REVERSINGLABS

Spectra Assure Community/Community+

Automatically Protect Development Teams from Using Insecure or Malicious OSS

Automate Curation of OSS with Spectra Assure Community

Spectra Assure® Community continuously monitors changes in over seven million open-source packages to identify malware, vulnerabilities, malicious code tampering, and other indicators of zero-day supply chain attacks like Shai-hulud.

Deep risk assessments across npm, PyPI, and other repository packages are performed as they are uploaded to their repositories. This analysis is translated into a clear Pass/Fail status which can be used to:

- Deliver a pre-vetted stream of OSS components and updates that are free from malicious code and critical flaws.
- Block malicious open source code from being used without introducing developer friction.
- Ensure that only safe and properly vetted open-source components are integrated into internally developed applications.

Overall software quality can be elevated by integrating only the most trustworthy open source into builds. Centralized, predefined policies for critical issues act as a gatekeeper, ensuring your proprietary software is built exclusively on a foundation of high-integrity OSS.

With out-of-the-box integrations, APIs, and CLI tools, you can easily protect your development processes from risky open source code. Automated curation of safe packages and updated versions are seamlessly integrated into your workflows. OSS risks can be automatically assessed by scanning manifest and lock files in your CI/CD pipelines or GitHub repositories with the rl-protect tool.

The bottom line: Spectra Assure empowers developers with a seamless solution that ensures only safe OSS components enter development pipelines, yielding software that is both secure and high-integrity.

