



# JFrog Security

## SOLUTION SHEET

# Holistic DevOps-Centric Security for Trusted Software Supply Chains



### THE CHALLENGE

Securing your software supply chain is an increasingly complex problem with evolving attack methods and a mix of security point solutions, which can leave you with security blind spots and gaps across your supply chain. DevOps and security professionals are left to figure out how to maintain development speed without sacrificing the trust in your releases. Ensuring developers have integrated security automation and knowledge at their fingertips is the panacea of secure software delivery at the speed of DevOps.

### THE SOLUTION

JFrog's Software Supply Chain security integrates advanced security automation and know-how directly into DevOps workflows, enabling teams to deliver trusted software faster. JFrog fortifies your software supply chain with OSS package curation, source code security, enhanced SCA, secrets detection, container and IaC Security and spans your entire pipeline from code to release.

### THE BENEFITS

#### See what no one else sees

Drive cross-team cooperation and trust centered on deep security research that automatically delivers unparalleled visibility into issues, their impact, and actionable advice for developers.

#### Find, fix & fortify

Sharpen developer focus with prioritized, contextual remediation advice that identifies what matters most to ensure you're protected.

#### Secure from one place

Execute with confidence, taking holistic action across code, configurations, and binaries throughout your portfolio from a single platform.

## Hitachi Vantara



*Something that's going to scan everything in that central repository of truth, automatically, with zero customization required, that's really, really powerful...*

*The capabilities of Artifactory are what allow us to do what we can do today...With Xray, security is a no-brainer- it's built in, just turn it on, wow! I'll take that all day long.*



Larry Grill, DevSecOps Sr. Manager,  
Hitachi Vantara

#### Comply with confidence

Automate regulatory and governmental compliance tasks with all must-have actions for SBOM generation, sharing, and reporting out of the box.

#### Protect against malicious activity

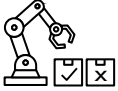
Stop security issues that arise post-code generation with binary-based analysis across the software supply chain, including in curation, dev, test, staging, and production.

#### Take intelligent action.

Know where vulnerabilities live, and deploy fixes across your portfolio with integrated binary management and distribution capabilities based on complete lifecycle metadata.

## THE JFROG SOLUTION

JFrog Security and the JFrog Platform intelligently identify significant supply chain security issues that attackers use to compromise developers' processes, and application code with:



### Curate OSS packages entering your organization

Seamlessly prevent malicious or risky packages from being downloaded and used by any software development pipeline.



### Enhanced Software Composition Analysis (SCA)

Modern SCA to eliminate known CVEs in evolving software artifacts in repositories, builds, and containers across your software supply chain.



### Exposed secrets detection

Detect secrets left exposed in any containers stored in JFrog Artifactory to prevent any accidental leak of passwords, API keys, internal tokens, or credentials.



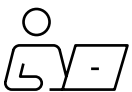
### Infrastructure-as-Code (IaC) Security

Secure IaC files stored in JFrog Artifactory for early detection of cloud and infrastructure misconfigurations that can be exploitable.



### Enhanced CVE remediation data

Speed mitigation with enhanced remediation for critical CVEs, enabling developers, DevOps, and security teams to understand more about how to easily & intelligently address vulnerabilities, often with simple code or configuration changes.



### Developer-oriented features

Security know-how is at their fingertips with Integration directly into the most popular IDEs, Docker Desktop, vulnerability scanning via CLI, and Frogbot scanner for discovering vulnerabilities in git repositories.



### Source Code Security Scanning (SAST)

Develop and commit trusted code with a seamless developer-focused source code scanning experience.



### Contextual CVE prioritization

Advanced container security analysis to identify and prioritize whether the open source software vulnerabilities are actually exploitable in your application – an industry first.



### Mitigate operational risk

Enable automated handling of open source software risks like package maintenance issues & technical debt.



### Insecure use of OSS libraries and services

Discover whether common OSS libraries and services are used or configured insecurely, causing exposure to attacks.



### Enhanced CVE data and severity assessment

Understand critical CVEs and learn additional insights to enable developers, DevOps, and security teams to understand issues across OSS and commercial environments. Driven by our dedicated security research team's advanced analysis.



