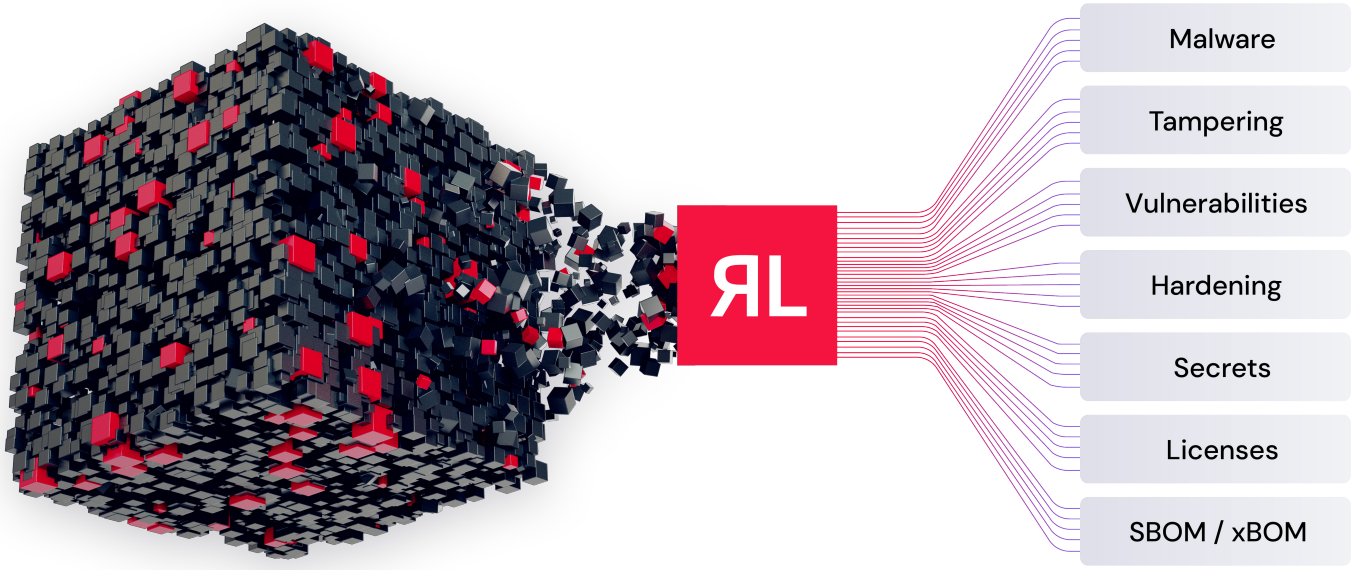
REVERSINGLABS

ReversingLabs Spectra Assure

See and Stop Software Supply Chain Attacks

RL Spectra Assure™ identifies and stops software supply chain attacks. It does this with the industry's only AI-driven Complex Binary Analysis that identifies malware, tampering, exposed secrets, vulnerabilities, improper hardening techniques, and more within minutes - all without the need for source code. The analysis generates the Spectra Assure Software Assurance Foundational Evaluation (SAFE) report which delivers the most comprehensive SBOM and risk assessment of an application.

Spectra Assure provides a critical final exam of the entire software binary, including proprietary, open source, commercial software, and any artifacts added during the build process. Software producers and enterprise buyers rely on Spectra Assure to trust the software they release, acquire, deploy, or update by eliminating coverage gaps, prioritizing alerts, enforcing custom policies, validating build integrity, and helping meet risk and compliance needs.



"Software supply chain is one of the biggest challenges that we face as an industry. We really need to be able to know how much we trust that piece of software. And that's where Spectra Assure comes in."

Tim Brown | CISO

SOLARWINDS

Spectra Assure SAFE Report Features

Malware and Threat Detection
Find real threats by tapping into the world's largest private repository of malware and goodware covering 40 billion+ searchable files.

Tampering Detection
Detect novel software supply chain attacks by flagging suspicious and outright malicious behaviors without the overhead of dynamic analysis.

Secrets Identification
Identify and remediate secrets and sensitive information that are live and exploitable.

Digital Signature Validation
Protect software integrity by discovering invalid, malformed, or altered digital signatures and certificates.

Reproducible Build Analysis
Verify the integrity of software build environments by identifying indicators of build tampering.

Version Differential Analysis
Flag new threats introduced and track remediation progress with each new version, and update.

Custom Policy Enforcement
Customize policy rules to focus on specific threat categories and specify severity levels based on business risk criteria.

Vulnerability Detection
Detect embedded vulnerabilities and prioritize those that are patch mandated or actively exploited by malware.

Secure SAFE Report Sharing
Foster collaboration with software vendors by generating and sharing security reports via secure, private links.

CI/CD Integration
Generate SAFE reports by integrating testing into CI/CD pipelines through native plugins, a command line interface (CLI) tool, or an easy-to-use Docker image to prevent threats from being pushed to production.

Benchmark Maturity Levels
Measure tangible security improvements over time with predefined security policy levels highlighting an actionable remediation roadmap.

