WHITE PAPER

REVERSINGLABS

# Assess & Manage Commercial Software Risk

with RL Spectra Assure

# The Commercial Software Risk

"How do I know the commercial software coming into my organization is safe?" That is a fundamental question businesses must be able to answer. It is a question the importance of which has increased exponentially in light of the growing software supply chain attacks impacting commercial software. Gartner recently reported that software supply chain attacks have seen triple-digit increases. The 2024 Verizon Data Breach Investigation Report (DBIR) found that breaches stemming from third-party software development organizations played a role in 15% of the more than 10,000 data breaches Verizon documented, a 68% jump from last year's report alone. And RL reported a 1300% increase in threats in its State of Software Supply Chain Security 2024 Report. Malicious actors exploit the good reputation of commercial software vendors to clandestinely introduce malware, ransomware, and other malicious code to enterprise networks and systems, often by compromising the vendor's own development pipeline. We have already seen this unfold multiple times over the past few years in these notable instances.

- **SolarWinds (2020)** - Thousands of SolarWinds customers were impacted when nation-state actors compromised SolarWinds' software build and code signing infrastructure, directly modifying proprietary source code to include a malicious backdoor in the form of a signed Orion software patch. This impacted roughly 18,000 customers.
- **3CX (2023)** - North Korean threat actor Lazarus Group compromised the endpoint client of VoIP software vendor 3CX with a first-of-its-kind cascading software supply chain attack, delivering malware to a significant portion of 3CX's 600,000 customers.
- **MOVEit (2023)** - Progress Software's MOVEit file transfer management program was compromised, impacting more than 2,600 organizations and 77 million people worldwide, making it one of the most significant supply chain attacks to date.

The fact is that software represents the greatest under-addressed attack surface facing businesses.

# Regulations Target Software Supply Chain Risks

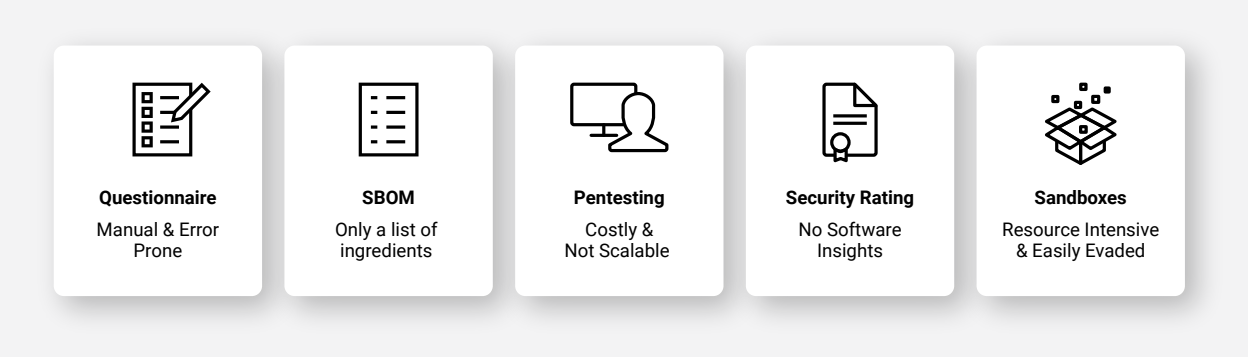
While loss of customer data and brand trust are challenging enough, companies are also confronted with the prospect of paying millions in breach mitigation costs and rising regulatory fines and litigation. Research from the 2023 edition of IBM's Cost of a Data Breach Report showcased that a data breach costs businesses $4.45 million on average. However, massive breaches impacting millions of customer records like those that affected SolarWinds, 3CX, and Progress Software can cost anywhere from $36 million to $332 million. New changes to global regulatory requirements have emphasized regulator's determination to examine and penalize failure to maintain detailed software security controls and report sharing. The European Union's Digital Operational Resilience Act (DORA), for example, emphasizes the necessity for visibility into a broader range of commercial third-party software risks. DORA specifically calls out the need to assess a broader spectrum of software supply chain threats, asking businesses to "Implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and shall check for corresponding new security updates."

**EU DORA calls out businesses to identify malicious code, possible information leakages, and other security threats.**

Even existing data protection laws like the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the US hold businesses accountable for any customer data loss, even if the breach is traced back to a third-party vendor.

# Going Beyond Questionnaires and SBOMs

The increase in software supply chain attacks, regulations, and guidelines means CISOs and risk managers need to properly identify the risks in the commercial software used across their organization. However, the current tools do not allow enterprises purchasing software the adequate insights or protection.




