Going Beyond the SBOM

Thank you for downloading this ReversingLabs whitepaper. Carahsoft is the distributor for ReversingLabs Cybersecurity solutions available via TX DIR and other contract vehicles.

To learn how to take the next step toward acquiring ReversingLabs solutions, please check out the following resources and information:

For additional resources:
carah.io/ReversingLabsResources

For upcoming events:
carah.io/ReversingLabsEvents

For additional ReversingLabs solutions:
carah.io/ReversingLabsSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
ReversingLabs@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/ReversingLabsContracts

WHITE PAPER

REVERSINGLABS

Going Beyond the SBOM

Bring Control to Third-Party Software Security Risk with Spectra Assure SAFE

Modern Enterprises Run on Third-Party Software

You often hear that the world runs in open source. But your enterprise doesn't. It runs on commercial software. Does your organization run on an open-source payroll system? Open-source web conferencing tool? Open-source ERP or HR system? Most 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. This vast array of vendors include independent software vendors (ISVs), business process outsourcers, OEMs, professional service providers, and more. However, in recent years, Third-Party Cyber Risk Managers and IT Security professionals are paying special attention to software vendors and the layers of risk that commercial software poses to their business.

The growing concern in third-party commercial software is attributed to its proliferation in powering critical business functions, coupled with increasing frequency and complexity of software supply chain attacks that can affect any organization with that software deployed. A recent study by the European Supervisory Authorities found that software vendors make up more than a third of the entire ICT (Information, Communication, Technology) service landscape, with 40% of those vendors supporting critical business functions.[1] 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 emerging threat.

Source: Gartner, Chris Audet, Stay Ahead of Third Party Risk, 2019
https://www.gartner.com/en/legal-compliance/insights/third-party-risk-management

Legacy Methods Have Failed to Close Third-Party Software Visibility Gaps

To date, third-party risk professionals rely on a suite of highly manual, often cumbersome solutions to evaluate vendor software risk. While these solutions may provide some insight into a vendor's security hygiene, they simply are not built to scale with the size and complexity of modern commercial software. As a result, their output is often superficial or outright omits entire categories of software supply chain threats.

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.

Anti-Virus/Malware
Despite what their name might suggest, anti-virus (AV) or anti-malware tools are extremely limited in detecting malware hidden in commercial software packages. Most AV tools were designed to detect large volumes of much smaller files deployed to endpoints or runtime environments and, thus, fail to handle large and complex enterprise software packages.

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.

The SBOM Presents Progress, But It's Not Enough

Over the last few years, several high-profile commercial software vendors have demonstrated the incredible impact of unsecured software supply chains. From the SolarWinds Orion breach in 2020, the CodeCov breach in 2021, and courtroom recording software, JAVS in 2024, trusting commercial software vendors solely on their reputation is no longer enough in today's threat landscape. Further still, legislative and regulatory oversight hold organizations responsible for ensuring that even commercial applications not built in-house require the same level of security scrutiny as proprietary software.

Because of this, the practice of generating a software bill of materials (SBOM) to bring transparency to the software procurement process has resurged within many CISO circles. The concept behind SBOMs is to present an "ingredient list" of any commercial software package, listing each individual components and dependencies that makes up the package so that TPRM, AppSec, and Procurement teams can perform deeper investigations into potentially vulnerable components.

Recently, government intervention has expedited SBOM adoption within the public sector with landmark legislation like Executive Order 14028, CISA's Guidance on SBOM Consumption, and the FDA's Cybersecurity in Medical Devices requirement. The private industry is also rapidly adopting language into vendor contracts that require SBOMs. Gartner reported that 60% of organizations procuring mission-critical software solutions will mandate software bill of materials (SBOM) disclosures in their license and support agreements[2].

While an SBOM is a foundational first step towards building security transparency between enterprise software producers and buyers, it is merely a list of ingredients, providing little context to how internal software components pose imminent risk to the business. Many organizations lack the tools to efficiently parse through SBOM data to unearth any meaningful risk insights. Furthermore, security vendors that generate SBOMs, specifically AST and SCA vendors, are simply not designed to provide insight into the entire software package, delivering details into open-source dependencies while ignoring proprietary, and commercial components.

