



FROM MONTHS TO MINUTES:

# Securely Accelerating Third-Party Software Acquisition

Fast, Informed, & Secure

# The Escalating Software Supply Chain Security Challenge

Businesses face unprecedented challenges in securing their third-party commercial software. The inherent trust model and traditional approaches to third-party risk management (TPRM) have proven inadequate against sophisticated threats like those seen in the SolarWinds breach. Security questionnaires, penetration tests, and spreadsheet-based assessments cannot provide the depth of analysis required to identify embedded threats in increasingly complex software packages.

As third-party breaches continue to rise (100% increase in the last year, according to the [2025 Verizon DBIR](#)), businesses must implement solutions that provide comprehensive protection for the commercial software they use without creating operational bottlenecks.

Additionally, today organizations must address new guidelines such as Executive Order 14028 or the EU's Digital Operational Resilience Act (DORA) about the software they are using.

- Comprehensive software security verification
- Software Bill of Materials (SBOM) documentation
- Enhanced vendor risk assessment
- Proactive monitoring for emerging threats

Meeting these new requirements without impacting operational efficiency presents a significant challenge for cybersecurity and TPRM teams.

## Enhancing Operational Efficiency in Third-Party Software Risk Management

Spectra Assure™ delivers a comprehensive software supply chain security solution that significantly reduces resource requirements by automating in-depth risk assessments of third-party software. By leveraging its complex binary analysis capability across the software supply chain, cybersecurity and third-party risk managers can significantly reduce the time and person hours lost to manual assessments and reviews, while delivering risk analysis for a heightened security vigilance against emerging threats. In the same motion, this capability generates the most comprehensive SBOM, ML-BOM, SaaS-BOM, and CBOM to drive compliance and visibility with maximum efficiency.

**“ We get a lot of requests to install different applications. Spectra Assure lets us know if that software is safe or not, and simplifies that ‘yes’ or ‘no’ discussion with employees. ”**

**Security Operations Manager | Local Municipality**

# Complex Binary Analysis Without Source Code Access

Spectra Assure introduces a primary control for third-party software that goes beyond questionnaires and security scorecards, as well as addresses the limitations of traditional application security testing. Through AI-driven Complex Binary Analysis, Spectra Assure identifies material risks in software in minutes, without requiring source code access. This revolutionary approach enables agencies to:

- Detect malware, tampering, and malicious code before software is deployed
- Identify embedded vulnerabilities, particularly those actively exploited by threat actors
- Discover exposed secrets and sensitive information that could be exploited
- Validate digital signatures to verify software integrity
- Generate comprehensive SBOMs in compliance with federal standards

## Key Benefits

### Before Purchase

Spectra Assure enables rapid pre-purchase assessment of third-party software, allowing agencies to:

- Quickly identify security and compliance risks before procurement commitments
- Share actionable reports with vendors, cybersecurity teams, and procurement officers
- Make informed purchasing decisions with clear pass/fail reporting
- Eliminate lengthy procurement cycles by streamlining security assessments

### Before Deployment

Critical security issues are identified before software enters the production environment:

- Comprehensive risk analysis identifies threats that other security tools miss
- Security teams receive actionable intelligence for immediate remediation
- Secure SAFE report sharing facilitates collaboration with vendors on critical fixes
- Pre-established security benchmarks (SAFE Levels) streamline approval processes

### Continuous Monitoring

Ongoing risk management becomes significantly more efficient:

- Automated threat analysis on software updates proactively identifies new risks
- Version differential analysis flags new threats introduced with patches and updates
- Rapid response capabilities address newly reported supply chain vulnerabilities
- Continuous monitoring reduces resource requirements for security teams

## Use Case 1

# Employee Requests for Software/Freeware

**700%**  
INCREASE IN EFFICIENCY

### Challenge:

A growing number of individual software and potentially freeware requests come from employees to businesses every day. As new software is requested, it is important to thoroughly assess the package for malware, tampering, vulnerabilities, or other potential risks. With current approaches, time is lost in discussions with the requester or running insufficient analysis solutions. Correctly surfacing these threats manually is time-consuming and can miss sophisticated attack techniques.

### Impact:

For a recent government customer, Spectra Assure reduced the process from request to decision from eight hours to one hour - a 700% increase in efficiency. For each requested piece of software, Spectra Assure provides a comprehensive risk assessment in minutes. IT personnel were able to share the SAFE report to offer a clear "go/no go" to share the risk report with the requestor.

