REVERSINGLABS

Software Supply Chain Security Risk Report

Tooling Gap Leaves Organizations Exposed

Eighty eight percent of organizations recognize software supply chain security as an enterprise-wide risk, but 74% say traditional application security solutions are inadequate to fortify their software supply chains against the rising threat. Here's why — and how to develop a mature supply chain security program.

Chris Wilder, TAG Cyber
TAG CYBER

Contents

Executive Summary

In April 2023, ReversingLabs partnered with Dimensional Research to survey 321 security and IT professionals on their software supply chains for its report, "Software Supply Chain Security Risk Survey." This analysis presents key findings and actionable recommendations for security organizations in four key areas:

TRADITIONAL APPLICATION SECURITY SHORTCOMINGS

Existing application security testing tools alone aren't sufficient to handle evolving — and costly — software supply chain security threats. More adaptable measures are needed.

SOFTWARE SUPPLY CHAIN COMPLEXITY AND SECURITY

Security teams should take a comprehensive approach that includes continuous risk visibility, threat detection and remediation, and software integrity validation.

SECURITY IN SOFTWARE DEVELOPMENT

Security concerns for internally developed and open-source software require comprehensive measures from all contributors.

ENTERPRISE-WIDE SECURITY RISKS

Software supply chain security is a company-wide risk that requires an integrated response by application security and Security Operations teams at all stages of the software development lifecycle.

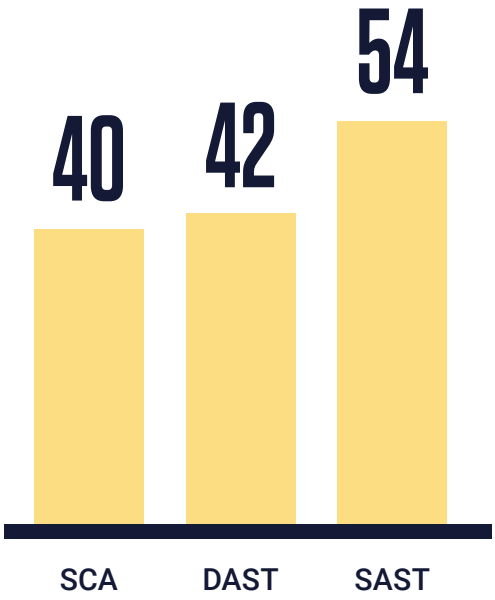
Organizations can enhance software supply chain security and fortify their overall cybersecurity posture by:

- Implementing continuous security practices.
- Validating third-party components.
- Strengthening threat intelligence capabilities.
- Fostering a security culture.
- Embracing automation that helps to prioritize what you're remediating.

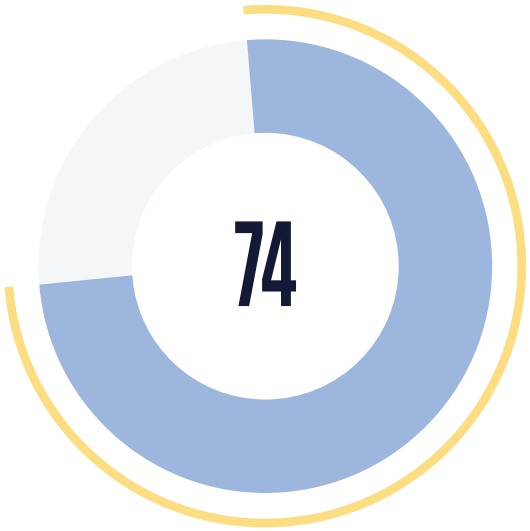
This report sheds light on software supply chain vulnerabilities and risks and provides insights as to how organizations can proactively address threats and protect critical assets.

Traditional application security is falling short

Traditional application security testing tools are only part of the software supply chain solution. They're great as far as they go, but nearly three quarters of survey respondents said they were insufficient to protect against all software supply chain threats.



Percent of respondents who say their organizations use traditional SCA, SAST or DAST tools.



Percent of IT pros who say traditional tools aren't adequate to fully protect against software supply chain threats.

Application security teams need more than traditional vulnerability management tools to address today's evolving threat landscape.

To cope with the complexity of modern attacks, such as the SolarWinds, 3CX, and CircleCI incidents, these teams need a deep understanding of evolving attack vectors and supply chain risks. These incidents underscore the critical need to monitor software behavior across versions, enabling organizations to detect tampering, verify software integrity, and bolster the resilience of the software development life cycle (SDLC).

