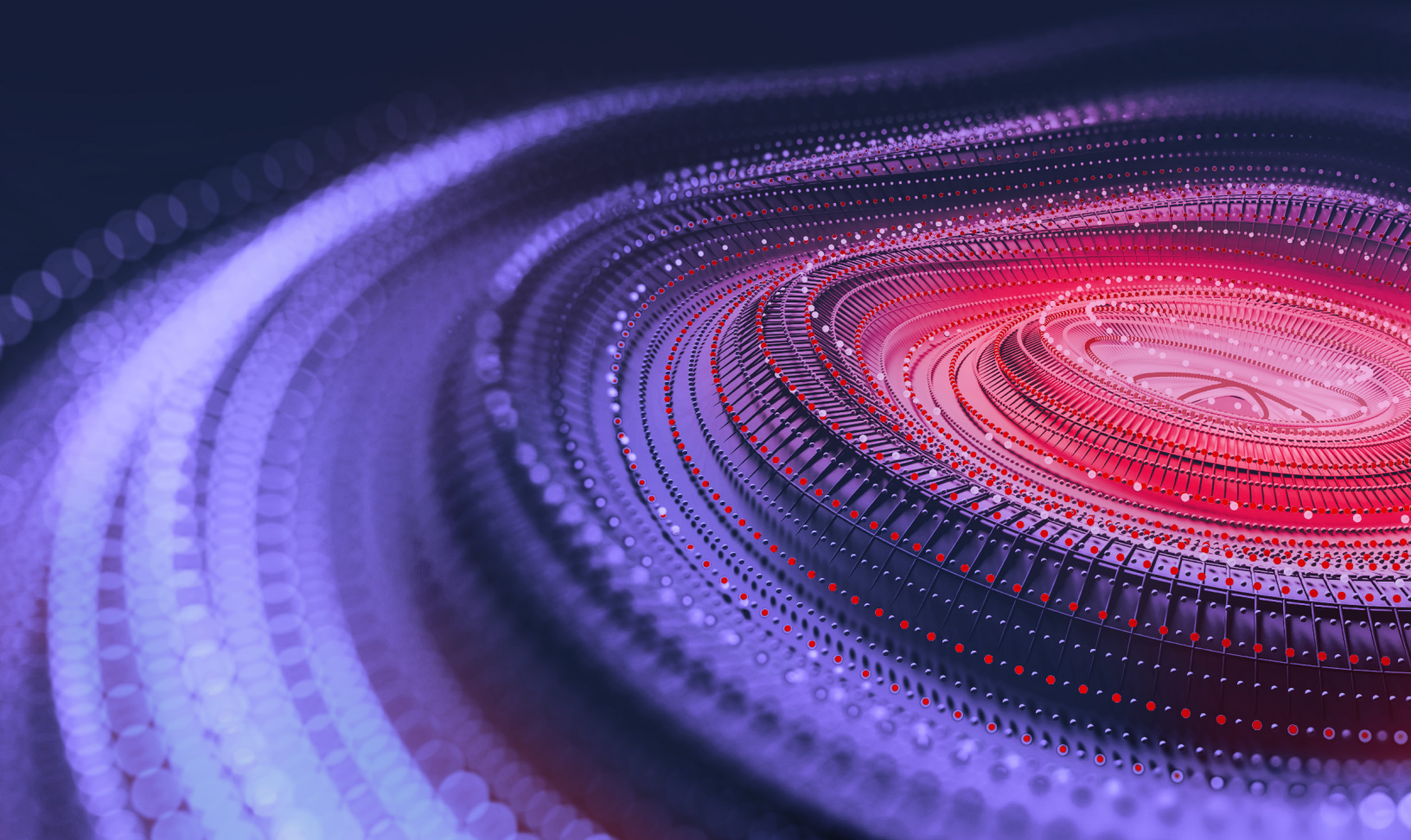
SOLUTION BRIEF

REVERSINGLABS

Assess and Manage Third-Party Software Risk with Software Supply Chain Security



Software Supply Chain: An Evolving Threat Landscape

The inescapable blast radius of recent supply chain attacks demonstrates the reliance of modern enterprises on open-source software, which the Linux Foundation estimates to make up 70-90% of modern software packages. Malicious actors are now exploiting enterprise dependencies on the open-source ecosystem as an initial entry point into the software supply chain. In fact, ReversingLabs observed a nearly 100x increase in the number of malicious packages that have been uploaded to popular open-source package repositories (e.g. npm) last year that are commonly used by large-enterprise software developers.

