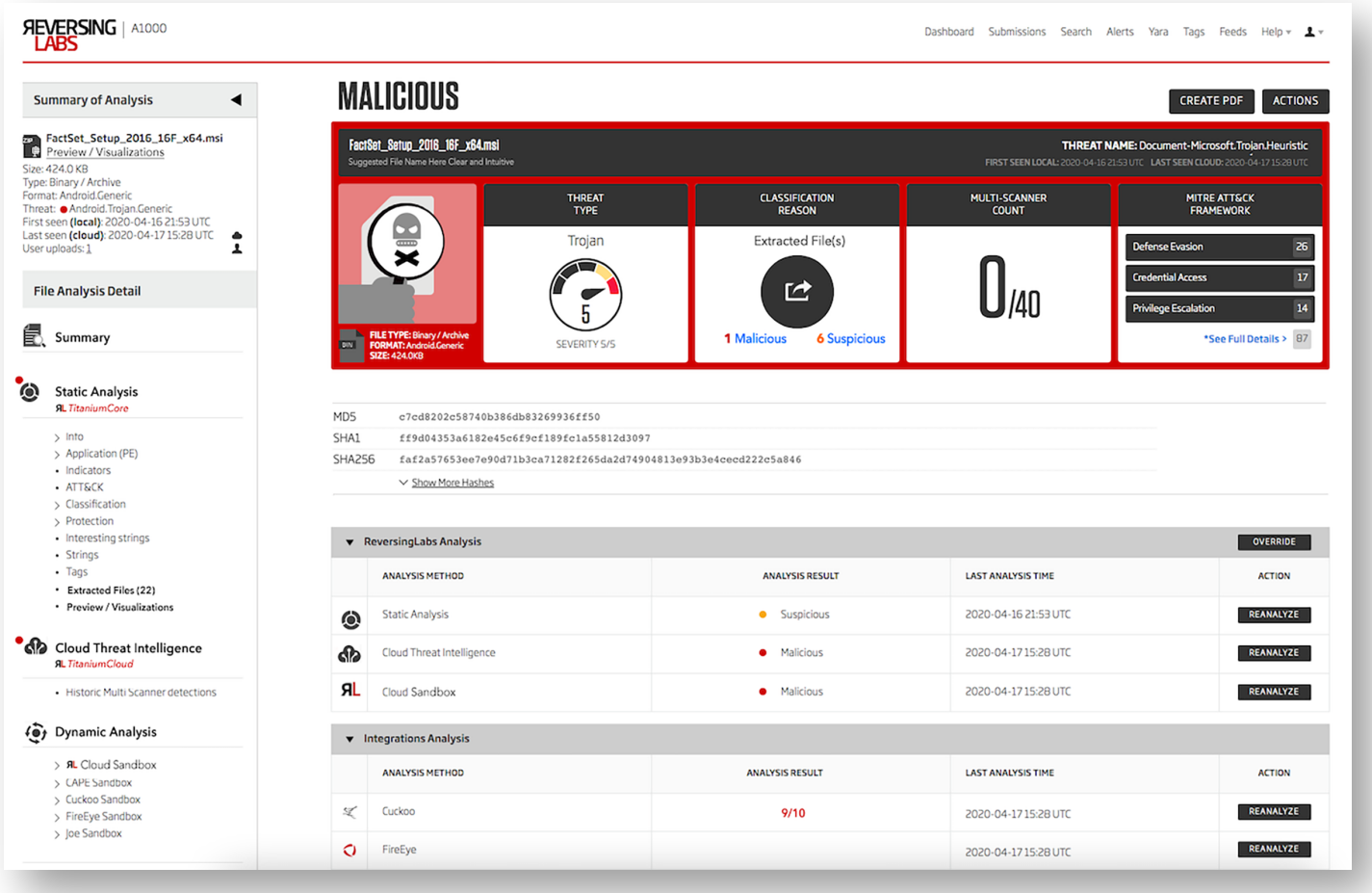
A1000 Malware Analysis Workbench

Hunt, Identify and Analyze Advanced Malware

The A1000 Malware Analysis Workbench provides high-speed binary analysis using proprietary techniques that include static, dynamic and machine learning file analysis. The A1000 is integrated with world-class file reputation services using the tens of billions of files in the classification database to provide in-depth rich context and threat classification and intelligence. 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 and provides deep file analysis, accelerating investigations and response activities.

Native integration with TitaniumCloud enables users to search across the tens of billions of goodware and malware files. Detailed analysis results provide actionable intelligence organized into categories to show what a sample would do if launched. Categories such as Search, Settings, Evasion, Executions 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 tens of 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 4,000 file formats from diverse platforms, applications & 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 that provide 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 Features

Private File Analysis

- Provides safe storage of malicious or suspicious files.
- Stores file context in an onboard searchable database.
- Enables private, safe sample sharing and historical analysis.