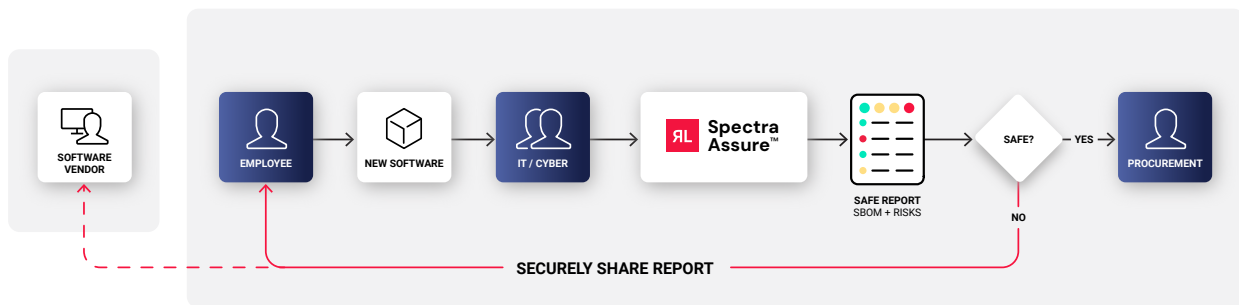


Figure 1: Employee requests are quickly analyzed and SAFE report is shared.

Read the case study: [Local Municipality: Streamlining the Third-Party Software Approval Process with Spectra Assure.](#)

## Not All SBOMs Are Created Equal

An often time-consuming aspect of TPRM is the struggle to get an SBOM, let alone any assurance that it is truly complete. With Spectra Assure, organizations are empowered to generate SBOMs independently, without having to rely on their vendors. Not only does this provide the most comprehensive SBOM, but it eliminates any time that would be spent procuring these from vendors.

This capability extends to emerging xBOM capabilities such as CBOM, SaaS BOM, and ML-BOM, which streamline the ability to prepare for quantum computing threats, understand SaaS dependencies, and gain AI supply chain visibility. Ultimately, the ability to get fast, independent, and consistent SBOMs and xBOMs helps drive the overall efficiency of the software acquisition process.

## Use Case 2

# Automating Third-Party Cyber Risk Management

**1200%**  
INCREASE IN EFFICIENCY

### Challenge:

The acquisition process for core software used across an organization can be a long and tedious process, taking months. These processes are mostly manual, requiring the acquisition of security scorecards or questionnaires, software bill of materials (SBOMs), and potentially, in some cases, pentesting before navigating the process of obtaining the necessary approvals. Besides being time consuming, none of these items provide a verified assessment of the risk or threats within business-critical commercial software. Additionally, to maintain compliance with various regulations, much of this software is deployed as virtual machines that are too large to scan effectively with traditional tools.

### Impact:

A global finance organization recently turned to Spectra Assure to help automate their historically twelve-week process for software procurement, review, and approvals to reduce it to just one week - a 1200% increase in efficiency. Spectra Assure provides a complete SBOM and full risk assessment of commercial software in minutes, rapidly deconstructing large, complex software packages and virtual machines before purchase or deployment - all without requiring the source code. Via API, software is automatically uploaded to Spectra Assure, and the SAFE report is automatically routed to the reviewing Third-Party Cyber Risk Management (TPCRM) team, as well as Procurement and SOC. Procurement processes the contract or engages the vendor if issues are identified. The Spectra Assure SAFE Report is also archived for compliance and future access.

