

HOW TO SECURE THE SOFTWARE SUPPLY CHAIN



Software supply chain attacks have seen triple-digit increases, but few organizations have taken steps to evaluate the risks of these attacks.

61%



of U.S. businesses were directly impacted by a software supply chain attack in the 12-month period ending in April 2023.

60%



of organizations procuring mission-critical software solutions will mandate SBOMs by 2025, up from less than 20% in 2022.

90%



of SCA tools will be able to generate and verify SBOMs to help securely consume open-source software, up from 30% in 2022.

Source: Gartner

AND THE SUPPLY CHAIN IS VULNERABLE IN THESE WAYS



Limited Visibility and Control

Many organizations are using multiple disparate security tools, making it almost impossible to gain full visibility across their software supply chain.



Operation Complexity and Overhead

Meeting today's expected time-to-deliver of new software versions on a daily basis across the globe is challenging.



Growing Attack Surface

Malicious actors target the software supply chain at each step of the development lifecycle, even in the runtime environment.



Open Source Software Risks

Open source is highly accessible and used by organizations of all sizes and industries, making this a direct target for threat actors.



Friction Between Development And Security Teams

Security incidents can fall through cracks and may not be identified or remediated in a timely manner.

WHAT TO DO?



HERE ARE 6 STEPS TO SECURE THE SOFTWARE SUPPLY CHAIN



1. Curate open-source package entering your organization



2. Scan packages (SCA) for open source vulnerabilities in both source code and binary files



3. Analyze proprietary or first-party code (SAST)



4. Reduce false positives and vulnerability noise with contextual analysis



5. Detect potential security issues in your configurations and usage of open-source libraries in code



6. Protect your business applications from critical vulnerabilities in runtime environment

TRANSFORM YOUR APPROACH TO SOFTWARE SUPPLY CHAIN SECURITY

with **actionable insights** from the JFrog Software Supply Chain State of the Union 2024 report, **backed by insights from 1,200+ industry leaders.**

Get the report →