A list of software ingredients on its own is not enough to flag the most sophisticated embedded threat categories lurking inside commercial software. From embedded threats like malware, tampering, and exposed secrets, SBOMs on their own do little to showcase and map the modern software threats to individual components at the file level. More importantly, traditional SBOMs fail to provide cyber risk professionals with a clear roadmap supporting collaboration with software providers to address these issues.

"Formal testing and evaluation of commercial software for potential vulnerabilities or malicious code are rarely performed by customers — even for systems supporting high-value or sensitive processes. The lack of formal testing creates a path for lateral movement, and facilitates the introduction of malicious code that steals data and intellectual property," according to the Gartner® report Mitigate Enterprise Software Supply Chain Security Risks.

Third-Party Cyber Risk Managers Need to Go Beyond the SBOM

For cybersecurity professionals overseeing third-party software risk, a new standard for commercial software risk evaluation is critical - one that goes beyond a mere list of ingredients to bring meaningful and actionable security insights. Deconstructing vendor software to its fundamental components and showcasing how those components map to the most sophisticated software supply chain threats in a digestible format is the only way to scale and fully assess vendor software risk, supporting risk mitigation collaboration with software providers.

The Spectra Assure SAFE Report: Raising the Bar for Software Risk Assessments

The Spectra Assure™ SAFE (Software Assurance Foundational Evaluation) report introduces a greater visibility into commercial software risks and threats, enabling transparency and collaboration between enterprise software buyers and their vendor partners. The Spectra Assure SAFE report exceeds a typical SBOM by providing not only software bill of materials, but detailed and contextual threat insights into the most sophisticated software supply chain threat vectors like malware, tampering, suspicious behaviors, and more. This critical level of detail takes the burden of manual risk assessments off the shoulders of cybersecurity teams and enables more informed risk decisions before purchasing, deploying, or updating commercial software packages.

How SAFE Delivers Value for Cyber Risk Professionals

The SAFE report brings visibility to hidden software supply chain threats, including attack vectors beyond just vulnerabilities, to effectively manage software supply chain risk. Additionally, due to increased regulatory scrutiny from oversight bodies like the SEC, FDA, NIST, and EU, SAFE aims to showcase due diligence on software purchased from vendors.

The SAFE report goes beyond just a simple list of ingredients like an SBOM and, instead, provides a comprehensive software security risk assessment. The SAFE report is generated using Spectra Assure's AI-driven complex binary analysis to recursively deconstruct even the largest and most complex software packages to flag embedded threats like malware, tampering, exposed secrets, malicious behaviors, and more. This data is then synthesized into an easily digestible, actionable, and shareable report that helps to benchmark your software's security maturity, expedite vendor onboarding, and demonstrate compliance.

The SAFE report is meant to demonstrate what secure, trusted software should be. Its contents far exceed regulatory expectations and demonstrates a level of analysis well beyond the scope of traditional third-party security testing tools and methods.

SAFE vs SBOM

The SAFE report goes beyond the SBOM in a multitude of ways. While many application security tools can generate an SBOM, those templates are still a mere list of ingredients at their core. AST and SCA vendors who generate SBOMs do so by providing a list of open-source dependencies, ignoring proprietary and commercial code, as well as all the artifacts and components that are included in the final software package. Security data is also very limited to known open-source vulnerabilities and typically only found within CycloneDX formats. To extract any sort of usable security data from SBOMs requires a series of extra steps that involve thorough and manual investigation into individual components' reputation and history.

The SAFE report meets the required data elements of the SBOM, including a full inventory of every first-, second-, and third-party component, publishers, and licenses (not just open source) in exportable CycloneDX and SPDX formats. However, it goes beyond by presenting security data and insights in a clear, digestible format that promotes immediate action.

To illustrate the stark differences in the risk insights cyber risk professionals can instantly digest from the Spectra Assure SAFE Report compared to an SBOM, below is a detailed breakdown of how the SAFE report expands upon the SBOM by detailing threat categories that affect modern enterprise software supply chains.

Data Field	SBOM	Spectra Assure SAFE
Inventory & Licenses	✓	✓
Malware		✓
Tampering		✓
Exposed Secrets		✓
Application Hardening		✓
Version Differential Analysis		✓
Vulnerabilities		✓

Summary of the Spectra Assure SAFE Report

The SAFE report combines the SBOM with digestible and actionable security insights into the risks and threats of third-party software packages. Each section serves specific purposes that range from placing findings into specific threat categories; prioritizing security issues based on criticality or exploitability; and helping to gauge an acceptable level of risk to your organization. Below are some examples of sections within the SAFE report that can help security and risk professionals make informed decisions about the software they deploy from third-parties.

