JFrog Unveils Universal MCP Registry, Delivering a Secure System of Record for the AI-Driven Software Supply Chain

New JFrog MCP Registry provides a single source of truth to store and manage MCP servers from all vendors, while monitoring enterprise AI connections and instantly blocking unsafe developer tools

SUNNYVALE, Calif. – March 18, 2026 – JFrog Ltd (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, the system of record for software artifacts, binaries, and AI assets, today introduced its JFrog MCP Registry. Expanding on current capabilities in JFrog AI Catalog, the new registry acts as a single source of truth for securely governing Model Context Protocol (MCP) Servers, helping companies transition AI usage from an enterprise-wide compliance and security risk into a competitive advantage.

“Today, developers across the enterprise are rapidly adopting MCP servers from multiple AI tools and vendors, creating a growing challenge for organizations that lack the visibility and control to monitor these connections,” said Yuval Fernbach, CTO, JFrog MLOps. “We’re witnessing a fundamental shift in how software is built and deployed, with AI agents becoming active participants in the software supply chain. This innovation cannot come at the expense of security, visibility, control, or compliance. By establishing a system of record for MCP server usage, and treating them like any other binary asset, organizations can confidently innovate at scale while maintaining the trust and control required across the AI-driven software supply chain.”

The Hidden Risks of Unmanaged MCP Servers

As AI shifts from simple chat interfaces to autonomous, long-running agents, developers rely on MCP servers to act as "enablers of integration," giving AI models direct access to internal and external enterprise systems, APIs, and data. However, these servers, which act as trusted intermediaries, can also execute arbitrary, potentially malicious code directly on a user's machine or on remote systems with high privileges. If left unmanaged, they expose organizations to severe risks, including prompt hijacking vulnerabilities, over-privileged access, and credential exposure.

This need for AI governance is backed by Gartner research[1], stating that security and AI leaders must establish MCPs as the foundational method for agents to communicate with external resources by implementing a centralized MCP server registry, enforcing layered security controls, and defining clear ownership and governance policies.

Delivering a System of Record for MCP Servers: The JFrog MCP Registry

The new JFrog MCP Registry provides a system of record and AI infrastructure trust layer for all MCP Servers, agent skills, models, and agentic binary assets. By treating MCP servers with the same rigorous security standards as software packages, the JFrog MCP Registry helps eliminate blind spots across the AI software supply chain. At its core the JFrog MCP Registry is designed to bring:

- **Native security by design** to proactively block the download and execution of malicious or non-compliant MCP servers, otherwise pulled naively by humans or AI agents, rather than waiting for an issue to occur and remediating it after the fact.
- **Centralized governance and management** enabling developers to instantly access a registry of pre-approved local and remote MCP servers directly from their Integrated Development Environments (e.g., Claude Code, Cursor, VS-Code).
- **Enterprise-grade policy enforcement on every agentic workflow,** replacing "blind trust" with granular control, by treating every MCP server as a governed artifact with centralized discovery, configuration and project-level permissions management alongside all other AI models and software artifacts in a unified AI Catalog.
- **Platform universality,** which allows companies to seamlessly manage agent ecosystems from private marketplaces and across vendors, enabling teams to seamlessly switch coding agents without ever needing to rebuild their secure system of record.

The JFrog MCP Registry is available immediately as part of JFrog AI Catalog. To learn more about how it works, read this blog, visit https://jfrog.com/ai-catalog/mcp-registry, or register for the "*The Right Tools for the Job: Securing Your AI Agents*" webinar on March 31 at 10 AM PST.

Like this Story? Share this on X: *Secure and compliant adoption of #AI technology is key to innovating without sacrificing visibility and control. JFrog MCP Registry gives companies the ability to manage the risks associated with agentic AI and automated workflows, without stifling innovation. Learn more: https://bit.ly/4sRXTPJ #MCP #AI #softwaresupplychainn #security #DevGovOps*

[1] *Source: Gartner: Adopt MCP as a Strategic Approach for integrating AI Solutions, 7 November 2025.*

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 JFrog MCP Registry.

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.

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.

Media Contact:

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

Investor Contact:

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