Advanced detection techniques, rooted in extensive threat intelligence, are now mandatory. These provide the foundation for early identification of malicious components, offering a strategic advantage in an environment where time is of the essence.

Application security teams should broaden their security outlook and integrate more advanced strategies. This represents a fundamental shift in how organizations are approaching software supply chain security.

Why Traditional Application Security Testing Alone Can't Mitigate Software Supply Chain Attacks

LEARN MORE IN OUR SPECIAL REPORT

Software Supply Chain Security Is About Maturity: Shift Up Your Thinking

MATT ROSE
Field CISO, ReversingLabs

Why do 87% of companies say they have detected security issues in their software supply chain in the last 12 months? Developers and the development ecosystem are now a primary target for attackers. Software supply chain security attacks are rising in part because most organizations don't fully understand what the practice of supply chain security entails — or how to approach the problem. They're using a dated process and tools to deal with a modern problem. Let's start there.

THE TRADITIONAL APP SEC PROCESS

- **Deploy software composition analysis (SCA) tools.**
- **Review open source code.**
- **Review your DevOps tooling capabilities**
- **You're done.**

Not so fast. How are you going to ensure that malware hasn't been slipped into your final product somewhere along the way? You can't depend on application security testing (AST) tools. Here's why:

- **They're very good at finding vulnerabilities, but not malware specifically.**
- **They don't have a reputational database of known malware, which is required to detect the presence of malware.**

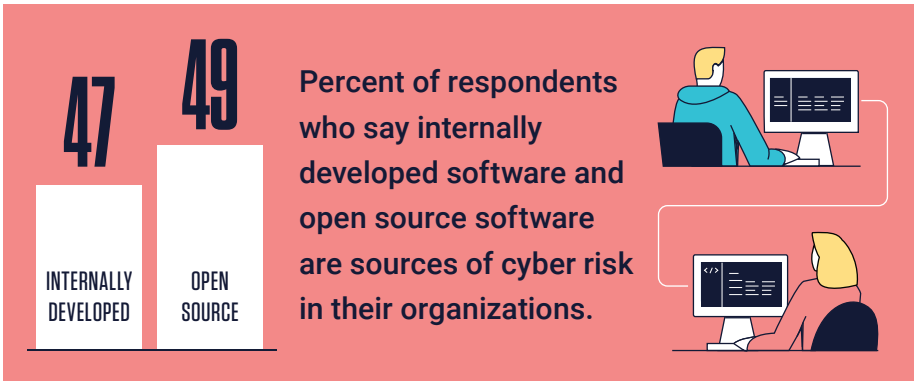
That's why AST tool vendors don't mention malware anywhere in their product descriptions.

The ReversingLabs Software Supply Chain Risk Survey found that 74% of practitioners believe traditional application security solutions are ineffective at protecting companies from supply chain threats.

CONTINUED

Software supply chain complexity has created security issues

Internally developed software nearly ties open-source software as the top source of software issues. More than 50% of companies use contractors and third-party developers in addition to employees to create "internally developed" software.



Survey respondents identified both internally developed and open-source software as significant sources of security issues. This situation is further complicated because over half of companies incorporate contractors and third-party developers into their development processes, increasing potential risks.

Traditional application security approaches that primarily target vulnerabilities in open-source components, such as software composition analysis (SCA) tools, are no longer sufficient. Modern threats require broader security measures that cover all software types and development participants, necessitating a comprehensive approach to software supply chain security that includes monitoring and verifying software integrity across the SDLC, and implementing secure development practices.

To enhance security in internally developed and open-source software, application security teams should adopt a holistic strategy that includes consistent monitoring, lifecycle integrity checks, and the fostering of secure coding practices among all contributors, whether internal or external.

ReversingLabs NVD Analysis 2022: A Call to Action on Software Supply Chain Security

LEARN MORE IN OUR SPECIAL REPORT

CONTINUED FROM PAGE 4

THE MODERN APPROACH TO SOFTWARE SUPPLY CHAIN SECURITY

Software supply chain security is a problem that can't be solved using traditional application security tools alone. It's about preventing malware from getting into the supply chain that you use to create software, so you need to think holistically about the end product — the entire compiled package — whether you're deploying it to the cloud, a container, or inside a data center.

