A1000 Malware Analysis Workbench

Hunt, Identify and Analyze Advanced Malware

Key Product Features

PRIVATE FILE ANALYSIS
for proprietary files

HIGH SPEED FILE AND URL ANALYSIS
unpacks files, extracts internal indicators, and detects embedded threats

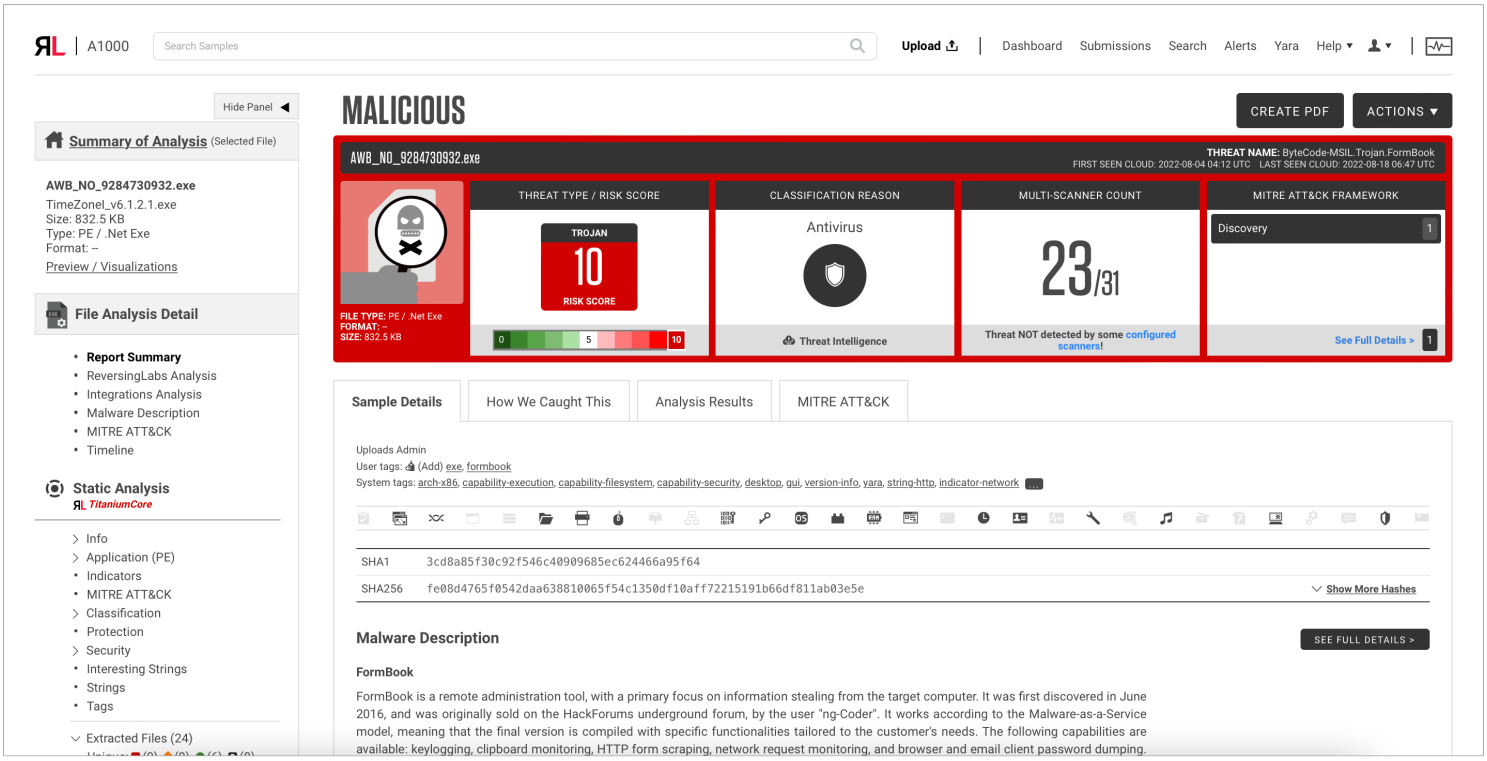
DYNAMIC ANALYSIS
via the ReversingLabs Cloud Sandbox out- of -the box integration with the A1000

INTEGRATED YARA ENGINE
supports ReversingLabs and user defined YARA rules for matching, threat detection and retro hunting

MITRE ATT&CK FRAMEWORK
provides human readable indicators for each threat

The A1000 Malware Analysis Workbench provides high-speed binary analysis using proprietary techniques that include static and dynamic file analysis. The A1000 is integrated with TitaniumCloud, a world-class file reputation service that contains tens of billions of files in the classification database to provide in-depth rich context, threat classification and intelligence. This classification corpus increases by millions each day. Security teams can correlate a single sample with the billions of goodware and malware samples to understand the intent of a file. This context allows analysts to effectively defend against both global and targeted attacks, accelerating investigations and response activities.

