

JFrog Introduces Native Integration for Hugging Face, Delivering Robust Support for ML Models to Harmonize DevOps, Security and AI

DevOps teams, ML Engineers and Data Scientists can now store, secure, govern and manage AI components with confidence, including industry-first platform for detecting malicious ML models

swampUP San Jose – September 13, 2023 — [JFrog Ltd.](#) (“JFrog”) (Nasdaq: FROG), the Liquid Software company and creators of the [JFrog Software Supply Chain Platform](#), today introduced [ML Model Management](#) capabilities, an industry-first set of functionality designed to streamline the management and security of Machine Learning [ML] models. The new ML Model Management capabilities in the JFrog Platform bring AI deliveries in line with an organization’s existing DevOps and DevSecOps practices to accelerate, secure and govern the release of ML components.

“Today, Data Scientists, ML Engineers, and DevOps teams do not have a common process for delivering software. This can often introduce friction between teams, difficulty in scale, and a lack of standards in management and compliance across a portfolio,” said Yoav Landman, Co-founder and CTO, JFrog. “Machine learning model artifacts are incomplete without Python and other packages they depend on and are often served using Docker containers. Our customers already trust JFrog as the gold standard for artifact management and DevSecOps processes. Data scientists and software engineers are the creators of modern AI capabilities, and already JFrog-native users. Therefore, we look at this release as the next logical step for us as we bring machine learning model management, as well as model security and compliance, into a unified software supply chain platform to help them deliver trusted software at scale in the era of AI.”

AI and ML usage continues to grow rapidly. IDC Research indicates the worldwide AI/ML market, including software, hardware, and services, is forecast to grow 19.6 percent to over \$500B in 2023. However, as more ML models are being moved to production, the end users often face challenges including cost, lack of automation, lack of expertise, and ability to scale.¹

“It can take significant time and effort to deploy ML models into production from start to finish. However, even once in production, users face challenges with model performance, model drift, and bias,” said Jim Mercer, Research Vice President, DevOps & DevSecOps, IDC. So, having a single system of record that can help automate the development, ongoing management, and security of ML Models alongside all other components that get packaged into applications offers a compelling alternative for optimizing the process.”

Using JFrog’s new ML Model Management capabilities organizations can:

- Proxy the popular public ML repository [Hugging Face](#) to cache open source AI models companies rely on, bringing them closer to development and production, protecting them from deletion or modification.
- Detect and block use of malicious ML models.
- Scan ML model licenses to ensure compliance with company policies.

¹ IDC, “MLOps – where ML meets DevOps,” by Jim Mercer, Research Vice President, DevOps & DevSecOps, March 2022

<https://www.idc.com/getdoc.jsp?containerId=US48544922&pageType=PRINTFRIENDLY>

- 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.

“Increasing numbers of organizations are starting to incorporate ML models into their applications and with several government regulations requiring software vendors to list exactly what’s inside their software, we believe it won’t be long before these guidelines grow to include ML and AI models as well,” said Yossi Shaul, SVP Product and Engineering, JFrog. “We’re excited to give customers an easy way to proxy, store, secure, and manage models alongside their other software components to help accelerate their pace of innovation while remaining well-positioned for tomorrow’s demands.”

For more information on the beta release of the new ML Model Management capabilities in the JFrog Platform, read [this blog](#) or visit <https://jfrog.com/mlops/>.

###

Like this story? Tweet this: .@jfrog unveils new #MLOps capabilities in #Artifactory to deliver complete visibility and governance of ML Models being built and in production: bit.ly/3Pz4jIY
#SoftwareSupplyChain #DevSecOps

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 JFrog’s Machine Learning Model Management capabilities, the anticipated benefits to customers, the projected growth of the AI/ML market and potential government regulation.

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 the impact of JFrog’s products 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