High-speed File Analysis

- Analysis engine performs high-speed analysis to unpack files, extract internal indicators and detect embedded threats.
- Identifies more than 4,000 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 packaged, installers, executable packers & compressors.
- Integrated database enables safe, secure storage of results and enables file search by threat indicators.

Advanced 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 Explainable 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.

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.
- Run hunting queries in the local A1000 dataset and Titanium Cloud simultaneously.
- Pivot the dataset by metadata properties and similarity to discover related threats.
- 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.

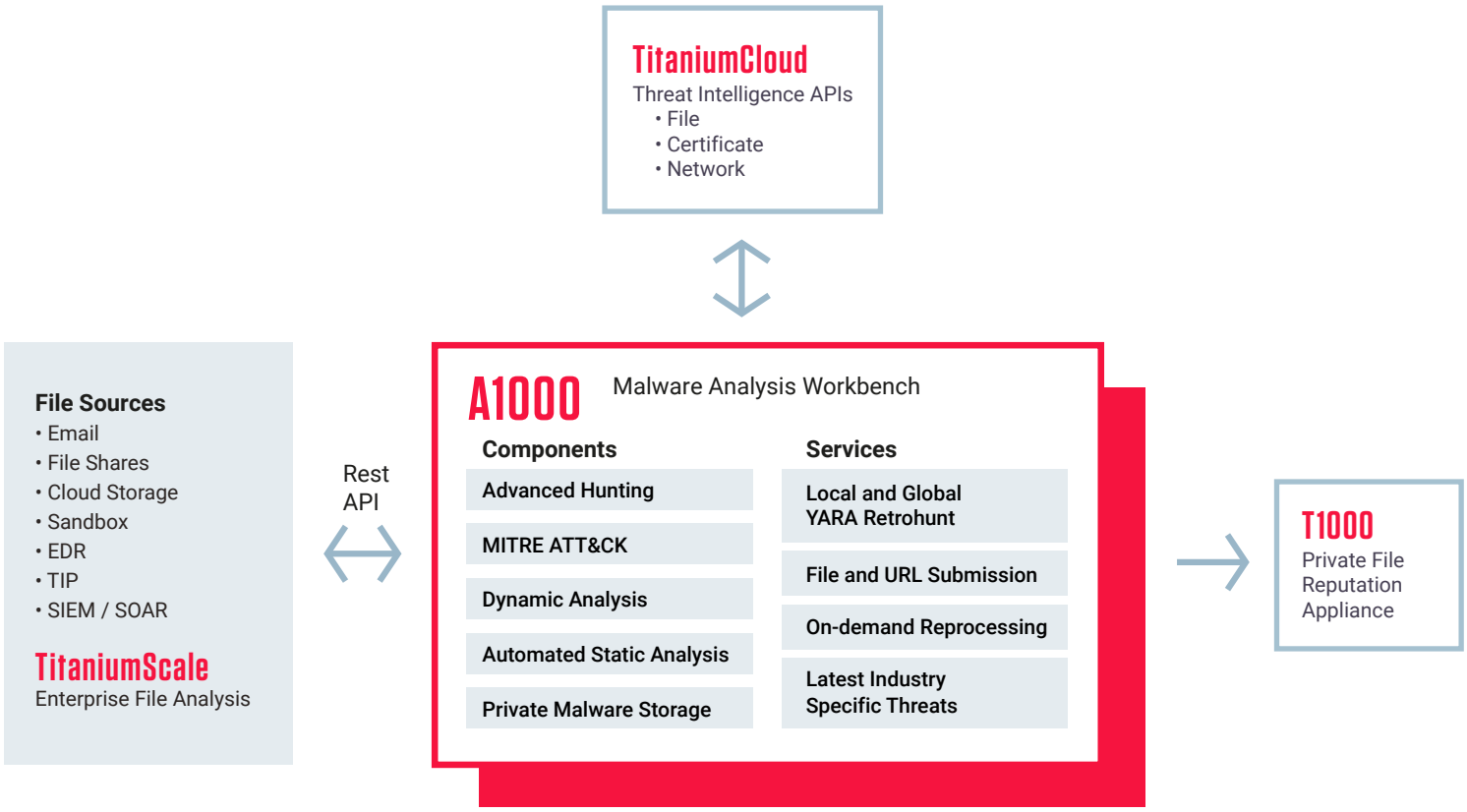
Integration with REST API's and Connectors

- Automated analysis workflows and orchestration via REST Web services API.
- Integrates directly with on-premise third-party Sandbox.
- Out of the box connectors automatically ingest samples from network file shares (SMB or NFS), cloud storage, SMTP and ICAP.
- Simple integration with dozens of third party security partners allows complete visibility across the organization.

Deployment Options

The A1000 is deployed locally as a virtual appliance. For customers who don't need the 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
Samples Publicly Accessible by Hash 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	
Alerting	X	



REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com