Detailed analysis results provide actionable intelligence organized into categories to show what a sample would do if executed. Indicators such as Search, Settings, Evasion, and Execution allow analysts to see if the malware is attempting to evade common security tools, collect system information, or create child processes as part of the attack. These analysis outcomes are mapped to the industry standard MITRE ATT&CK framework for ease of use and correlation with other security solutions.



Advanced Analysis, Intelligence, and Reporting

The A1000 securely analyzes thousands of files per day and correlates them against billions of malware and goodware artifacts. With the ability to process over 400 file formats and identify over 4,800 file formats from diverse platforms, applications and malware families, the A1000 provides a global and a local view of malware, along with historical insights to find new malware faster.

Advanced file decomposition automates and accelerates threat detection and file analysis. This unique technology performs high-speed, static analysis to unpack files, extract internal indicators and detect embedded threats. Files are not executed so processing can be accomplished in milliseconds, obtaining faster results and broader coverage than is possible with dynamic solutions alone.

The A1000 provides the ability to pivot and drill down on all file activities and metadata, allowing analysts to dive deeper. Combining static, dynamic and machine learning analysis engines provides a full understanding of malware behavior and identification of malicious files masquerading as benign. The A1000 user-interface is equipped with workflows designed for security operations center (SOC) analysts, malware analysts, and forensic investigators.

A1000 Malware Analysis Workbench Features and Benefits:

FEATURE	BENEFIT
Private File Analysis	• Provides safe storage of malicious or suspicious files enabling safe sharing of malware samples and historical analysis. • Stores file context in an onboard searchable database. • Enables private file analysis for proprietary files and data, like confidential company documents and emails.
High-speed File Analysis	• Analysis engine performs high-speed analysis to unpack files, extract internal indicators and detect embedded threats. • Identifies more than 4,800 file formats across Windows, MacOS, Linux, IOS, and Android and includes PE, ELF, Mach-O, .NET, Java, JS, documents, firmware, software libraries, and installation packages. • Unpacks over 400 file formats of archives, emails, documents, multimedia, software packages, installers, executable packers and compressors. • Integrated database enables safe, secure storage of results and enables file search by threat indicators.

Advanced, Actionable Threat Detection	• ReversingLabs proprietary threat detection technologies based on format identification (malware packers), signatures (byte pattern matches), file structure validation (format exploits), extracted file hierarchy, file similarity (RHA1), certificates, machine learning (for Windows executables and scripts), heuristics (scripts and fileless malware) and YARA rules.
	• ReversingLabs Machine Learning detection based on human readable indicators provides unparalleled explainability, transparency and relevance to ML-based threat detection.
	• ReversingLabs Cloud Sandbox dynamic analysis delivers comprehensive insights into malware behavior.
	• ReversingLabs Classification Algorithm (RCA): Provides users with a 'Risk Score' value for classification, taking into consideration all classifiers and classification components available to ReversingLabs. This includes signatures, heuristics, YARA rules, file source, reputation, etc. from TitaniumCore.
	  • RCA Classification provides several customer benefits including:
	  • Classification Accuracy - accurate security outcomes and more efficient investigation workflows
	  • Classification Coverage - great threat landscape coverage
	  • Classification Coverage - great threat landscape coverage

