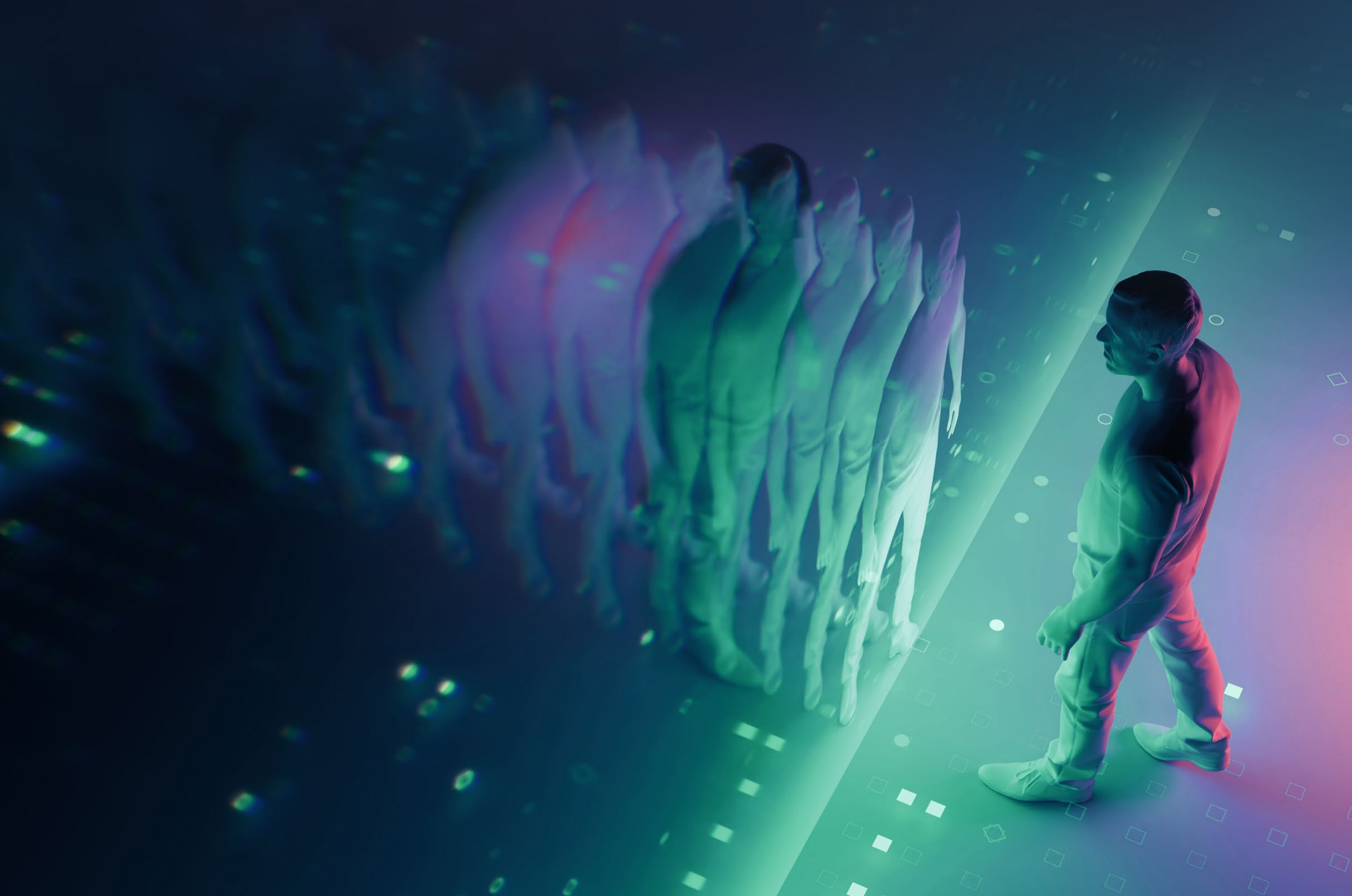
REVERSINGLABS

SBOMs: Surfacing Critical Software Supply Chain Risks



The Rise of Supply Chain Attacks and SBOMs

This solution brief explores:

- The rise of software supply chain attacks
- The popularity of software bills of material
- Users' main concerns when collecting them
- How ReversingLabs SSCS addresses those concerns
- How ReversingLabs' SBOM compares to those collected by SCA tools

In 2020, Solarwinds suffered from the largest software supply chain attack in history, which compromised 18,000[1] organizations and cost them $40 million to remediate[2]. Shortly thereafter, the amount of supply chain attacks spiked, increasing by 300% in 2021[3].

