

JFrog Introduces Zero-Touch Remediation to its Self-Healing Software Supply Chain, Broadening its Footprint through Secure Open-Source Partnerships

Broadcom, Chainguard, Echo, IBM, Red Hat, Moderne, TuxCare, and Seal Security partner with JFrog to deliver a unified, policy-driven pipeline for automated vulnerability resolution at agentic speed

SUNNYVALE, Calif. and NEW YORK — swampUP 2026 — September 2, 2026 — [JFrog Ltd.](#) (Nasdaq: FROG), creators of the [JFrog Software Supply Chain Platform](#), the system of record for trusted software artifacts, binaries, and AI assets, today introduced [JFrog Zero-Touch Remediation](#) and announced the initial partners in its [JFrog Self-Healing Software Supply Chain Security Ecosystem](#). Zero-Touch Remediation automatically finds the best available fix for a known vulnerability from any ecosystem partner and applies it through the customer's pipeline, without breaking a build, forcing a version update, or disrupting developer workflows. Together, JFrog and its ecosystem partners neutralize vulnerabilities before attackers can exploit them - shrinking the gap between discovery and remediated patch to near-zero – turning the self-healing software supply chain from a concept into a working reality.

"The traditional security playbook – finding vulnerabilities, opening tickets, waiting weeks for manual patching – has become a liability in the frontier AI era. Enterprises now face adversaries who move at agentic speed and regulators who demand provable evidence at every step," said Eyal Dymant, Vice President of Security Products, JFrog. "Our customers need a supply chain that identifies vulnerabilities and remediates them, without human intervention, as soon as a fix is available – collapsing the remediation SLAs their boards now mandate from weeks to minutes. Zero-Touch Remediation makes that possible – using Artifactory's role in the organization as the single source of truth for all artifacts, it consumes every partner fix natively, applies the best available match, serves the fixed version to new builds and attests every action through JFrog AppTrust."

The security team's job has always been to move faster than the attacker. When AI can find and weaponize a vulnerability in minutes and hours, that race is no longer a human-scale problem. [Gartner identified software supply chain attacks](#) among the top four critical security threats where attackers currently hold the advantage due to Frontier AI – and the firm's inaugural Magic Quadrant for Software Supply Chain Security - in which JFrog was positioned as a Leader confirmed the industry's shift toward dynamic, self-healing

platforms as the answer. AI has moved from an assistant to a skilled attacker, to now autonomously finding vulnerabilities that were previously overlooked in critical attack paths and generating working exploits without human guidance – before any CVE is ever published.

From Vulnerability to Fix in Minutes, without a Human in the Loop

The [JFrog Self-Healing Software Supply Chain](#) operationalizes the five pillars of software security – prevention, detection, prioritization, remediation, and provable auditability – as one continuous, machine-speed workflow.

- **Prevent: Stop threats before they enter** – To help developers ship secure software without adding friction, JFrog Curation with Compliant Version Selection blocks risky packages, AI assets, IDE extensions, and third-party components the moment a developer tries to pull them – transparently serving the policy-compliant version instead.
- **Detect: See the full chain before the attacker does** – [JFrog Xray](#) and [JFrog Advanced Security](#) deliver unified detection from a single system of record – scanning release artifacts for every dependency, catching vulnerable code patterns before they ship, and surfacing exposed credentials across every artifact type.
- **Prioritize: Act on real vs. theoretical risk** – Helping to cut CVE noise, JFrog Contextual Analysis evaluates every finding for reachability and exploitability. JFrog Runtime narrows the list further to what is actually loaded in production and JFrog AppTrust adds business criticality – reducing thousands of tickets to a short list of confirmed exposures.
- **Remediate: Fix faster than the threat spreads** – For third-party software packages, the new [JFrog Zero-Touch Remediation](#) automatically pulls the best available patch from ecosystem partners and applies it transparently. For first-party code, JFrog's complementary Agentic Remediation enables developers to generate and validate AI-driven fixes at the pull-request level for developers to review and validate before merges.
- **Prove: Every fix, every attestation, one evidence chain** – JFrog AppTrust automatically records cryptographically signed attestations for every action, delivering a comprehensive, regulator-ready audit trail of the entire software supply chain's status for every release, available at any point in time. This is DevGovOps: governance ingrained into the pipeline itself, so when the auditor asks, compliance proof is already there.

Why Only JFrog can deliver a Self-Healing Software Supply Chain

"Frontier AI has forced every enterprise to ask the same question: how do you remediate faster than an autonomous adversary can weaponize a vulnerability? No single vendor solves that challenge alone," said Gal Marder, Chief Strategy Officer, JFrog. "Each of our ecosystem partners has built differentiated patching capabilities no single company could replicate. JFrog Artifactory is the single source of truth for Artifacts – where every artifact lives – binaries, containers, libraries, AI models, MCP servers, agent skills. It is the control plane allowing organizations to serve every fix with zero-touch. We ingest each partner's fix natively, use the customer's policy to apply the best one, and produce a complete signed evidence chain the auditor can verify. Customers keep the freedom to choose the best fix. JFrog delivers the governance that makes it work."

Self-healing is what becomes possible when every artifact in the enterprise flows through a single system of record, which in turn acts as a single source of truth. Together with Broadcom Tanzu, Chainguard, Echo, IBM/Red Hat, Moderne, Seal Security and TuxCare, JFrog Zero-Touch Remediation matches each fix to the vulnerable artifact, applies it without breaking builds, and attests it through JFrog AppTrust – regardless of which partner produced the fix.

