NEWS RELEASE

JFrog Delivers Trust Layer for AI-Driven Software with NVIDIA

2026-04-08

Enterprise AI agents can now operate at scale with built-in governance through the JFrog Agent Skills Registry, a secure system of record for MCPs, models, agent skills, and agentic binary assets

SUNNYVALE, Calif.--(BUSINESS WIRE)-- **NVIDIA GTC** – 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 announced its new JFrog Agent Skills Registry. Validated through early integration with NVIDIA, the platform provides governance and a verifiable trust layer required for agentic workforces to operate securely at enterprise speed and scale.

The new JFrog Agent Skills Registry will support NVIDIA Agent Toolkit, including NVIDIA NemoClaw, to provide the governance and verifiable trust layer required for agentic workforces to operate securely at enterprise speed and scale.

The new JFrog Agent Skills Registry will support NVIDIA Agent Toolkit, including NVIDIA NemoClaw, an open-source runtime for building and deploying safe, autonomous, long-running AI agents. JFrog Agent Skills Registry is built to provide the governance and verifiable trust layer required for agentic workforces to operate securely at enterprise speed and scale. Additionally, JFrog Artifactory will serve as a registry for AI models and agent skills with NVIDIA AI-Q Blueprint, as part of NVIDIA Agent Toolkit.

“AI agents are fundamentally reshaping how software is created and operated, but without a dedicated trust layer to enforce governance and secure workflows, they introduce significant enterprise risk,” said Gal Marder, JFrog’s Chief Strategy Officer. “Just as a malicious software package can compromise an application, an unvetted skill can guide an agent to perform harmful actions. To safely deploy

autonomous agents at scale, organizations must move beyond blind trust. Working closely with the NVIDIA Enterprise AI Factory team, we are establishing a reliable system of record to store, scan, and govern all agentic binary assets across the software supply chain."

The rapid evolution of AI has made autonomous agents, which rely on skills, a standard part of the software supply chain. However, an infrastructure layer beneath them is needed to enforce policies, security, and privacy controls required to make them safe for use. Without a standardized infrastructure, organizations face unprecedented security and compliance risks, as demonstrated by recent OpenClaw manipulations and breaches.

JFrog's universal solution supports all agents, including NVIDIA NemoClaw, which delivers a trust layer to:

- **Enhance security and governance** of all MCPs, agent skills, models, and software packages using a single source of truth to scan and block those with malicious intent or vulnerabilities.
- **Enable secure adoption and scale of autonomous, long-running agents** without increasing risk or compromising compliance.
- **Power agentic workflows and developer innovation across the enterprise**, safely and continuously, without disruption.

"Security and governance are key to deploying AI agents in the enterprise," said Pat Lee, vice president, Enterprise Partnerships, NVIDIA. "JFrog's Agent Skills Registry for NVIDIA NemoClaw supports security and control for deploying long-running agents to help scale enterprise productivity with powerful new AI tools."

By establishing the JFrog Platform as an integrated, secure registry for NVIDIA AI-Q Blueprint and NVIDIA NemoClaw runtime, enterprises will be able to safely operate agents using verified skills, MCP servers, models, and software packages. The NVIDIA and JFrog teams worked closely to validate a workflow for the ingestion and management of Artifactory as a skills registry, including support for NVIDIA-developed skills, using NVIDIA cuOpt as the first example of a packaged skill. This integration gives NVIDIA a single, governed endpoint for distributing verified AI skills across all agent platforms, with a promotion model that enforces increasing security gates from team to enterprise-wide use.

JFrog's new offering includes:

- **Certified NVIDIA AI-Q Blueprint:** The JFrog Platform is validated for the NVIDIA AI-Q Blueprint for lifecycle management and governance of agent skills.
- **Native NVIDIA NemoClaw Integration:**JFrog Artifactory natively integrates with NVIDIA NemoClaw runtime, designed to provide secure, private, and scanned resources.
- **Centralized Agent System of Record:** The JFrog AI Catalog and Agent Skills Registry act as the central control plane for NVIDIA NemoClaw, providing a single source of truth to track, audit, and manage the provenance of agents, NVIDIA NIM, and MCP servers.
- **Secure Agents and Behaviors:** JFrog AI Catalog automatically scans, verifies, and signs all AI skills upon upload to detect vulnerabilities, malicious payloads, and compliance risks before NVIDIA NemoClaw – or other agents – ever adopt them.
- **Policy-Driven Governance and Control:** The JFrog Platform allows organizations to set strict approval workflows, ensuring developers and AI agents can only access permitted, verified skills for specific projects and business units. The NVIDIA NemoClaw runtime then sandboxes each agent in an isolated, virtual environment, enabling safe execution of code without risk of broader network infection.

To learn more about how JFrog and NVIDIA are securing the future of the agentic AI software supply chain, read this blog on the JFrog Agent Skills Registry or visit the solutions page.

Like this Story? Share this on X: *@JFrog partners with @NVIDIA to provide a trust layer to govern, scan, and secure #AI agent skills and tools across the #softwaresupplychain. Learn more: https://bit.ly/4t6TF75 #DevGovOps #DevSecOps #security #GTC*

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 Agent Skills 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 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 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

Source: JFrog Ltd.