SOLUTION BRIEF

ЯEVERSINGLABS

Software Supply Chain Security for ITSM & Third-Party Risk

87%

of IT and third-party risk management (TPRM) professionals believe that software tampering is an emerging threat

37%

stated that they could detect it across their software supply chain as IT teams struggle to validate the integrity of the third-party software deployed to endpoints across their infrastructure

SCRM

Supply
Chain
Risk
Management

TPRM

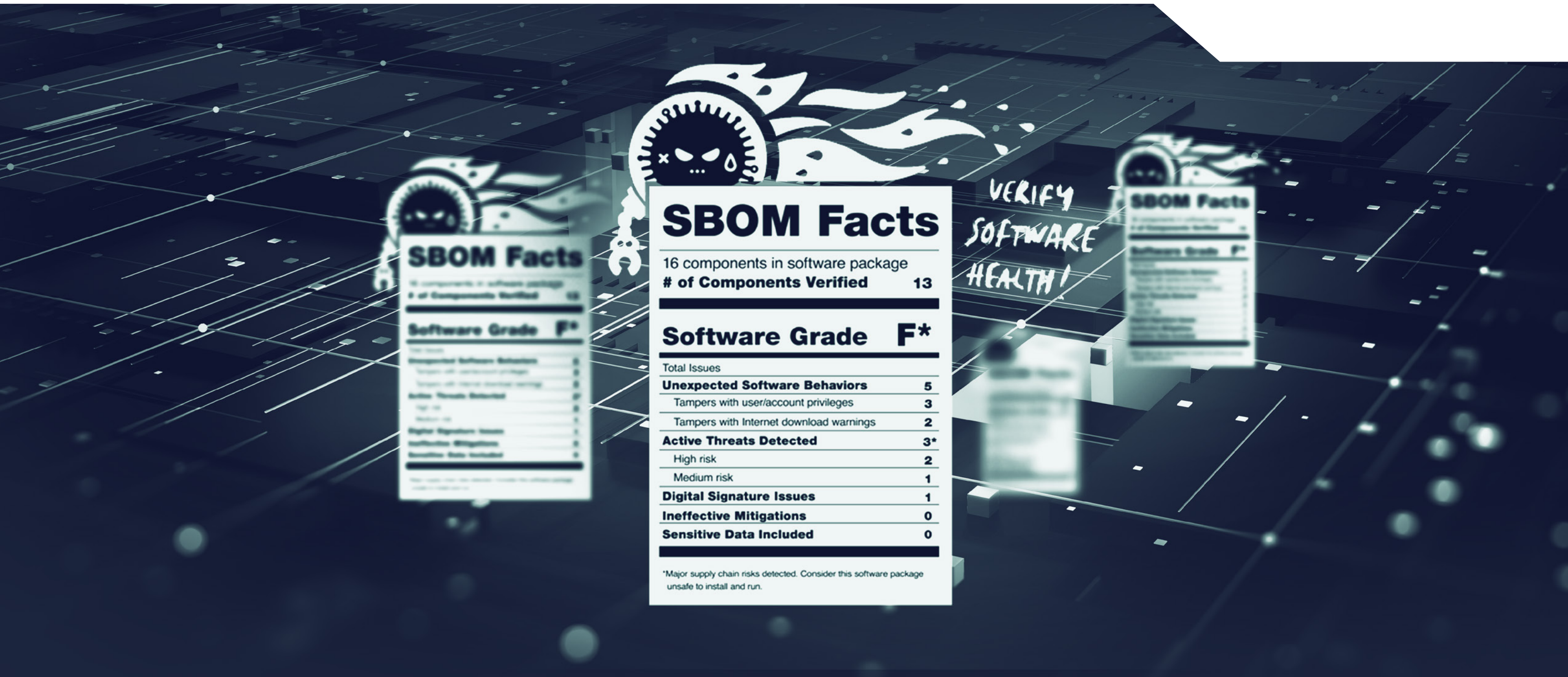
Third-Party Risk
Management

Why Software Supply Chain Security Matters to IT and Third-Party Risk Management

Threat actors are constantly exploring novel techniques to exploit enterprise systems, and the rise in successful supply chain attacks is a clear indicator of a largely unaddressed attack surface. Despite the emergence of standards and methodologies surrounding supply chain risk management (SCRM), organizations often lack the critical tools to enable them to gain visibility and control over the software that they consume. These unknown and unmitigated risks, such as software tampering and vulnerabilities, introduce unprecedented security and privacy risks to enterprises. And these security implications continue to rise as software systems become more interconnected and dependent on each other.

In a recent ReversingLabs survey, 87% of IT and third-party risk management (TPRM) professionals believe that software tampering is an emerging threat. However, only 37% stated that they could detect it across their software supply chain as IT teams struggle to validate the integrity of the third-party software deployed to endpoints across their infrastructure.

Many security teams fail to continuously monitor their attack surface and identify malicious behaviors and code in software updates, making them unaware of supply chain threats. And with attacks becoming increasingly sophisticated, primitive or insecure business processes will likely be exploited, putting enterprises and their data, customers, and brand at risk. As a result, it is important to understand how software supply chain attacks occur and impact organizations, to improve supply chain security and resolve common challenges.



