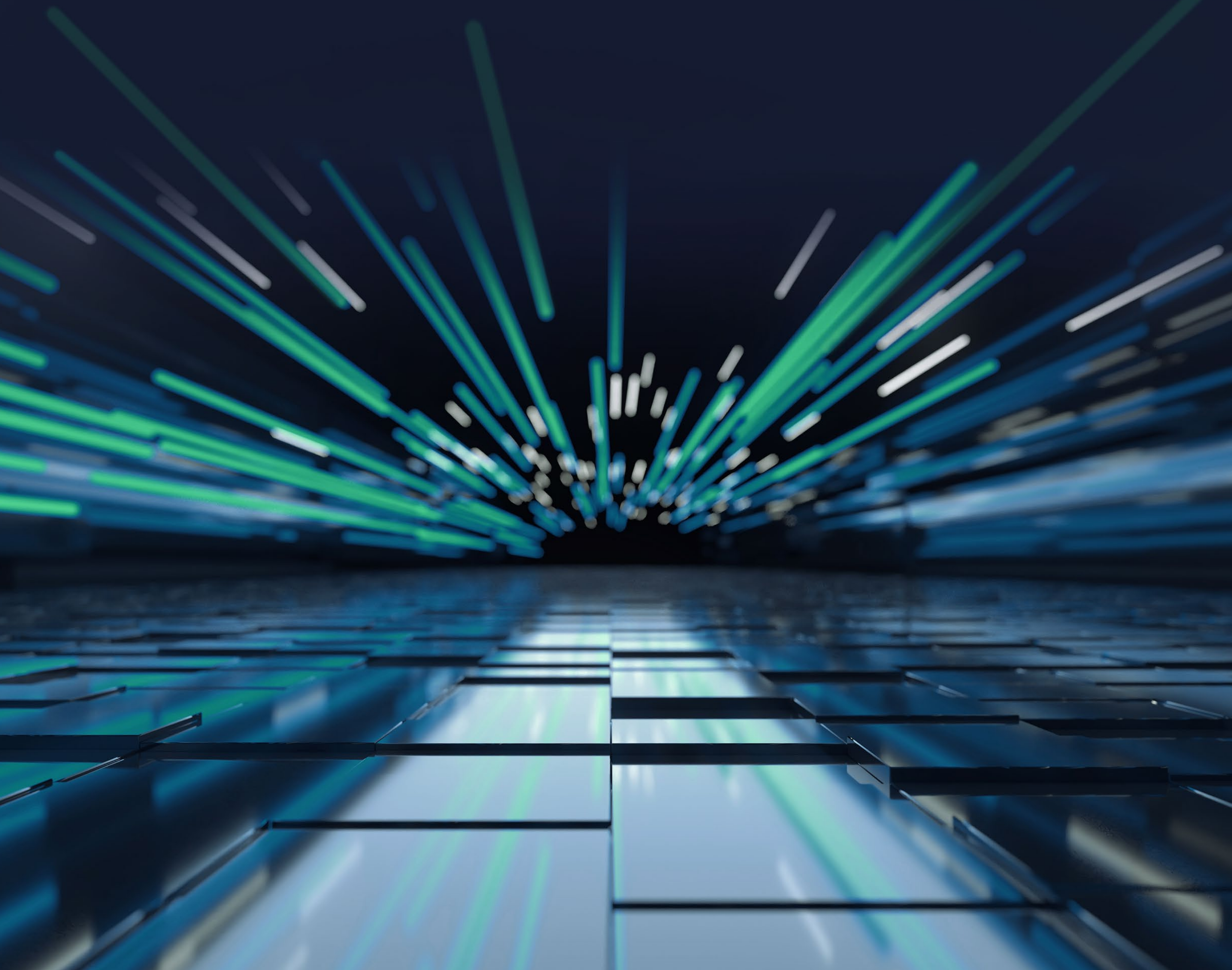
BUSINESS BRIEF

REVERSINGLABS

SYNOPSYS®

SCA Tools & SSCS - Better Together



Introduction

Highly publicized supply chain attacks, like Log4j and SolarWinds, highlighted the shortcomings that many security teams and tools face as they have limited processes around securing their open source and third party software components. And with supply chain attacks targeting 62% of organizations[1], it is important for AppSec, DevSecOps, ITSM, and SOC teams to implement the right tools to help improve their best practices around supply chain security.