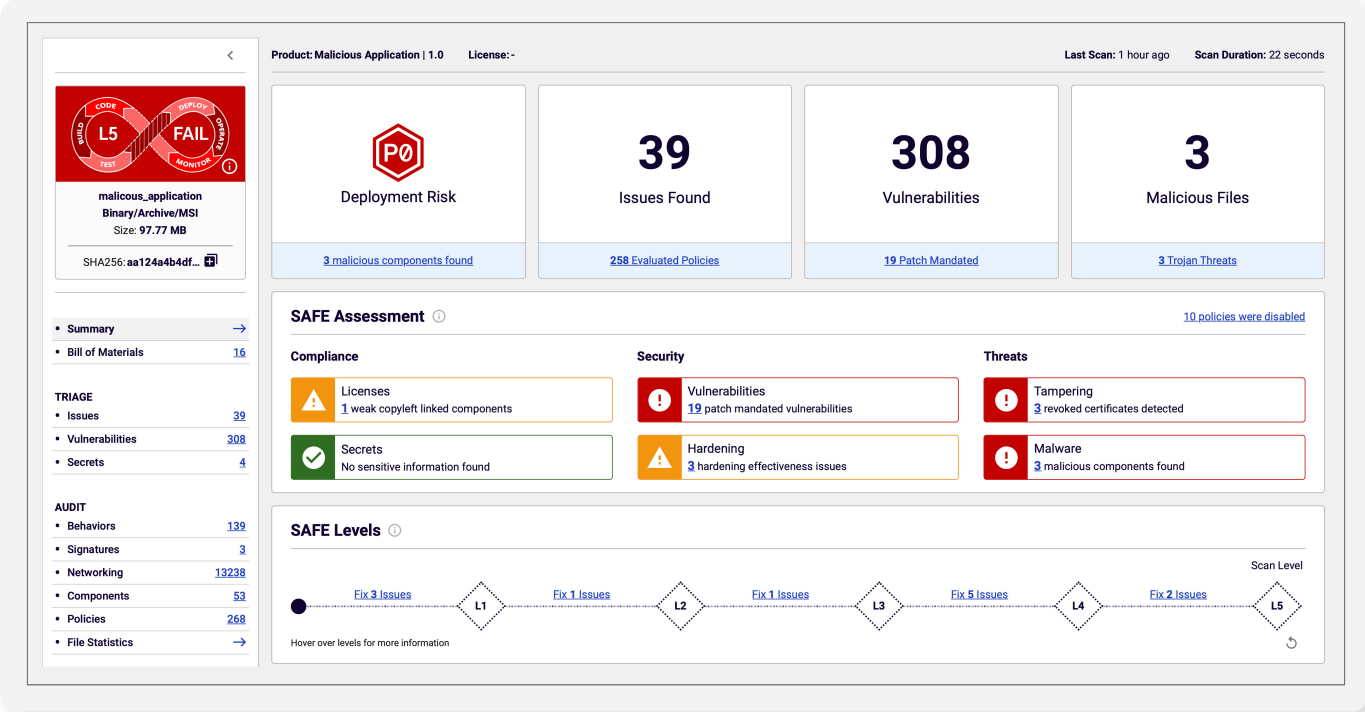

Figure 1: The SAFE report is your single source of truth to gauge the security hygiene of third-party software deployed across your organization.

The advantages of complex binary analysis are particularly evident when considering the real-time insights it provides. It enables teams to understand how the software will interact with its environment without having to execute the program itself. This granular observation uncovers hidden threats like tampering, exposed secrets, vulnerabilities, abused signatures, licensing issues, and malicious code that traditional application security testing tools miss.

