JFrog Unveils Secure AI Model Delivery Accelerated by NVIDIA NIM Microservices

New integration accelerates secure GenAI and LLM model deployment - including Meta's Llama 3 and Mistral AI LLMs packaged as NVIDIA NIM- with increased transparency, traceability and trust

Sunnyvale, Calif. & NEW YORK – March 4, 2025 – JFrog Ltd (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, is announcing general availability of its integration with NVIDIA NIM microservices, part of the NVIDIA AI Enterprise software platform. The JFrog Platform is the only unified, end-to-end, and secure DevSecOps and MLOps solution with native NVIDIA NIM integration. This enables rapid deployment of GPU-optimized, pre-approved machine learning (ML) models, and large language models (LLMs) to production with enterprise-grade security, increased visibility, and governance controls. This unified infrastructure enables developers to create and deliver AI-powered applications with greater efficiency and peace of mind.

"The demand for secure and efficient AI implementations continues to rise, with many businesses aiming to expand their AI strategies in 2025. However, AI deployments often struggle to reach production due to significant security challenges," said Gal Marder, Chief Strategy Officer at JFrog. "AI-powered applications are inherently complex to secure, deploy, and manage, and concerns around the security of open-source AI models and platforms continue to grow. We're excited to collaborate with NVIDIA to deliver an easy-to-deploy, end-to-end solution that enables companies to accelerate the delivery of their AI/ML models with enterprise-grade security, compliance, and provenance."

With the rise and accelerated demand for AI in software applications, data scientists and ML engineers face significant challenges when attempting to scale their enterprise ML model deployments. The complexities of integrating AI workflows with existing software development processes—coupled with fragmented asset management, security vulnerabilities, and compliance issues—can lead to lengthy, costly deployment cycles and, often, failed AI initiatives. According to IDC, by 2028, 65% of organizations will use DevOps tools that combine MLOps, LLMOps, DataOps, CloudOps, and DevOps capabilities to optimize the route to AI value in software delivery processes.

“The rise of open source MLOps platforms has made AI more accessible to developers of all skill levels to quickly build amazing AI applications, but this process needs to be done securely and in compliance with today’s quickly evolving government regulations,” said Jim Mercer, IDC’s Program Vice President, Software Development, DevOps & DevSecOps. “As enterprises scale their generative AI deployments, having a central repository of pre-approved, fully compliant, performance-optimized models developers can choose from and quickly deploy while maintaining high levels of visibility, traceability, and control through the use of existing DevSecOps workflows is compelling.”

The JFrog integration with NVIDIA NIM enables enterprises to seamlessly deploy and manage the latest foundational LLMs – including Meta's Llama 3 and Mistral AI – while maintaining enterprise-grade security and governance controls throughout their software supply chain. JFrog Artifactory - the heart of the JFrog Platform – provides a single solution for hosting and seamlessly managing all software artifacts, binaries, packages, ML Models, LLMs, container images, and components throughout the software development lifecycle. By integrating NVIDIA NIM into the JFrog Platform developers can easily access NVIDIA NGC – a hub for GPU-optimized deep learning, ML, and HPC models, providing customers with a single source for software models, software and tools \while leveraging enterprise DevSecOps best practices to gain visibility, governance, and control across their software supply chain.

The JFrog Platform update provides AI developers and DevSecOps teams with multiple benefits, including:

- **Unified ML & DevOps Workflows:** Data Scientists and ML Engineers can now version, secure, and deploy models using the same JFrog DevSecOps software development workflows they already know and trust. This eliminates the need for teams to use separate ML tools while ensuring automated compliance checks, audit trails, and governance of ML Models using JFrog Curation.
- **End-to-End Security & Integrity:** Implement continuous security scanning across containers, AI models and dependencies – delivering contextual insights across NIM microservices - to identify vulnerabilities, supplemented by smart threat detection that focuses on real risks and proactive protection against compromised AI models and packages.
- **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. Easily bundle ML models with dependencies to reduce external

requirements and utilize existing workflows for seamless AI deployment. Additionally, the JFrog Platform offers flexible deployment options for increased scalability, including self-hosted, multi-cloud, and air-gap deployments.

"Performance and security are crucial for successful enterprise AI deployments," said Pat Lee, vice president, Enterprise Strategic Partnerships, NVIDIA. "With NVIDIA NIM integrated directly into the JFrog Platform, developers can accelerate AI adoption with a unified, end-to-end solution for building, deploying, and managing production AI agents at scale."

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. You can also meet JFrog and NVIDIA at the inaugural MLOps Days community event, taking place March 4 in New York City, or during NVIDIA GTC, the premiere AI conference, taking place March 17 - 21, 2024 in San Jose, California. Get started and register, and book a meeting or hands-on demo here.

###

Like this story? Post this on X (Twitter): .@jfrog + @nvidia delivers the industry's first #softwaresupplychain solution, offering a secure, streamlined path for rapidly building world-class #GenAI solutions. Learn more: https://jfrog.co/4igNess #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 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 related to an anticipated increase in efficiencies in the development and accelerated delivery of AI-powered applications, and anticipated benefits to AI developers and DevSecOps team, including an expected increase in security, integrity and scalability.

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. Mngr. Global Communications, siobhanL@jfrog.cm

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