- **Vendor Security Questionnaires:** Security questionnaires, while helping to collect written statements from vendors regarding their security practices, are slow and expensive to oversee. Most glaringly, they hinge on the vendor providing truthful and accurate self-attestation to the secure development of the software they ship to customers. The "inherent trust model" of software acquisition is not sufficient.
- **Software Bill of Materials (SBOM):** While the practice of requesting a software bill of materials (SBOM) from vendors is now gaining traction, SBOMs are ultimately just a list of ingredients. They don't identify risks and threats such as malware, tampering, or context into how internal software components correlate to threats.
- **Penetration Testing:** Penetration testing, or pentesting, is a fundamental practice that mimics a real-world threat actor's actions to compromise an application deployed to production. However, pentests are often hyper-focused in scope, omitting a large portion of the codebase, and the fees associated with scoping and managing penetration tests are untenable at a larger scale.
- **Security Rating Services:** Security rating services aim to convey a vendor's exposure to cybersecurity risk by providing a letter grade (e.g. A-F, or 1-100) based on passive scans of the vendor's externally-facing infrastructure. However, these findings are often irrelevant as they are superficial in scope and do not address the security posture of the software package itself.
- **Application Sandboxes:** Sandboxes are sometimes used to "detonate" potentially risky commercial software in a contained environment. However they are resource intensive, and can be easily evaded using malicious techniques such as time-based payload execution delay methods like those used within the SolarWinds software supply chain attack.

With 83% of TPRM leaders still finding risks embedded in vendor applications according to Gartner, it's easy to see why third-party risk managers, cybersecurity, and even procurement teams are eager to adopt more sophisticated and scalable methods to adapt to this endpoint threat; methods that can also address the increasing size and complexity of software packages where threats can hide. It is increasingly common to find software packages in the 10 GB range that contain over 30 thousand software components and over two million files. This creates an extremely difficult "needle in a haystack" situation for traditional endpoint detection anti-virus solutions to address effectively.

# Addressing Your Commercial Software Risk

To know if the commercial software they are using is safe, organizations need to be able to open up the black box of commercial software and see what risks or threats exist across the entire binary. RL Spectra Assure™ goes beyond a simple inventory of software components. It delivers the visibility and scalability for all software used in the modern enterprise - in minutes and without the need for source code.

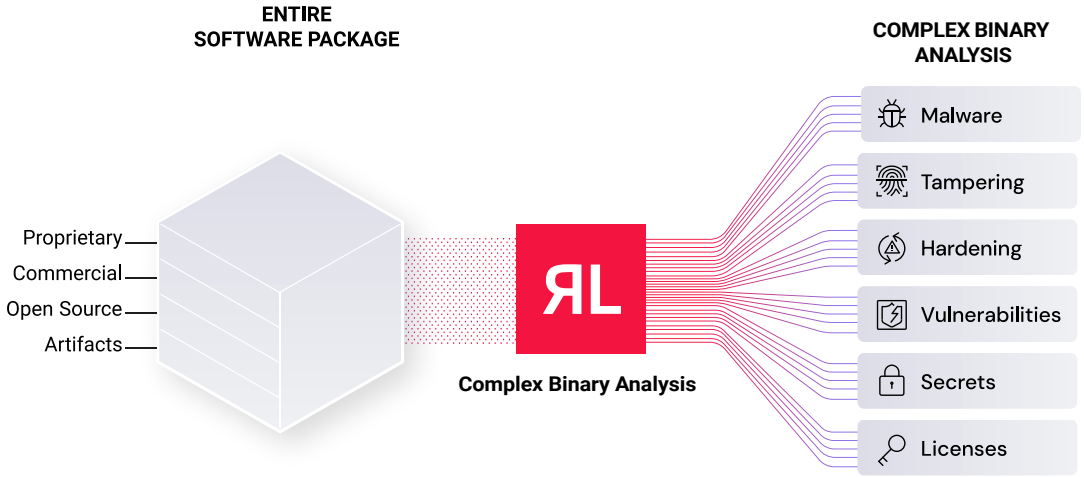



Figure 1: AI-driven complex binary analysis powering Spectra Assure deconconstructs custom, commercial, and open-source components, along with any executables, files, containers, or other elements to find embedded software supply chain threats.

It delivers a comprehensive software risk analysis that identifies threats undetectable by traditional third-party risk assessment tools, including:

**Malware**
is detected leveraging the world's largest threat intelligence database covering 40 billion files with 16 proprietary malware detection engines to prevent advanced threats from spreading throughout the software supply chain.