SBOM/xBOM
Generate the comprehensive SBOM, SaaSBOM, MLBOM, CBOM, and more from fully compiled commercial software. Supports CycloneDX and SPDX standards.

Release Your Software with Confidence

Spectra Assure analyzes the complete software packages at the binary level, including proprietary, commercial, and open source components, plus any artifacts added during the build process. This critical build exam identifies software supply chain threats like malware, tampering, exposed secrets, malicious behaviors, vulnerabilities, and more to provide the confidence you need before you release to your customers. Additionally, Spectra Assure seamlessly integrates into CI/CD workflows for early detection of advanced software supply chain threats. By enabling developers to add Spectra Assure into their existing pipelines through native integrations or simple scripts, Spectra Assure can flag the most sophisticated and elusive software supply chain attacks before ever releasing to production. Spectra Assure empowers Product Security and AppSec teams to enforce security policy controls at any point in the SDLC (Software Development Life Cycle). Customizable policies can trigger prioritized alerts during the development stage, testing stage, and prior to final release on the fully compiled package, ensuring continuous security throughout the development process, and generate SAFE reports to share comprehensive SBOM data and attest to the efficacy of secure development processes.

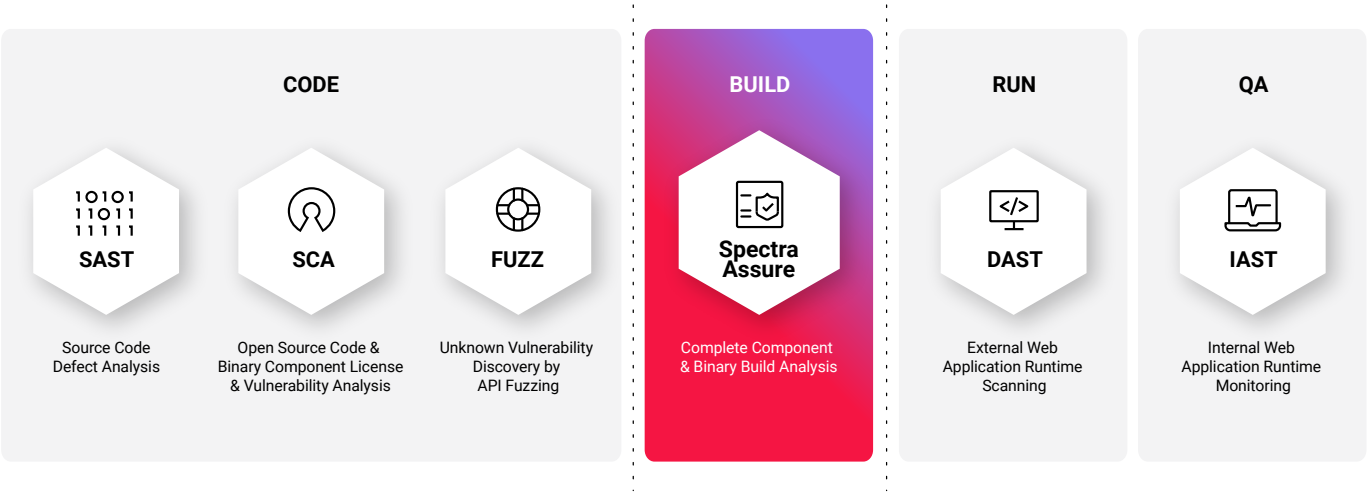


Figure 1: Spectra Assure provides the critical build exam to close the gap in the software development life cycle with complete binary analysis without the need for source code

Open the Black Box of Commercial Software Risk

For third-party cyber risk professionals, Spectra Assure delivers detailed transparency into commercial software risk without requiring source code. It thoroughly analyzes the complete software binary, deconstructing it to its individual components and categorizes findings across key risk categories. With the Spectra Assure SAFE report, third-party cyber risk professionals can make informed decisions throughout the software consumption life cycle. Version-to-version differential analysis highlights the progress vendors have made in addressing known security threats, as well as informing security teams of any net new threats that may have been introduced with a recent update. Furthermore, Spectra Assure's comprehensive risk reports are shareable, allowing enterprises to share security findings directly with vendors through a time bound, secure link. This mechanism empowers enterprises and software vendors to collaborate towards actionable remediation plans.

