

JFrog Collaborates with NVIDIA to Deliver Secure AI Models with NVIDIA NIM

Aiming to meet the increasing demand for enterprise-ready generative AI, the JFrog Platform integrates NVIDIA NIM to deliver GPU-optimized AI model services

Sunnyvale, Calif. and Austin, TX – [JFrog swampUP](#) – September 10, 2024 – [JFrog Ltd.](#) (“JFrog”) (Nasdaq: FROG), the Liquid Software company and creators of the [JFrog Software Supply Chain Platform](#), now expanded to include a unified MLOps platform through the [acquisition of Qwak AI](#), today announced a new product integration with [NVIDIA NIM microservices, part of the NVIDIA AI Enterprise software platform](#). The integration of the JFrog Platform with the JFrog Artifactory model registry and NVIDIA NIM is expected to combine GPU-optimized, pre-approved AI models with centralized DevSecOps processes in an end-to-end software supply chain workflow. This allows organizations to bring secure machine learning (ML) models and large language models (LLMs) to production at lightning speed, with increased transparency, traceability, and trust.

“As organizations rapidly adopt AI technology, it's essential to implement practices that ensure their efficiency and safety, and that incorporate AI responsibly,” said Gal Marder, EVP Strategy, JFrog. “By integrating DevOps, security, and MLOps processes into an end-to-end software supply chain workflow with NVIDIA NIM microservices, customers will be able to efficiently bring secure models to production while maintaining high levels of visibility, traceability, and control throughout the pipeline.”

With the rise and accelerated demand for AI in software applications, data scientists and ML engineers face significant challenges when scaling ML model deployments in enterprise environments. Fragmented asset management, security vulnerabilities, compliance issues, and performance bottlenecks are compounded by the complexities of integrating AI workflows with existing software development processes and the requirement for flexible, secure deployment options across various environments. This compounded complexity can result in very long, expensive deployment cycles and, in many cases, failure of AI initiatives.

“As enterprises scale their generative AI deployments, a central repository can help them rapidly select and deploy models that are approved for development,” said Pat Lee, Vice President, Enterprise Strategic Partnerships, NVIDIA. “The integration of NVIDIA NIM

microservices into the JFrog Platform can help developers quickly get fully compliant, performance-optimized models quickly running in production.”

JFrog Artifactory provides a single solution for housing and managing all the artifacts, binaries, packages, files, containers, and components for use throughout software supply chains. The JFrog Platform’s integration with NVIDIA NIM is expected to incorporate containerized AI models as software packages into existing software development workflows. By coupling [NVIDIA NGC](#) – a hub for GPU-optimized deep learning, ML and HPC models – with the JFrog platform and JFrog Artifactory model registry, organizations will be able to maintain a single source of truth for all software packages and AI models, while leveraging enterprise DevSecOps best practices to gain visibility, governance, and control across their software supply chain.

The integration between the JFrog Platform and NVIDIA NIM is anticipated to deliver multiple benefits, including:

- **Unified Management:** Centralized access control and management of NIM microservice containers alongside all other assets, including proprietary artifacts and open-source software dependencies, in JFrog Artifactory as the model registry to enable seamless integration with existing DevSecOps workflows.
- **Comprehensive Security and Integrity:** Continuous scanning at every stage of development - including containers and dependencies - delivering contextual insights across NIM microservices with JFrog auditing and usage statistics that drive compliance.
- **Exceptional Model Performance and Scalability:** Optimized AI application performance using NVIDIA accelerated computing infrastructure, offering low latency and high throughput for scalable deployment of LLMs to large-scale production environments.
- **Flexible Deployment:** Flexible deployment options via JFrog Artifactory, including self-hosted, multi-cloud, and air-gap deployment options.

For a deeper look at the integration of NVIDIA NIM into the JFrog Platform, read [this blog](#) or visit <https://jfrog.com/nvidia-and-jfrog>, where interested parties can also sign up for the beta program.

###

Like this story? Post this on X (Twitter): .@jfrog + @nvidia to deliver #secure, streamlined path for quickly building world-class #GenAI solutions. Learn more: <https://bit.ly/4fXMMz4> #MLOps #DevSecOps #GPUs #MachineLearning #AI

About JFrog

JFrog Ltd. (Nasdaq: FROG) is on a mission to create a world of software delivered without friction from developer to device. Driven by a “Liquid Software” vision, the JFrog Software Supply Chain Platform is a single system of record that powers organizations to build, manage, and distribute software quickly and securely, ensuring it is available, traceable, and tamper-proof. The integrated security features also help identify, protect, and remediate against threats and vulnerabilities. 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 Twitter: [@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 our expectations regarding the planned integration between the JFrog Platform and NVIDIA AI Enterprise and NVIDIA NIM, the anticipated enhanced security related to software supply chain workflows, the expected optimization of AI application performance, and potential benefits to developers and customers.

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, 2023, 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:

jfrog@bocacommunications.com

Investor Contact:

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