SAFE Summary

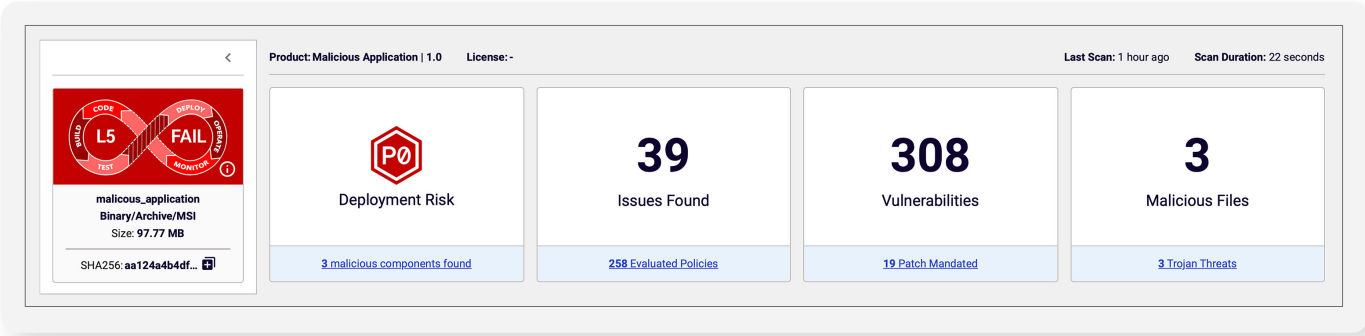

Figure 2: The SAFE Summary panel provides a snapshot of relevant security data points from which your team can take immediate action.

The top summary panels of the SAFE report display a number of fields meant to provide a high-level snapshot of relevant security issues along with the current policy standing of the application. These fields include:

- **Pass/Fail Status:** This field indicates whether the software package meets the desired policy criteria to be acceptable for deployment
- **Deployment Risk:** This field indicates the most severe security issues that need to be addressed prior to deployment
- **Issues Found:** This field gives the total number of security issues flagged across all assessment categories
- **Vulnerabilities:** This field gives the total number vulnerabilities that align to a Common Vulnerability Enumeration (CVE)
- **Malicious Files:** Malicious files that are categorized as malware are denoted here along with the number of instances within the analyzed binary

SAFE Assessment

The **SAFE Assessment** provides a summary of the key software safety concerns critical to third-party cyber risk professionals. Detected risks are grouped according to their shared characteristics. This helps identify, prioritize, and mitigate issues based on the category they belong to.

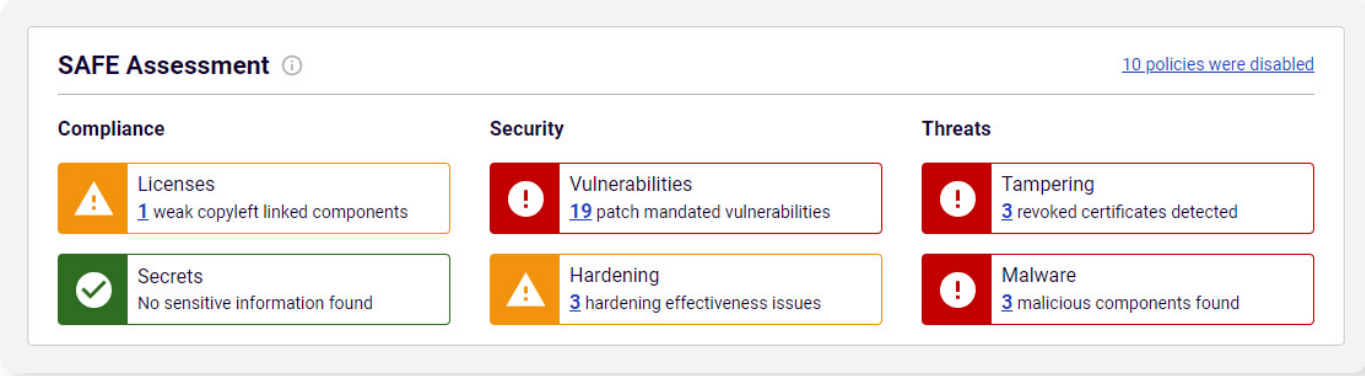

Figure 3: The SAFE Assessment provides a summary of all findings flagged in the most recent analysis and buckets them across six risk categories based on shared characteristics.

These risk categories include:

- **Malware:** Malicious files found during software package analysis. Malware is identified via known malware signatures and threat indicators
- **Tampering:** Suspicious attributes or changes to the application such as invalid digital signatures, or files that are erroneously added, removed or modified
- **Exposed Secrets:** Confidential credentials such as SSH keys, passwords, or API tokens that could give unauthorized access to the publisher's internal development environment
- **Hardening:** Lack of proper safeguards and mitigations within the compiled code like vulnerability protections, updated toolchains, and adequate prevention methods
- **Licenses:** Any occurrences of copy-left licenses or unauthorized use of proprietary or third-party components that may compromise the software's IP
- **Vulnerabilities:** Vulnerabilities are denoted by their CVE ID and whether the vulnerability is actively exploited by malicious actors

Each of these risk categories are broken out in depth to provide more context and insights for cybersecurity and third-party software risk professionals.

