REVERSINGLABS

Software Supply Chain Security for Application Security Teams

Controlling Complex Releases

Introduction

Software supply chain attacks are an efficient and stealthy means for cybercriminals and nation-state adversaries to gain access to thousands of targets that are customers of a single software provider.

Software supply chains exist because development teams use agile development practices, continuous integration and delivery (CI/CD) technologies, and DevOps automation techniques to assemble applications from a myriad of software components. These software components come from many different suppliers, including internal development teams, open-source package repositories, third-party organizations, and commercial packages or platforms.

1000s

of targets that are customers of a single software provider

Attacks can happen at

ANY

stage of software development, assembly, and delivery

Attacks can involve

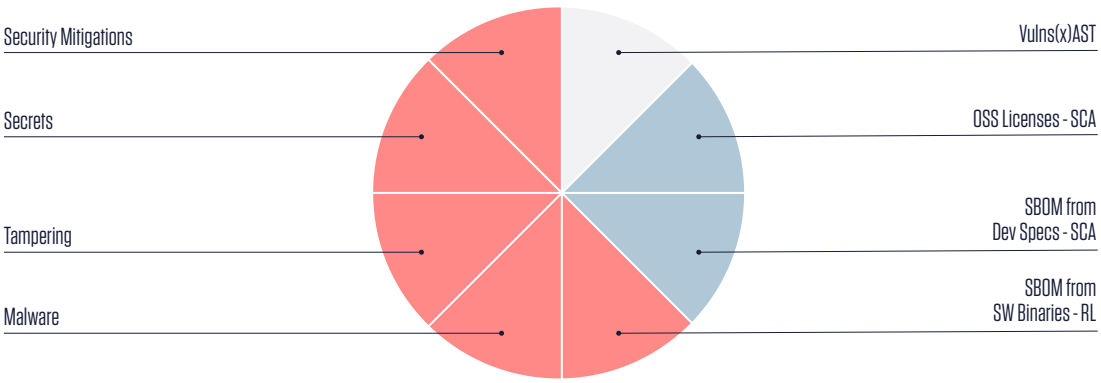
ANY

type of software components and non-executable files within the final software release package

Recent supply chain attacks & breaches of large-scale campaigns such as CircleCI, Solarwinds, CodeCov, and more prove attacks can:

- Happen at any stage of software development, assembly, and delivery
- Involve any type of software components and non-executable files within the final software release package

The fact that successful attacks keep happening is evidence that software supply chain security is a very different problem to solve than helping developers to write less vulnerable source code.



Software Supply Chain Security Is Not Vulnerability Management

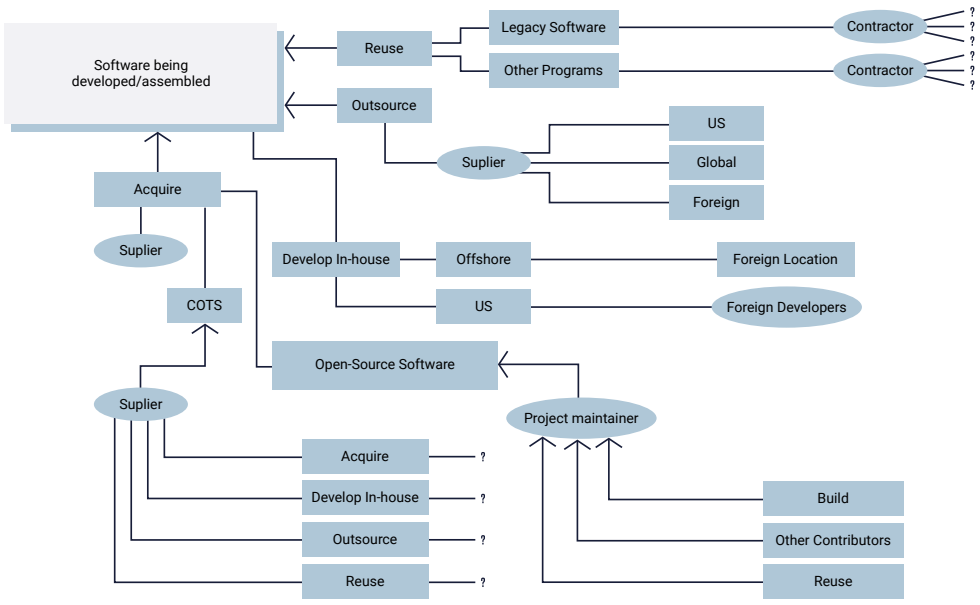
Software supply chain attacks focus on introducing threats into a software release that can independently act once the package is deployed in production or customer environments. Introduced threats can range from overtly malicious (e.g., inserting known malware) to more subtle additions of software behaviors or permissions that appear to be part of normal application operations. If this malicious software tampering is digitally signed and released by the software producer, then no amount of signature validation or hash checking will indicate that anything is wrong. Given this attack pattern, it should be clear that helping developers write more secure code (i.e., with few vulnerabilities) is very different from checking software components and packages for active threats inserted by a malicious actor.