FEATURE	BENEFIT
	• Classification Efficacy - RCA brings to bear all ReversingLabs technologies (data, sources and processing systems to deliver a new standard of classification to the industry) • Explainability/Transparency - Users receive human-readable explanations for classification reasons and a clear list of classifier results helping address any skills gaps • RCA propagates classifications from child to parent files (malware) AND parent to child files (goodware), making classification workflows richer than ever before • Users have the option to update Cloud database file classifications using RCA based on in-house threat intelligence.
Integrated YARA Engine	• Utilize ReversingLabs open source rules to identify advanced malware. • Supports user-defined YARA rules for matching, threat detection and retro hunting. • Match enabled YARA rules on all files unpacked by ReversingLabs Advanced File Decomposition, enhancing their coverage and multiplying their value.
Advanced Threat Hunting	• Access threat, actor, and vulnerability descriptions with global prevalence information. • Hunt for advanced malware threats with file, certificate, and network indicators with text search. • Run YARA hunting queries in the local A1000 dataset and TitaniumCloud simultaneously. • Pivot the dataset by metadata properties and similarity to discover related threats using ReversingLabs Hash Algorithm (RHA). • Automate analysis tasks by creating alerts based on classification change, or file analysis results.
MITRE ATT&CK Framework	• Indicators are mapped to the MITRE ATT&CK framework to provide an understanding of the tactics and techniques used in malware. • Allows security operations teams (SOC) to strengthen defenses and find operational issues in existing controls. • Provides human readable indicators for each threat to enable analysts to react faster and with more confidence.
REST APIs, Integrations and Connectors	• Automated analysis workflows and orchestration via REST API, for example automatically forward samples to A1000 from other tools or forward reports from A1000 to internal tools. • Report Summary API optional parameters allow retrieval of URL and domain threat intelligence as part of the API response. • URL and domain threat intelligence added to URL status API responses • Integrates directly with on-premise third-party sandboxes. • A1000 can connect to a several email sources (IMAP, Microsoft Exchange, SMTP servers) and analyze retrieved emails • A1000 integrates with cloud storage (S3, Azure Data Lake, OneDrive) • Simple integration with dozens of third party security partners allows complete visibility across the organization. • Out-of-the-box connectors automatically ingest samples from network file shares (SMB or NFS)
Dynamic Analysis / RL Cloud Sandbox	The ReversingLabs Cloud Sandbox adds dynamic analysis capability to the A1000 Malware Workbench. Customers may want to use the highly available, scalable Cloud Sandbox in addition to, or instead of, a local sandbox instance because it requires no additional resources for setup, configuration and maintenance costs.

FEATURE	BENEFIT

	RL Cloud Sandbox
	• Out of the box integration with the A1000
	• User friendly single-page file analysis report with drop-down to view individual historical reports
	• MITRE ATT&CK tab shows a table with techniques detected during dynamic analysis.
	• File types supported:
	  • Windows executables: EXE, DLL, BAT, CHM, WSF, JS, JSE, VBS, VBE, PS1, CMD, PIF, LNK, SCR, CPL, HWP
	  • Microsoft Office: DOC(X)(M), XLS(X)(M), PPT(X)(M), MSG, EML
	  • PDF documents
	  • Java: JAR
	  • Misc: CRX (Chrome extension)
	  • Archive: .zip
	• Behavior analysis section with Process tree to filter actions for richer investigations
	• Simplified network analysis tabbed navigation containing HTTP values, TCP IPs/ports, UDP IPs/ports, and DNS values provides easier investigation
	• Summary tab for data dropped from file sample during dynamic analysis
	• Default Snort and Sigma rules- automatically available without any additional set-up
	• Download Screenshots, PCAP and Memory Strings from individual analysis

