JFrog Becomes an AI System of Record, Launches JFrog ML – Industry's First End-to-End DevOps, DevSecOps & MLOps Platform for Trusted AI Delivery

JFrog ML Drives MLOps practices coupled with AI Security - Unifying Developer, Data Science & Operations Teams with Enterprise-wide Automation & Control of AI-powered Software Delivery

Sunnyvale, Calif. & NEW YORK – March 4, 2025 — JFrog Ltd (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today released JFrog ML, a revolutionary MLOps solution as part of the JFrog Platform designed to enable development teams, data scientists and ML engineers to quickly develop and deploy enterprise-ready AI applications at scale. As enterprise AI initiatives increasingly face security, scalability and management challenges, JFrog is now the only platform in the world that drives the secure delivery of machine learning technologies alongside all other application components in a single solution. JFrog ML is the first addition to the platform that resulted from QWAK.ai acquisition in 2024.

By seamlessly uniting machine learning (ML) practices with traditional DevSecOps development processes, organizations can help ensure their models are seamlessly deployed, secured, and maintained, which is expected to enhance model performance and dependability in real-world, production applications. The delivery of JFrog ML is an outcropping of JFrog's commitment to address the demand for more scalable, secure AI application delivery, including integrations with Hugging Face, AWS Sagemaker, MLflow (developed by Databricks), and NVIDIA NIM.

"As the demand for AI-powered applications continues to grow rapidly, so do the concerns around the ability to control and manage this new domain on all fronts – from MLOps to ML security. In fact, our own team of security researchers were the first to find and help remediate new, zero-day malicious ML models in Hugging Face," said Alon Lev, VP & GM, MLOps, JFrog. "JFrog ML combines superior, straightforward and hassle-free user experience for bringing models to production, combined with the level of trust and provenance enterprises expect from JFrog, allowing customers to accelerate their AI initiatives with confidence."

Developing ML models and making them production-ready is an extremely complex process, today demanding a blend of technical expertise and a deep understanding of software delivery. Models require careful planning and testing to ensure reliability and

efficiency in a live environment. Additionally, Data Scientists building models don't work in isolation—they need data engineers to structure and prepare data, software engineers to deploy models as microservices, and DevSecOps teams to ensure smooth and secure integration into production. JFrog ML helps overcome these often-crippling challenges with a structured framework designed to support the entire organization and ensure that models successfully get promoted out of experimental stages.

"Building and maintaining robust ML workflows requires a complex infrastructure, from feature engineering to model deployment and monitoring. JFrog ML is designed to enable these capabilities by utilizing JFrog Artifactory as the model registry of choice and JFrog Xray for scanning and securing ML models, making it possible to enhance user efficiency by providing a unified platform experience for DevOps, DevSecOps, and MLOps," said Yuval Fernbach, VP & CTO, JFrog ML. "As AI evolves, organizations can leverage JFrog ML to continuously adapt their infrastructure to support everything from traditional ML models to cutting-edge GenAI applications."

By treating ML models as software packages from the start of development and converging ML model management and software development into a single source of truth, the friction and errors between stages and teams can be significantly reduced. JFrog ML delivers AI development and deployment with full traceability, governance and security.

Key features include:

- **A unified DevOps, DevSecOps and MLSecOps platform:** JFrog ML as part of the JFrog Platform provides a holistic view of the entire software supply chain, from traditional software packages to LLMs and GenAI, streamlining AI pipelines and ensuring models are securely managed alongside other software artifacts.
- **Secured ML Models:** Enables AI innovation while keeping companies secure with the only platform providing off-the-shelf, enterprise-grade model security scanning of malicious or vulnerable models generated by your company - or those brought in from open source.
- **A single AI system of record:** Part of the JFrog Software Supply Chain Platform, JFrog ML manages ML models and datasets alongside other building blocks such as containers and Python packages, creating one place to enforce customizable security and compliance policies throughout the AI development process.
- **Intuitive model serving to production:** JFrog ML helps supercharge AI initiatives with simplified model development and deployment processes, helping data science and ML engineering teams accelerate model serving in production while dramatically improving security and simplifying model governance, rollback, and redeployment.

- **Model training and quality monitoring:** Complete dataset management and feature store support.
- **Trusted ML environment:** JFrog ML creates a reproducible artifact of every model built with the JFrog Platform, allowing for security scans and automated quality checks to ensure your models have been as rigorously vetted as your other software components.
- **Support for NVIDIA NIM enterprise-grade AI Models:** JFrog ML catalog will also include serving NIM-based models as part of its model library, allowing for one-click deployment.

For more information on JFrog ML read this blog or visit https://jfrog.com/jfrog-ml. You can also connect with JFrog ML experts at the inaugural MLOps Days community event, taking place March 4, 2025 in New York City, or during NVIDIA GTC, the premiere AI conference, taking place March 17 - 21, 2025 in San Jose, California. Learn more, register, and book a meeting or hands-on demo here.

###

Like this story? Post this on X (formerly Twitter): .@jfrog doubles-down on #MLOps with JFrog ML, bridging the gap between ML and #DevSecOps teams. Learn more: https://bit.ly/41BnHVm #DevOps #developers #JFrogML #machinelearning

About JFrog

JFrog Ltd. (Nasdaq: FROG) is on a mission to securely power the world with "Liquid Software," streamlining application delivery from developer to device. Our JFrog Software Supply Chain Platform enables organizations to build, manage, and securely distribute software, ensuring applications are traceable and tamper-proof. Built for advancing the world of AI, our platform aligns ML models with development processes, providing a unified source of truth for Engineering, MLOps, DevOps, and DevSecOps teams. This integration allows faster AI application releases with minimized risks and costs. Additionally, our platform features robust security to identify and remediate threats. Available as both self-hosted and SaaS services, JFrog is trusted by millions, including many Fortune 100 companies, to facilitate secure digital transformation. Discover 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 expected enhancements in model performance and dependability, anticipated acceleration of AI initiatives, anticipated reduction of friction and errors in the development process, and expected improvements in security and simplification of model governance.

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. MarComm Manager, JFrog, siobhanL@jfrog.com

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