Attacks on Open-Source in Public Repositories

Tricking developers into using malicious open-source packages or updates from public repositories has become an effective way to spread malware through a software supply chain. Nearly 7,000 malicious packages were uploaded to the npm open-source repository between January and October of 2022 – almost a 100% increase over the 75 malicious packages discovered in 2020.[1] The volume will only increase as attackers launch more large-scale campaigns such as “IconBurst” or “CuteBoi” to automate hundreds of malicious uploads

Stealthy CI/CD Tampering Evades Traditional Application Security Testing

Attacks on developers’ credentials, CI/CD environments, and workflows pose a unique set of challenges to developers and application security teams. While software's source code can be checked for vulnerabilities or flawed coding patterns in a developer’s IDE or during code reviews, most software is distributed as compiled binaries. This is often completed without any checks to verify the software’s integrity or high-risk exposures, such as authentication credentials, source code files, or other intellectual property. This gap in threat detection encourages malicious attacks against software delivery infrastructure and processes where visibility is limited.



Software’s Attack Surface Is Enormous & Complex.

The attack surface of software releases is often more significant than most development and application security teams realize. Release packages and containers can:

- Have thousands of executable components with many layers of dependencies from internal, open-source, third party, and commercial suppliers – often beyond the discovery scope of many software composition analysis tools
- Contain several gigabytes of non-executable files where malware can reside yet remain unexamined by source code analysis or dynamic vulnerability scanners or penetration tests.

Sources:

[1] ReversingLabs Report: The State of Software Supply Chain Security 2023 | https://www.reversinglabs.com/reports/state-of-supply-chain-security-22

ReversingLabs Software Supply Chain Security

ReversingLabs provides a unified platform for understanding and managing risks arising from your software portfolio's supply chains. It automates and integrates software testing, policy controls, risk-based prioritization, and auditing at various stages of software development and delivery. It creates a single point of reference for software supply chain security across all applications and projects, which empowers the collaboration between development and security teams required to deliver trusted software at DevOps speeds.

How ReversingLabs Addresses The Security Gaps

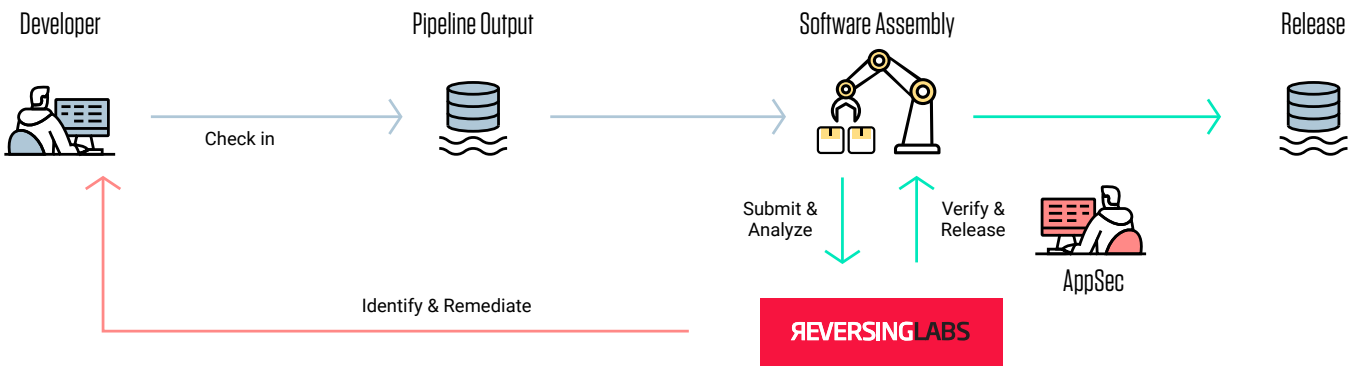
Comprehensive Visibility - Delivers unparalleled insight into a wide range of active threats (e.g., malware, tampering, malicious or risky software behavior changes) and high-risk exposures (e.g., security mitigations, authorization secrets, source code, intellectual property) that are not always visible in source code

Industry-leading Detection. Provides better detection of malicious components and files than any other method by using unique threat intelligence curated from billions of files harvested continuously for 10+ years.

Suspicious Behavior Identification – Uncovers unwanted or unexpected changes in software behaviors across multiple software builds, which is the only means of detecting stealthy attacks on CI/CD environments, pipeline automation, and highly targeted or new malware.

SBOM & Prioritized Risks - The only interactive SBOM that reports and prioritizes active supply chain threats, exposures, and supply chain security policy failures for every component and dependency and also verifies third-party and open-source component integrity with comparisons against trusted binary repositories.

Policy Customization - Create custom policies to locate and prioritize threats and risks specific to your environment, application threat models, and even individual software components while also enforcing consistent security standards.



People, Process, Technology Section

People:	Process:	Technology:
Dev and AppSec can collaborate to: **Eliminate threats** Release software that maintains customer trust **Protect integrity** Fortify CI/CD workflows and build systems against tampering and software supply chain attacks **Improve quality** Minimize exposures that can lead to future attacks	**Submit & Analyze** Rapidly analyze software binaries, containers, open-source libraries, and third-party software for threats **Identify & Remediate** Find and fix threats and high-risk exposures buried deep within layers of software dependencies **Verify & Release** Confirm security quality with custom approval policies and release safely to production and customer environments	**Depth of coverage:** open-source, third-party, outsourced, proprietary, internal, and commercial components in the largest, most complex software releases or containers **Breadth of visibility:** malware, tampering, newly added malicious or risky behaviors, security mitigations, code signing issues, and secrets exposure introduced through software supply chains **Automation:** Integrates with the majority of CI/CD, Cloud and ITSM tools

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 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.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com