### Security-oriented features

Make compliance a breeze with SBOMs out of the box, industry-standard SPDX and CycloneDX and new security UI screens, with all security scans shown in one place.

## HOW IS JFROG DIFFERENT?

JFrog's differentiated approach is to deliver a unified Platform that bridges the gap between Developers, DevOps and Security teams, driving a single source of record for software supply chain security. JFrog is uniquely positioned to intelligently unify these groups with the following key differentiating themes:



### Binary focus

The modern software supply chain has only one core asset delivered into production: the software binary. Therefore, today's attackers try to reverse-engineer, break or entice the shipment of compromised binaries. Because they contain more information than source code, JFrog's focus on the binary, reveals issues that are not always visible in source code.



### Security that really works for DevOps

Security teams set security strategies and compliance policies. Development teams build, remediate and manage code bases. Binaries, infrastructure, integrations, releases and flows all must be addressed to enable a DevOps-centric workflow that works for core DevOps teams, not just security and developers.



### End-to-End software supply chain coverage

DevOps becomes the security pivot point for organizations, since every process, and tool requires and incorporates security. JFrog Xray and the advanced security features are deeply integrated, allowing companies to unify, accelerate & secure their software delivery. An enterprise-grade offering, that supports cloud, multicloud and hybrid deployments and can even deliver to the edge/ IoT at any scale.



### Comprehensive coverage, including context

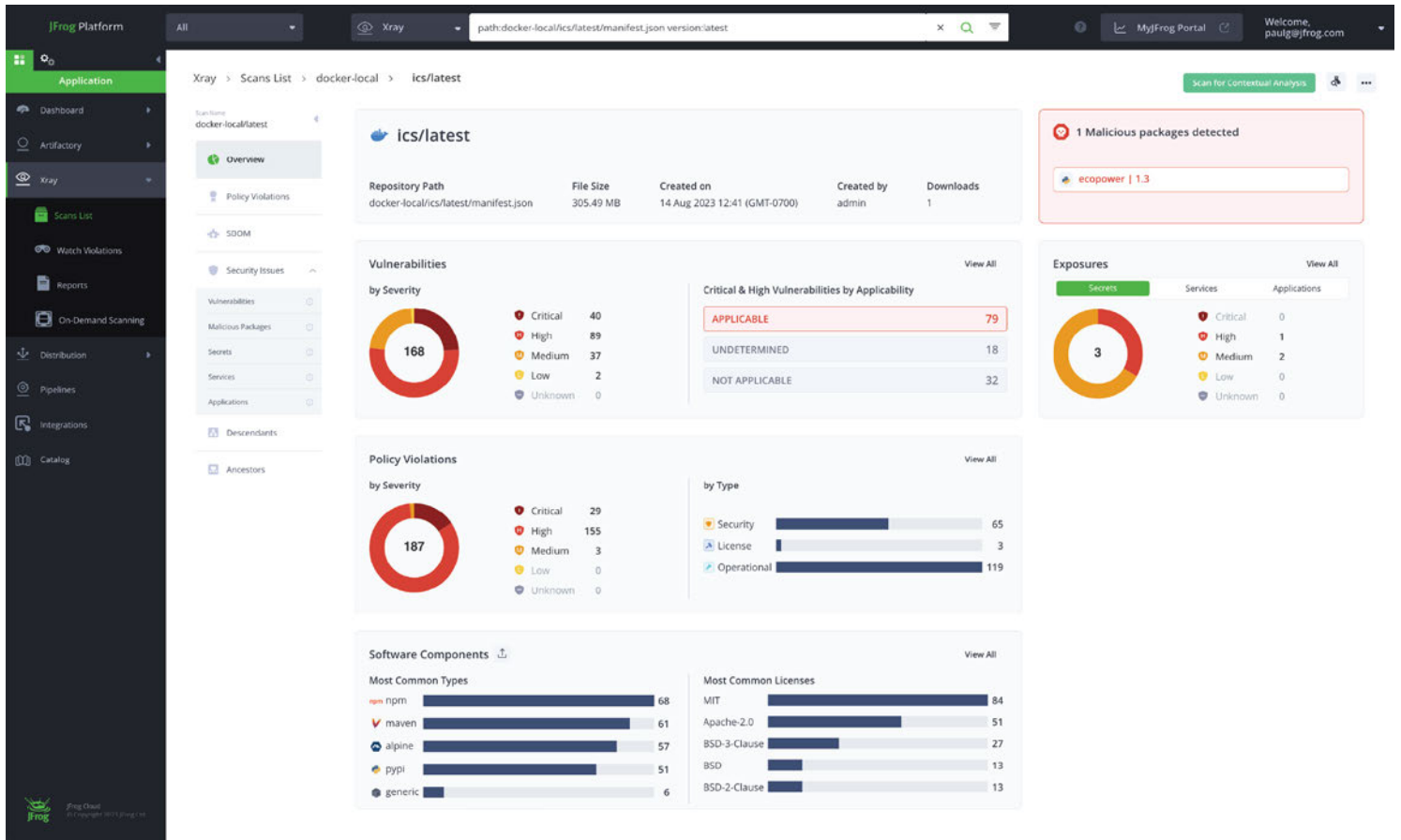
JFrog identifies OSS vulnerabilities, any OSS library misuse, insecure use of services, exposed secrets, IaC configuration issues, and identification of the applicability and exploitability of the most serious vulnerabilities in your application - all in a single platform. CVEs may or may not be exploitable depending on the application's configurations, reachability paths, and compile flags.



