REVERSINGLABS

The CISO Survival Guide:

Operationalizing Third-Party Software Risk Management

Modern Enterprises Run on Third-Party Software

Your business runs on commercial software. Payroll, HR, IT, and most other business-critical applications were provided by a vendor. Today's businesses rely on a dense ecosystem of dozens, if not hundreds, of different technology providers to deliver business-critical products and services. Yet, despite these facts, enterprises lack a primary control to determine whether these third-party applications pose a material risk to their business.

The drastic rise in supply chain attacks targeting software suppliers, combined with increased government and regulatory oversight have spurred Third-Party Cyber Risk Managers and IT Security professionals to pay special attention to software vendors and the layers of risk that commercial software poses to their business.

1300%

Increase in software supply chain threats from 2021 to 2023

RL State of SSCS Report, 2024

200%

Predicted increase in costs stemming from software supply chain attacks by 2031

Gartner®: Leader's Guide to Software Supply Chain Security

83%

Cyber risk professionals find risks embedded within vendor applications after deployment

Gartner® Third Party Risk Management (TPRM)

68%

Increase in software supply chain attacks targeting third-party software vendors

Verizon DBIR, 2024

Existing TPRM Methods Leave Gaps

SBOMs

A software bill of materials (SBOM) is simply an ingredient list cataloging software components but failing to account for embedded threats like malware, tampering, and suspicious behaviors.

Vendor Questionnaires

Vendor questionnaires are slow and expensive to execute. They also hinge on vendors providing truthful and accurate answers attesting to the security of the software they provide to customers.

Penetration Testing

Pentesting is largely a compliance driver and is extremely costly to scale. Results can also be inconsistent with each re-test as new testers are assigned based on availability.

Anti-Virus & Sandboxes

Anti-virus (AV) and sandboxing tools are not equipped to detect malware in large and complex commercial software packages and are easily evaded by certain malware varieties.

Security Rating Services

Security rating services provide a glimpse into a vendor's risk exposure via passive scans of public-facing infrastructure. However, the data collected is irrelevant to the software package itself.

The Inherent Trust Model Is Not Viable

Enterprises lack a primary control to identify software supply chain threats in the third-party commercial software that is deployed across their environment. In order to make informed buying and deployment decisions for enterprise software, third-party cybersecurity and risk professionals need an independent assessment of the software they procure to run their business.

SEC Cybersecurity Disclosure (Form 8-K)

The SEC's newly unveiled Rules of Disclosure (Form 8-K) mandates that enterprises must disclose cybersecurity incidents that pose material risk to customers. It not only covers disclosure of an issue, but requires registrants to describe their processes, if any, for assessing, identifying, and managing material risks.

Challenges Across the Software Acquisition Lifecycle

Existing TPRM tools and methods create challenges for cyber risk and security professionals when attempting to mitigate risk across each stage of the software consumption lifecycle. These stages include acquiring, deploying, maintaining, and monitoring third-party commercial software.

Acquisition

Challenge

Enterprises struggle to gather relevant information to make risk-based software procurement decisions. Vendors are reluctant to share software composition and risk analysis reports, while existing third-party software risk reporting fails to provide details into the software package itself.

Deployment

Challenge

Once a software package is procured, inadequate insight into risks means that the deployment team is unable to implement system and network hardening mechanisms or compensating controls.

Maintenance

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.

Monitoring

Challenge

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.

Third-Party Software Risk Stakeholders

GRC, TPRM

ROLE:
Identifies cyber, regulatory, and operational risks presented to the organization by its third parties, including vendors, suppliers, contractors, customers, or regulators.

CHALLENGES:
Not enough resources to properly assess all vendors equally;
Questionnaires, SBOMs, and security rating services are ineffectual;
Held responsible for vendor security policies without proper cybersecurity training.

Security Operations (SecOps)

ROLE:
Monitors, logs, and contains security events across multiple IT layers while prioritizing incidents for business owners.

CHALLENGES:
Lack of security telemetry from hundreds of applications deployed across the enterprise; Overwhelmed by volume of events within queue; Lack of event prioritization and remediation guidance.

Application Security (AppSec)

ROLE:
Responsible for identifying application-level risks and threats while ensuring that security checks do not impede business velocity.

