JFrog and Anthropic Bring Enterprise-Grade Software Supply Chain Governance and Security to Claude Code

Anthropic Claude Code users can now run governed, supply-chain-aware AI coding agents, assisted by JFrog's trusted, universal, multi-agent platform

SUNNYVALE, Calif. – June 10, 2026 – JFrog Ltd (Nasdaq: FROG), the creators of the JFrog Software Supply Chain Platform, the system of record for trusted software artifacts, binaries, and AI assets, unveiled its JFrog Platform plugin for Claude Code, in collaboration with Anthropic. Available immediately to all Claude Code users, the new plugin represents a significant milestone in bringing enterprise-grade software supply chain governance to one of the fastest-growing AI coding agent platforms in the world, reinforcing JFrog's position as a critical trust layer and system of record for the rapidly expanding AI agent environment.

The need for agent-specific security has been highlighted by Anthropic, stating, "As agents grow more capable, attack surfaces are constantly shifting. The types of failures we've seen are likely to be repeated across industries and labs. We need collective investment in agent-specific security posture, from shared benchmarks and disclosure norms to common identity standards and cross-vendor red-teaming."

"AI agents are active participants in the software supply chain, making decisions about dependencies, builds, and deployments – but most of them are doing it blind, without any supply chain context. This is often how malicious packages, vulnerabilities, and ungoverned AI assets enter production today, exposing organizations to software supply chain attacks," said Yoav Landman, Co-Founder and CTO of JFrog. "AI-enabled innovation cannot come at the expense of security or compliance. Enterprises need a universal system of record with real-time control and visibility into the decisions these agents make, that's what this integration enables."

Governing the Binaries Surge with Agentic DevSecOps

AI coding agents are driving a surge of binaries, with the JFrog Platform currently managing over 18 billion artifacts, a 136% increase from the previous year[1]. The new JFrog Platform plugin for Claude Code is designed to help organizations tame unorthodox AI agent behavior by providing developers with governed access to scan, curate, and secure every artifact and dependency their agents consume. It also extends Claude Code with deep,

[1] JFrog 2026 Software Supply Chain Security State of the Union: https://jfrog.com/software-supply-chain-state-of-union/

domain-specific JFrog Platform Skills, designed to give developers and their agents the ability to execute platform operations using natural language. Combined with the recently announced JFrog MCP Registry and JFrog Agent Skills Registry, the new plugin is expected to deliver:

- **Real-time, Upstream Governance:** Governance, package security and license compliance, and provenance validation happen inside the development workflow, not after it. Agents enforce policies as code is written, eliminating the manual handoffs that slow releases and introduce risk.
- **MCP and Agent Skills Governance:** Ensures agents, developers, and AI users only pull verified, secure, and governed MCP servers and agent skills – blocking rogue access to sensitive internal data and preventing unauthorized actions.
- **Accelerated DevOps Workflows:** Engineering time is no longer wasted on coding repetitive platform tasks. Repository management, project provisioning, and routine operations are handled by agents through JFrog Platform Skills – so developers stay focused on building, not configuring.
- **Strengthened Auditability:** When an incident or audit happens, teams need answers in minutes, not days. The JFrog Platform plugin provides end-to-end traceability from source commits to build artifacts, so security teams can respond faster and prove compliance without scrambling.

Why Agent Universality Matters Now

The new plugin reflects how JFrog sees the market for trusted agents evolving: teams will use different AI agents and JFrog's role is to support those choices while maintaining governance and control. Rather than building one agent at a time, the JFrog Platform provides three layers of agent connectivity that work across any AI coding environment, including:

- **JFrog Platform Skills,** giving agents deep, domain-specific knowledge around the JFrog Platform, enabling complex operations like vulnerability scanning, curation checks, and provenance verification through simple natural language.
- **JFrog MCP Tools,** join JFrog Skills in providing standardized access to security, compliance, and artifact data across the JFrog Platform, ensuring consistent governance regardless of which agent initiates the request.
- **Additional Agent-Native Plugins Support,** starting with Claude Code, alongside Cursor and VS Code Copilot. Collectively, these plugins aim to bring the full JFrog Platform into each agent's native environment with streamlined deployment and simple authentication.

Together, these layers establish the JFrog Platform as the foundational system of record across multi-agent environments – ensuring that governance, provenance, and security travel with the developer, not with any single tool.

The JFrog Platform plugin for Claude Code is available immediately at https://claude.com/plugins/jfrog. For more information on the new JFrog Platform plugin for Claude Code and more details on JFrog's agentic interfaces, read this blog or check out this video.

###

Like this Story? Share this on X: Accelerate your #AI development without sacrificing #governance or security with the new JFrog Platform plugin for @Anthropic's #ClaudeCode. Give your AI agents the full software supply chain context needed to automatically enforce governance, security, and compliance right from your IDE workflow. Learn how to harness the power of agentic #DevSecOps with new JFrog Platform Skills and MCP tools. *Learn more: https://bit.ly/41O6RBZ #security #DevGovOps*

About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps, DevGovOps and MLOps platform, is on a mission to create a world of software delivered 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, 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 www.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 our expectations with respect to the anticipated performance of the JFrog Platform plugin for Claude Code.

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@[2]jfrog.com

[2] *Anthropic's Claude Code has 30 million monthly active users according to: https://fatjoe.com/blog/claude-ai-stats/*