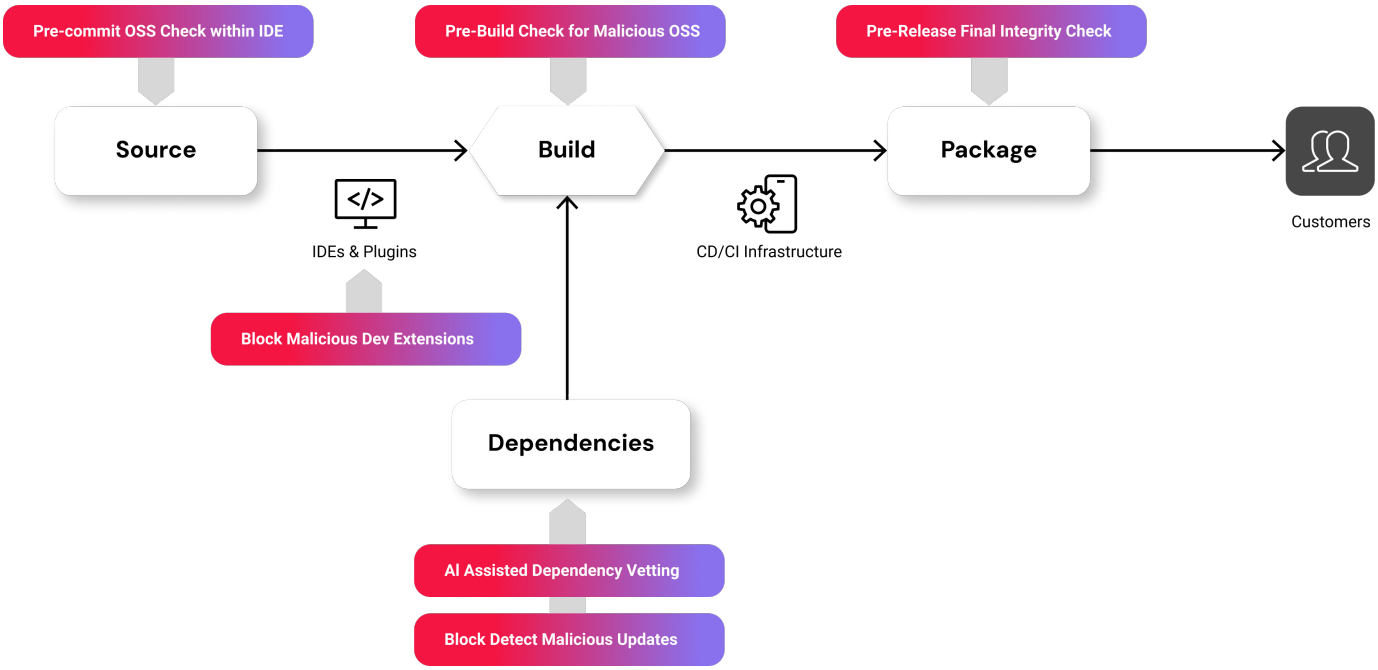

Figure 1: Spectra Assure Community: Integrate Safe Open Source Across the SDLC

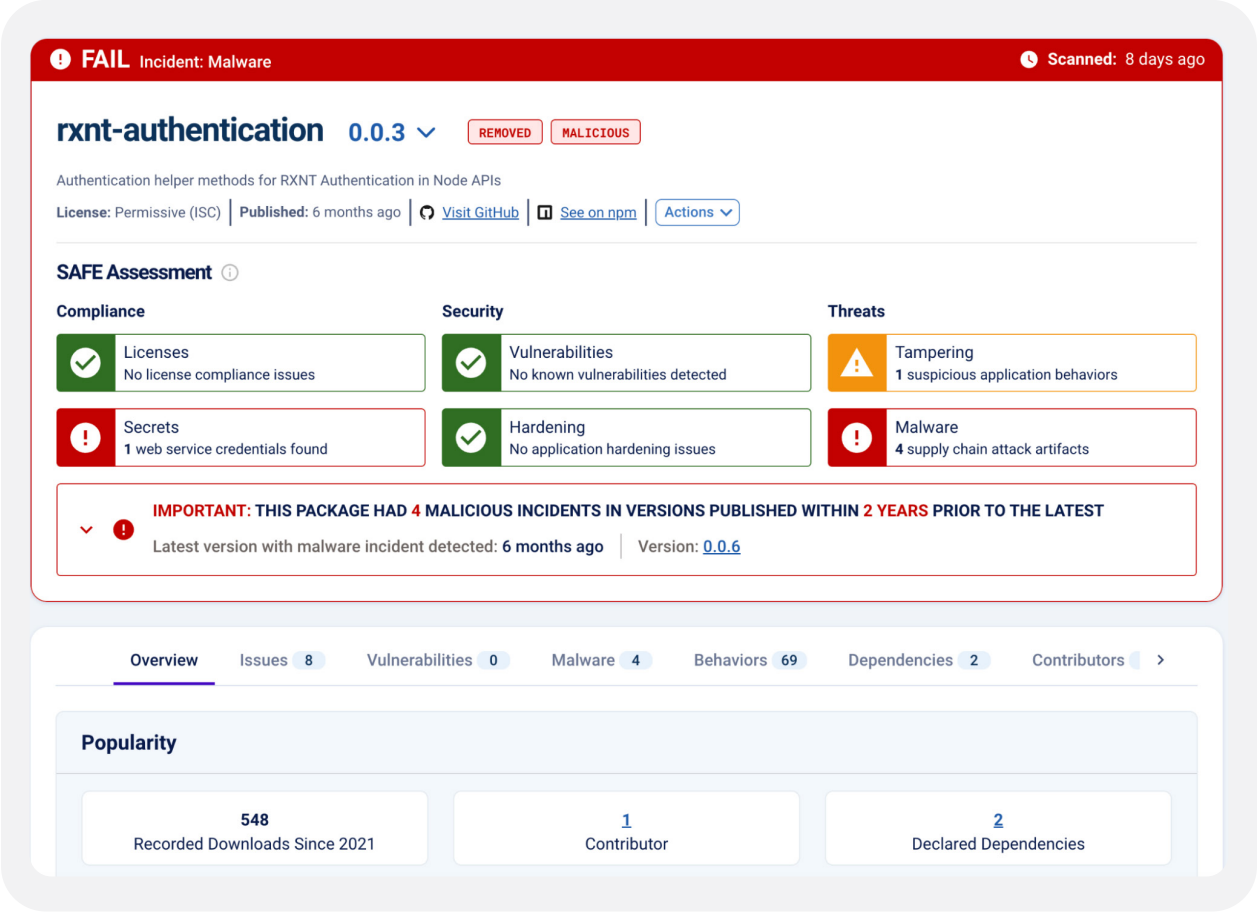

Figure 2: Spectra Assure Translates Deep Analysis Into Pass/Fail Outcomes for Automation