An executive order was issued to address software supply chain security, which details how to acquire, deploy, use, and manage software and services. It recommends that enterprises collect a software bill of materials (SBOM).

SBOMs help users determine their supply chain risk and identify vulnerable, suspicious, or counterfeit software or open source tools by listing all components to determine the size of the attack surface, stating how software interacts with each other to calculate the blast radius, and locating active threats like malicious code tampering to prevent supply chain attacks[4].

Currently, 49% of American enterprises are "very concerned" about the integrity of their components with 88% of security teams being projected to collect SBOMs by the end of 2023 to improve visibility, understand risks, and make informed decisions[5].

However, many enterprises lack proper security measures and tools to protect themselves from these attacks by commonly using software composition analysis (SCA) tools which have partial coverage, failing to identify the entire attack surface and severe threats, making teams unaware of severe risks, how to react to them, and making them susceptible to supply chain attacks.

Sources:

[1] "Solarwinds Says 18,000 Organizations Were Impacted by Recent Hack"
https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/

[2] "One Year Later: Has Solarwinds Changed How the Industry Builds Software"
https://www.cybersecuritydive.com/news/solarwinds-1-year-later-cyber-attack-orion/610990/

[3] "Software Supply Chain Attacks Emerge in Full Force"
https://www.dynatrace.com/news/blog/why-software-supply-chain-attacks-are-increasing/#:~:text=Software%20supply%20chain%20attacks%20emerge%20in%20full%20force,-The%20COVID%2D19&text=In%202021%2C%20these%20attacks%20grew,cyberattacks%20targeting%20software%20supply%20chains

[4] "Framing Software Component Transparency: Establishing a Common Software Bill of Material"
https://ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

[5] "Software Bill of Material and Cybersecurity Readiness"
https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/LF%20Research/State%20of%20Software%20Bill%20of%20Materials%20-%20Report.pdf

Common Problems with SBOMs

The Linux Foundation conducted a study detailing SBOM's usage, purpose, and public perception. They found that SBOM users' main concerns is that they are unclear of key practices to follow, which tools are in place to assemble SBOMs, and how to properly use them[6].

The purpose of an SBOM is to regularly audit and identify risks within components and across environments. To effectively assess supply chain risk, SBOMs must identify the total amount of components, their information and function, and vulnerabilities and threats embedded within them[7].

As a result, there are several key practices that teams should follow when collecting SBOMs, which help them evaluate their risk, understand how components function, and consistently discover and quickly remediate vulnerabilities and threats.

4 key practices for SBOMs and risk assessment	Why they're important	How ReversingLabs helps	How SCA tools' SBOMs fall short
1. Understand your attack surface	Assess your risk by determining the amount of open source and third party software components in your environment	Identifies open source and third party software components	Only identifies open source components
2. Review how components function	Validate the integrity of your components by seeing whether they are up to date, how they interact with each other, and how often you collect SBOMs	Discovers components' general information such as: Supplier, version, and author name, relationships with other dependencies, as well as the last time an SBOM was used	Finds licenses for open source components
3. Locate vulnerabilities and threats	Find common vulnerability exploits (CVEs), code tampering, and suspicious behaviors to discover immediate issues which lead to supply chain attacks	Detects CVEs, malware, tampering, and suspicious behaviors with every SBOM and ranks alerts and provides rich context for quick remediation	Detects CVEs, contributor reputation for open source packages, and provides alerts with little to no context
4. Consistently assess your environment	Continuously collect SBOMs to identify your risk in real time and remediate emerging problems	Automatically generates SBOMs in CycloneDX format	Generates SBOMs in a general format

Sources:

[6] "Software Bill of Material and Cybersecurity Readiness"
https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/LF%20Research/State%20of%20Software%20Bill%20of%20Materials%20-%20Report.pdf

