REVERSINGLABS

SOLUTION BRIEF

ReversingLabs Titanium Platform

Delivers explainable threat intelligence into every destructive file and object to help Security Operations Center (SOC) teams detect, identify, and respond to the latest attacks and risks associated with third-party software.

Key Features

- **SPEED FILE ANALYSIS WITH ACTIONABLE INTELLIGENCE**
  Speed detection of files and objects through automated static and dynamic file analysis, determining file reputation and prioritizing the highest risk files with actionable details, in only milliseconds.

- **ACCURATE THREAT DETECTION**
  Accurately detect threats with the largest repository of 25 billion malware and goodware files and over 4000 formats, while maintaining privacy.

- **SEAMLESSLY INTEGRATE AT SCALE**
  Enterprise customers process billions of objects per week while integrating insights across the entire enterprise.

- **DEEP INVESTIGATION**
  Deep investigation of malware infected files for threat hunters and incident responders through advanced search, custom YARA rules and retro-hunt.

Business Challenge

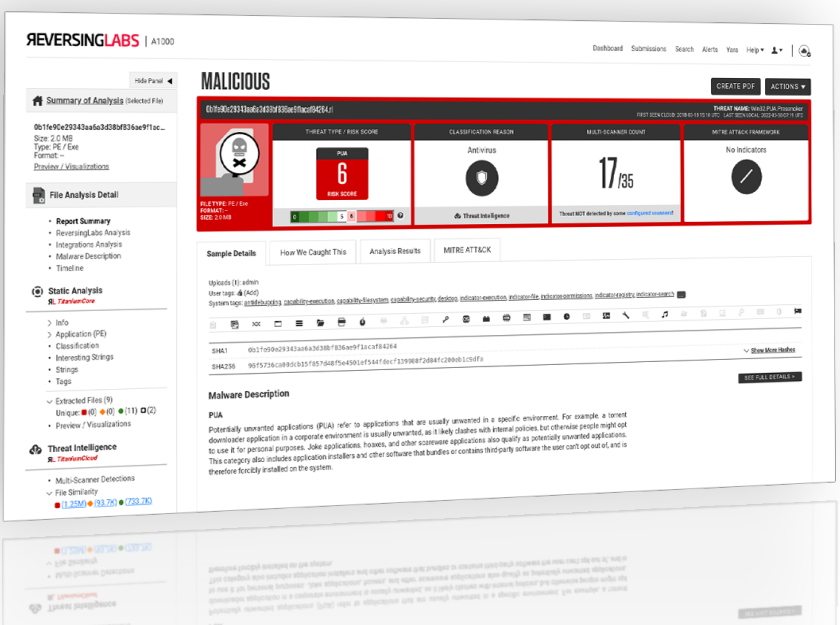
Organizations advancing their business through new digital strategies continue to take on brand, financial and information risks due to the growth of malware infected files and objects sourced from the web, email, supply chain, cloud, mobile, and APIs. These advanced and destructive objects are armed to circumvent existing anti-virus, EDR, email protection, sandbox and threat intelligence solutions leaving companies blind to threats lurking within their network. This is having an impact on the CISO's ability to achieve top security and business initiatives. Whether it's clearer security metrics focused on high risk threat vectors such as ransomware and phishing, automating security and SOC operational processes to help fill the security skills gap, enabling the secure migration of apps to more modern architectures, or the acceleration of secure app development to compete in today's digital economy, malware infected objects are the primary issue in mitigating today's attacks.

Solution

ReversingLabs solves the problem of meeting security objectives, through the delivery of advanced malware analysis and insights into destructive files and objects. The automated static and dynamic analysis and file reputation platform delivers the fastest and most accurate malware insights in the industry. The Titanium Platform is delivered as a hybrid cloud delivery model providing connectors that integrate with EDR, Network Security, Email, SIEM, TIP, and Sandboxes. The platform reduces incident response time for SOC analysts by enabling them to prioritize "bad" over "good" files for investigation and speed incident response to avoid attack risk. Malware analysts benefit from high-speed static file investigation but can use dynamic deep-file analysis for files of interest to locate malicious software.ReversingLabs delivers automated tools and processes for SOC maturity, which integrate with the tech stack and improve staff efficiency, automate incident response and develop threat skills one event at a time.