As these open-source components get packaged into commercial off-the-shelf (COTS) software products, organizations lose visibility into the components of software that often supports critical business processes. Without control over the software, organizations struggle to manage the security risk that might be introduced through either inadvertent or malicious intent.

Linux Foundation estimates to make up

70–90%

of modern software packages

≈ 100x

increase in the number of malicious packages that have been uploaded to popular open-source package repositories

Attacks on Software Causing Financial Loss and Operational Impact

We are now seeing this risk translate into financial loss and operational impact. In 2022, IBM found that the cost of a data breach due to vulnerabilities in third-party software cost on average $4.55 million USD. In fact, the threat of attack on third-party software ranked among the top four of all enterprise attack vectors when considering not only cost of data breach, but also mean time to detect and contain, as well as frequency of breach occurrence.[1]

IBM found that the cost of a data breach due to vulnerabilities in third-party software cost on average

$4.55 M

[1] https://www.ibm.com/uk-en/reports/data-breach

Asses Software for Supply Chain Security Threats

ReversingLabs Spectra Assure solution ensures that as long as you have access to the software binary you intend to use, you can regain visibility and control over your software supply chain. Powered by our complex binary analysis engine, you can automatically unpack large software to generate a bill of materials (SBOM), and determine software provenance. Further, our automated reporting allows security practitioners to quickly detect and mitigate threats within the software.

The solution unifies stakeholders from across the business, in a single platform, to better understand and more efficiently remediate risks within the software supply chain:

- **Senior executives (CIO, CISO, CTO)** can gain visibility into supply chain risk by comparing the security posture of vendors that make up their software ecosystem
- **Procurement & Legal** functions can quickly compare the results of different packages to aid in software procurement and acquisition decision making
- **Third-Party Risk Management (TPRM)** can automate software assurance testing, thus eliminating the need to perform manual questionnaire-based assessments required for software suppliers.
- **IT Operations** can more granularly control what software is approved for use, and if needed revoked from end user workstations
- **Security Operations (SOC)** can quickly identify and triage issues related to compliance, exposures and threats
- **Application Security (AppSec)** teams can complement existing cyber toolchains, which are good at finding vulnerabilities across the software usage lifecycle, but cannot detect modern software supply chain attacks

Spectra Assure digs deep into the many layers of software, components, and dependencies, regardless of toolchain choices or the size of builds, releases, or containers being analyzed. It detects unauthorized software changes, malware or backdoors, and exposed secrets that can be used in software supply chain attacks.

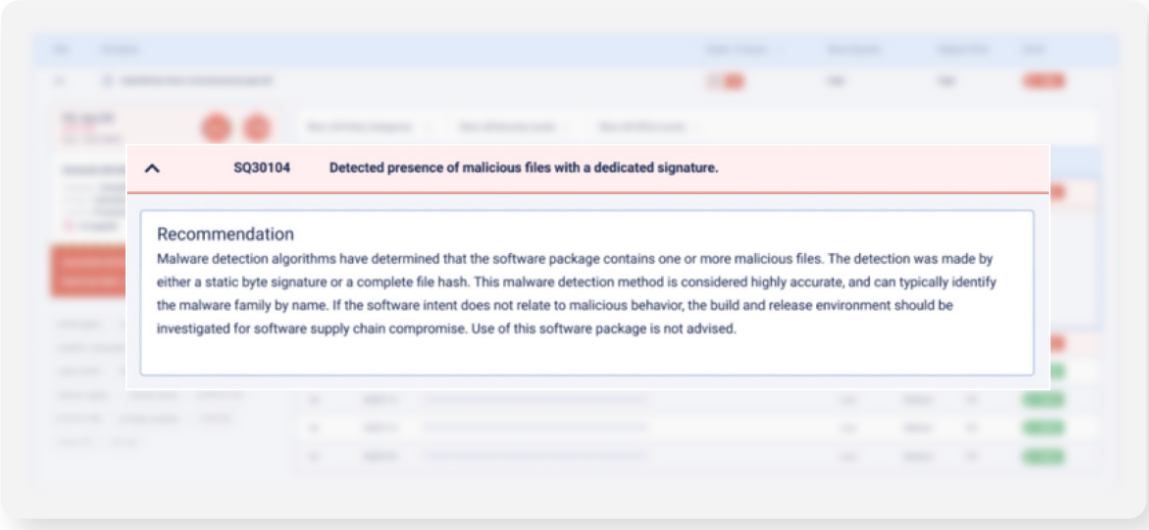


Figure 1: Sunburst attack identified by malware analysis and suspicious behavior changes

ReversingLabs Benefits Across the Software Use Lifecycle

Spectra Assure provides a unified platform for addressing a variety of challenges that software consumers face at different stages of their software use lifecycle (i.e. acquisition, deployment, maintenance, monitoring).