SAFE Levels

SAFE Levels contained within the SAFE report provide an accessible means by which to assess the risk that the entire software package may pose to your business. SAFE Levels offer this through a series of predefined, increasingly robust security policies. Each of the five SAFE Levels represents an increasingly strict set of security requirements that can help call out gaps in a vendor's testing regimen. Think of SAFE Levels as the most fundamental standards an organization should expect of a third-party application for it to be considered safe. For those without formal cybersecurity training, this guidance helps streamline vendor selection processes by providing a digestible way to assess how individual vendors expose the business to risk.

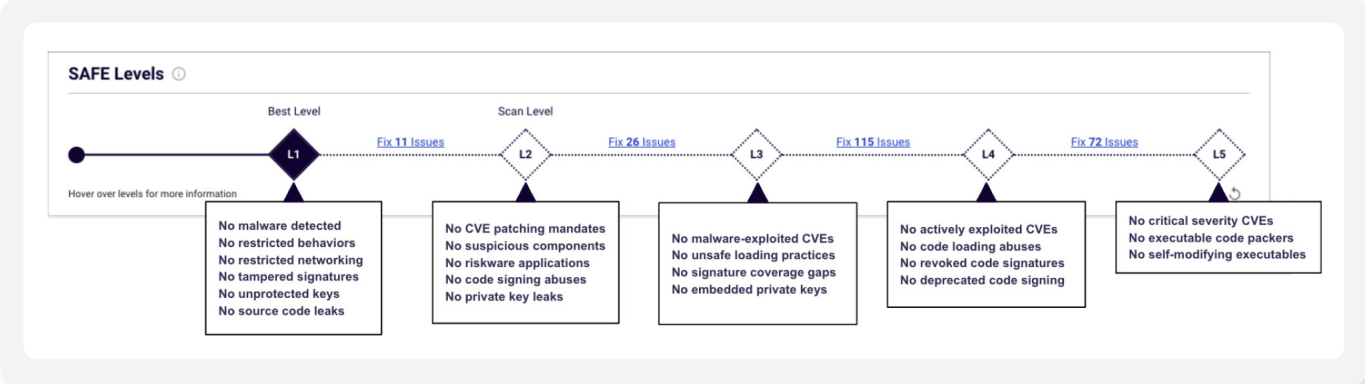

Figure 4: SAFE Levels makes it simple to gauge the risk that a specific software package presents to your business through a series of predefined, increasingly strict security policies.

Issues

The **Issues** section of the SAFE report guides cyber and risk professionals on which risks and threats demand immediate attention. The top issues across all policy categories are ranked based on remediation priority and files impacted. Policy rules can also be activated or deactivated based on your organization's risk appetite. This section summarizes which of the underlying policies were analyzed, suppressed, or disabled entirely. This helps promote transparency between the software vendor and buyer to clarify the completeness of testing and any deviations that were made from the default policy settings. The Issues section also includes a radar chart that provides visual signposts for the type and severity of Issues that were flagged during analysis.