The goal: Go beyond trust, and validate that the deployable package is free of malware on a consistent and repeatable basis as part of your CI/CD pipeline.

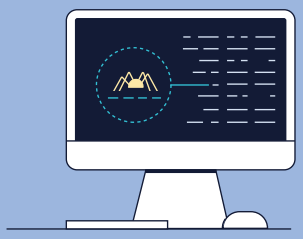
- **Look beyond the day-to-day gyrations of examining your source code, open-source code, third-party packages, and build systems.**
- **Focus on the entity that your supply chain is creating.**
- **Evaluate your complete application package as a whole, in addition to evaluating the individual pieces of it. The critical point for this check should come at the post-compilation / pre-deployment stage.**
- **Review the analysis to identify which behaviors the package is designed to do — and compare them with what the program actually does.**

It's not about doing a runtime analysis to see what the application is doing from a functional standpoint — you're programmatically reverse engineering it down to the most granular level to say, "Here's everything this application does. Is this what's expected?"

Organizations are struggling to keep ahead of software development security issues

Eighty-seven percent of respondents said they have detected issues in their software supply chain in the last 12 months, and 65% said their software supply chain security strategies need to catch up.

87 **Percent of IT pros who say their companies have detected security issues in their supply chain in the last 12 months**



These numbers underscore the need for stringent security measures and increased visibility. Security in the final software package or container, deployed in production or delivered to customers, is crucial and should be the prime focus of any security strategy.

Binary analysis is key to addressing these concerns. This approach goes beyond surface-level scrutiny, diving deep into all software aspects, including dependencies, components added during automated builds, installation software, and even non-executable files. It provides a comprehensive software bill of materials (SBOM), which — when done right — is critical in understanding and managing security risks. An SBOM provides a complete inventory of components, libraries, and modules used in building a software product, serving as a tool for understanding and managing security risks in software supply chains.

Binary analysis is key to addressing these concerns. This approach goes beyond surface-level scrutiny, diving deep into all software aspects, including dependencies, components added during automated builds, installation software, and even non-executable files.

In the face of the immense complexity of modern software packages, having a tool that excels at large, complex package analysis is non-negotiable. Organizations must ensure that every part of their software systems, no matter how intricate or extensive, falls under the lens of security scrutiny. Organizations must strike a balance between the speed of software development and the deliberation of application security.

Application security tools must integrate seamlessly into the continuous integration/continuous delivery (CI/CD) pipeline. They should be agile, offering real-time feedback and immediate remediation of issues to stay ahead in the ongoing pursuit of software security.

CONTINUED

CONTINUED FROM PAGE 5

GO BEYOND VULNERABILITIES: FOCUS ON MALWARE

The other key focus change should be shifting from vulnerabilities to malware.

Malware can be very difficult to find — especially if you do not have a tool that can focus on behaviors — but it does exhibit some key "tells," including:

- **Privilege escalation.**
- **Opening port or socket connections.**

When those behaviors aren't part of the application's architecture, you know you could have a malware problem.

NEXT STEPS FOR A MATURE SOFTWARE SUPPLY CHAIN SECURITY APPROACH

Do you feel that you have an effective program to identify all malware in the software you develop and release? If you're among the 65% of practitioners who say their supply chain security program is behind where it should be, you should:

- **Stop thinking only about the individual components of application security.**
- **Start thinking about your application security as a whole.**
- **Invest in the right tools to have a mature software supply chain security approach.**

By taking these steps, you can effectively manage the risk coming from the software your company develops or depends on.

65

Percent of IT pros who say their organizations do not have a mature software supply chain security program

Sixty-five percent of survey respondents acknowledged that their software supply chain security initiatives aren't where they need to be. The survey shows a striking convergence in the concerns of both security teams and developers, hinting at an untapped synergy. Further, there's a noticeable divide between security and DevOps teams. That could be linked to the torrent of reported security issues or critical vulnerabilities, which can lead to developer burnout and additional workload.

Managing software supply chain risk requires more than merely detecting threats. Organizations need to have a system that identifies threats and makes security remediation accessible and achievable for development teams. Carefully designed policy controls can provide a structured roadmap for continuous improvement, helping teams know where to start and how to proceed to reduce remediation noise and prioritize what matters most.

