

RL REVERSINGLABS

Advanced Malware Analysis Suite

Save Time. Save Money. Get More Verdicts.



Malware Analysis Challenges

Enterprise SOC's find themselves spending more time and money, yet getting less out of their malware analysis solutions. Many rely on multiple products from multiple vendors, including expensive sandboxes, a myriad of threat feeds, reputation lookup services, and ad-hoc tools. This approach has proven insufficient and costly in the face of growing file volumes, increased file complexity, and more sophisticated malware threats.

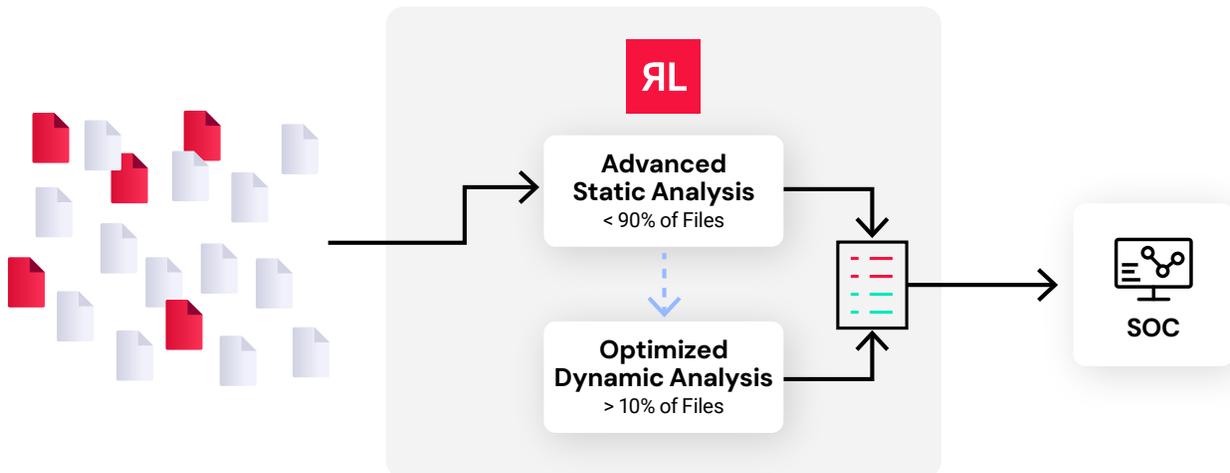
RL solves this problem with an Advanced Malware Analysis Suite that combines the power of next-gen static analysis with optimized dynamic analysis, plus real-time intelligence from the world's largest repository of goodware and malware. Our comprehensive, unified approach provides best-in-class file coverage and unmatched threat visibility, while delivering more value with superior results than other solutions.

Solution Highlights

- Advanced static analysis combined with optimized dynamic analysis to deliver faster, more accurate verdicts at less cost
- High-speed, fully recursive binary deconstruction to uncover threats at the deepest levels in seconds
- Broadest file coverage in the industry with support for 4800+ file types and multi-gigabyte file sizes
- Most up-to-date reputation data and threat intelligence from the world's largest repository of malware and goodware
- Privacy by default, including private file analysis and private data store

Save Valuable Time and Resources

RL's approach to malware analysis streamlines workflows and delivers vastly improved threat detection. It starts with our proprietary, AI-driven complex binary analysis engine that performs high-speed, fully recursive file deconstruction to identify embedded threats in seconds. This means more files are classified up front in real time. Our advanced static analysis technology is complemented by RL's integrated sandbox for optimized dynamic analysis. By applying each technique at the right time, SOC teams can analyze and convict more files, more efficiently, and at lower cost, while achieving the most accurate threat verdicts.



✓ Greater File Coverage

✓ Faster Threat Verdicts

✓ Higher Detection Rates

Get the Broadest File Coverage

RL provides the broadest file coverage in the industry, enabling security teams to comprehensively analyze and classify over 4800 file types and unpack over 400 formats of archives, installers, packers, and compressors – all without the file size constraints emblematic of other malware analysis solutions. RL's ability to analyze any file or object, regardless of size or type, allows enterprises to bridge critical detection gaps and identify malware wherever it may reside.

Defeat Evasive Malware

RL's unique binary deconstruction technology uncovers hidden malware threats at the deepest levels. Our analysis engine completely dissects any file or object down to its base elements, recursively unpacking, deobfuscating, and extracting all relevant indicators and metadata to identify suspicious signs in the file's "DNA". This proprietary pre-execution analysis overcomes the increasingly sophisticated sandbox evasion techniques employed by malware developers, while also speeding the detection of advanced threats so action can be taken sooner rather than later.

Outpace Emerging Threats

RL enables organizations to stay ahead of threats with the industry's largest, most up-to-date corpus of malware and goodware, which grows by the millions each day. Samples are continuously harvested and analyzed to provide early, actionable, high-fidelity intelligence about threats before they infiltrate customer infrastructures. SOC teams get crucial visibility into emerging threats and "in-the-wild" exploits to prepare defenses, proactively hunt, and ultimately preempt a costly malware attack.

Optimize Security Infrastructure

RL extends the power of existing security infrastructure, including SIEM/SOAR platforms, TIPs, and EDR solutions by providing a level of malware insights that no other tool can provide. Context-rich threat intelligence can be easily plugged into enterprise workflows through RL's flexible REST API and pre-built integrations, optimizing the performance and efficiency of security tools and SOC teams alike, and delivering maximum return on investments for the organization as a whole.

Get Started!

Experience the ReversingLabs Difference
www.reversinglabs.com

REQUEST A DEMO

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 400 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.