CHALLENGES:
Accelerating the secure management and release of software updates;
Releasing secure code to production quickly without sacrificing quality.

IT Operations

ROLE:
Assist users in business units to leverage technology securely without downtime.

CHALLENGES:
Business need trumps risk when making application deployment decisions;
A software supply chain attack would result in significant downtime.

Procurement

ROLE:
Responsible for defining, communicating, and managing vendor research and qualification, and ensuring the risk analysis results are considered throughout the selection and onboarding processes.

CHALLENGES:
Not enough data on third-party software risks to make educated decision on approving or rejecting vendors.

Threat Intelligence

ROLE:
Proactively search for cyber threats and indicators of compromise (IOC) and take remedial action in case of a breach.

CHALLENGES:
Without access to source code, lack of intelligence on third-party applications affects mean-time-to-response (MTTR); Balancing manual threat research processes with pressure to be fast and accurate.

Division of Responsibilities for Securing Third-Party Software

Although the responsibility for evaluating supply chain security risk of any prospective or new vendor may reside with the TPRM team, the ongoing management and remediation of security issues presented by software consumed will undoubtedly fall across a variety of business functions.

As a result, it is critically important that organizations clearly define the roles and responsibilities within the organization to identify, detect, respond, and recover from software supply chain security issues that may arise throughout the lifecycle of software use. This includes the acquisition, deployment, maintenance, and ongoing monitoring of software.

This graphic presents a high-level example RACI demonstrating a potential distribution of responsibilities across job functions for managing software supply chain risk:

Software Use Lifecycle Stages				
	Acquire	**Deploy**	**Maintain**	**Monitor**
Procurement	**A**			
TPRM	**R**	**C**	**C**	**I**
AppSec	**C**	**A**	**I**	
IT Operations		**R**	**A / R**	**I**
Threat Intel				**R**
SOC				**A**

Legend:

