JFrog and AWS Accelerate Secure Machine Learning Development

New JFrog Artifactory and Amazon SageMaker integration empowers developers and data scientists to build, train, and deploy ML Models in the cloud

Sunnyvale, Calif. – January 17, 2024 — JFrog Ltd. ("JFrog") (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today announced a new integration with Amazon SageMaker, which helps companies build, train, and deploy machine learning (ML) models for any use case with fully managed infrastructure, tools, and workflows. By pairing JFrog Artifactory with Amazon SageMaker, ML models can be delivered alongside all other software development components in a modern DevSecOps workflow, making each model immutable, traceable, secure, and validated as it matures for release. JFrog also unveiled new versioning capabilities for its ML Model management solution, which help ensure compliance and security are incorporated at every step of ML model development.

"As more companies begin managing big data in the cloud, DevOps team leaders are asking how they can scale data science and ML capabilities to accelerate software delivery without introducing risk and complexity," said Kelly Hartman, SVP, Global Channels and Alliances, JFrog. "The combination of Artifactory and Amazon SageMaker creates a single source of truth that indoctrinates DevSecOps best practices to ML model development in the cloud – delivering flexibility, speed, security, and peace of mind – breaking into a new frontier of MLSecOps."

According to a recent Forrester survey 50 percent of data decision-makers cited applying governance policies within AI/ML as the biggest challenge to widespread usage, while 45 percent cited data and model security as the gating factor. JFrog's Amazon SageMaker integration applies DevSecOps best practices to ML model management, allowing developers and data scientists to expand, accelerate, and secure the development of ML projects in a manner that is enterprise-grade, secure, and abides by regulatory and organizational compliance.

JFrog's new Amazon SageMaker integration allows organizations to:

- Maintain a single source of truth for data scientists and developers, ensuring all models are readily accessible, traceable, and tamper-proof.
- Bring ML closer to the software development and production lifecycle workflows, protecting models from deletion or modification.

- Develop, train, secure and deploy ML models.
- Detect and block the use of malicious ML models across the organization.
- Scan ML model licenses to ensure compliance with company policies and regulatory requirements.
- Store home-grown or internally augmented ML models with robust access controls and versioning history for greater transparency.
- Bundle and distribute ML models as part of any software release.

“Traditional software development processes and machine learning stand apart, lacking integration with existing tools,” said Larry Carvalho, Principal and founder of RobustCloud. “Together, JFrog Artifactory and Amazon SageMaker provide an integrated end-to-end, governed environment for machine learning. Bringing these worlds together represents significant progress towards harmonizing machine learning pipelines with established software development lifecycles and best practices.”

Along with its Amazon SageMaker integration, JFrog unveiled new versioning capabilities for its ML Model Management solution that incorporate model development into an organization’s DevSecOps workflow to increase transparency around each model version so developers, DevOps teams, and data scientists can ensure the correct, secure version of a model is utilized.

The JFrog integration with Amazon SageMaker, available now for JFrog customers and Amazon SageMaker users, ensures all artifacts consumed by data scientists or used to develop ML applications are pulled from and saved in JFrog Artifactory.

For a deeper look at the integration and how it works read this blog. You can also register to join JFrog and AWS on Wednesday, January 31 at 1 p.m. ET/10 a.m. PT for an educational webinar, "*Building for the future: DevSecOps in the era of AI/ML model development*," describing best practices for introducing model use and development into secure software supply chain and development processes.

###

Like this story? Post this on X (formerly Twitter): .@jfrog rolls out new integration with @awscloud SageMaker to unlock greater #ML #security and innovation across the software development lifecycle. Learn more: https://jfrog.co/4aW18gT #SoftwareSupplyChain #DevSecOps #SDLC #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.

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 for 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, 2022, 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.

Media Contact:
Siobhan Lyons, Sr. MarComm Manager, JFrog, siobhanL@jfrog.com

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