**Tampering**
is identified as soon as the application changes in a suspicious way, such as when files are erroneously added, removed or modified, or if the application exhibits suspicious behavior that may be an indicator of tampering.

**Exposed secrets**
are reported with automatic prioritization of active SaaS login credentials and threat repository data helps to avoid overreporting secrets for enhanced remediation effectiveness.

**Application hardening**
ensures that proper safeguards exist within the compiled code and flags gaps such as missing vulnerability protections, insecure coding practices, outdated toolchains, inadequate prevention methods, and missing fortified functions.

**Version differentials**
verify which security issues have been patched or added with the latest release or update, along with highlighting any new issues introduced between software versions.

**Vulnerabilities**
actively exploited are reported to help organizations focus their remediation efforts based on the level of risk.

Spectra Assure is able to do this because of its AI-Driven Complex Binary Analysis, which:

- Assesses software without the need for the vendor's source code, enabling enterprise buyers to test commercial software on their own terms and and gain critical insights before deployment
- Recursively unpacks over 4800 file types down to individual DLLs, containers, and other post-build artifacts to correlate against a repository of over 3000 threat indicators
- Scans large and complex files rapidly, as fast as 1 GB in as little as 5 minutes, enabling enterprise risk organizations to match pace with business requirements
- Verifies all component integrity and provenance using comparisons against trusted binary repositories
- Leverages the world's largest Threat Repository with over 40+ billion searchable files

Spectra Assure indicates exactly which software components contain the identified risks. It also automatically generates a plan for addressing those risky components, recommending a series of manageable remediation projects. These reports can be securely shared externally with third-party vendors through a private, time-gated link to enable more effective collaboration with your vendor partners.

# Benefits Across the Enterprise Software Consumption Life Cycle

Spectra Assure addresses a variety of challenges that enterprises face at different stages of their software usage (i.e. acquisition, deployment, maintenance, monitoring).

| | Acquire | Deploy |
|---|---|---|
| **Challenge** | Enterprises struggle to gather relevant information to make risk-based software procurement decisions, because:<br>• Vendors are reluctant to share software composition and risk analysis reports<br>• Existing third-party software risk reporting lacks details about specific software solutions | Once a software package is procured, inadequate insight into risks means that the deployment team is unable to implement system and network hardening mechanisms to mitigate enterprise risk. |
| **Spectra Assure** | Provides a comprehensive risk report of any commercial software package at the binary level. It deconstructs and analyzes the entire software package against a series of dozens of robust security policies - all without requiring access to source code.<br><br>Consistently compares a vendor's risk posture by summarizing findings against customizable policies and aggregating results to determine security maturity within predefined Levels. | Enables informed deployment decisions based on issues flagged during analysis and coordination with SOC teams to spin up proper mitigating controls downstream.<br><br>Shareable reports from Spectra Assure enable collaboration between internal and vendor teams on environment hardening mechanisms prior to deployment. |

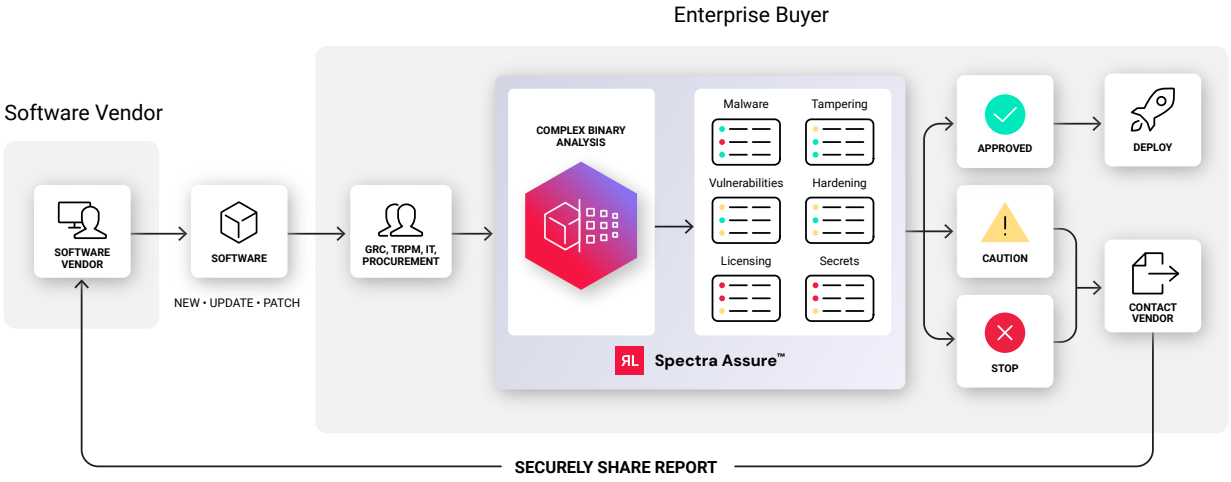



Figure 3: Assess for embedded threats within new vendor deployments, along with new versions and updates for existing deployments and share results back with the vendor for expedited remediation.

