

JFrog Embeds Security into the Agentic Workforce

New JFrog Platform capabilities help ensure AI agents only consume and produce trusted, scanned artifacts using a single source of truth

SUNNYVALE, Calif. and NEW YORK — swampUP 2026 — September 2, 2026 — [JFrog Ltd.](#) ("JFrog") (NASDAQ: FROG), the Liquid Software company and creators of the [JFrog Software Supply Chain Platform](#), the system of record for trusted software artifacts, binaries, and AI assets, today unveiled a new suite of capabilities to secure and govern the agentic workforce. By natively connecting AI assets to the JFrog Platform and implementing an always-on AgentSecOps workflow, JFrog becomes the single source of truth for every artifact agents consume or produce – helping ensure everything is policy-compliant and secure from initial consumption to final delivery.

"AI coding agents not only write software at machine speed but also consume software at scale. The DevSecOps controls we built over a decade assumed a human developer was at the keyboard. Today, that assumption has broken - a software supply chain run by agents doesn't stop for reviews. Agents make decisions about finding and pulling dependencies without a human in the loop, installing traditional packages and AI assets such as skills, context files and MCPs from various sources," said Yoav Landman, Co-founder and CTO, JFrog. "In order to scale agents responsibly and make sure they are compliant, these dependencies must come from a trusted source. The only way to achieve that is by ingraining an intrinsic immune layer directly into the software supply chain that guarantees every input consumed by agents originates from a single, trusted, secure system of record."

Why Traditional Security Fails in the Agentic Workforce Era

[Gartner's Hype Cycle for Agentic AI, 2026](#), states only 17% of organizations have deployed AI agents to date, yet more than 60% expect to do so within the next two years. However, Gartner also predicts that [over 40% of agentic AI projects will be canceled by the end of 2027](#) due to escalating costs, unclear business value, or inadequate risk controls. [Recent exploits have demonstrated](#) coding agents are relentlessly task-driven and will bypass safety configurations to complete their task, opening direct pathways for software supply chain attacks.

How to Build a Trusted Agentic Workforce

The new enhancements to the JFrog Platform ensure customers can secure, govern, and control AI agents at scale. New capabilities supporting this AgentSecOps flow include:

Protect What Agents Consume:

- **[AI Asset Scanning](#)**: Index, scan, and block risky or malicious models, MCPs, skills, and plugins. JFrog performs proactive semantic scanning of markdown files, skills scripts, and instruction sets to block malicious behaviors before they touch a developer's workstation.
- **[Agent Plugins Registry](#)**: Governs coding-agent plugins using Agent Guard, ensuring agents across Claude Code, Cursor, VS Code, and more only use vetted, approved plugins.
- **[Agent Package Manager \(APM\) Registry](#)**: Integrates the Microsoft-led APM standard into Artifactory, allowing organizations to package, version, and manage AI assets – including prompts, skills, and MCP servers – with full dependency tracking and pinned versions to prevent drift and unvetted sources.
- **[Agent Guard](#)**: Natively enforces project-scoped allow/deny policies from AI Catalog inside developer tools – Claude Code, Cursor, VS Code, and more – so coding agents never bypass organizational guidelines and consume only approved AI assets

Control How Agents Build:

- **[JFrog Agent Plugin](#)**: Connects agents to your JFrog Platform to bring your organizational standards and policies directly to agent workflows, and completely transparent to developers. Natively integrates across Claude Code, Cursor, Codex, CoPilot, Kiro, and more.
- **[Agent Package Resolution](#)**: Authenticates and provides a trusted path for agents to resolve package dependencies through JFrog Artifactory, helping ensure agents consume only trusted, verified, audited components governed by your security policies.
- **Network-Layer Protection ([Traffic Controller](#))**: JFrog Traffic Controller and SASE partners ([Cloudflare](#), [Netskope](#), [Zscaler](#)) block public registry calls at the network layer, rerouting all traffic through Artifactory for visibility and control.

Enabling Innovation Without Compromising Safety

By centralizing both human-written and agent-generated artifacts in a single, universal system of record, enterprises neutralize vulnerabilities at the point of ingestion (shifting left) without slowing down developer velocity.

"By deploying JFrog, we've seen fewer vulnerabilities, which has given our developers more time to focus on building new applications. With all our development teams on one platform, the process is centralized and streamlined," said Billy Norwood, Chief Information

Security Officer at FFF Enterprises. "We're handling risks further up the chain by shifting left, so vulnerabilities are remediated before anything gets published."

The new JFrog capabilities announced herein are available to customers immediately. To learn more about building a trusted agentic workforce visit <https://jfrog.com/ai/> or [read this blog](#).

###

Like this Story? Share this on X: *From sandbox escapes to compromised configuration files, the vulnerabilities in coding agents are real. Security can't be bolted on after the fact. New @JFrog capabilities provide #AgentSecOps controls to help secure what agents download and how they build inside @Cursor, @Claude Code, and #VSCode. #AppSec #softwaresupplychain #DevSecOps #security #DevGovOps #Artifactory*

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 About 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 the anticipated performance of JFrog's new AgentSecOps.

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