> "The Malware and Threat Intelligence teams love it. I hear feedback from them all day about products that don't meet expectations, but ReversingLabs is never mentioned on that list! I can't wait to find out how we can leverage ReversingLabs in more ways across our SOC. I've had a really great experience dealing with ReversingLabs, especially with support.

Insurance Company,
Enterprise Architect



Titanium Platform Capabilities

Automated Static and Dynamic Analysis

- ***Formats:*** Identifies more than 4,000 file formats across Windows, MacOS, Linux, iOS, and Android platforms and unpacks over 400 file formats, including archives, emails, documents, multimedia, software.
- ***Decomposition:***
  - Automated Static Analysis decomposes files and runs high-speed file inspection without execution, in combination with file reputation and other context-rich tools.
  - Automated Dynamic Analysis via ReversingLabs Cloud Sandbox provides highly available and scalable static analysis paired with dynamic analysis for comprehensive, deep file investigation for "files of interest." Since Cloud Sandbox requires no additional resources for setup, and no configuration or maintenance costs, it can replace a local sandbox instance.
- ***Classification:*** Provides users with a 'Risk Score' value for threat level classification, taking into consideration all classification components available to ReversingLabs. This includes machine learning models, heuristics, signatures, YARA rules, file and certificate reputation, etc. for better coverage with improved classification understanding, accuracy, and threat landscape coverage.
- ***Comparison:*** Utilizes functional similarity analysis based on the ReversingLabs Hashing Algorithm (RHA) to discover new malware variants.

File and Network Threat Intelligence

- ***Human-Readable Indicators:*** Threat indicators generated for every sample and extracted from all objects. 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 on the organization.
- ***URL + Network Analysis:*** Provides URL threat intelligence, enriching URL sample investigation and providing users with additional details beyond Static and Dynamic Analysis.

Products and Services

Malware Analysis Workbench [A1000] (Includes Titanium Platform Features)

- ***Persona UI:*** Threat intelligence, analysis and hunting used by teams 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 provides out of the box support for ReversingLabs- or customer-supplied YARA rules used to classify files.
- ***Integration:*** Directly with on-premises third-party Sandbox.

Threat Intelligence Feeds and APIs [TitaniumCloud] (Includes Titanium Platform Features)

- ***File Reputation of Goodware/Malware:*** Over 25 billion files stored for goodware and malware search queries, with 7 million new files analyzed daily for the most up-to-date file reputation status.
- ***AV:*** Historical detection results from 40+ AV Vendors yields industry reputation consensus while showing changes over time.
- ***Privacy:*** Single source of global file reputation data - retains privacy, not publicly searchable.
- ***APIs and Feeds:*** 50+ APIs and feeds automate processing, analysis and threat status information gathering.

High-Volume Processing and Integration [TitaniumScale]

- ***Runtime:*** Real-time, deep inspection of files from the web, email, endpoints or storage, or file transfers, scalable to 100 million files per day.
- ***Connectors:*** Seamlessly integrated with industry-leading network file shares, email, and storage platforms

Optimize Your Existing Security Tools

Email
Find high priority threats missed by email gateways and abuse boxes

EDR
Enrich malware detection with detailed malware threat information

AppSec
Inspect release images for third-party software risks including malware, compromised certificates, etc.

SIEM & SOAR
Reduce MTTR and automate response with high-priority good/bad malware classification

Anti-Virus
Detect files without signatures, with a size and complexity not addressed by AV

Sandbox
Based on your needs, either replace your sandbox with automated high-speed static analysis + dynamic analysis or enrich your sandbox investigation with ReveringLabs threat intelligence

Threat Intel
Complement external threat intelligence platforms with local file and object visibility

Integration
Unify and seamlessly integrate into existing security investments with malware insights

Get Started!

www.reversinglabs.com

REQUEST A DEMO

Simple integration with dozens of third-party security partners allows complete visibility across the organization. Integration partners include:

FIREEYE™ JoeSecurity splunk> Microsoft IBM cuckoo

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com