

Spectra Detect: Enterprise File Analysis

High-Volume, Large-File Analysis at Speed and Scale

Highlights

Real-time, deep inspection of files, scalable to millions of files per day without execution.

Large-file analysis with the ability to process complex, multi-layered files up to 100GB in size.

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

Automated file ingestion from email, endpoints, cloud storage, network shares, collaboration tools, and more.

ICAP connector for plug-and-play integration with existing infrastructure.

Enterprise-wide YARA scanning with custom rule matching against thousands of object characteristics.

Powerful threat hunting with the ability to conduct YARA retro-hunts against private files at scale.

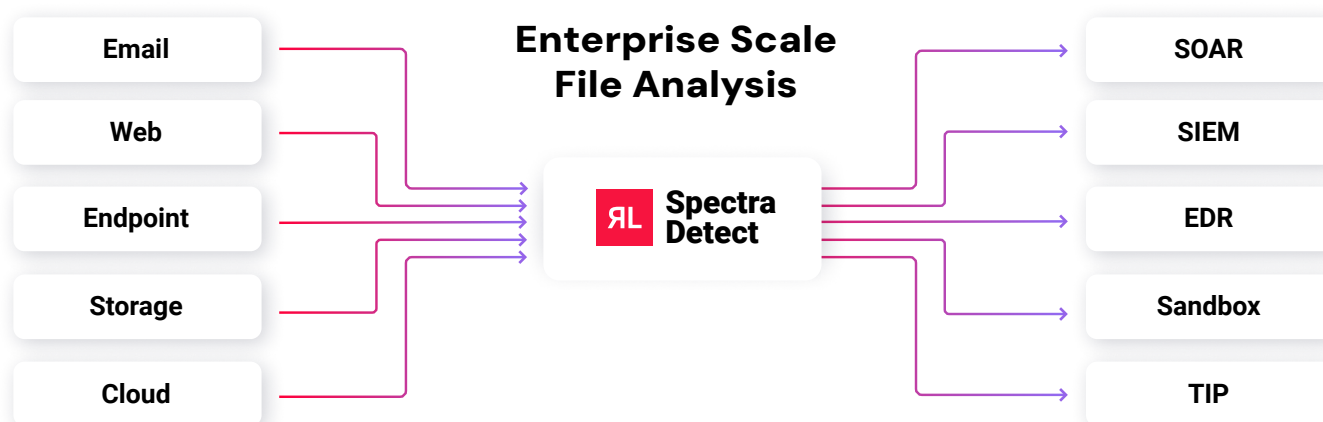
Workflow integrations to feed results to SIEM/SOAR platforms, EDR solutions, S3 storage, and more.

Real-time classification change alerts on file reputation data and threat status.

Highly scalable architecture to meet volume and capacity requirements as business needs grow.

RL Spectra Detect provides comprehensive, enterprise-wide visibility into malicious files and objects to identify threats wherever they reside. High-volume, high-speed file inspection and definitive threat classification empowers security operations teams with real-time, context-rich intelligence to drive faster, more effective threat detection and response, along with more powerful and precise hunting, so dangerous malware can no longer hide and dwell within the organization.

With Spectra Detect, enterprises can automatically ingest and assess millions of files a day from web traffic, email, endpoints, cloud storage, network shares, collaboration tools, and more – at unprecedented speed and accuracy. The solution uses ReversingLabs' proprietary complex binary analysis technology to perform deep file inspection and provide a verified threat verdict in real time. The results can be seamlessly integrated into industry-leading security tools and enterprise workflows, providing in-depth, file-level insights and malware intelligence with the needed context and relevance to detect, investigate, and remediate advanced threats at record speed and scale.



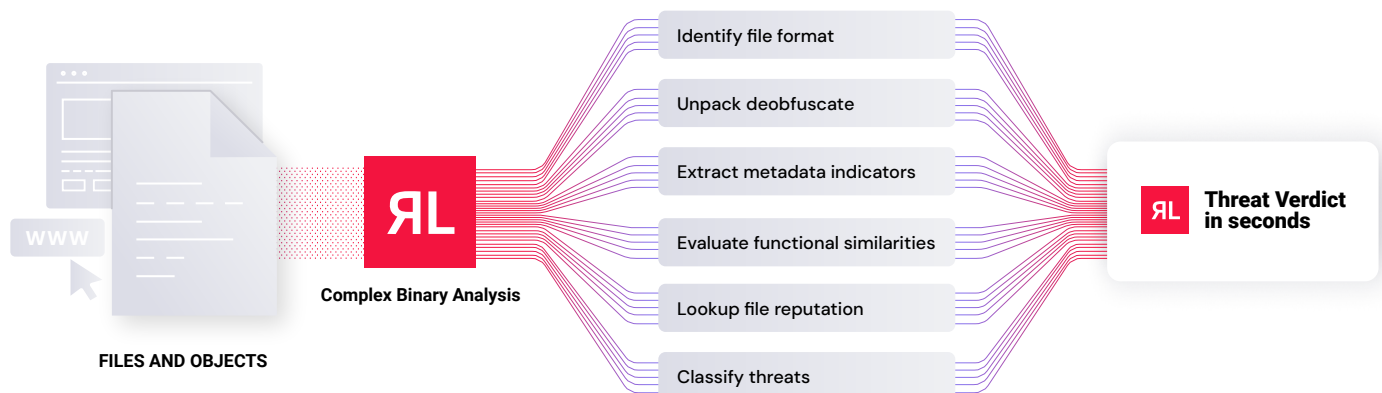
Spectra Detect Use Cases

High-Speed File Inspection	Close the malware visibility gap with real-time file inspection and classification
High-Volume Email Scanning	Scan and analyze all emails, links, and attachments at the speed of business
YARA at Scale	Match against thousands of object characteristics from any file or email source
File Share Security	Inspect and monitor file shares and cloud storage for new and latent malware threats

AI-Driven Complex Binary Analysis: The Power Behind Spectra Detect

Spectra Detect is powered by ReversingLabs' AI-driven complex 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 industry-leading data corpus of goodware and malware, and delivering a verified threat classification – all without executing the file. The result is a complete characterization of each file and next-level intelligence to enrich security tools in real-time, drive response actions, and perform advanced threat hunting, enabling organizations to close malware visibility gaps before a costly breach occurs.

Proprietary, High-Speed File Deconstruction and Threat Classification



Spectra Core Analysis Features

- **Speed:** Files cataloged in milliseconds to support real-time, high-volume processing
- **Coverage:** 400+ formats unpacked, and 4800+ file formats identified from Windows, Linux, MacOS, Android, iOS, media, documents, and applications
- **Depth:** Unlimited recursive unpacking and extraction of 20,000+ file behavior indicators
- **Reputation:** Files checked against the industry's most comprehensive reputation database with over 400 billion goodwill and malware samples
- **Classification:** Multi-factor threat classification including advanced rules engine that supports ReversingLabs and customer-supplied YARA rules

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, RL Spectra Core powers the software supply chain and file security insights, tracking over 422 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 RL Spectra Detect analyzes complex and large-volume files

[REQUEST A DEMO](#)

reversinglabs.com