### Native integration with binary management

JFrog Artifactory manages all artifacts and repositories in one place, which becomes a single source of truth for an organization. Security becomes an easy process when you have control of your entire portfolio and are deeply integrated. Your single source of truth becomes a single source of trust.

# THE JFROG USER EXPERIENCE

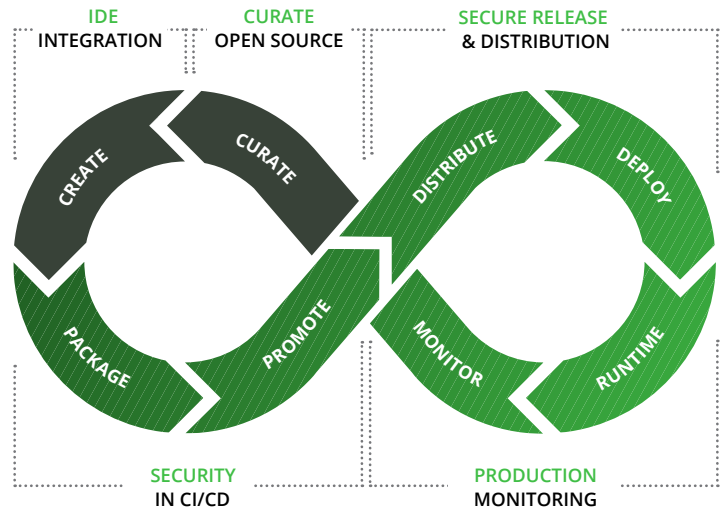


## ADDRESSING TODAY'S SECURITY CHALLENGES WITH A HOLISTIC APPROACH

**Deliver trusted software**, reduce risk and fortify your brand with strong protection from a broad range of security threats across the software supply chain.

**Innovate with speed and scale** while safeguarding your software and your customers. Make automated security a natural part of your SDLC workflows and minimize the effort required to identify, prioritize and fix vulnerabilities.

**Simplify compliance** with security regulations, standards, and internal policies by consistently implementing software security controls and best practices across your SDLC.



v2.0230826

### 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 Software supply chain Platform.

### LEGAL STATEMENT

Copyright © 2023 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.



Request your personalized Xray demo at [jfrog.com/xray/#book-a-demo](https://jfrog.com/xray/#book-a-demo)



[www.jfrog.com](https://www.jfrog.com)



[www.twitter.com/jfrog](https://www.twitter.com/jfrog)



[www.facebook.com/artifrog](https://www.facebook.com/artifrog)



[www.linkedin.com/company/jfrog-ltd](https://www.linkedin.com/company/jfrog-ltd)