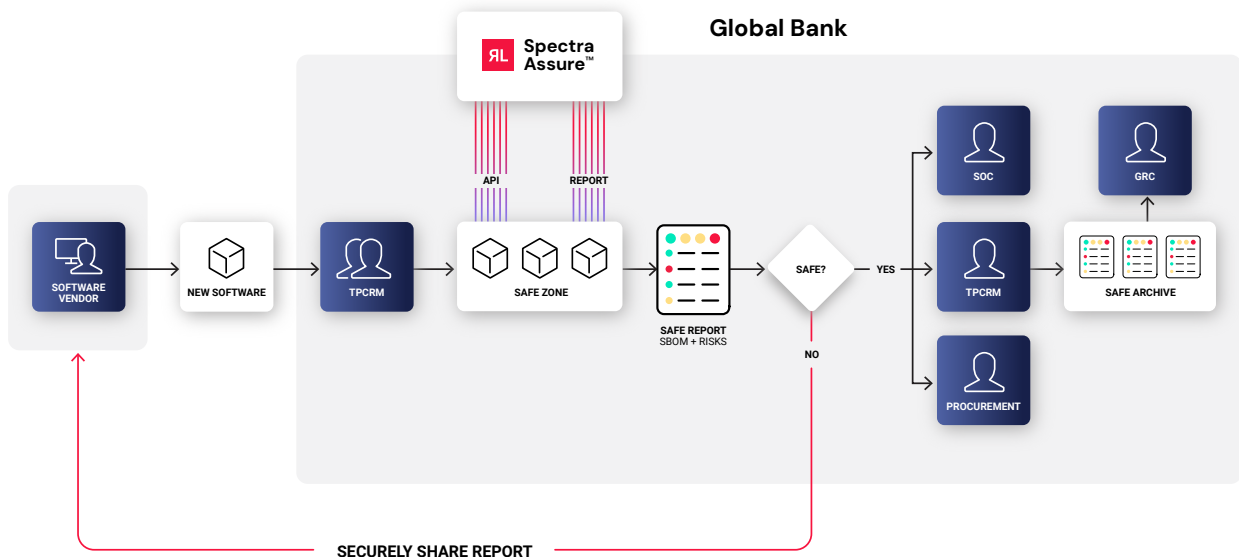


Figure 2: A Large global organization streamlines its third-party commercial software acquisition process.

Read the case study: [Accelerating Software Acquisition and Reducing Risk with Spectra Assure](#).



## Use Case 3

# Securing Virtual Machines

**1500%**  
INCREASE IN EFFICIENCY

### Challenge:

A large global manufacturing organization faced the growing challenge of managing software risk, particularly with virtual machines (VMs) entering the environment from various business units worldwide. Motivated by the need for better security and due diligence, the team sought to ensure that no risks were embedded in incoming software. However, their existing process was time consuming and inefficient: they manually recreated isolated network environments, deployed test tools, and then installed each VM for analysis. These requests spanned a wide range of software types—from mouse drivers to manufacturing tools, container images, and ISOs—often with no context about their purpose or origin. While they used VMRay and standard virus scans, the effort required for each analysis consumed up to eight hours, would not scale, and did not provide the level of insights and analysis desired.

### Impact:

With Spectra Assure, the organization drastically streamlined its workflow. They were able to scan VMs in minutes, automatically identifying all components and generating a full risk report detailing any malware, tampering, or vulnerabilities. The SAFE report provided deeper, more actionable insights than traditional sandboxing or virus scans. Additionally, the report enabled them to quickly identify issues, as well as conduct deeper analysis, if desired. The end-to-end analysis process was reduced from eight hours to approximately 30 minutes—a 1500% increase in efficiency. As one team member put it, “Having a solution where you can just upload the VM and it provides the analysis in minutes is huge.”

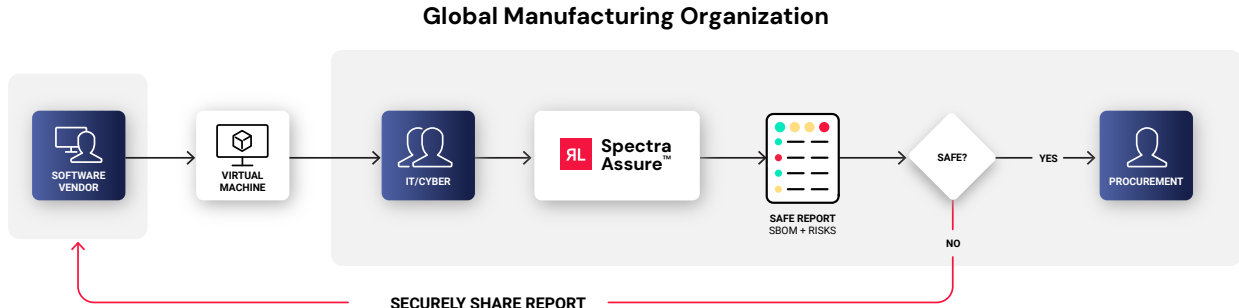


Figure 3: Manufacturer accelerates VM risk analysis, eliminating hours of work previously.



Spectra Assure dramatically reduces the cost and time of assessing the risk of a VM because it does not require any deployment of the VM, runtime access, and agent installation.

“ Having a solution where you can just upload the VM and then get the risk analysis in minutes is huge. ”

Security Engineer | Global Manufacturer

# Conclusion

Spectra Assure delivers the operational efficiency organizations require while ensuring compliance with US cybersecurity guidelines, the EU's DORA, or CRA or similar directives. By automating complex binary analysis, streamlining compliance documentation, and enabling secure collaboration across teams and with software vendors, Spectra Assure transforms third-party software risk from a resource-intensive burden into an efficient, proactive security function.

The result is not merely improved security posture, but significant operational efficiencies that align with and empower existing security, risk, and procurement teams.

## Get Started!

Experience the ReversingLabs Difference

REQUEST A DEMO

[www.reversinglabs.com](http://www.reversinglabs.com)

## 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.