R = Responsible

A = Accountable

C = Consulted

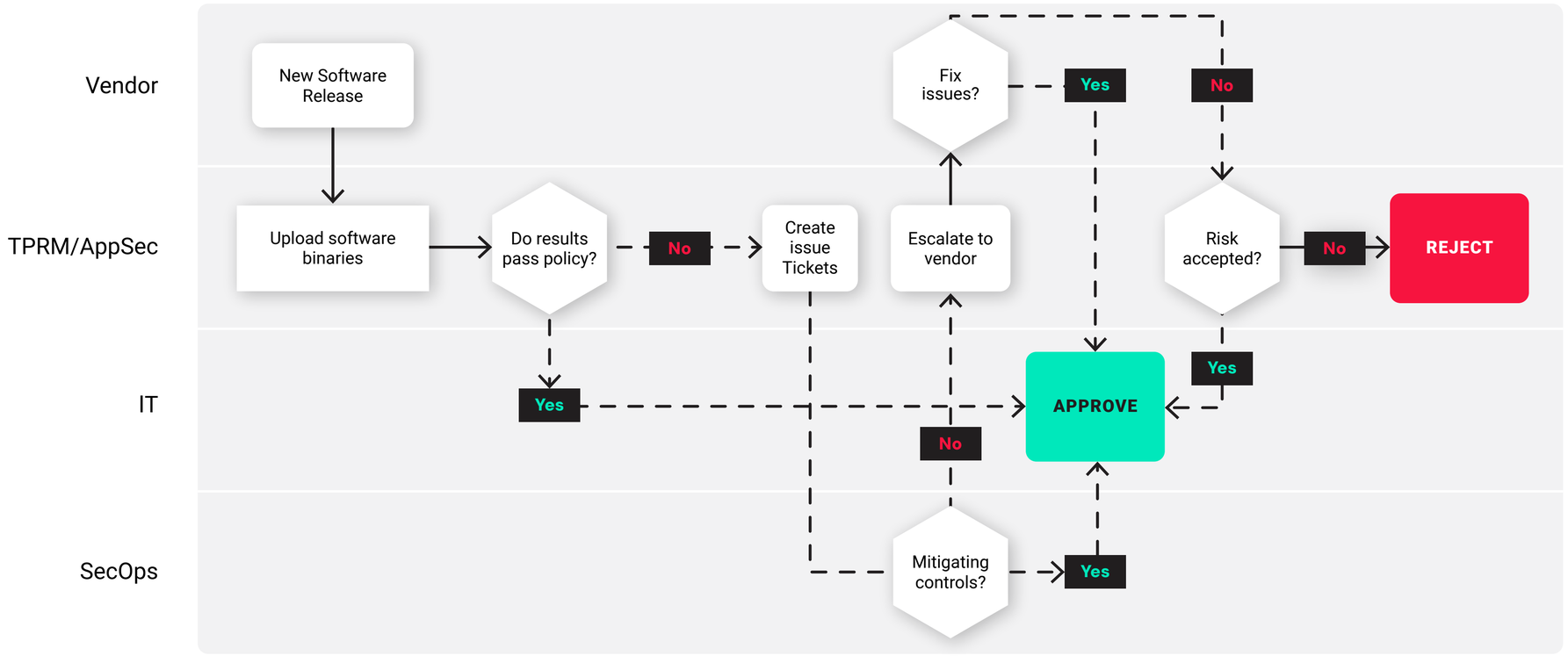
I = Informed

Deployment Decision Tree Example

Secure Software Procurement and Deployment

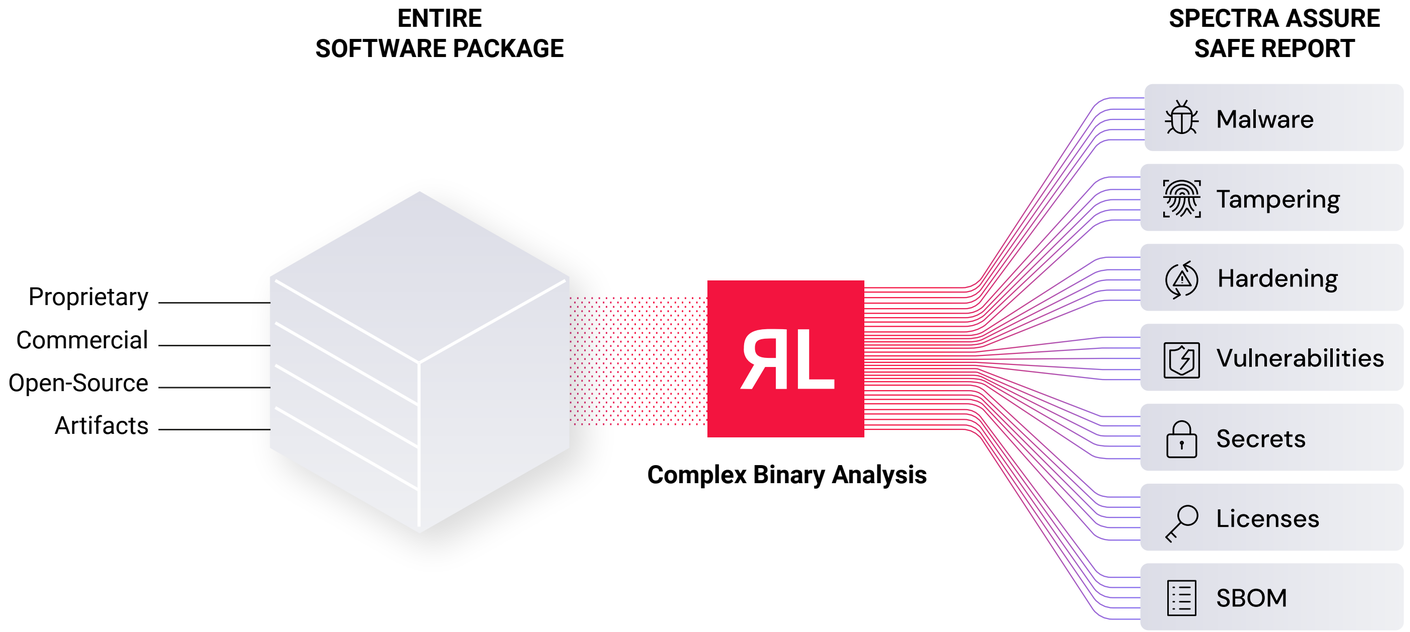
Here is an example of a repeatable approval and deployment workflow to assess and manage third-party software risk.

This process can be applied to new software deployments, or whenever a vendor issues a new version, patch, or update for an existing application deployed in production.