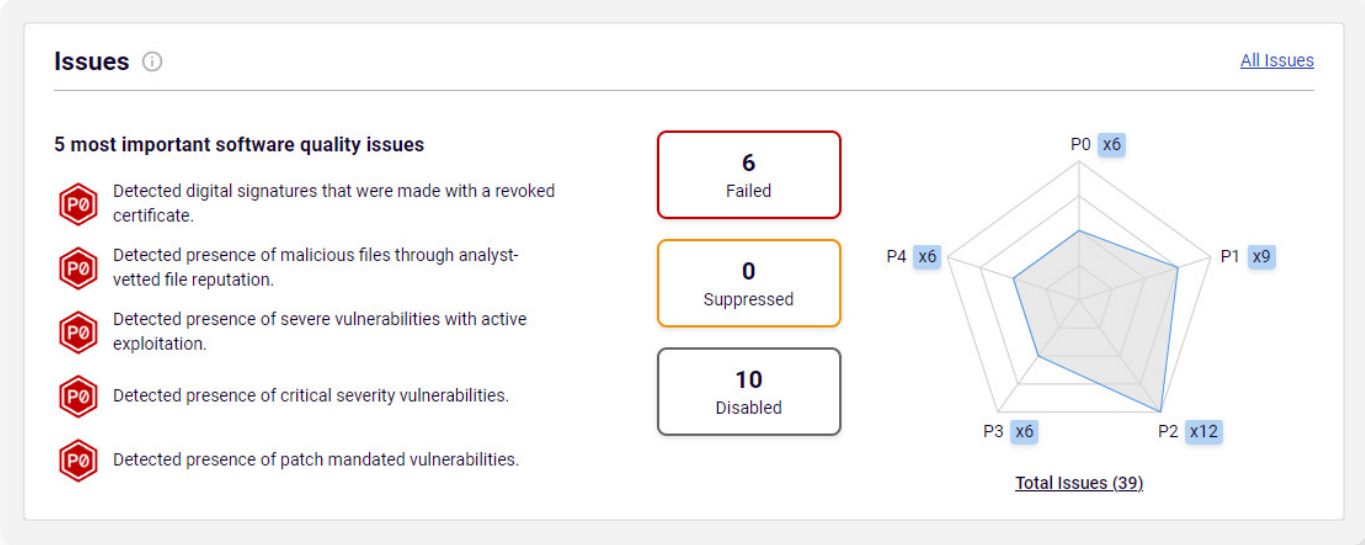

Figure 5: The Issues section of the SAFE report ranks the most critical security risks based on priority level, along with details on how individual security policies are triggered by specific files within the software package.

Performed Checks

The Performed Checks section of the SAFE report breaks down the specific analysis types performed on the software package. For security and cyber risk professionals evaluating third-party software, there are two analysis types that will be most relevant for maintaining and monitoring third-party software deployed in your IT environment:

- **Software Package Analysis:** The software package has undergone complex binary analysis which recursively deconstructs the software binary to flag hidden threats and risk within its core components

- **Version Differential Analysis:** Version-to-version differential analysis helps to monitor new threats and risks introduced with subsequent versions or patches of the software package. Conversely, any risks and threats that have been remediated since the last version are also cataloged

