



JFROG SOFTWARE SUPPLY CHAIN PLATFORM

Secure Manufacturing from Code Commit to Factory Floor



Modern manufacturing runs on software, firmware in PLCs, containerized factory automation, embedded IoT sensors, AI-powered quality control. Each is part of your software supply chain. Each is a potential attack vector. And for the fifth consecutive year, manufacturing is the most-attacked industry on the planet.

The JFrog Software Supply Chain Platform provides DevOps and AppSec teams with the end-to-end visibility, security, and control needed to govern every artifact that ships, from developer workstation to production line controller, without slowing down engineering velocity.

27.7%

Of all cyberattacks target manufacturing

IBM X-Force 2026

61%

YoY ransomware surge in manufacturing

KELA 2025

30%

Of breaches via third-party software

Verizon DBIR 2025

282%

ROI with JFrog Platform

Forrester TEI 2026

THE CHALLENGE

Unique Challenges in Manufacturing

No Single Source of Truth

Artifact Governance



Acquisition-driven growth leaves engineering organizations with fragmented artifact stores across dozens of incompatible systems. Build drift between environments is inevitable. SBOMs require days of manual assembly. No one can answer with certainty: what exactly shipped in last quarter's firmware release?

CVE Noise without Context

Vulnerability Management



A single embedded firmware build generates thousands of CVE findings. Without applicability context, whether a vulnerable function is actually called in the specific build, security teams either chase false alarms or deprioritize alerts entirely. The genuinely critical issues get buried.

Unverified Software Delivery

Distribution & Integrity



Pushing firmware updates to remote facilities, air-gapped OT environments, and constrained industrial networks without cryptographic signing provides no chain of custody. Teams cannot confirm that what arrived at a production controller matches what the build system produced.

The Platform Built for What Manufacturing Security Actually Demands

JFrog ARTIFACTORY

The gold standard for managing the lifecycle of software artifacts, containers, and ML models, with native support for over 60 different package technologies.

JFrog DISTRIBUTION

Extend your circle of trust to the last mile of software delivery and take software to the ideal location for optimal consumption.

JFrog CONNECT

Bring enterprise DevOps and security practices to IoT development to manage IoT fleets and software updates at scale.

JFrog CURATION

Defend your software supply chain with automated, proactive blocking of malicious or risky open-source packages and ML models.

JFrog XRAY

Identify and resolve open source vulnerabilities and license compliance issues in your software and models with DevOps-centric security.

JFrog ADVANCED SECURITY

Take supply chain security to the next level with software supply chain security exposure scanning, code scanning, and contextualized impact analysis.

JFrog RUNTIME

Get real-time visibility into runtime vulnerabilities at the package level, prioritize potential threats and quickly identify its source and developer for fast remediation.

JFrog ML

Go from idea to production with the all-in-one solution to build, deploy, manage and monitor all your AI workflows, from GenAI and LLMs to classic ML.

JFrog is the leading Software Supply Chain Platform

83%
Fortune 100

7400+
Customers

Why Manufacturing Organizations Choose JFrog

One Platform. No Integration Overhead.

Point solutions require integration, maintenance, and create coverage gaps at the seams. JFrog provides artifact management, SCA, secrets detection, IaC scanning, SBOM generation, curation, and distribution in a single data model, with consistent policy enforcement across every environment from developer workstation to production OT system.

Built for the Complexity of Manufacturing Scale

JFrog supports organizations with 50,000+ developers across multiple acquired engineering teams, global site replication, and firmware delivery to thousands of edge controllers. The platform was designed for this operational scale, not retrofitted to it.

Conan for Embedded C/C++ — the Most Underscanned Ecosystem in Manufacturing

Most security platforms have no native support for Conan, the package manager used by teams building firmware and embedded software. JFrog is the only platform with first-class Conan support, bringing the same governance model applied to Docker and Python to the C/C++ ecosystem.

Air-Gapped and OT-Ready

JFrog Edge nodes are designed for the constrained, intermittent-connectivity environments that define OT networks. Artifact delivery doesn't depend on central infrastructure availability, remote production sites remain operational regardless of WAN status.

Compliance by Design

IEC 62443, NIST SP 800-82, EO 14028 SBOM mandates, and sector-specific regulations (FDA, ISO/SAE 21434, UN R155) are addressed through immutable artifact storage, automated SBOM generation, build traceability, and evidence-based policy gates, not manual compliance exercises.

How Manufacturing Teams Deploy JFrog



Consolidating Artifact Management Across Acquired Engineering Organizations

Manufacturers that grow through acquisition inherit incompatible artifact stores, build conventions, and package approval processes. JFrog Artifactory replaces this fragmented landscape with a single source of truth, every team pulls from the same verified images, containers, and packages. Acquired teams onboard into a documented, enforced standard from day one. Build reproducibility is guaranteed. SBOMs are generated continuously rather than assembled manually.

Eliminating Alert Fatigue in Firmware and Embedded Software Security Programs

A single firmware build can surface thousands of CVE findings. Without applicability context, security teams either chase false alarms or deprioritize alerts, both of which leave real vulnerabilities unaddressed. JFrog Xray's contextual analysis determines whether a CVE is reachable in the actual build environment, reducing the actionable remediation list to the findings that genuinely matter. Teams move from reactive triage to proactive, prioritized remediation.

Securing Firmware Distribution to Remote Facilities and Air-Gapped OT Environments

Global manufacturers pushing firmware updates to production line controllers at remote sites face a distribution problem that standard DevOps tooling wasn't designed to solve. JFrog Release Bundles provide cryptographically signed, immutable units of software promotion with a provable chain of custody from build system to target environment. JFrog Edge nodes deployed at remote facilities maintain local artifact caches that operate independently of WAN availability, ensuring continuous operations even in constrained OT network environments.

Governing AI/ML Models in Smart Manufacturing Environments

Manufacturing organizations using AI for predictive maintenance, computer vision quality control, or autonomous material handling are frequently consuming open-source models from public repositories without any formal governance process. JFrog's AI Catalog proxies Hugging Face and other public model repositories through governed internal infrastructure, scanning every model and its dependency chain before it reaches a production environment. AI-BOM generation ensures every model promoted to a production system has a documented provenance and security posture.

Audit-Ready by Default

Every binary that moves through JFrog carries its own evidence trail: a CycloneDX or SPDX SBOM generated at build time, a signed provenance record tying it to source and build environment, and an immutable log of every promotion, scan result, and policy decision applied to it. When an auditor asks what shipped, when, with which components, and against which controls, the answer is a query, not a fire drill. The same evidence stream satisfies IEC 62443 lifecycle documentation, EO 14028 SBOM attestations, ISO/SAE 21434 and UN R155 traceability obligations, and FDA premarket cybersecurity submissions, one system of record, many regulatory outputs.

Get Started with the JFrog Platform

[Learn More](#)[Start a Trial](#)[Speak to an Expert](#)

v1.0220620

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

Copyright © 2025 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.



www.jfrog.com



www.x.com/jfrog



www.facebook.com/artifrog/



www.linkedin.com/company/jfrog-ltd



Request your personalized Artifactory demo at jfrog.com/demo