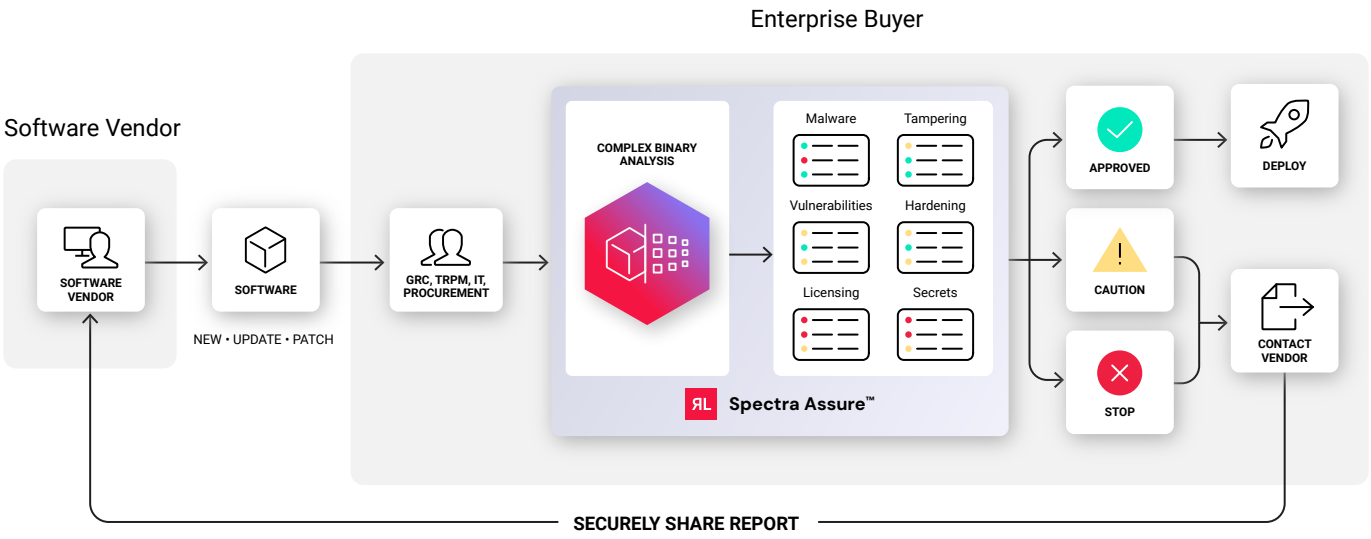


Figure 2: Make informed risk decisions when acquiring and deploying new commercial software, or pushing new versions and updates, and share assessments back with the vendor for expedited remediation.

Spectra Assure Features

AI-Driven Complex Binary Analysis

- Recursively unpack over 4800 file types down to individual DLLs, containers, and other post-build artifacts to correlate against a repository of over 3000 threat indicators
- Scan large and complex files rapidly, as fast as 1 GB in as little as 5 minutes to keep pace with business requirements
- Explainable artificial intelligence (xAI) enables threat hunting by identifying human-readable threat indicators that signify potential novel malware threats
- Analyze proprietary, commercial, open source, and all artifacts of software packages without requiring source code

Advanced Software Supply Chain Threat Detection

- The world's largest threat repository containing 422+ billion searchable files, methodically analyzed and categorized as malware or goodware
- Identify advanced software supply chain attacks that mimic SolarWinds and 3CX
- Detect tampering with version differential analysis and reproducible builds, coupled with AI-driven threat hunting and behavioral analysis
- Generates the SAFE report to provide the most comprehensive SBOM, SaaSBOM, MLBOM, CBOM and risk assessment for an application - enabling editing and declaration of components for attestation.
- Identify exposed secrets like login credentials, API keys, certificates or encryption keys that are exposed due to hard coding, weak cryptography, packaging automation mistakes, insider threats, or other means
- Ensure proper application hardening techniques by flagging missing vulnerability protections, insecure coding practices, outdated toolchains, inadequate prevention methods, and missing fortified functions
- Analyze the entire executable software package for known exploitable vulnerabilities
- Verify that any open-source or third-party components are free of risky copyleft licensing terms that can compromise the compliance standing of your proprietary software

Secure Software Build and Release

- Go beyond traditional AST tools like SAST, DAST, and SCA to detect a wider scope of software supply chain threats beyond vulnerabilities like malware, tampering, exposed secrets, and more
- Integrate security testing into existing CI/CD environments like GitHub, GitLab, Azure DevOps, and TeamCity through native plug-ins, CLI scripts, or Docker images
- Enforce policy controls at successive stages of the SDLC from development, to test, to the final release exam before production
- RL Levels tracks your program maturity with a gradual, guided approach that measures security posture against a series of predefined policy levels meant to show tangible improvement over time
- Maintain software security compliance standards such as those outlined by CISA, NIST, FDA and the European Union's NIS2, DORA, and Cyber Resilience Act

Assess and Manage Commercial Software Risk

- Ensure governance, risk, and compliance alignment with acquiring or deploying software
- Overcome limitations of high-level vendor risk assessments by deconstructing commercial applications at the binary level and analyze against dozens of robust security policies - all without requiring access to source code
- Categorize findings across key risk categories including: Malware, Tampering, Application Hardening, Secrets, Vulnerabilities, and Licenses
- Collaborate with vendors on questions and remediation action plans by directly sharing SAFE reports through timegated, password-protected links
- Make informed risk decision before updating with version-to-version comparisons that highlight new security threats introduced with code changes
- Assess vendor security practices by aggregating threat findings into predetermined maturity Levels
- Provides broad xBOM capabilities for detailed SBOM, SaaSBOM, CBOM, and MLBOMs in SPDX or CycloneDX formats

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!

Learn more about RL Spectra Assure.

REQUEST A DEMO

reversinglabs.com

DS-Rev-04.22.25

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com