NEWS RELEASE

JFrog Brings Enterprise-Grade Software Supply Chain Security to Over 1M AI Developers with New Cursor AI Coding Agent

2026-04-15

JFrog Platform plugin for Cursor gives developers the freedom to create and deliver next generation AI-powered software with built-in governance

SUNNYVALE, Calif.--(BUSINESS WIRE)-- 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, announced its Platform is now available in the Cursor marketplace. Over 1 million Cursor active daily users now have access to robust software supply chain security within their workflows via the new plugin, reinforcing JFrog's position as a critical trust layer and system of record for the rapidly expanding AI agent ecosystem.

The new JFrog Platform plugin for Cursor gives developers the freedom to create and deliver next generation AI-powered software with built-in governance.

"Today's enterprises wanting to fully leverage AI-driven software creation are rightfully concerned about the security risks open source and autonomous tools used by AI will create," said Yoav Landman, Co-Founder and CTO of JFrog. "Issues like Shadow AI, ungoverned MCP server access, malicious skills, and uncontrolled dependencies can create massive blind spots and lead to significant security vulnerabilities. By bringing the full power of the JFrog Platform directly into the Cursor coding agent, we are giving enterprises the guardrails they demand from the very beginning."

Research from IDC Link states: "As enterprises transition from simple chatbots to autonomous AI

agents, the need for security and governance has moved from the model itself to the actions those models take…However, challenges remain since the market for AI governance is rapidly evolving, with new entrants and approaches emerging. Standards for agentic components, such as skills and MCP servers, are still in flux. In addition, enterprises are still in the early stages of adopting autonomous agents, and the pace of adoption may vary significantly across industries."[1]

Empowering a Diverse Ecosystem of AI Builders with Seamless Security and Governance

Cursor is one of the industry's leading AI coding agents designed for developers, data scientists, and engineers, that emphasizes agentic capabilities via plugins and MCP servers (not just UI extensions like the VS Code marketplace). Modern developer workflows start inside AI-native Integrated Developer Environments (IDEs) like Cursor, where agents suggest code, pull dependencies, and make supply chain decisions in real time. However, agents often do this without any visibility into whether packages are safe, compliant, or policy approved.

Building upon its recently announced JFrog Agent Skills Registry – a unified repository to centrally manage, govern, and version control AI skills across all environments by treating them as software packages – the new JFrog Cursor plugin brings the full power of the JFrog Platform directly into the developer's AI-native IDE without context switching or manual lookups, eliminating friction. Enterprises can now leverage JFrog as a system of record and control point designed for agentic development to allow for increased accuracy, consistency, and security across AI pipelines and the software supply chain.

The new plugin ships with four integrated components:

- **A remote MCP server connection:** Authenticated seamlessly with the JFrog Platform via OAuth without the need for API keys.
- **Conversational AI Skills:** Enables developers to manage artifacts, scan for vulnerabilities, and enforce policies using natural language interactions.
- **Automated Security Rules:** Automatically enforces supply-chain best practices whenever a dependency file is touched.
- **Dedicated Supply Chain Security:** Proactively audits dependencies for CVEs, license risks, and curation policy violations.

Additionally, the JFrog Platform plugin for Cursor offers seamless integration with JFrog Xray and JFrog Advanced Security, allowing vulnerabilities, exposed secrets, and infrastructure misconfigurations to be flagged as developers code. It also provides real-time security insights with clear context, along with easy-to-follow remediation advice and one-click dependency upgrades. The JFrog plugin for Cursor also provides AI agents with the necessary information and guidance to check dependencies in real-time, ensuring every software component is fully compliant with organizational standards and safe for use before it is ever committed.

The JFrog Platform plugin has been officially verified by Cursor and is available immediately in the Cursor marketplace and in GitHub. Users can browse and install the plugin directly through the marketplace panel within the editor or by visiting cursor.com/marketplace (marketplace access details provided in user prompt). Furthermore, customers using the recently announced JFrog MCP Registry can access a repository of pre-approved local and remote MCP servers directly from their preferred coding agents, inclusive of Claude Code, Cursor, and VS Code Copilot.

For more information on the new JFrog Platform plugin for Cursor read this blog or visit the support page here https://docs.jfrog.com/security/docs/cursor-1.

Like this Story? Share this on X: *The future of software is autonomous, but it shouldn't be unmanaged! Our award-winning JFrog Platform is now available as a plugin in the @Cursor Marketplace. Bring enterprise-grade #softwaresupplychainsecurity into your AI-native IDE to catch #vulnerabilities, license risks, and policy violations before your code is ever committed. Build a foundation of trust so your #AI agents can scale as fast as your ambition. Learn more: https://bit.ly/47xnF3s #DevSecOps #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 Cursor.

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.

1 *Source: IDC Link: "JFrog Establishes a Trust Layer for Agentic AI: Extending the Software Supply Chain to Skills, Models, and MCPs," by Jim Mercer, March 23, 2026.*

Media Contact:
Siobhan Lyons, Director, Global Communications, siobhanL@jfrog.com

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

Source: JFrog Ltd.