Make Risk-Informed Software Buying Decisions

Spectra Assure™ prevents software supply chain incidents by serving as the primary control to ensure third-party risk and cybersecurity professionals that the software they purchase is free of costly threats.



The analysis is synthesized into the Spectra Assure SAFE Report - the most comprehensive SBOM and software risk analysis that identifies embedded threats like malware, tampering, vulnerabilities, suspicious behaviors, and more.

Spectra Assure's AI-Driven Complex Binary Analysis delivers deep analysis of third-party software without the need for source code, providing a primary control to assess third-party software risk.

"The ideal case is that you're running ReversingLabs on everything prior to purchase. I not only get the SBOM, I also get insights into malicious code or tampering."

Tim Brown, CISO

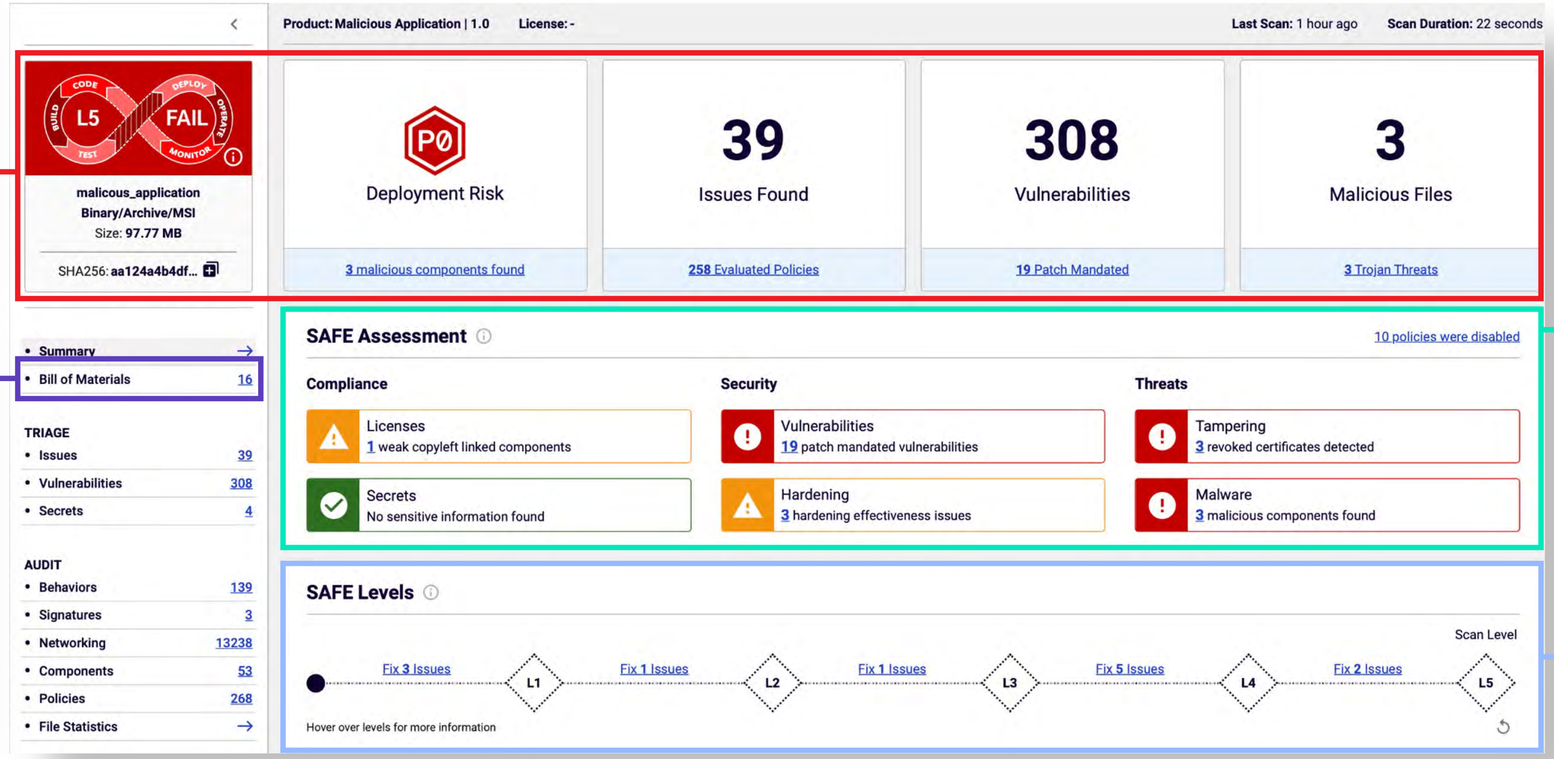
SOLARWINDS

The Spectra Assure SAFE Report

The SAFE report combines an SBOM with digestible and actionable security insights into the risks and threats of third-party software packages. Each section serves specific purposes to identify threats, prioritize fixes, and gauge an acceptable level of risk to your cybersecurity and third-party risk management teams.