Software composition analysis (SCA) tools and ReversingLabs' Software Supply Chain Security (SSCS) Platform were released to help enterprises successfully protect themselves from supply chain attacks. However, while SSCS and SCA tools address common attack vectors, they solve different problems and address different use cases across the software supply chain.

Software composition analysis consumption is projected to grow by

21.7%

by 2028

1.2 billion

vulnerable dependencies are downloaded each month

Software supply chain attacks increased by

742%

over the last 3 years

84%

of codebases contain vulnerabilities

78%

of organizations want to improve their software supply chain security over the next 12 months

The influence, use cases, and composition for SSCS

According to Moody's analytics, 74% of enterprises considered their third party risk management practices to be "poor or mediocre", with 69% of businesses lacking the necessary supply chain visibility to uncover risks[2]. Because of inadequate security practices and growing attack surfaces, organizations struggle to protect themselves from active supply chain threats facilitated through open source and third party software components.

In September 2019[3], threat actors inserted malware into Solarwinds' Orion platform's repositories, and when they updated their platform, they unknowingly distributed malware into their users' systems. This compromised over 18,000 organizations and cost $40 million for Solarwinds to remediate[4].

ReversingLabs developed SSCS when working with Solarwinds and their users to recover from this attack and protect them from future targeted, highly sophisticated supply chain incidents. They accomplish this by supporting several use cases.

Sources:

[1] https://securityintelligence.com/articles/62-of-surveyed-organizations-hit-by-supply-chain-attacks-in-2021/

[2] https://www.moodysanalytics.com/about-us/press-releases/2023-4-17-moodys-analytics-70-percent-businesses-ramp-up-supplier-risk-detection-investment

[3] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know#:~:text=Here%20is%20a%20timeline%20of,unauthorized%20access%20to%20SolarWinds%20network

[4] https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

MANAGE THIRD PARTY RISK

ITSM teams must verify that third party software is safe to consume and can analyze third party software updates to determine the behaviors leading up to the release and threats embedded in them.

FIND ACTIVE THREATS

AppSec and DevSecOps teams need to determine whether open source components are safe to integrate into builds and their environment. SSCS detects tampering and malware embedded in open source and third party software components up to 10GB in pre- and active production.

APPLY SCANNING AND COMPLIANCE POLICIES

AppSec and compliance teams must establish consistent security practices and achieve compliance across the software supply chain. They accomplish this by creating custom scanning policies where they decide what to scan for and how alerts are prioritized.

SUPPORT RAPID AND TARGETED REMEDIATION

SOC and AppSec teams need to efficiently remediate risks and threats. SSCS ranks alerts by severity, provides recommended steps for remediation, supports scanning suppression, and verifies that severe issues are resolved, limiting false positives and supporting efficient and effective remediation.

ReversingLabs' SSCS uses the world's largest private repository of malware and goodware when scanning for threats and uses version differencing, determining how components change over time to detect tampering. It also uses recursive binary analysis to find transitive dependencies between components, calculating the blast radius when running risk reports. Additionally, users can suppress scanning for incidents which lead to false positives with customizable detection rules when scanning for threats, vulnerabilities, and leaked secrets. These features support SSCS' use cases for third party risk management, threat hunting and analysis, and compliance.

SSCS identifies malware and tampering in product updates and open source packages, allows users to create and enforce custom policies, and generates contextual alerts. This promotes consistently enforced security practices and fast remediation for supply chain threats which directly lead to attacks.

The influence, use cases, and composition of SCA tools

Malware was inserted into the codebase of Log4j open source packages, and when teams updated these packages, malware entered their systems. Because of this, Log4j packages were considered vulnerabilities, and users needed to determine if they were using those packages, and if so, which version to see if their systems were compromised.

According to the Neustar International Security Council, the Log4j attack impacted 61% of enterprises with 21% of them having "significant security impacts"[5]. This is because, according to Synopsys, 75% of code stored in codebases are open source[6]. With large attack surfaces and limited security measures to monitor and protect their components, many organizations are at high risk for supply chain attacks.

SCA tools were developed to remediate this issue, protect against similar attacks, and ensure that teams effectively and securely use open source components. They consistently verify that they are safe and legal to implement, and support several use cases.