Acquisition

Challenge:

Organizations find it difficult to obtain relevant information or perform testing over the software they consume from suppliers. This is due largely to an unwillingness by suppliers to share information which may be deemed sensitive. Organizations are thus left without the necessary information to articulate to management whether these software suppliers present security risk to the business, driving uninformed procurement and architecture design decisions.

Solution:

The analysis results can help compare the security posture of software provided by multiple prospective software vendors. This will enable organizations to ensure cybersecurity risk is considered during procurement and acquisition (e.g. M&A) decision making.

Benefits:

- Non-invasive software assurance testing using just a binary package (no access to supplier source code is needed)
- Compliance with directives or policies related to software acquisition and security
- Closes security testing gap while maintaining business velocity

Deployment

Challenge:

Without adequate insight into the development processes used to build software packages, consuming organizations are left with a black box of risk, waiting to be exposed and exploited. As a result, security practitioners lack the visibility into necessary hardening mechanisms that may be required to ensure the software deployed is protected from future attack.

Solution:

Once a software package is procured, issues reported by Spectra Assure may require remediation. If the software vendor is unable/unwilling to action these issues prior to go-live, an organization may require additional protection mechanisms.
The analysis results can inform secure deployment options to enable effective risk mitigation.

Benefits:

- Software deployments future proofed from downstream supply chain attacks
- Minimized release delays by prioritizing critical deployment threats for remediation
- Improved automation of supply chain security guardrails earlier in the software use lifecycle

Maintenance

Challenge:

Relying solely on a point-in-time software assurance testing program cannot deliver the required level of insight to ensure that regularly updated applications, even from a trusted vendor, remain secure. While a check-the-box approach can flag potential problems, it can overlook newer exposures, providing an incomplete view of risk.

Solution:

The platform scans subsequent releases (e.g. patches, hotfixes) to highlight how the security posture of software evolves throughout its use lifecycle, and if any new risks are introduced through maintenance activities. Over time, Spectra Assure can be used as a repository of verified and trusted software by defining the packages that can be downloaded and if needed, revoked, from user workstations.

Benefits:

- Ability to detect malware and tampering attempts hidden within release packages
- Creation of a comprehensive software inventory
- More granular control over software usage

Monitoring

Challenge:

The traditional approach to responding to supply chain attacks relies heavily on engagement with external parties. During times of distress, communication channels with suppliers often become unresponsive or contentious. Organizations need a way of equipping themselves with the information they need to independently monitor and respond to attacks on the software supply chain in real time.

Solution:

When organizations become aware of malicious or vulnerable software within their supply chain, Spectra Assure can support incident response efforts by helping investigate the blast radius of an attack (i.e. query packages affected by a vulnerable component such as Log4J) using the queryable SBOM interface.

Benefits:

- Reduced reliance on external parties for incident investigation
- Faster and more targeted incident response efforts
- Queryable and easy to navigate solution interface

1. Submit & Analyze:

Rapidly analyze large release packages, containers, open-source libraries, and third-party software for threats

2. Review & Fix:

Rapidly analyze large-release packages, containers, open-source libraries, and third-party software for threats

3. Verify & Release:

Confidently confirm security quality and ensure compliance requirements are met

4. Continuously Monitor:

Identify, investigate, and respond to new risks which are introduced throughout the software use lifecycle

Learn More about ReversingLabs

ReversingLabs is the trusted authority in file and application security, protecting software development and powering advanced security solutions for the most advanced cybersecurity and Fortune 500 companies. The ReversingLabs Titanium Platform® powers the software supply chain security and threat intelligence solutions essential to advancing enterprise cybersecurity maturity globally. Tracking over 35 billion files daily, and the ability to deconstruct full software binaries in seconds or minutes, only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk.

Get Started!

We'll Show You How To Reduce Software Supply Chain Risks With ReversingLabs

REQUEST A DEMO

www.reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com