The **SAFE Summary** panel provides a snapshot of relevant security data points from which your team can take immediate action.

SBOMs within the SAFE report can be exported in CycloneDX and SPDX formats and meet NTIA standards by including the version and publisher of each component, along with critical risk information including embedded malware, vulnerabilities, and other threats.



The **SAFE Assessment** provides a summary of all findings flagged in the most recent analysis and buckets them across six risk categories based on shared characteristics.

The **SAFE Levels** makes it simple to gauge the risk that a specific software package presents to your business through a series of predefined, increasingly strict security policies.

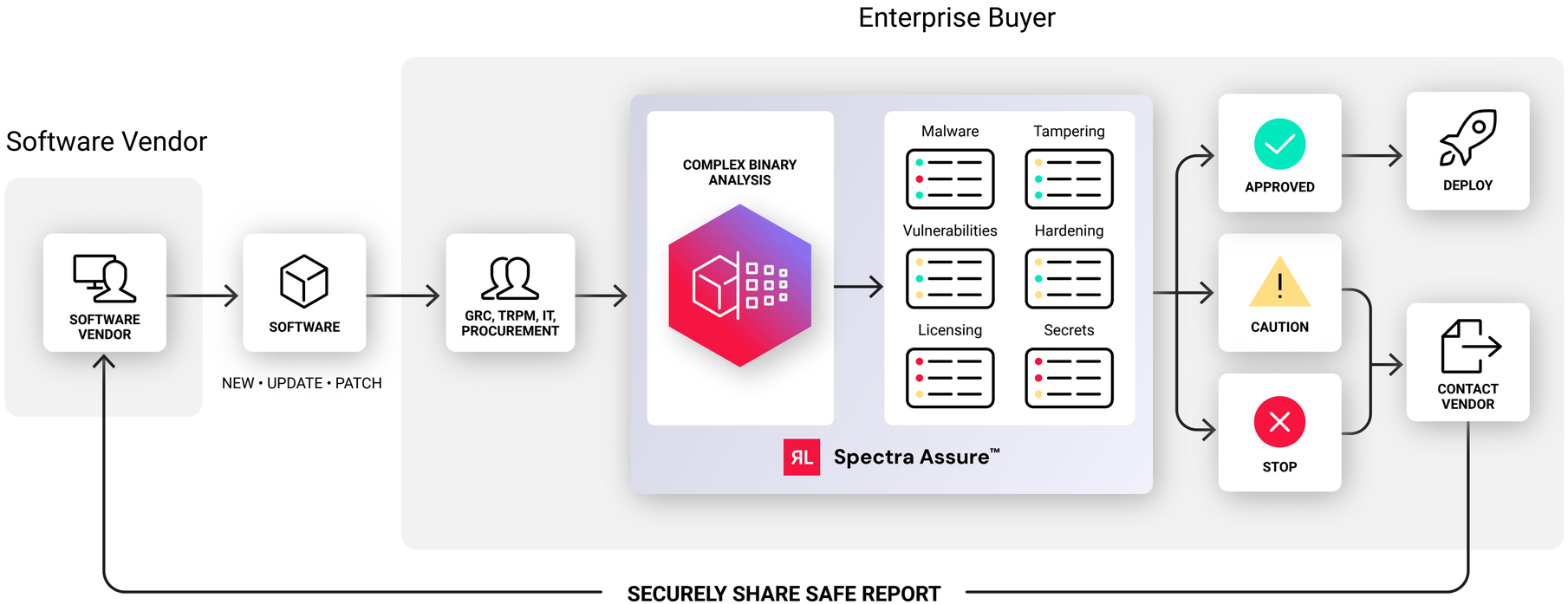
Applying Spectra Assure Across the Acquisition Lifecycle

Spectra Assure addresses a variety of challenges that enterprises face at different stages of their software usage lifecycle including the acquisition, deployment, maintenance, and monitoring of third-party commercial software.