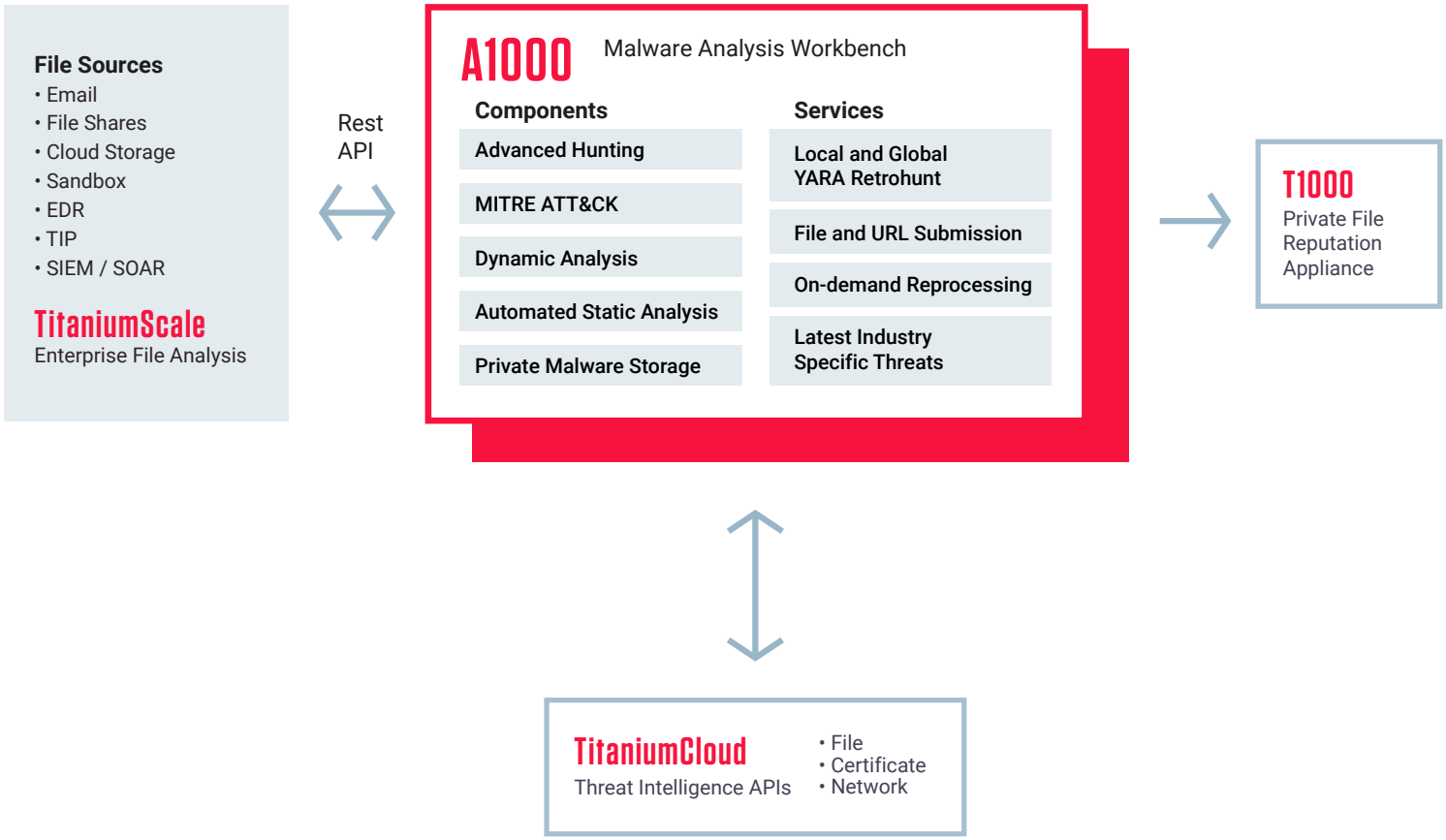
URL/Domain/IP Network Analysis	• URL, domain and IP analysis for enriched investigations that include reputation and maliciousness of the URL, domain or IP address • Even if a URL cannot be accessed for analysis (e.g., website is down), network threat intelligence can provide additional information for investigation • URL, domain and IP address analysis provides additional details beyond Static and Dynamic Analysis

Deployment Options

The A1000 can be deployed on premise as a virtual appliance or Docker container. ReversingLabs provides a Hosted A1000 option as well in all major Cloud providers.

For customers who don't need the full power of the A1000, we offer ReversingLabs Insights (RLI) as a streamlined always-on cloud-based option.

Capability	A1000 / A1000E	RLI
Deployment	On Premise / Hosted	Cloud only
Multi Tenant Web Interface		X
Manual Submission and Workflows	X	X
Automated Submission via API	X	
Advanced Search	X	X
Private, Local and Global analysis with global intelligence	X	
Cloud Based YARA Rules	X	X
Local and Custom YARA	X	
API Access	X	
Third Party Integrations	X	
Titanium Platform Integration	X	
Dynamic Analysis / RL Cloud Sandbox	X	
URL / Network Analysis	X	
Alerting	X	
Custom User Roles	X	



Get Started!

www.reversinglabs.com

WE'LL SHOW YOU HOW REVERSINGLABS DETECTS AND ANALYZES MORE HIDDEN THREATS

REQUEST A DEMO

About ReversingLabs

ReversingLabs is the leading provider of explainable threat intelligence solutions that dissect complex file-based threats for enterprises stretched for time and expertise. Its hybrid-cloud Titanium Platform enables digital business resiliency, protects against new modern architecture exposures, and automates manual SOC processes with a transparency that arms analysts to confidently take action and hunt threats.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com