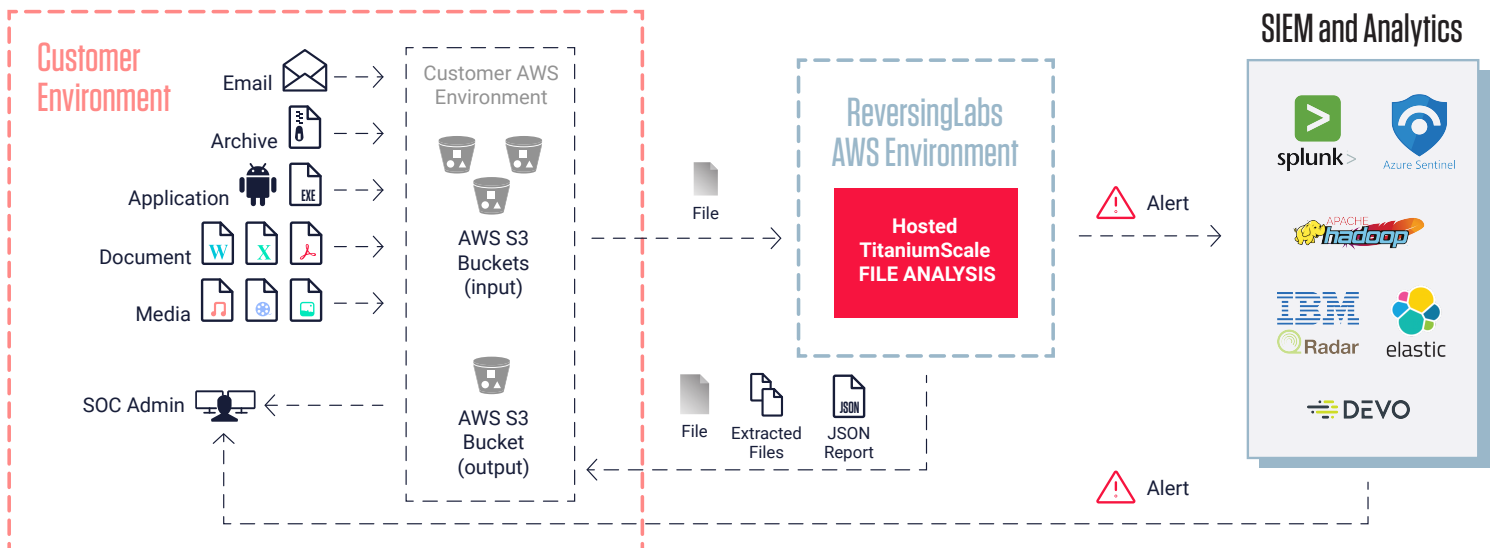
Hosted TitaniumScale enables an organization to profile and classify large volumes of files in real-time to create relevant data for advanced analytics platforms, supporting threat correlation, hunting and response. To solve the pain point of day-to-day management of enterprise scale file processing solutions, ReversingLabs provides infrastructure and lifecycle management with Hosted TitaniumScale. This eliminates the complexity of setup, configuration, administration, and operational expenses, making it a more compelling option for organizations without dedicated operations resources.