	Acquisition	Deployment	Maintenance	Monitoring
Challenge	Enterprises struggle to gather relevant information to make risk-based software procurement decisions. Vendors are reluctant to share software composition and risk analysis reports, while existing third-party software risk reporting fails to provide details of the software package itself.	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.	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. .
How Spectra Assure Helps	Deconstruct and analyze third-party software packages for threats without requiring source code providing: • Streamlined selection process when assessing multiple vendors • Maintained business velocity with a simplified Go/No-Go selection criteria	The SAFE report identifies and prioritizes the most critical security issues which provides risk and security teams and cybersecurity teams a digestible means to: • Communicate with IT Ops and SOC teams to implement the proper controls for known attack vectors • Collaborate with vendors on required security fixes via shareable SAFE reports	Rapidly deconstruct and analyze large and complex packages to: • Quickly analyze software packages with frequent updates and patches • Proactively stay ahead of changes to software risk posture stemming from compromised software updates	Search capabilities via SBOM UI or YARA rules enable incident response teams to: • Identify software that may be impacted by a newly reported vulnerable component Sharing SAFE reports with vendors focuses and facilitates communication during incidents.

Sample Operational Workflow

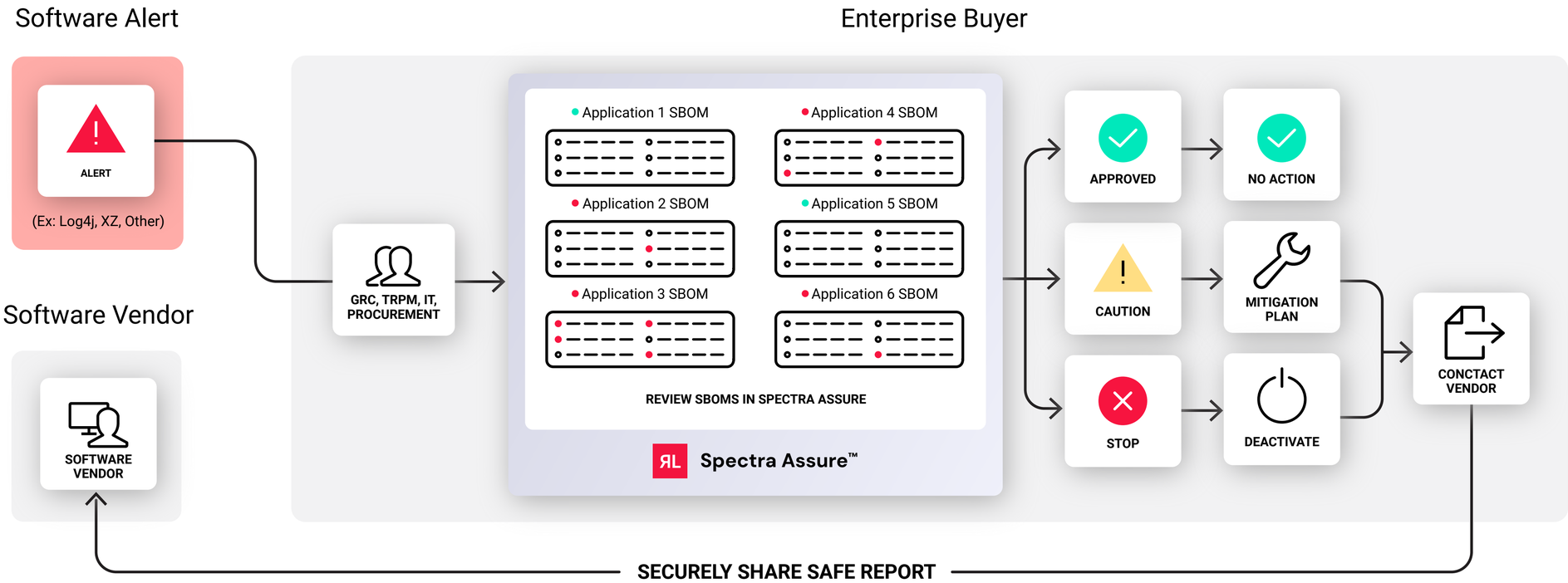
Acquiring, Deploying, and Maintaining Software



Spectra Assure can be implemented to assess for embedded threats within new vendor deployments, along with new versions and updates for existing deployments. The SAFE report can then be shared back with the vendor for expedited remediation.