One often neglected aspect of managing software supply chain risk is sensitive data such as passwords, API keys, credentials, and certificates. Prioritizing the remediation of exposed secrets, with the help of contextually relevant intelligence feeds, can considerably reinforce an organization's overall security posture. Prioritization of secrets is an example of how security teams can render remediation more effective for developers. While detection tools can easily discover thousands of secrets in a software package, a lengthy to-do list is more likely to be ignored entirely due to its overwhelming nature. When organizations use threat intelligence to provide context, developers are presented only with the secrets they can act upon, making the process more manageable and efficient. Secrets management is a key feature of open source software repositories such as GitHub, GitLab, Bitbucket, SourceForge, and DockerHub.

Finally, organizations should leverage automation to enforce risk-based policy controls and tracking changes in their security posture. Customization features that allow for the specification of scan targets, alert prioritization, and remediation roadmaps can greatly enhance the efficiency and effectiveness of software supply chain security programs. The aim should be to create a proactive, responsive, and resilient security ecosystem that continually adapts to evolving threats.

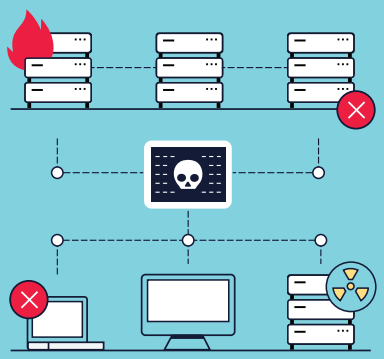
The State of Software Supply Chain Security 2022-23

LEARN MORE IN OUR SPECIAL REPORT

END

Supply chain security presents enterprise-wide risks

Eighty-eight percent of organizations recognize software supply chain security as an enterprise-wide risk, so solutions should cater to the needs of multiple teams. That means delivering the necessary data to various systems and processes, enabling each team to confidently contribute to maintaining customer trust, accepting external software safely, accelerating threat responses, and simplifying audit and compliance efforts.



Percent of IT pros who say software supply chain security presents an enterprise-wide risk to their organizations

88

HERE'S HOW SIX DIFFERENT TEAMS SHOULD USE THIS APPROACH:

- **DEVELOPERS** should proactively resolve security policy violations and safeguard against exposed secrets.
- **APPLICATION SECURITY TEAMS** should preemptively detect supply chain threats such as malware and unauthorized updates.
- **IT PROCUREMENT AND THIRD-PARTY RISK TEAMS** should rigorously assess pre-acquisition risks and compliance.
- **IT/OPERATIONS TEAMS** should scrutinize software packages or containers before deployment and evaluate the risk impact of any modifications.
- **SOC TEAMS** should be responsible for swift isolation and response to post-deployment breaches.
- **RISK AND COMPLIANCE TEAMS** should use analytical data to handle inquiries from auditors, customers, and regulators efficiently.

Effective software supply chain security hinges on cohesive action by all six teams that is underpinned by a robust security solution.

Software Supply Chain and the SOC: End-to-End Security is Key

LEARN MORE IN OUR SPECIAL REPORT

4 steps to a mature software supply chain security approach

Enterprises are grappling with an increasingly complex and evolving cyber threat environment. The gravity of this situation is reflected in the fact that nearly three quarters of organizations believe that traditional application security solutions are ineffective against software supply chain threats, and more than half admit that their software supply chain security programs aren't where they should be. These organizations must reevaluate their current strategies and shift toward more comprehensive and adaptable security measures.

The software supply chain is more than just a series of tools and components. It represents the intersection of relationships between developers, vendors, security, and users. Consequently, security in this context is more than merely vulnerability management. It requires a proactive, holistic approach with comprehensive visibility into supply chain risks, consistent threat remediation, and enterprise-wide risk management. Here are four things that every organization should do now:

1 RECOGNIZE THAT SOFTWARE SUPPLY CHAIN SECURITY IS AN ENTERPRISE-WIDE RESPONSIBILITY

Eighty-eight percent of survey respondents acknowledged this, underscoring the need for a solution that supports the requirements of multiple teams and that integrates seamlessly into various stages of software development and deployment.

2 ENHANCE SECURITY ACROSS ALL TYPES OF SOFTWARE — INCLUDING INTERNALLY DEVELOPED SOFTWARE

More than 50% of companies rely on contractors and third-party developers to create software used internally, further complicating the security landscape. Therefore, effective security measures should cover these areas and include binary analysis tools to assess risks in open-source, third-party, or proprietary software and dependencies.