- **[Broadcom](#)**: Spring patches from the maintainers, authored before public disclosure and built to SLSA Level 3; Plus, curated, verified builds across Java, Python, and Node.js.
- **[Chainguard Libraries](#)**: Malware-free Java, Python, and JavaScript packages that also have built-from-source backported versions that fix critical and high-severity CVEs.
- **[Echo Libraries](#)**: Coverage for npm, PyPI, Java, Go, dotnet, Perl, and more, with critical and high CVE patches on the versions teams already declare, including transitive dependencies.
- **[Lightwell](#)**: Lightwell, a joint initiative between Red Hat and IBM, provides organizations with critical access to security remediations and mitigations, helping them more easily and quickly address vulnerable third-party open-source dependencies.
- **[Moderne Backpatch Alliance](#)**: Critical end-of-life OSS packages backpatched by the original maintainers, cherry-picked from upstream commits and published as standard Maven artifacts.
- **[TuxCare SecureChain](#)**: Open-source packages rebuilt from source, screened for malware, and continuously patched – including Endless Lifecycle Support after upstream maintenance ends.
- **[Seal Security](#)**: Standalone backported patches that keep the same version number, cryptographically signed, with a 72-hour SLA for both high and critical CVEs.

“True supply chain resilience requires more than just speed, but authoritative provenance,” said Kevin Strohmeier, Head of Tanzu Marketing, Broadcom. “Our integration with JFrog’s Zero-Touch Remediation and Spring Enterprise Repository enables development teams to leverage self-healing in their app builds. By providing verified, backward-compatible patches for Spring Enterprise, we’re working with JFrog to empower developers to consume the latest security updates automatically. This eliminates the toil of manual dependency overrides, allowing teams to stay protected against vulnerabilities without sacrificing development velocity.”

“Open source libraries have become a critical attack surface for modern applications,” said Patrick Donahue, Senior Vice President, Product, Chainguard. “By integrating Chainguard Libraries with JFrog Zero-Touch Remediation, we’re making it easy for mutual customers to replace vulnerable dependencies with Chainguard’s secure-by-default language libraries directly within JFrog, preventing malware and CVEs without adding friction for developers.”

“AI has collapsed threat timelines and accumulated security debt is now an immediate operational risk. The industry needs active remediation, not just vulnerability detection,” said Gunnar Hellekson, vice president and general manager, Lightwell Business Unit, Red Hat. “To help address this need, Lightwell serves as a collaborative clearinghouse – combining AI-driven speed with trusted human expertise to deliver tested fixes to customers and the open source community. By connecting Lightwell’s intelligence directly into the JFrog artifact workflow, we’re enabling customers to neutralize threats automatically while preserving the trust, governance, and community integrity essential to open source.”

JFrog Zero-Touch Remediation is available immediately as part of JFrog Unified Security. Interested customers can schedule a live demonstration [here](#). To learn more about [JFrog Zero-Touch Remediation](#) read [this blog](#) or register for the “[Secure at Frontier Speed](#),” webinar on Wednesday, September 30 at 11 AM PT/2 PM ET.

###

Like this Story? Share this on X: What if your #SoftwareSupplyChain fixed itself? Now it can. At #swampUP New York, JFrog introduced Zero-Touch Remediation: automatically match, apply, and attest the best fix across your artifact estate – at machine speed, with no human in the loop. The self-healing supply chain is here. #AI #DevSecOps #AgentSecOps #DevGovOps #security #softwaresupplychain #self-healingsupplychain #ecosystem

About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps, DevGovOps, and AgentSecOps platform, is on a mission to create a world of trusted software delivery without friction from development to production. Driven by a “Liquid Software” vision, the JFrog Platform is a software supply chain system of record that is designed to power organizations as they build, manage, govern, and distribute secure software with speed and scale. Holistic security features help identify, protect, and remediate against threats and vulnerabilities. The universal, hybrid, multi-cloud JFrog Platform is available as both SaaS services across major cloud service providers and self-hosted. Millions of users and approximately 6,600 organizations worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation in the AI era. Learn more at <https://jfrog.com> or follow us on X @JFrog.

Cautionary Note Regarding Forward-Looking Statements

This press release contains “forward-looking” statements, as that term is defined under the U.S. federal securities laws, including, but not limited to, statements regarding JFrog’s expectations with respect to the anticipated capabilities and performance of JFrog Zero-Touch Remediation and the JFrog Self-Healing Software Supply Chain, the anticipated timing of general availability of JFrog Zero-Touch Remediation, the expected benefits of JFrog’s security partner ecosystem integrations, and JFrog’s ability to help customers automatically detect, prioritize, remediate, and prevent software vulnerabilities.

These forward-looking statements are based on our current assumptions, expectations and beliefs and are subject to substantial risks, uncertainties, assumptions and changes in circumstances that may cause JFrog’s actual results, performance or achievements to differ materially from those expressed or implied in any forward-looking statement. There are a significant number of factors that could cause actual results, performance or achievements to differ materially from statements made in this press release, including but not limited to risks detailed in our filings with the Securities and Exchange Commission, including in our annual report on Form 10-K for the year ended December 31, 2025, our quarterly reports on Form 10-Q, and other filings and reports that we may file from time to time with the Securities and Exchange Commission. Forward-looking statements represent our beliefs and assumptions only as of the date of this press release. We disclaim any obligation to update forward-looking statements, except as required by law.

Media Contact:

Siobhan Lyons, Director, Global Communications, siobhanL@jfrog.com

Investor Contact:

Jeff Schreiner, VP of Investor Relations, jeffS@jfrog.com