[7] "SBOM at a Glance"
https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf

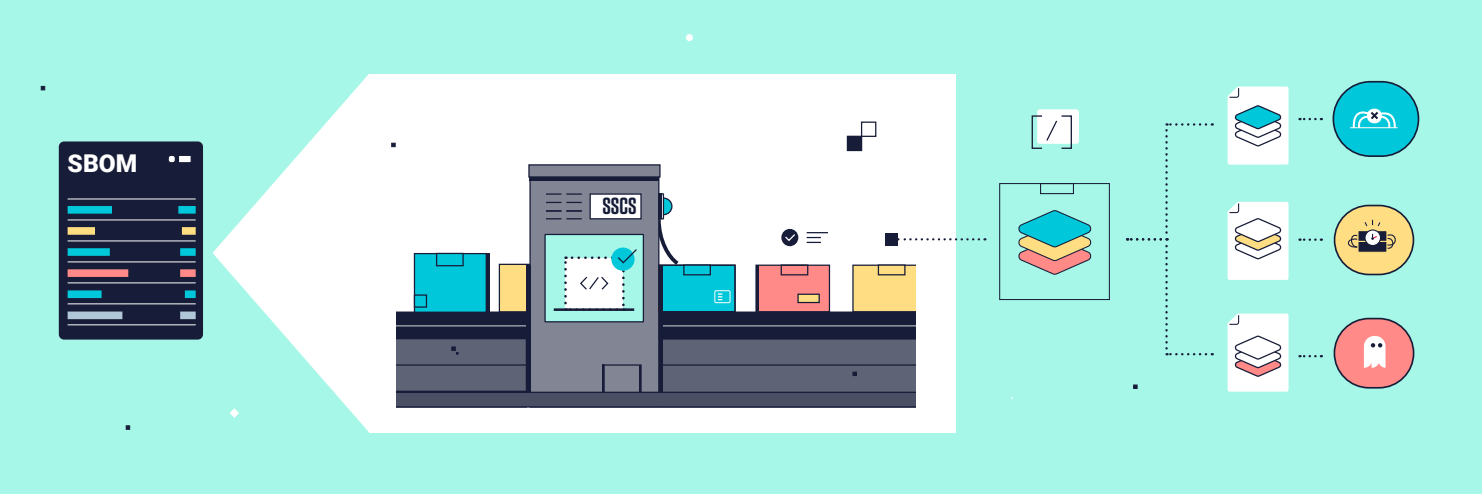
These key practices help teams define the size of the attack surface, how components are monitored and maintained, and if there are severe issues that must be addressed, outlining their risk profile and helping them effectively respond to vulnerabilities and threats across the software supply chain.

ReversingLabs vs SCA SBOMs

Software Bill of Materials (SBOM) are a vital resource to improve visibility and manage supply chain risk. It is important for security teams to adopt the right tools to monitor and protect the right things.

While software composition analysis (SCA) tools collect SBOMs, they cannot detect third party software components, have limited background information about open source packages and files, and cannot detect active threats and behaviors that lead to supply chain attacks. This gap in coverage prevents users from seeing their entire attack surface, understanding their risk, and identifying issues that directly lead to supply chain attacks.

ReversingLabs' software supply chain security (SSCS) platform assembles an SBOM. This identifies third party software and open source components as well as active threats, with alerts ranked by severity with recommended steps for remediation, providing users with a detailed view of their supply chain risks, helping them locate and respond to malware and tampering, and understanding their risk profile.



ReversingLabs SSCS Features

The ReversingLabs SSCS platform secures open source and third party software components and protects organizations from persistent and major threats and risks. With a holistic approach to supply chain security, our platform enables enterprises to prevent attacks.

Risk Auditing

Collect a software bill of materials (SBOM) and historical record to identify all 3rd party software and open source components that existed in your environment to visualize your attack surface.

Comprehensive Security Coverage

Monitor and secure open source and 3rd 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.

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.

Get Started!

REQUEST A DEMO

www.reversinglabs.com

About ReversingLabs

ReversingLabs, the leader in software supply chain security, offers the only holistic software supply chain solution that secures 3rd 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.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com