REVERSINGLABS

ReversingLabs Spectra Analyze

Advanced Malware Analysis and Threat Hunting Workbench

Key Features

In-depth, high-speed analysis fully dissects complex files in seconds, detecting embedded threats missed by other tools.

Verified threat classifications for reduced false positives, faster alert triage, and more effective response actions.

Broadest coverage in the industry with more than 4800 file types identified and over 400 file formats unpacked.

Built-in privacy controls including private file analysis, secure queries, and local datastore.

Advanced search functionality with 500+ unique search expressions, targeted, multi-conditional queries, and file similarity searches.

Simplified YARA rule development to quickly and easily import, build, test, and deploy rules – all from a single interface.

Continuous and retroactive matching across local dataset and RL's global threat repository for more powerful malware discovery.

Real-time alerting on changes to malware classification and analysis results to stay ahead of threats, including zero-day attacks.

Intuitive relationship graph to quickly see the bigger picture and intelligently pivot on interconnected malware artifacts.

Integrated cloud sandbox to perform runtime analysis on files and URLs in a private environment.

Pre-built connectors and REST API to automate analysis workflows with enterprise infrastructure and existing security tools.

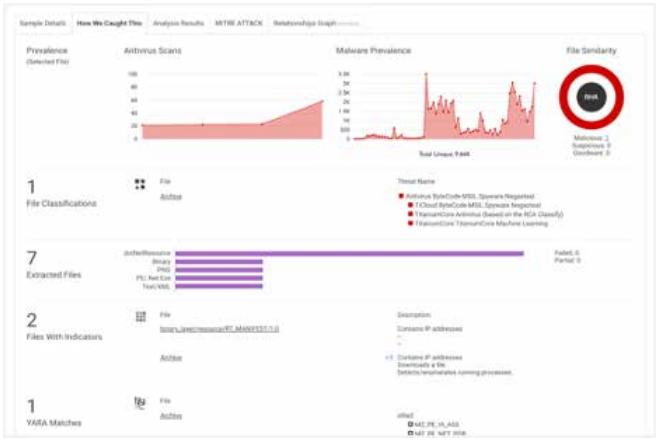
Spectra Analyze empowers the SOC with a malware analysis and threat hunting workbench that delivers the speed, depth, coverage, and accuracy analysts need to speed alert triage, enrich security tools, and accelerate response actions.

Powered by RL's proprietary, AI-driven, complex binary analysis technology and the industry's largest repository of file and network intelligence, Spectra Analyze is a powerful, integrated, out-of-the-box solution that makes malware threat detection, deep analysis, and analyst collaboration more effective and productive.

Spectra Analyze accelerates threat detection and response capabilities for all skill levels throughout the SOC. From L1 analysts doing initial evaluation and triage, to L2 analysts performing deeper malware inspection and investigation, to L3 analysts writing YARA rules and conducting threat hunting, Spectra Analyze provides the tooling and intelligence required to optimize SOC workflows and outpace advanced malware threats.

Advanced Analysis. Rich Context. Actionable Malware Intelligence.

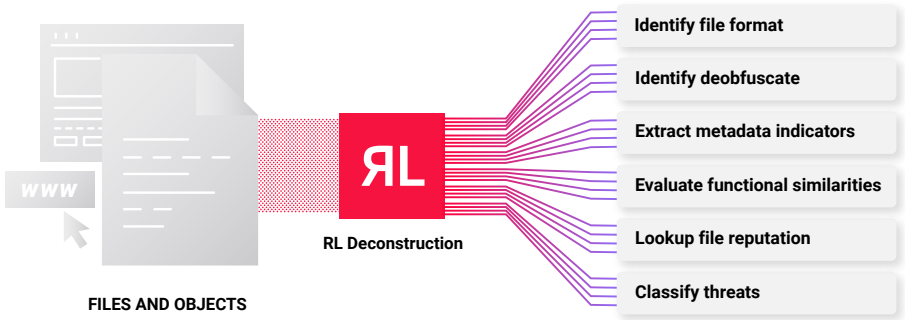
Security analysts can leverage the power of RL's malware analysis capabilities and context-rich results through an instinctive, easy-to-navigate GUI, as well as a robust REST API. Regardless of how analysts use Spectra Analyze, the result is truly actionable file and network intelligence, backed by verifiable threat verdicts that explain the "why" behind RL's risk score and classification. SOC analysts, incident responders, and threat hunters alike get the intelligence they need to more effectively and efficiently carry out their responsibilities to keep the organization safe from advanced malware and sophisticated cyber attacks.



RL Complex Binary Analysis: The Power Behind Spectra Analyze

Spectra Analyze is powered by RL's unique binary analysis engine, which can fully deconstruct the internal contents of a file, in milliseconds, to reveal hidden threats with the fastest times in the industry. This proprietary technology recursively unpacks and de-obfuscates files, including large, complex files, extracting thousands of indicators and rich metadata, applying global threat context from RL's authoritative database of goodware and malware, and delivering a verified threat verdict – all without executing the file. The result is real-time, next-level threat intelligence to prioritize alerts, enrich security tools, drive response actions, and perform advanced threat hunting with context, clarity, accuracy, and speed.

RL's Complex Binary Analysis Process



Spectra Analyze Features

High-Speed Binary Analysis

- In-depth file and network analysis
- Identifies more than 4,800 file formats across Windows, MacOS, Linux, iOS, and Android platforms
- Unpacks over 400 file formats of archives, emails, documents, multimedia, software packages, installers, executable packers and compressors
- Extracts over 20,000 file intent behavior indicators
- Extracts network IOCs from URL, domain and IP address analysis

Privacy Controls

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

Advanced Search

- Build more than 500 unique search queries using Boolean operators
- Leverage the autocomplete functionality for faster research
- Use Quick Search feature for advanced capabilities without knowing the syntax
- Perform targeted queries on large sample datasets
- Search by hash, imphash, file name, tags and more
- Find files based on functional similarity

YARA Hunting

- Leverage RL-supplied or user-defined YARA rules for matching and hunting
- Import, build, test, and deploy YARA rules from a single interface
- Match on thousands of characteristics from all files and objects unpacked and extracted during RL's binary analysis process
- Perform YARA hunting and retro-hunting across local dataset and RL's threat repository, simultaneously

RL Spectra Sandbox / Dynamic Analysis

- Highly available, scalable cloud sandbox integrated with Spectra Analyze Malware Workbench
- User friendly single-page file analysis report with drop-down to view individual historical reports
- Simplified network analysis tabbed navigation containing HTTP values, TCP IPs/ports, UDP IPs/ports, and DNS values provides easier investigation
- Default Snort and Sigma rules- automatically available without any additional set-up
- Download Screenshots, PCAP and Memory Strings from individual analysis

MITRE ATT&CK Mapping

- 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

API Integrations

- Automate analysis workflows and orchestration via pre-built connectors and REST API
- Built-in connectors to ingest samples from web, email, endpoint, local and cloud storage, and collaboration tools
- Connect to email sources (IMAP, Microsoft Exchange, SMTP servers) and analyze retrieved emails
- Connect to cloud and local storage, including cloud storage (S3, Azure Data Lake) and network file shares (SMB or NFS)
- Extensive API and direct integrations for feeding intelligence into SIEM/SOAR, EDR, TIPs, and sandboxes

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

We will show you how to empower your SOC with
RL Spectra Analyze

REQUEST A DEMO

reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com