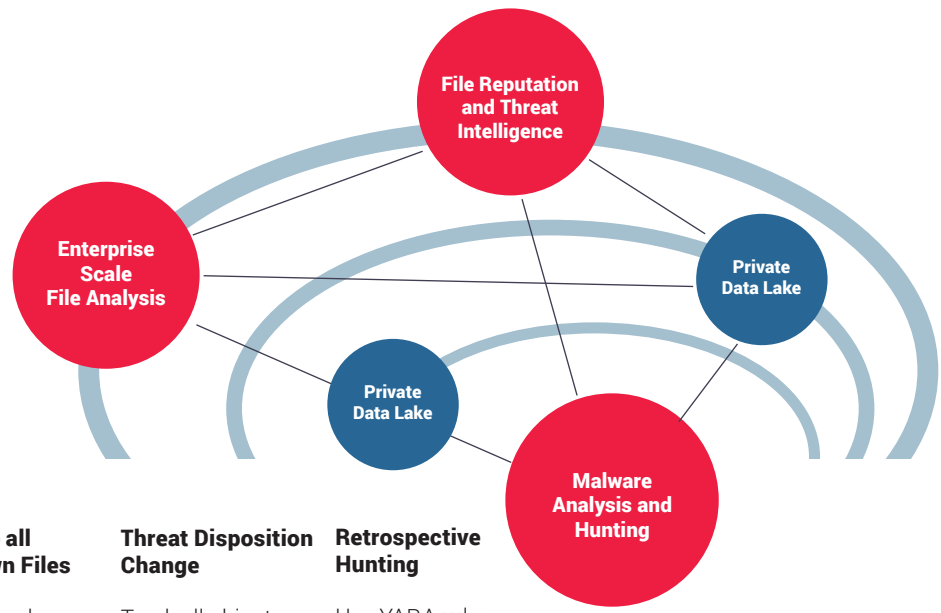
REVERSINGLABS

SOLUTION SUMMARY

Advanced Malware Detection, Hunting, & Threat Intelligence

ReversingLabs solutions provide unparalleled visibility, awareness and insight for defeating advanced malware. ReversingLabs enables security operations, malware analysis, threat intelligence, and incident response teams to reduce costs and disruptions by identifying more malware before detonation, accelerating response to cyber events, and strengthening defenses through better insight. Our unique File Decomposition technology powers solutions for enterprise scale file analysis, malware analysis and hunting.



ReversingLabs provides the only solution for comprehensive file inspection at enterprise scale for early identification of threats across email, web and storage.

Analyze all Unknown Files

Analyze unknown files at enterprise scale to identify and characterize malware early in the attack cycle.

Threat Disposition Change

Track all objects across the organization and report as they are determined to be malicious.

Retrospective Hunting

Use YARA rules to threat hunt through local file collections and against the world's largest collection of malware and goodware in the ReversingLabs Cloud.

File Reputation & Threat Intelligence

Global awareness of threats in-the-wild

ReversingLabs TitaniumCloud File Reputation service is an authoritative file intelligence solution with up-to-date threat classification and rich context on over 6B goodware and malware files. ReversingLabs curates the harvesting of files from software vendors and diverse malware sources. All files are processed using ReversingLabs unique File Decomposition technology combined with third party anti-virus scanners to provide industry reputation consensus. TitaniumCloud supports powerful query and feed functions for threat identification, analysis, intelligence development and hunting. Flexible deployment options include a cloud-based or an on-premises solution.

Enterprise Scale File Analysis

Visibility to expose and resolve breaches

ReversingLabs enterprise scale analysis solutions profile and classify large volumes of files in real-time to create relevant data to support threat correlation, hunting and response. This closes the visibility gap between malware detection 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 N1000 is focused on network file flow detection covering HTTP, SMTP and FTP. Both solutions integrate with SIEMs, analytics and response tools, and big data warehouses.

Malware Analysis and Hunting

Insight to classify and understand threats

The A1000 Malware Analysis platform delivers advanced threat analysis and hunting through high-speed File Decompositions and deep file examination integrated with ReversingLabs' File Reputation Services.

The A1000 supports a GUI for visualization, APIs for integration with automated workflows, a dedicated database for malware search, and YARA rules for local & global matching. The A1000 is fully integrated with SIEM, SOAR and third party sandbox tools.

ReversingLabs File Decomposition

The World's Most Powerful File Analysis Technology

ReversingLabs File Decomposition technology utilizes automated static analysis to decompose and analyze files from diverse platforms, applications and malware toolkits in milliseconds. The system recursively unpacks files, looks up file reputation, checks for functional similarity to known malware, extracts thousands of internal indicators and classifies the files for threat level and severity. All files are checked against ReversingLabs authoritative File Intelligence database. The result is a full characterization of each file which is delivered to SIEM and analytics platforms for prioritization, in-depth investigation and proper response.

Integration Partners

ReversingLabs recognizes that solutions must easily integrate into and significantly enhance a Customer's existing security infrastructure. For this reason, we partner and integrate with industry leading vendors to increase the effectiveness of end customer's security operations without additional operational workload.

Select Integration Partners

Endpoint & Network Solutions

TANIUM

When Tanium Trace finds a "file of interest" on an endpoint, it automatically adds threat classification and rich context to the output through an integration with ReversingLabs TitaniumCloud. If the file needs deeper analysis, it is sent directly to ReversingLabs A1000 for further forensic investigation.

SIEM & Analytics

splunk>

ReversingLabs and Splunk integrate in a number of ways. One integration uses TitaniumScale to analyze and classify all inbound traffic. Information on files classified as threats or "of interest" are sent to Splunk so analysts can initiate the proper response or determine if deeper investigation is needed. ReversingLabs A1000 integration enables Splunk users to complete an in-depth file analysis with a single mouse click.

Automation, Orchestration, Threat Intelligence

Phantom

ReversingLabs integrates with three Phantom Apps that drive multiple play books. The TitaniumCloud App automatically delivers rich file context to Phantom malware hunting and investigation playbooks for immediate malware identification. The A1000 App, launched from the investigation and hunting playbooks, allows analysts to visualize ReversingLabs' File Decomposition results, identifying threats and decreasing triage response times. The TitaniumScale App classifies file threat levels in high-volume environments, sending only known malicious or "of interest" files with with enriched context to the Phantom investigation playbook.

Big Data Analysis & Visualization

IBM i2

ReversingLabs rich file and malware context, both file reputation from TitaniumCloud and file/malware analysis results from the A1000, provide i2 with valuable threat data that drives highly efficient forensic investigations and supports more effective post-mortem threat hunting.

REVERSINGLABS

Worldwide Sales +1.617.250.7518
sales@reversinglabs.com

© Copyright 2018. ReversingLabs. All rights reserved. ReversingLabs is the registered trademark of ReversingLabs US Inc. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2018 April Solution Summary SSNA