

JFrog Partners with NVIDIA to Accelerate Agentic AI, Integrating the JFrog Platform with NVIDIA Enterprise AI Factory

New Full-Stack, Validated Design Aims to Accelerate AI/ML Model Engineering, Security, Operations and Delivery for the AI-powered Enterprise

Sunnyvale, Calif. - [COMPUTEX 2025](#) - May 18, 2025 — [JFrog Ltd](#) (Nasdaq: FROG), the Liquid Software company and creators of the award-winning [JFrog Software Supply Chain Platform](#), today announced the integration of its foundational DevSecOps tools with the [NVIDIA Enterprise AI Factory validated design](#). JFrog will serve as the cornerstone software artifact repository and secure model registry for the landmark agentic AI architecture.

Following a successful [NVIDIA NIM integration](#) with the JFrog Platform, this new collaboration delivers a full-spectrum MLOps solution, designed to ensure scalable, secure and seamless deployment of AI-powered applications using the [NVIDIA Blackwell platform](#).

"The future of AI depends not only on innovation - but on trust, control, and seamless execution," said Shlomi Ben Haim, CEO and co-founder of JFrog. "To deliver AI at scale, enterprises need to adopt the same concepts applied to software: developer-friendly workflows, strong security, robust governance, and full lifecycle management. ML models are binaries, and they must be managed as first-class software artifacts. That's why we're excited to partner with NVIDIA to bring JFrog's Software Supply Chain Platform as the single source of truth for all software and AI assets to the NVIDIA Enterprise AI Factory so organizations can build and scale trusted AI solutions with confidence."

Delivering Critical Infrastructure to Enable Future AI Innovation

The JFrog Platform provides customers with a "single source of truth" for software components within NVIDIA Enterprise AI Factory, which contains an integrated and validated suite of software technology solutions enterprises can use to develop, deploy, and manage agentic AI, physical AI, and HPC workloads on-premises. This validated design aims to allow organizations to have full control of their data and operate advanced AI agents in a secure environment. Key capabilities include:

- **Secure & Governed Software Component Visibility:** Enables all ML models, engines, and software artifacts to be scanned for security issues, versioned, governed, and traceable across the entire software development lifecycle.

- **End-to-End Software Artifact & ML Model Management:** Enables the seamless pulling, uploading, and hosting of AI models and datasets, AI containers, Docker containers, and dependencies optimized for the NVIDIA Enterprise AI Factory validated design.
- **Rapid, Trusted AI/ML Application Provisioning in Runtime:** Simplifies configuration of AI environments by eliminating the need for runtime environments to pull components from outside of the organization, thanks to the universality, proven scalability and robustness of [JFrog Artifactory](#).
- **Future-proofed for Evolving GenAI Applications:** Quickly and easily manages ML model versioning and upgrades to new and approved model generations.

“Enterprises building AI factories need to manage the complexity of AI adoption while ensuring performance, governance and trust,” said Justin Boitano, Vice President, Enterprise AI Software Products, NVIDIA. “JFrog’s unified software supply chain platform, paired with the NVIDIA Enterprise AI Factory validated design, enables rapid, responsible AI innovation at scale.”

The integration is designed to enable the JFrog Platform to run natively on [NVIDIA Blackwell](#) systems to help reduce latency and process tasks with unparalleled performance, efficiency, and scale. It supports a wide range of AI-enabled enterprise applications, agentic and physical AI workflows, autonomous decision-making, and real-time data analysis across various industries, including financial services, healthcare, telecommunications, retail, media, and manufacturing. Additionally, the system leverages NVIDIA’s engineering know-how and partner ecosystem to help enterprises accelerate time-to-value and mitigate the risks of AI deployment.

Those interested in learning more about JFrog and NVIDIA integrations or going hands-on with the NVIDIA NIM trial should visit <https://jfrog.com/jfrog-and-nvidia/>.

###

Like this Story? Share this on X: Big news! @JFrog is proud to serve as a cornerstone in @nvidia #Enterprise #AI Factory to accelerate the next generation of #agenticAI innovation. Read more: <https://bit.ly/432sW1a> #SoftwareSupplyChain #DevOps #DevSecOps #cybersecurity #developer #COMPUTEX

About JFrog

JFrog Ltd. (Nasdaq: FROG) is on a mission to power the world with liquid software. We are replacing endless software updates with a single system of record that seamlessly delivers secure applications from developer to device. The JFrog Software Supply Chain Platform helps organizations build, manage, and distribute software quickly and securely, making applications available, traceable, and tamper-proof. Its integrated security features also help identify, protect, and remediate against threats and vulnerabilities. The Platform also brings ML models in line with all other software development processes, providing a single source of truth for all software components across Engineering, MLOps, DevOps, and DevSecOps teams so they can build and release AI applications faster, with minimal risk and less cost. JFrog's hybrid, universal, multi-cloud platform is available as both self-hosted and SaaS services across major cloud service providers. Millions of users and 7K+ customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation. Once you leap forward, you won't go back! Learn more at jfrog.com and follow us on X: [@jfrog](https://twitter.com/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 JFrog's artifact repository and secure model registry's integration with NVIDIA's agentic AI architecture delivering a full-spectrum MLOps solution.

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, 2024, 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, Sr. Manager, Global Communications, siobhanL@jfrog.com

Investor Contact:

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