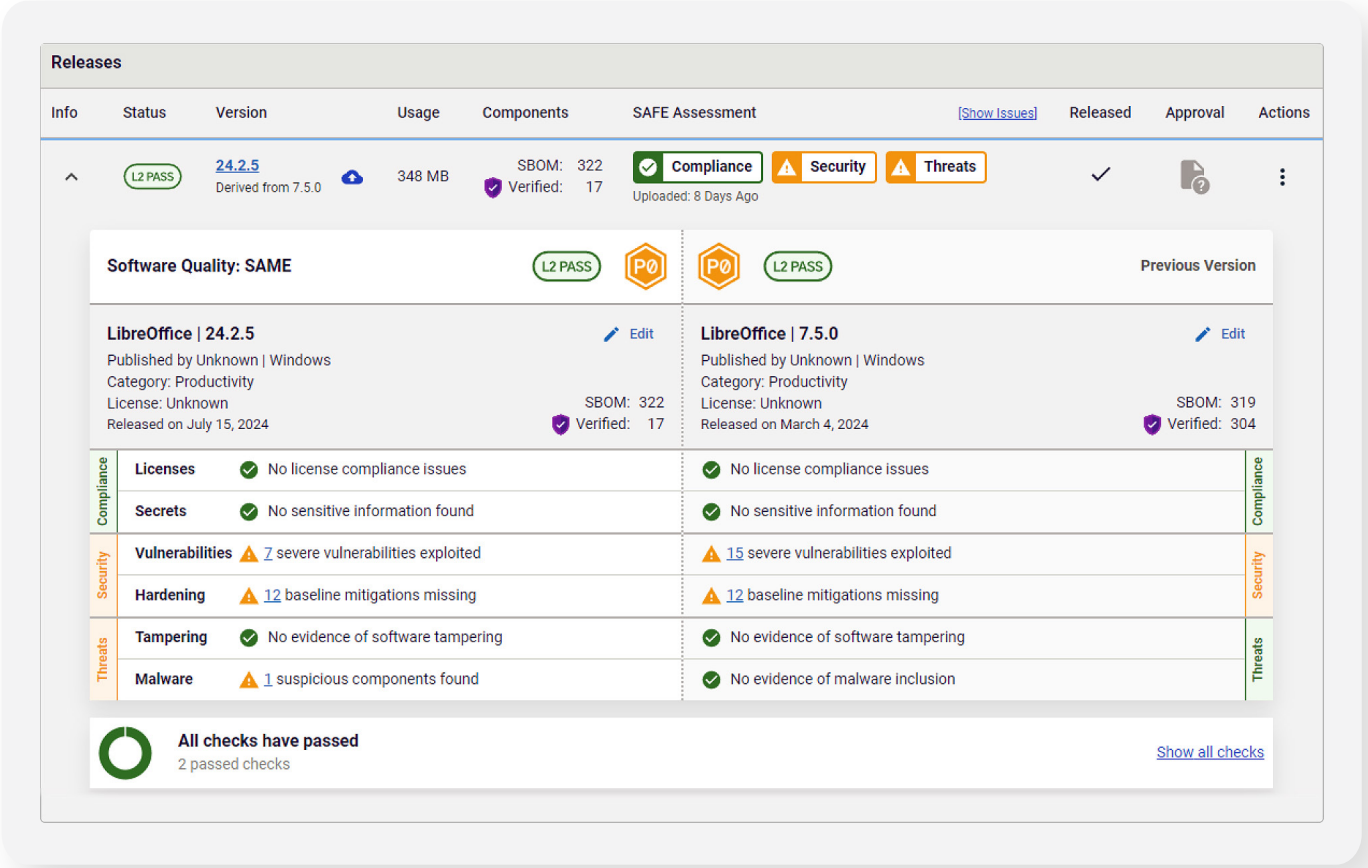

Figure 6: The Diff tab within the Performed Checks section of the SAFE report helps security and risk teams monitor the security standing of deployed software as new versions and patches are introduced.

SAFE Enables Effective Third-Party Cyber Risk Management

Beyond the software supply chain risk and threat information detailed within the SAFE report, it also includes a series of capabilities that can be incorporated into existing third-party software procurement processes to better operationalize third-party cyber risk management.

Software Bill of Materials (SBOM)

The SAFE report also includes a searchable and comprehensive software bill of materials (SBOM) that can fulfill compliance requirements, customer requests, and even aid in zero-day incident response. Security teams can readily respond to zero-day disclosures by searching for specific components to assess their exposure. SBOMs within the SAFE report exceed the NTIA's minimum SBOM requirements by mapping specific software supply chain threats like malware, tampering, vulnerabilities, and exposed secrets to specific components, further enabling businesses to validate the integrity of the components used in their software.

