ACCELERATE YOUR SOFTWARE BILL OF MATERIALS JOURNEY WITH THE JFROG DEVOPS PLATFORM

The World Economic Forum cites cybersecurity threats among top the global risks as infrastructure attacks, fraud, and digital safety harm public trust in digital systems and increase costs for stakeholders.

With 98%[1] of organizations reliant on open source software, customers are demanding software bill of materials (SBOM) for greater transparency and to audit their systems for risk. Government entities in the US and EU require these disclosures and today, 82%[1] of organizations are either consuming SBOMs in production or are planning to in the next 6 to 24 months. And while SBOMs are a necessary foundation, to secure your software supply chain (SSC) with speed and flexibility other key elements are required.

To be ready for what's next, software producers must generate comprehensive, machine readable SBOMs as part of their SSC automation. Central artifact management with rich metadata, along with deep scanning for transitive dependencies in third-party components, enables risk management across the entire SDLC for all segments of the business.

KEY TAKEAWAYS

- ✔ Government regulations, such as the Cybersecurity Act require SBOM disclosures

- ✔ 82% of organizations are planning to consume SBOMs in the next 6 to 24 months

- ✔ SBOM generation requires key metadata from all components across development pipes

- ✔ JFrog helps organizations take SBOMs to the next level with advanced metadata capture and automation

CHALLENGES TODAY:
BUILD TRUST INTO EVERY DELIVERY WITH EVIDENCE

AUTOMATING SBOM PRODUCTION EVERYWHERE

Tracking provenance of all components in every pipeline requires centralized management of software artifacts under a single system that captures expansive and detailed metadata. Only when every asset is managed through a single system can organizations identify all the transitive dependencies in third-party components and export required data in a compliant SBOM automatically or on demand.

MITIGATING RISK WITH DATA

Building security and compliance enforcement into your DevOps automation is only possible through deep, actionable data about your software. The right systems are required to capture, ingest, augment, and action SBOM data to enforce compliance with your organization's open source security and license policies as well as remediate zero-day issues rapidly across your entire SSC.

MEETING TODAY'S REQUIREMENTS... AND TOMORROW'S

SBOMs must be generated in a set of commonly accepted standards. Today, SPDX and OWASP's CycloneDX are two of the most commonly used and preferred machine-readable SBOM formats. However, evolving regulations and a shifting security landscape may soon require additional rich contextual metadata around workflows, approvals, and developer information that augments standard SBOMs.

HOW THE JFROG CAN HELP:
COMPREHENSIVE INSIGHT INTO SOFTWARE COMPONENTS

BRING VISIBILITY AND CONTROL TO EVERY BUILD

Create operational consistency by managing all software component artifacts through JFrog Artifactory repositories, the industry standard binary management solution with native support for 30+ package and artifact types. Rich Artifactory metadata tracks the provenance, lineage, and use of every software component, creating the foundation for SBOM reporting in every SSC pipeline.
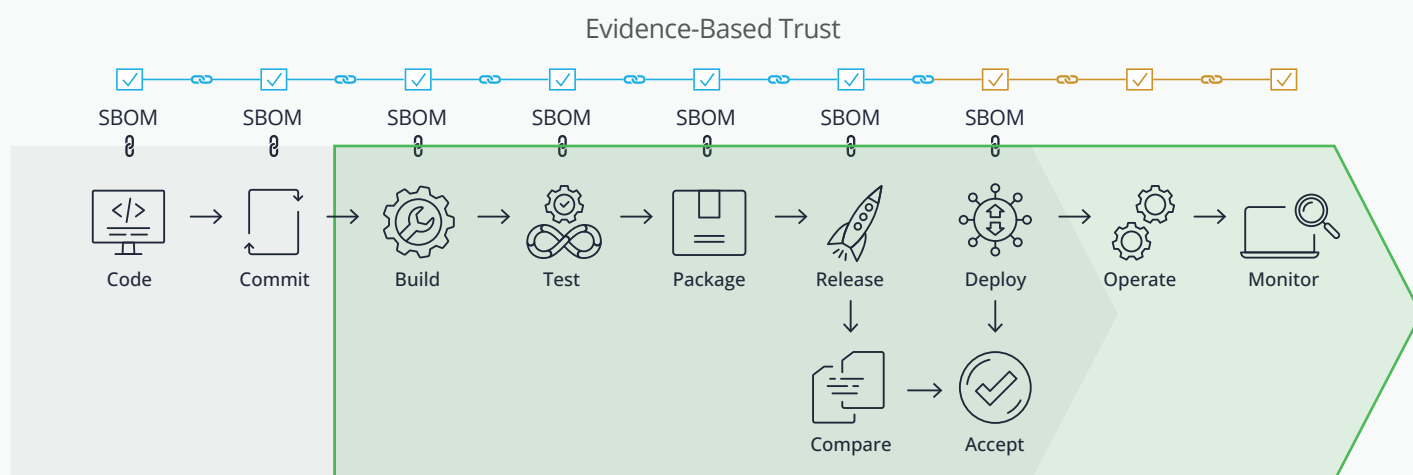
REVEAL DEPENDENCIES IN THIRD-PARTY COMPONENTS WITH TURNKEY SBOMS

Penetrate the opacity of third-party party components with deep binary scanning to uncover all transitive dependencies and their known vulnerabilities for complete SBOM reporting. Automate production of SPDX and/or CycloneDX SBOM reports and build regulatory and customer compliance into every step of software releases.

PROTECT AGAINST SECURITY AND LICENSE RISKS GLOBALLY

Put SBOM metadata to work to automatically identify all vulnerable components, enforce organization-wide license and vulnerability policies. Swiftly trace the blast radius of zero-day issues in your SSC for active remediation. Through JFrog's hybrid and multi-cloud capabilities, global teams can collaborate seamlessly using the same artifacts and SBOM metadata for a consistent security posture.

LEVERAGING SBOMS FOR SSC INTEGRITY

Evidence-Based Trust

SBOM   SBOM   SBOM   SBOM   SBOM   SBOM   SBOM

Code → Commit → Build → Test → Package → Release → Deploy → Operate → Monitor

Release → Compare → Accept ← Deploy

Secure & Hardened Build and Distribution Infrastructure

JFrog

With the JFrog DevOps Platform, you can unify, accelerate, and secure your software delivery, from development to distribution. The JFrog Platform offers deeper Dev, Sec, and Ops integration, in a flexible, and expandable platform that delivers increased security, visibility, and control on-premise, in the cloud, and at the edge.

---

[1] Source: Linux Foundation, Software Bill of Materials (SBOM) and Cybersecurity Readiness January 2022

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.

LEGAL STATEMENT

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd

Request your personalized Artifactory demo at jfrog.com/demo