Sample Operational Workflow

Zero-Day Monitoring and Response



With Spectra Assure, third-party risk and cybersecurity teams can 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.

How to Get Started

Foundational Steps to Ensure Success

Getting started with Spectra Assure does not require any advanced tuning or configuration. Its AI-driven Complex Binary Analysis does not require access to source code. Third-party risk and cybersecurity professionals can simply upload the software binary to Spectra Assure to automatically deconstruct and analyze the security posture of their third-party applications.

Step 1

Start by selecting your most important applications to get a baseline of potential security risks.

Step 2

Once known risks are identified, establish compensating controls and environmental hardening by coordinating with the SOC and IT Operations.

Step 3

TPRM and Procurement should consult with AppSec and other cyber security SMEs to establish security requirements as a key component of new vendor selections.

Step 4

Consult with Procurement and Legal to integrate security requirements, performance measures, and service-level agreements (SLAs) into contract language to ensure that security fixes are a required stipulation for vendor agreements.

Step 5

Once proper protections are implemented for the most critical applications, legacy applications can be introduced into testing pool.

Selecting Your Most Critical Applications

It is recommended that organizations first target the analysis of software that is most critical to the business and expand this to the larger population over time using a risk-based approach. This will enable organizations to quickly uplift the security posture of business-critical software which would have the most financial and operational impact if breached via a supply chain attack.

When determining how to segment your software estate based on risk, an organization can consider a variety of risk elements, including but not limited to the following:

- **Criticality of software vendor to business operations** (e.g. RTO if software/service becomes unavailable)
- **Breadth of deployment of software** (e.g. proportion of systems across IT landscape that use that software)
- **Location that software is deployed or integrated** (e.g. deployed at a network boundary or within a restricted network segment)
- **Connectivity and privilege required for installation** (e.g. local admin and connected to “crown-jewel” systems)
- **Level of current and historical investment and maintenance for software** (i.e. has software reached end-of-life?)

Priority Software Categories for Security Testing

Finance & ERP	Financial, operational, and customer data systems
Email	Internal or external email services
Data Warehouses	Critical data repository systems
Communications	Communication services, video conferencing, or messaging tools
Development Solutions	Development tools such as code repositories or build servers
Security Controls	Security solutions such as endpoint protection or other
Secure File Transfer	Critical secure file transfer systems

Learn More

Third-Party Software Risk Management (TPSRM) is an iterative process. With the right people, processes, and technology, businesses can have assurance that the software they rely on from trusted vendor partners is safe to use. For more insights on how to scale your TPSRM program, check out the latest content from ReversingLabs.

Website

Go Beyond the SBOM

Visit our solutions page to learn how the SBOM is not enough to manage third-party software risk.

White Paper

Assess and Manage Third-Party Software Risk

Download our white paper to read how Spectra Assure removes the black box surrounding commercial software risk.

Webinar

Don’t Stop at the SBOM

Learn how to take your software supply chain security to the next level whether you’re a software producer or buyer.

Blog

Why SAFE. Why Now.

RL Chief Trust Officer Saša Zdlelar discusses why the industry is ready for a more comprehensive software security assessment.

Get Started!

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

REQUEST A FREE TRIAL

reversinglabs.com

About ReversingLabs

ReversingLabs is the trusted authority in software and file security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Titanium Platform® powers the software supply chain and file security insights, tracking over 40 billion files daily. 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.

ReversingLabs Software Supply Chain Security, powered by AI-driven complex binary analysis, is able to identify compliance issues, exposures, and threats like malware, tampering, vulnerabilities, mitigations, exposed secrets, and license issues – all without the need for source code. Providing the "final build exam," ReversingLabs provides a comprehensive risk analysis that lets organizations identify, assess, and resolve critical issues, delivering the trust and assurance needed before you ship, deploy, or update your software.

GD-Rev-10.24.24

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com