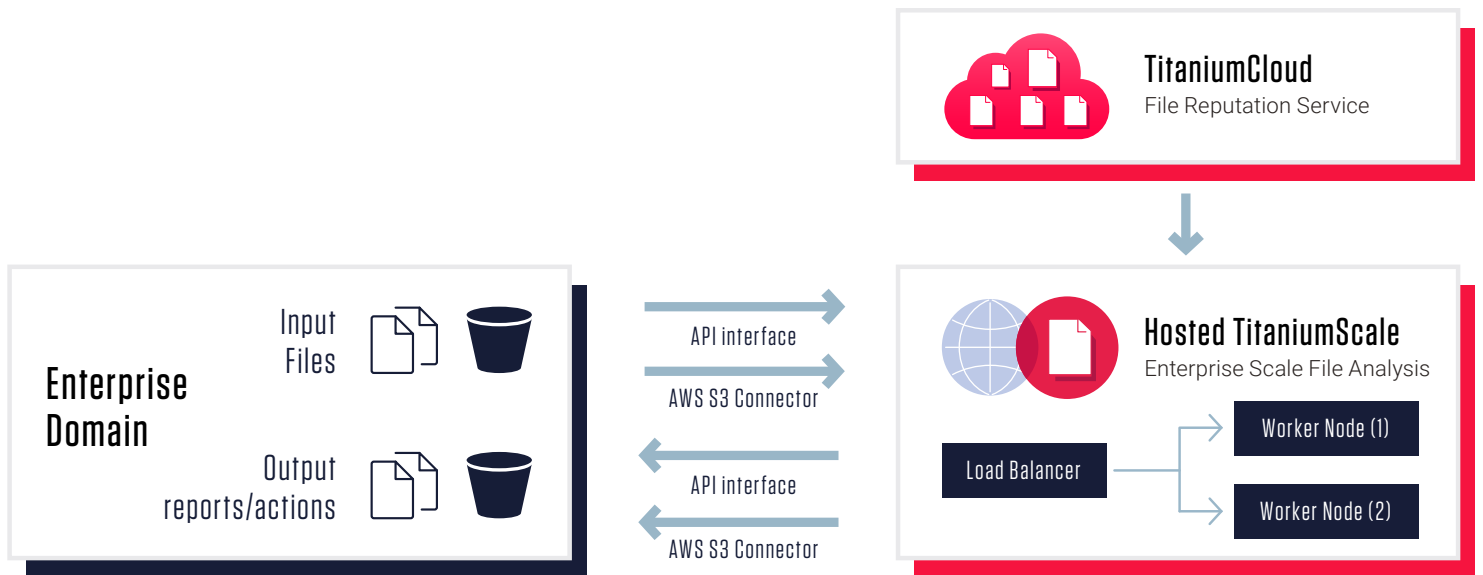
Files and applications are becoming larger and more complex. Endpoint solutions are not sophisticated enough to decompose multi-layered or multi-gigabyte files, so that many threats go undetected. Hosted TitaniumScale helps organizations classify and prioritize malware remediation in millions of files from web and mobile uploads, cloud storage, and the software supply chain. This intelligence data helps close the visibility gap between malware detection and onerous and expensive post-breach reconstruction.

The platform employs standards-based interfaces to process files. Hosted TitaniumScale can provide both simple output actions as well as detailed report metadata to support advanced hunting strategies and enable advanced policy enforcement.

Use Case

Accelerate Response to Threats with Real-Time Classification and SIEM Alerts





Hosted TitaniumScale can ingest files at scale via either a REST API or analyze files from an AWS S3 bucket. The hosted solution internally employs the ReversingLabs TitaniumCore static analysis engine and TitaniumCloud Threat Intelligence to unpack, analyze, and classify all ingested files. The results can be used to move files to specific S3 folders based on classification. A report is generated for each file with detailed metadata in a standard scheme that can be ingested by a wide range of security tools for additional analysis.

Hosted TitaniumScale Benefits

REDUCED COMPLEXITY AND COSTS	ReversingLabs experts manage all aspects of the platform components, reducing technical resource requirements and operational expenditures.
RAPID DEPLOYMENT	ReversingLabs rapidly deploys and provisions the solution on highly-available cloud infrastructure, speeding up the time to value and ROI.
LIFECYCLE MANAGEMENT	The ReversingLabs hosted platform includes regular upgrades to access to the latest features and enhancements, to maintain platform security, and to ensure the highest level of threat detection.
OPTIMAL PERFORMANCE	The ReversingLabs operations team has expensive expertise managing large-scale file analysis systems. They continuously monitor the platform and adjust the solution to ensure optimal performance.
DATA PROTECTION	Standards-based security ensures Hosted TitaniumScale protects enterprise data. Architecturally, the solution completely isolates critical data with dedicated infrastructure and processes, and the stateless approach does not retain any data. Operationally, ReversingLabs maintains stringent Service Organization Control 2 (SOC2) compliance.

Get Started!

www.reversinglabs.com

REQUEST A DEMO

REVERSINGLABS

Worldwide Sales : +1.617.250.7518

sales@reversinglabs.com