GAIN VISIBILITY INTO OPEN SOURCE AND THIRD-PARTY COMPONENTS

SCA tools analyze applications and their dependencies to create an inventory of the open source, third-party, and proprietary components being packaged, assembled, and utilized.

REDUCE LICENSE, VULNERABILITY, AND OPERATIONAL RISK

SCA tools are used by legal teams who are actively assessing license risk and reevaluating company policy as licenses evolve and new licenses are included.

APPLY CONSISTENT OPEN SOURCE POLICIES

Security teams must assess the overall risk presented by open source components across all applications, set consistent policies to keep risk to acceptable levels, and work with development teams to guide vulnerability detection and remediation.

SUPPORT SOFTWARE DEVELOPMENT

SCA tools deliver developers critical information about out-of-policy licenses, vulnerable components, and malicious packages while providing guidance about how to remediate them. Developers also use SCA tools to identify healthy and secure components by looking at the activity, provenance, and pedigree of open source projects[7].

Sources:

[5] https://www.helpnetsecurity.com/2022/03/02/log4j-vulnerability-security-professionals/

[6] https://www.darkreading.com/application-security/hundreds-of-open-source-components-could-undermine-security

[7] https://www.forrester.com/report/the-software-composition-analysis-landscape-q1-2023/RES178778

SCA tools collect software bills of materials (SBOMs) to find components' name, supplier, version, and license, and evaluate vulnerability databases when scanning codebases, containers, and registries to discover risks and weaknesses. They also use continuous scanning to identify issues in real time, automatically enforcing guardrails with out-of-the-box policies which trigger alerts or rollbacks when not followed. These workflows and features allow them to increase visibility, reduce risks, validate the health of open source components, and support the use cases listed above.

SCA tools identify vulnerabilities in open source components, collect SBOMs, and enforce policies to remove potential threats to quantify supply chain risk, and harden systems.

SCA tools and SSCS - Complementing Eachother for Software Supply Chain Security

SSCS protects enterprises from complex and focused supply chain attacks with open source and third party software, while SCA tools protect organizations from general supply chain risks in open source components.

The table below shows SCA tools' general features, according to Forrester[8], and compares that to SSCS' functionality.

SCA TOOLS - USE CASES	OBJECTIVE	SSCS - USE CASES	OBJECTIVE
Open source component health and package integrity	Identify vulnerabilities and determine the health of open source components	Open source and third party software health and package integrity	Identify vulnerabilities, malware, and tampering embedded in open source and third party software components in pre- and active production
Policy management for license validation	Ensure third party and open source components meet the organization's risk tolerance for license usage	Policy management for custom scanning	Users define what to scan for and how to classify alerts, allowing them to enforce consistent security practices that best fit their organization
Automatic Remediation	Automatically remediates vulnerabilities and license incompatibilities	Targeted Remediation	Ranks alerts by severity with recommended remediation steps for targeted responses

Sources:

[8] https://www.forrester.com/report/the-software-composition-analysis-landscape-q1-2023/RES178778

SCA Tools and SSCS - How they are better together

SCA tools find vulnerabilities, collect analytics, and use built-in policies to observe the health of users' environments, enforce common security protocols, and determine whether open source components are secure. They help users calculate open source risks and remediate common problems.

ReversingLabs' SSCS delivers deeper coverage across the entire software supply chain. For example, it locates malware and code tampering in open source and third party software components, validates the integrity of product updates and third party code before it is deployed, and provides detailed threat intelligence.

SCA tools and SSCS leverage different technologies to solve different problems across the software supply chain. For instance, SCA tools use source code analysis, vulnerability databases, automated workflows, and built-in policies to find components when collecting SBOMs, discovering vulnerabilities, automating remediation, and enforcing best practices. However, SSCS uses binary analysis, malware and goodware repositories, contextual alerting, and custom policies to find transitive dependencies in SBOMs, uncover active threats and promote targeted and effective responses, and support users' unique organizational and compliance best practices and needs.

SSCS and SCA tools are essential parts in effective supply chain security programs. SCA tools find common vulnerabilities and risks and support fast remediation, while SSCS discovers complex, active threats and promotes targeted responses. SCA tools manage the day-to-day for open source components while SSCS manages targeted and sophisticated attacks across the entire software supply chain, which consists of open source and third party software components.

Get Started!

www.reversinglabs.com

REQUEST A DEMO

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.