SOLUTION BRIEF

REVERSINGLABS

Securely Accelerating Third-Party Software Acquisition

Meeting the Mission of Improved Efficiency and Protection

The Escalating Federal Software Supply Chain Security Challenge

Government agencies face unprecedented challenges in securing their software supply chains. 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.

With the issuance of Executive Order 14028 in May 2021, federal agencies are now mandated to enhance cybersecurity through initiatives specifically targeting software supply chain security. Compliance requirements include:

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

Meeting these mandates without impacting operational efficiency presents a significant challenge for federal 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, federal agencies 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, SaaSBOM, 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 addresses the limitations of traditional application security testing. Through AI-driven Complex Binary Analysis, Spectra Assure identifies material risks in software 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 members of federal and local governments. 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.

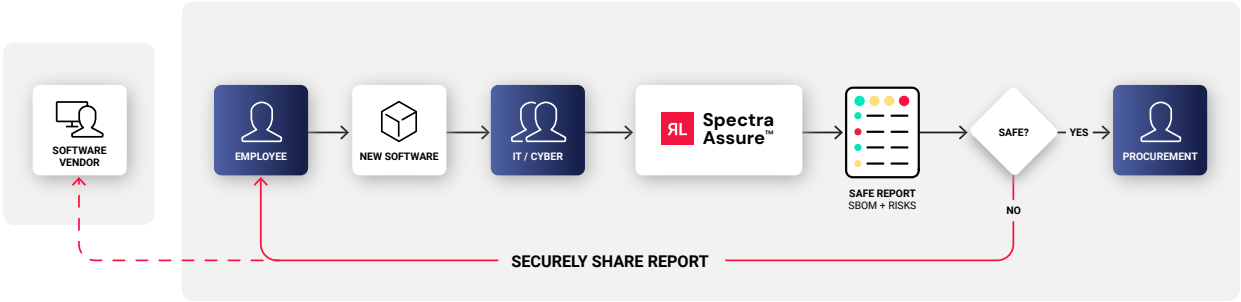

Figure 1: Employee requests quickly analyzed and SAFE report shared.

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, government agencies 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, SaaSBOM, 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

1100%
INCREASE IN EFFICIENCY

Challenge:
The acquisition process for core software used across government agencies 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 pentesting, in some cases, 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 mission-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 large global 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 provided the ability to provide 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.

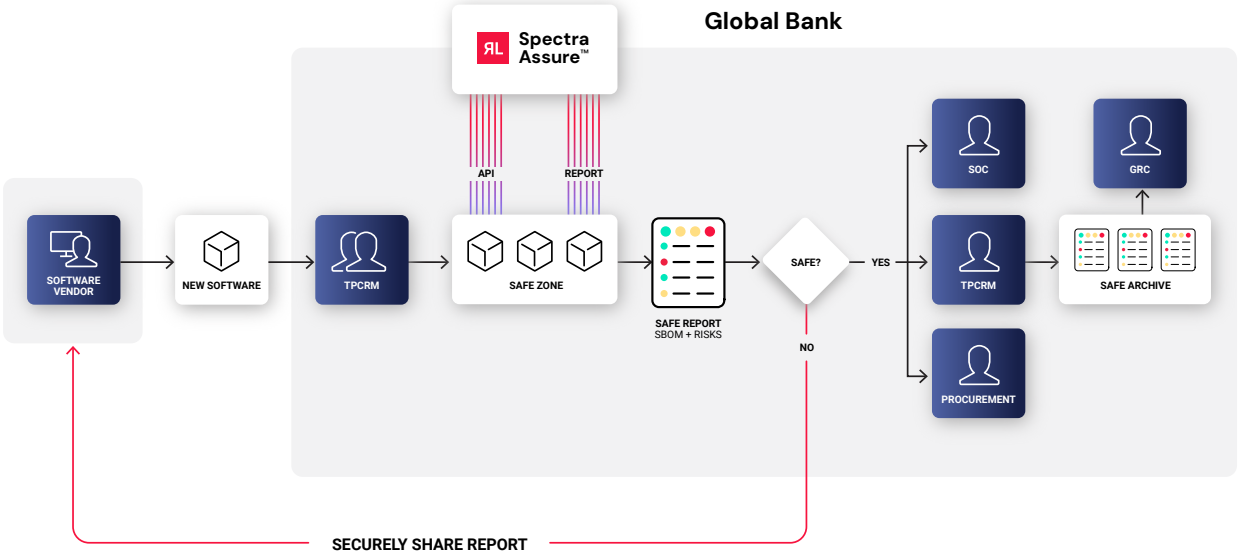

Figure 2: Large global organization streamlines its third-party commercial software acquisition process.

Read the case study: Accelerating Software Acquisition and Reducing Risk with Spectra Assure.

Conclusion

As software supply chain attacks continue to rise (100% increase in the last year, according to the 2025 Verizon DBIR), government agencies must implement solutions that provide comprehensive protection without creating operational bottlenecks.

Spectra Assure delivers the operational efficiency government agencies require while ensuring compliance with Executive Order 14028 and related 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 allow federal agencies to meet expanding cybersecurity mandates without proportional increases in resources or personnel.

Get Started!

Experience the ReversingLabs Difference

REQUEST A DEMO

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.

SB-Rev-05.16.25

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com