SBOM Facts

16 components in software package

# of Components Verified	13
Software Grade	F*
Total Issues	
Unexpected Software Behaviors	5
Tampers with user/account privileges	3
Tampers with Internet download warnings	2
Active Threats Detected	3*
High risk	2
Medium risk	1
Digital Signature Issues	1
Ineffective Mitigations	0
Sensitive Data Included	0

*Major supply chain risks detected. Consider this software package unsafe to install and run.

Threat actors inserted malware into the SolarWinds Orion platform repositories, causing them to unknowingly distribute malware into over

18,000

organizations' systems

$40 milion

spent towards the recovery in first nine months after the breach

Insecure Software Creates Security Risk

Supply chain attacks are becoming increasingly common while organizations lack proper security measures to protect themselves from this threat. These increasingly sophisticated attacks occur when threat actors access a vendor's software development and delivery environments and embed malicious changes into their products. These vulnerabilities immediately introduce critical risks to enterprises, and legacy toolsets and methodologies are limited in detecting and preventing critical data compromise.

Despite the expanding responsibilities placed on IT and TPRM teams as a critical step in the security positioning of enterprises, the legacy toolsets focused on supplier assessments are not providing the critical data needed from procurement to ongoing monitoring. The risks introduced through code tampering, unaddressed vulnerabilities, and malware insertion scale beyond the narrow focus of SCA, DAST, and SAST tools, leaving these teams exposed to the security risks introduced into their infrastructure.

Supply chain attacks greatly impact how enterprises operate. In the spring of 2020, threat actors inserted malware into the SolarWinds Orion platform repositories, causing them to unknowingly distribute malware into over 18,000 organizations' systems. Nine months after the breach, the impacted company had spent $40 million towards the recovery, but the true cost to business could be in the hundreds of billions of dollars. The fallout of this cyberattack still resonates years later as the brand continues to rebuild its image and position within the space.

Supply chain attacks will continue to be a common occurrence as Gartner predicts that by 2025, 45% of organizations will suffer this fate, making it essential that teams have effective preventative measures and tools in place.

It Is Critical To Monitor Vendors and Confirm Secure Product Updates

To ensure that product updates are secure, it is essential to consistently monitor vendors, scan for active threats, and enforce consistent security practices. This generates a repeatable process where IT teams can efficiently and effectively identify and remediate malware and tampering before they're deployed.

4 key practices to monitor vendors	Why it’s important	How ReversingLabs SSCS Helps
1. Establish a software supplier inventory	Know all of the vendors that you are working with and define your risk	Generate a software bill of materials (SBOM) that lists all third-party party software components
2. Establish criteria for a risk based approach	Monitor vendors for events such as malicious behaviors, weakening security postures, and deviations from compliance standards to identify new risks	Validate software components by analyzing codebase changes and who made them to detect tampering and malware before deploying product updates
3. Establish minimum software security standards for compliance tracking	Create policies to track vendors’ ability to follow risk and compliance standards	Test product updates and create custom policies to assess compliance with best practices
4. Continuous attack surface monitoring	Consistently reassess vendor integrity to ensure continued compliance and identify new risks and threats	Continuously scan your environment and assess third-party party risks in real-time

Introducing ReversingLabs Software Supply Chain Security

ReversingLabs Software Supply Chain Security (SSCS) platform provides a unified point for IT and TPRM teams to detect, understand, and manage risks arising from a software portfolio supply chain. It automates and integrates software testing, policy controls, risk-based prioritization, and auditing at various stages of software use and consumption. The platform creates a single point of reference for software supply chain security across all applications and projects, which empowers the collaboration between TPRM and security teams required to quickly deliver trusted software.

ReversingLabs Software Supply Chain Security platform enables IT and TPRM teams to address risks through the entire procurement and deployment lifecycle, including risk profiles, threat mitigation, and termination when necessary. The ongoing monitoring provided by this advanced platform offers real-time data, enabling the teams to make assessments and apply appropriate due diligence when and where required.

ReversingLabs combines the most advanced malware analysis engine with a highly scalable architecture and the largest commercial repository of goodware and malware to protect your organization from software supply chain, ransomware, and other file-based attacks.

ReversingLans Software Supply Chain Security Capabilities

Comprehensive Security Coverage

Monitor and secure open source and third-party software components to identify malicious updates and packages.

Active Threat Detection

Identify and eliminate malware and tampering before deployment.

Contextual Alerting

Ranks alerts by severity and time to resolve to help teams efficiently respond to the right threats and vulnerabilities.

Risk Auditing

Collect a software bill of materials (SBOM) and historical record to identify all third-party software and open source components that existed in your environment to visualize your attack surface.

Suspicious Behavior Identification

Understand baseline behaviors and identify suspicious actions and anomalies.

Policy Customization

Create custom policies to locate and prioritize threats and risks specific to your environment and enforce consistent security standards.

About ReversingLabs

ReversingLabs, the leader in software supply chain security, offers the only holistic software supply chain solution that secures third-party software and open source components and identifies active threats. ReversingLabs provides protection against malware and tampering in pre and active production. For more information or to schedule a demo, contact us today.

Get Started!

REQUEST A DEMO

www.reversinglabs.com

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com