| | Maintain | Monitor |
|---|---|---|
| **Challenge** | Enterprise software updates are the primary vector of software supply chain attacks. Enterprises need automated threat analysis on all software updates – even from trusted vendors. | Traditional response plans for supply chain attacks and new zero-day threats involve active engagement with software vendors. However, vendors may be overwhelmed and unresponsive or combative during these times, which can significantly delay mitigation efforts. |
| **Spectra Assure** | Rapid scan times – even for large, complex packages – facilitates analysis regardless of release frequency.<br><br>Automatically summarizes critical changes in risk posture, proactively preventing deployment of compromised software updates. | Search capabilities (via SBOM UI or YARA rules) enable incident response teams to identify software with the newly reported vulnerable component.<br><br>Sharing findings with vendors focuses and facilitates communication during incidents. |

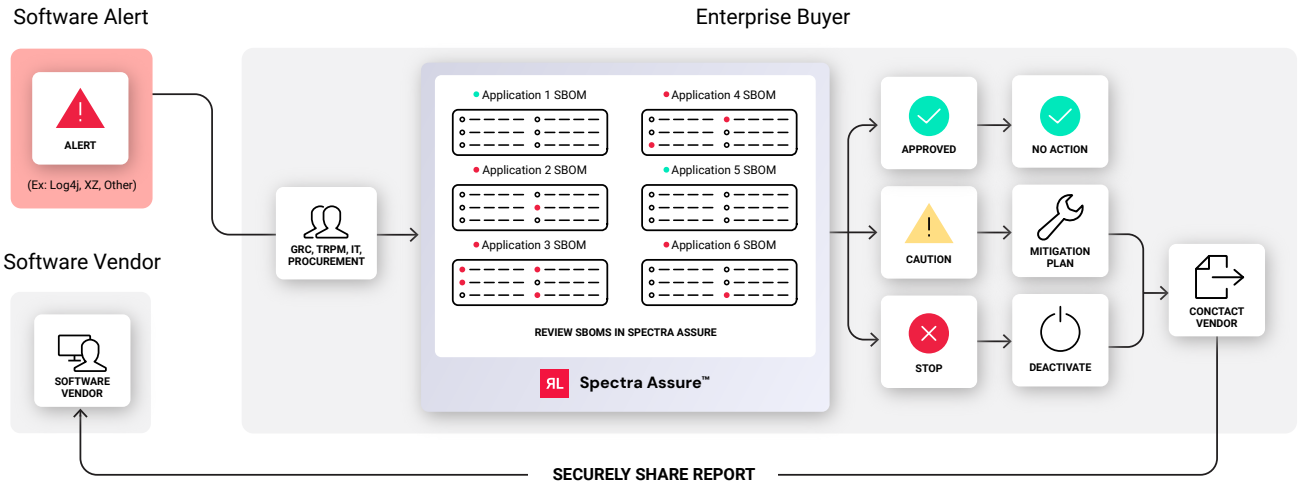



Figure 4: Ensure rapid response to new zero-day threats by refreshing results for deployed vendor software on-demand and querying the SBOM to quickly assess exposure.

# Summary

Right now, there is a perfect storm of software supply chain attacks specifically targeting software vendors, rising regulatory pressure, and clear deficiencies in existing third-party cyber risk assessment methods. These circumstances have expedited the need for a more scalable, cost-effective approach to ensuring commercial software is safe to deploy. Existing methods are providing businesses with only surface-level insights while omitting the very same threat categories that impacted SolarWinds, 3CX, and dozens of other organizations.

Spectra Assure delivers detailed transparency into commercial software risks and threats without requiring source code. It enables third-party cyber risk professionals to make informed decisions throughout the software consumption life cycle. Regardless of whether your business is onboarding a brand new software vendor or monitoring existing deployments, Spectra Assure provides the critical insights into software supply chain threats like malware, tampering, and suspicious behaviors to effectively assess and manage your commercial software risk.

# Learn More 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 40 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!

To learn more about ReversingLabs Software Supply Chain Security capabilities and solutions

REQUEST A FREE TRIAL

reversinglabs.com



REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com