JFrog and Hugging Face Team to Improve Machine Learning Security and Transparency for Developers

New integration significantly improves the quality and trustworthiness of open-source ML Models, resulting in safer, more responsible AI for everyone

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 announced it is partnering with Hugging Face, host of the world's largest repository of public machine learning (ML) models — the Hugging Face Hub — designed to achieve more robust security scans and analysis for every ML model in their library. The new integration is designed to provide higher levels of trust for scanning results by prominently displaying a "JFrog Certified" checkmark, so developers, data scientists, and ML Engineers know which models are safer to use.

"As ML models become integral to critical business applications, ensuring these models are secure is crucial for preventing breaches, data leaks, and decision-making errors," said Asaf Karas, CTO of JFrog Security. "We've been working with Hugging Face since 2023 to help securely bring ML Models to production. We also found intentionally malicious models in Hugging Face in early 2024, which prompted us to dedicate more of our security experts to help scan and assess the well-being of all Hugging Face models to ensure they are safe for use in AI application development."

Machine learning (ML) introduces a new set of supply chain assets, such as models and datasets, which not only come with their own security challenges but also increase an organization's attack surface. These newer areas of the ML supply chain may allow nefarious actors to achieve remote code execution to infiltrate and spread malicious code inside an organization through ML Models. This could potentially grant access to critical internal systems and pave the way for large-scale data breaches or even corporate espionage, impacting not just individual users but potentially entire organizations across the globe.

Ensuring ML Model Integrity with JFrog Advanced Security

JFrog Xray and JFrog Advanced Security – key components of the JFrog Software Supply Chain Platform – are designed to scan AI/ML model artifacts for threats at every stage of their lifecycle. These threats include model serialization attacks, known CVEs, backdoors, and more. Now Hugging Face will utilize JFrog Advanced Security scans in its Hugging Face

Hub, allowing each model contained within the platform to be scanned in advance of being downloaded for use. The results of each scan will be prominently displayed for all users to see.

This new advanced security integration between Hugging Face and JFrog differs from existing ML model scanners due to JFrog's malicious code decompilation and deep data flow analysis. While existing solutions simply check for automatically-executed code embedded in a model, JFrog's model scanner uses an enhanced approach to extract and analyze the embedded code which eliminates more than 96% of false positives produced by other scanners on current Hugging Face models.

In addition, JFrog's enhanced analysis highlighted 25 models as zero-day malicious in nature. These are machine learning models hosted in Hugging Face which were not identified as malicious by any other scanner available for Hugging Face based on our evaluation.

Surveys have found that while over 80% of enterprises are using or experimenting with AI applications, more than 90% feel they are unprepared for AI security challenges. Additionally, cybersecurity agencies from the U.S., the U.K., and Canada have jointly issued warnings, advising businesses to carefully scan any pre-trained models for harmful code.

"For a long time, AI was a researcher's field, and the security practices were quite basic, but as the popularity and widespread use of AI grows, so do the number of potentially bad actors who may want to target the AI community in general and our platform more specifically," said Julien Chaumond, CTO, Hugging Face. "As the leading collaboration platform for AI models, we're delighted to deepen our partnership with JFrog to implement high-quality scanning capabilities for our AI/ML models and deliver greater peace of mind for developers looking to create the next generation of AI-powered applications."

For a deeper look at how ML Model scanning of Hugging Face is being performed using the JFrog Platform, read this blog or learn more about JFrog's Hugging Face integration, scanning malicious AI models, and model threat categories.

You can also learn more about how JFrog and other AI industry players are contributing to AI/ML security 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, or book a meeting for a demo here.

We welcome the community to send feedback on this integration directly to JFrog's security research team at research@jfrog.com.

###

Like this story? Post this on X (formerly Twitter): @JFrog and @huggingface unite to provide integrated security scanning tools in the Hugging Face platform, helping users detect malicious code before downloading any #ML models. Learn more: https://jfrog.co/41kYaOT #MLOps #AI #softwaresupplychain #security #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 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 regarding increased levels of safety and security of the integrated product and anticipated increased trust of users related to the model scanner.

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. Manager, Global Communications, siobhanL@jfrog.com

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