Solution Highlights

Continuous OSS Threat Monitoring

- RL continuously monitors public repositories (e.g. npm, PyPI, NuGet, and more) for new and existing package versions.
- Every new or changed package is immediately analyzed, providing the most up-to-date threat information available anywhere.
- Entire repositories are reanalyzed regularly to inform users on the latest emerging threats and CVEs in every version.

Embed Automated OSS Controls

- Fortify software supply chains by establishing automated security controls for package curation and version updates.
- Seamlessly embed OSS security controls into workflows directly within CI/CD pipelines.

Comprehensive OSS Analysis

- Spectra Assure provides proactive detection of vulnerable and malicious changes in open-source packages.
- Our deep analysis turns complex code patterns into behavioral descriptions that explain what packages are capable of doing.
- By analyzing behaviors and changes to code, we uncover zero-day OSS supply chain attacks that have never been documented.

Secure Developer Toolchains

- Protect development teams from compromise and credential theft by restricting installations to only vetted VS Code extensions.
- Implement guardrails for AI-augmented development to ensure use of vetted open source or public MCP Server packages.

Compare Plan Capabilities	Community	Community+
Aggregate API lookups	**100k/mo**	**1M/mo**
REST API tokens	**10**	**10**
Advanced Malware & Threat Detection		
Novel malware detected by RL proprietary analysis	✓	✓
Code tampering detected by RL proprietary analysis	✓	✓
Malware detections confirmed by RL analysts	✓	✓
Automatic triage of common false positives by third parties	✓	✓
Known malicious OSS packages	✓	✓
Known protest, advertising, and potentially unwanted component detection	✓	✓
Known malicious URLs, domains, and IP addresses	✓	✓
Software behaviors related to malware activity (e.g. behavior is only detected in malware)	✓	✓
Behavior prevalence statistics (e.g. how often is this behavior used in npm packages)	✓	✓
Secrets Detection and Exposures		
Hardcoded web service credentials, tokens, and keys	✓	✓
Private keys and certificates	✓	✓
Exposure and liveness status for triage automation	✓	✓
Automatic triage of commonly shared open-source secrets	✓	✓

Compare Plan Capabilities	Community	Community+
Aggregate API lookups	**100k/mo**	**1M/mo**
REST API tokens	**10**	**10**
Vulnerability Detection and Reporting		
Known vulnerabilities from public sources (NVD, OSV, GitHub, KEV, etc.)	✓	✓
Proprietary vulnerability exploitation intelligence	✓	✓
AI-enriched vulnerability descriptions and CVSS	✓	✓
Software Bill of Materials (SBOM)		
SBOM generation with CycloneDX download	✓	✓
Software license analysis unwanted component detection	✓	✓
Cryptography and Post Quantum Attack Readiness		
Detection of unsafe digital signature cryptography usage	✓	✓
Detection of expired, revoked, malformed, and blacklisted certificate usage	✓	✓
Failed integrity validation checks	✓	✓
Integration Capabilities		
Out-of-the-box integrations, APIs, and CLI tools	✓	✓
Pre-build check of CI/CD manifests and lockfiles for malicious OSS	✓	✓
OpenAI Custom ChatGPT	✓	✓

Choose the Right Plan for You

Community

For individual developers to understand OSS risks.

GET STARTED

Community+

For individual developers to automate OSS supply chain protection.

REQUEST A QUOTE

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 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.

Rev-DS-04.14.26

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com