3 CREATE A DETAILED SBOM AND LEVERAGE AUTOMATION

Automated systems can enforce risk-based policy controls for individual SBOM components, track changes in security posture, and simplify audit and compliance efforts (as long as you create the SBOM from the release binary—not just the developer's code—so nothing gets missed). Doing so increases efficiency and allows teams to focus more on strategic initiatives than routine tasks.

4 UNDERSTAND THE IMPORTANCE OF REMEDIATION IN MANAGING SOFTWARE SUPPLY CHAIN RISK

Detection is only the first step; consistent remediation of detected threats is equally critical, if not more so. Tools that provide structured roadmaps for continuous improvement and secrets management can significantly bolster an organization's overall security posture.

Understanding the Requirement for Software Bill of Materials in Executive Order 14028

LEARN MORE IN OUR WHITEPAPER

Enterprises must adopt a proactive, comprehensive software supply chain security approach. By enhancing security measures, implementing a detailed SBOM, leveraging automation, focusing on remediation, and staying informed about the latest industry developments, organizations can build a resilient and adaptable security ecosystem that's ready to take on software supply chain threats.

TAG Cyber's take

Enterprises today face an increasingly complex and evolving cyber threat landscape. The prevalence of software supply chain attacks and the recognition that traditional application security solutions often fall short in protecting against these attacks necessitates a shift in strategy. TAG recommends adopting a proactive, holistic approach to software supply chain security that goes beyond vulnerability management and detection to include comprehensive visibility into supply chain risks, consistent threat remediation, and an enterprise-wide approach to risk management.

Enterprises should enhance security measures across all software types, including internally developed and open-source software. This includes, but is not limited to:

- **INTEGRATING** robust security practices into the software development lifecycle,
- **USING BINARY ANALYSIS** for comprehensive risk assessment,
- **IMPLEMENTING** a detailed SBOM to track software components.

Also, the importance of automation in enforcing risk-based policy controls, monitoring changes in security posture, and simplifying compliance efforts cannot be overstated. And finally, consider working with firms like ReversingLabs for expert insights and to stay updated on the latest threats, keep up with best practices in software development, and gain the expertise needed to help build a resilient and stronger software supply chain.

ReversingLabs Fills the Gaps

ReversingLabs can help fill these technology gaps by providing a software supply chain security solution with the following critical capabilities:

WORLD'S LARGEST ATTACK INTELLIGENCE REPOSITORY:

Over 14 years of experience aggregating malware / goodware privately based on 46 AV scanners and a threat intel platform that adds 8M+ per day.

PROPRIETARY RECURSIVE BINARY ANALYSIS:

Extensive coverage of binary formats. Unpacks, deobfuscates, extracts metadata, and classifies down to the lowest level. Unpacks more than 400 file formats to create the most comprehensive SBOM. Identifies more than 4,800 file types (JAVA, .NET, Python, Mac OS, Linux, MS Office, PDF, Docker, etc.) for malware detection.

INDUSTRY-LEADING ANALYSIS SPEED OF LARGE, COMPLEX SOFTWARE PACKAGES:

Analyzes the largest proprietary and open-source complex files in seconds – 10GB+ files at 10M files per day – enabling frictionless release and deployment.

COMPREHENSIVE SOFTWARE RISK VISIBILITY AND PRIORITIZATION:

Provides the most comprehensive software risk visibility of malware, tampering, differential behaviors, secrets, certificate misconfigurations and dependencies to prioritize remediation, release, deployment and decision making.

EXTENSIVE POLICY AND SOFTWARE SUPPORT:

Includes detection, prioritization, remediation, validation, and interactive reports and search. Customized policies for different projects, applications, and individual components.

END-TO-END DEVELOPMENT, SOC AND RISK TEAM SUPPORT AND WORKFLOWS:

Democratizes software decision making across teams, enabling development and application security teams to safely release, IT and procurement teams to securely deploy, the SOC to detect, isolate and respond, and risk and audit teams to comply with internal and external standards and mandates.

An end-to-end software supply chain security solution is the next evolution of application security, and is fast on its way to becoming a standard part of the most widely respected cybersecurity frameworks. The time for development, security operations, and third-party risk management teams to embrace that change with ReversingLabs is now.

DO YOU TRUST YOUR SOFTWARE?

Uncover the unknown with a free software analysis

START A FREE TRIAL

Worldwide Sales:
+1.617.250.7518
sales@reversinglabs.com