JFrog Empowers a Secure AI Journey for Developers, Integrates with Databricks’ MLflow for a Seamless Machine Learning Lifecycle

New JFrog Artifactory integration provides developers and data scientists with an Open Source Software solution to simplify and securely accelerate ML Model development

Sunnyvale, Calif. – April 25, 2024 — JFrog Ltd. (“JFrog”) (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today announced a new machine learning (ML) lifecycle integration between JFrog Artifactory and MLflow, an open source software platform originally developed by Databricks. Following native integrations released earlier this year with Qwak and Amazon SageMaker, JFrog extends their universal AI solutions, offering organizations a single system of record with Artifactory as a model registry. The new integration gives JFrog users a powerful way to build, manage and deliver ML models and generative AI (GenAI)-powered apps alongside all other software development components in a streamlined, end-to-end, DevSecOps workflow. By making each model immutable and traceable, companies can validate the security and provenance of ML models, enabling responsible AI practices.

Industry research suggests 80% or more of ML models built to create new AI-powered applications fail to deploy, largely due to technical hurdles with integrating the model into existing operations. JFrog’s integration with MLflow helps organizations overcome this by seamlessly uniting the MLflow popular open source model development solution with an organization’s mature DevOps workflows – delivering end-to-end visibility, automation, control and traceability of ML models from experimentation to production.

“For organizations to successfully embrace and deliver AI and GenAI–powered applications at scale, developers and data science teams must manage models with trust, the same way they manage all software packages,” said Yoav Landman, CTO, JFrog. “This is only possible using a universal, scalable, single system of record for all binaries that delivers versioning, lifecycle, and security controls, which our new integration with MLflow provides.”

JFrog MLOps: A single source of truth for all models
Building on its successful integrations with all major ML tools in the market, the combination of JFrog Artifactory and MLflow enables ML engineers, Python, Java, and R developers with the freedom to work with their preferred tool stack, using Artifactory as their gold-standard model registry. JFrog’s universal, scalable platform also natively proxies Hugging Face allowing developers to always access available open source models while simultaneously detecting malicious models and enforcing license compliance. The solution also comes with the software security features and scanners provided by the JFrog Platform to maintain risk-free ML applications.

MLSecOps - Trusted and Curated models

The JFrog Security Research team recently discovered hundreds of instances of malicious AI ML models on the public Hugging Face AI repository posing a significant risk of data breaches or attacks. This incident highlights the potential threats lurking within AI-powered systems and underscores the need for constant security vigilance and proactive cyber hygiene.

Uniting JFrog Artifactory with MLflow will empower users to more easily build, train, and deploy models with greater security, governance, versioning, traceability, and trust by leveraging JFrog's scanning environment to rigorously examine every new model uploaded to Hugging Face.

For a deeper look at JFrog's integration with MLflow to power ML and GenAI-powered app development, read this blog post. Developers interested in going hands-on with these new features can download the free plug-in here.

###

Like this story? Post this on X (formerly Twitter): .@jfrog adds integration with @MLflow to help users create powerful #MLOps workflows and #GenAI-powered apps. Learn more: https://jfrog.co/44hjUfu #SoftwareSupplyChain #MLSecOps #SDLC #MachineLearning

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, to aid in making it 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.

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 the JFrog Artifactory and Amazon SageMaker integration enabling collaboration on building and deploying ML Models, JFrog new versioning capabilities and anticipated performance of its ML Model Management solution and the anticipated benefits to 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:
Siobhan Lyons, Global Communications, JFrog, siobhanL@jfrog.com

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