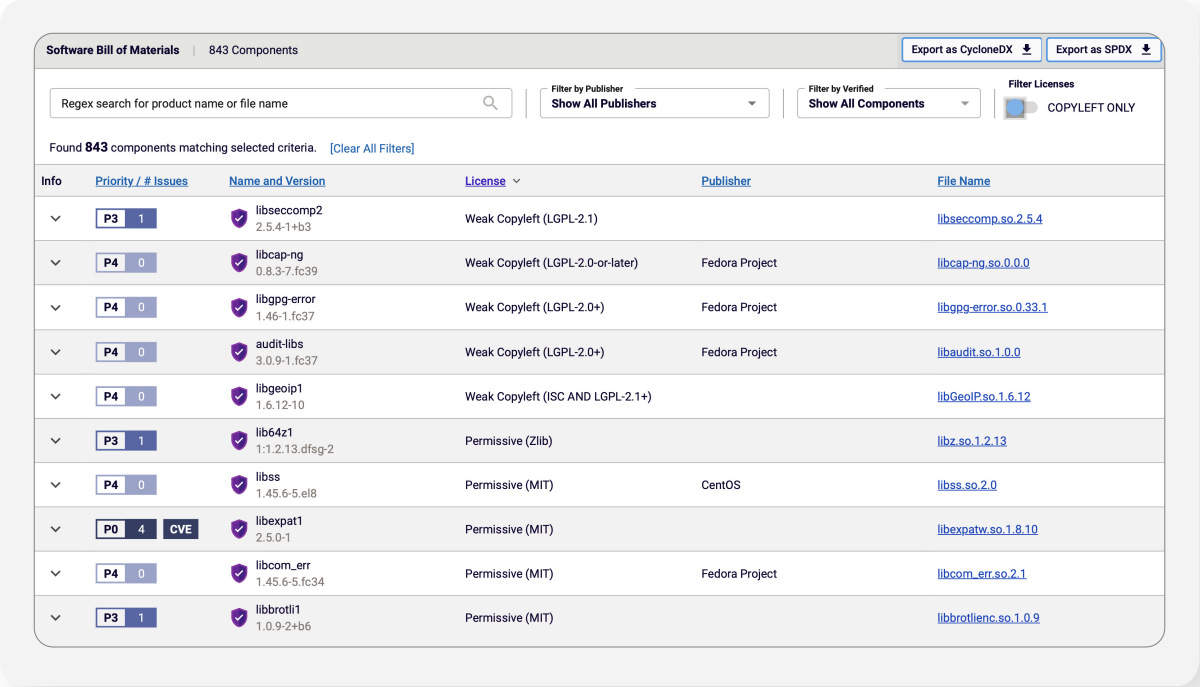

Figure 7: SBOMs within the SAFE report exceed NTIA standards by including the version and publisher of each component, along with critical risk information including embedded malware, vulnerabilities, and other threats.

Shareable SAFE Reports

The SAFE report enables collaboration and transparency with third-parties by allowing businesses to share their report directly with vendors and regulators. The SAFE report shareable link is:

- Secure
- Time-gated
- Password-protected
- Revocable

Sharing the SAFE report with vendors directly helps to bring awareness to the most imminent security issues embedded within third-party commercial software and expedites remediation action plans. Sharing reports can also help meet both internal and external compliance requirements in order to prove due diligence in assessing third-party software risk.

Customizable Go/No-Go Criteria

Depending on its purpose, different software applications may carry more inherent risk than others. For example, a third-party commercial application that processes customer data will carry more inherent risk than a backend ticketing system. To reflect varying criteria across different parts of your third-party software portfolio, security and risk teams can disable or modify different policy rules to adjust the Go/No-Go criteria for a particular piece or group of software. The SAFE report recognizes these policy changes and will update the policy standing of a software package based on the customized policy ruleset.

Acceptable Risk Approvals

The SAFE report also comes with a built-in mechanism for TPRM, VAST, GRC, AppSec, or Procurement teams to comment that a commercial software package is within acceptable risk range, even if the software package does not pass internal security and compliance policies. This mechanism serves as an internal audit record and allows third-party risk professionals to add notes that describe the business justification for accepting a particular software package.

Take Control of Your Third-Party Software Risk

While the SBOM is a fundamental step in benchmarking your software supply chain inventory, it is not an actionable source of risk information. Third-party risk professionals, including GRC, TPRM, AppSec, and Procurement teams, need to look beyond just the SBOM to make informed risk decisions regarding the third-party software they buy, download, and deploy. Spectra Assure provides cyber and risk managers with the primary control they have needed to identify and manage risk associated with third-party software.

The Spectra Assure SAFE Report provides a higher standard for third-party software risk evaluations for enterprise security and risk organizations. The SAFE report fills a significant gap in the third-party software procurement process by providing an actionable, detailed software threat and risk assessment without relying on manual processes, a stagnant list of ingredients, or unquestioningly trusting vendor self-attestations or security testing practices. It provides the most comprehensive risk analysis of third-party commercial software, dramatically simplifying third-party cyber risk evaluations and expediting vendor onboarding.

With each new update, the SAFE report provides new insights across a broader range of software supply chain threats, such as malware, tampering, suspicious behaviors, vulnerabilities, and more—well beyond what a typical SBOM can provide.

If third-party cyber risk professionals want to mitigate commercial software risk effectively, maintain due-diligence, and stay up to date with rising regulatory pressure, they must adopt new standards for third-party software cyber risk assessments. The Spectra Assure SAFE Report is the mechanism by which that standard is measured.

Get Started!

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

REQUEST A FREE TRIAL

www.reversinglabs.com

Learn More 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 Spectra Core powers the software supply chain and file security insights, tracking over 40 billion 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.

Citations

[1] European Supervisory Authorities. ESAs Report on the landscape of ICT third-party providers in the EU, 2023

[2] Source: Gartner, Chris Audet, Stay Ahead of Third Party Risk, 2019
https://www.gartner.com/en/legal-compliance/insights/third-party-risk-management

[3] Source: Gartner, Chris Audet, Stay Ahead of Third Party Risk, 2019

WP-Rev-07.31.24

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com