JFrog and Qwak Create Secure MLOps Workflows for Accelerating the Delivery of AI Apps at Scale

New native integration empowers organizations to deliver ML applications efficiently with end-to-end software supply chain visibility, governance, and security

Sunnyvale, Calif. – February 28, 2024 — JFrog Ltd. ("JFrog") (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today announced a new technology integration with Qwak, a fully managed ML Platform, that brings machine learning models alongside traditional software development processes to streamline, accelerate, and scale the secure delivery of ML applications.

"Currently, data scientists and ML engineers are using a myriad of disparate tools, which are mostly disconnected from standard DevOps processes within the organization, to mature models to release. This slows MLOps processes down, compromises security, and increases the cost of building AI powered applications," said Gal Marder, Executive Vice President of Strategy, JFrog. "The combination of the JFrog Platform – with Artifactory and Xray at its core - plus Qwak provides users with a complete MLSecOps solution that brings ML models in line with other software development processes, creating a single source of truth for all software components across Engineering, MLOps, DevOps and DevSecOps teams so they can build and release AI applications faster, with minimal risk and less cost."

Uniting JFrog Artifactory and Xray with Qwak's ML Platform brings ML apps alongside all other software development components in a modern DevSecOps and MLOps workflow, enabling data scientists, ML engineers, Developers, Security, and DevOps teams to easily build ML apps quickly, securely, and in compliance with all regulatory guidelines. The native Artifactory integration connects JFrog's universal ML Model registry with a centralized MLOps platform so users can easily build, train, and deploy models with greater visibility, governance, versioning, and security. Using a centralized platform for ML model deployment also allows users to focus less on infrastructure and more on their core data science tasks.

IDC research indicates that while AI/ML adoption is on the rise, the cost of implementing and training models, shortage of trained talent, and absence of solidified software

development life-cycle processes for AI/ML are among the top three inhibitors to realizing the full benefits of AI/ML at scale.[1]

"Building ML pipelines can be complicated, time-consuming, and costly to organizations looking to scale their MLOps capabilities. These homegrown solutions are not equipped to manage and protect the process of building, training, and tuning ML models at scale with little to no audibility," said Jim Mercer, Program Vice President Software Development, DevOps, and DevSecOps. "Having a single system of record that can help automate the development, providing a documented chain of provenance, and security of ML models alongside all other software components offers a compelling alternative for optimizing the ML process while injecting more model security and compliance."

Without the right infrastructure, platform and processes needed for ML operations (MLOps), it's challenging to build, manage, and scale complex ML infrastructure, deploy models quickly, and secure them without incurring excessive costs. Companies often struggle to manage infrastructure complexity causing expensive and time-consuming authentication and security protocols between various development environments.

"AI and ML have recently transformed from being a distant future prospect to a ubiquitous reality. Building ML models is a complex and time-intensive process, which is why many data scientists are still struggling to turn their ideas into production-ready models," said Alon Lev, CEO, Qwak. "While there are plenty of open source tools on the market, putting all of those together to build a comprehensive ML pipeline isn't easy, which is why we're thrilled to work with JFrog on a solution for automating ML artifacts and releases in the same, secure way customers manage their software supply chain with JFrog Artifactory and Xray."

Proof of why having secure, end-to-end MLOps processes is imperative was further confirmed by the JFrog Security Research team in their discovery of malicious ML Models in Hugging Face, a widely used AI model repository. Their research found that several malicious ML Models housed in Hugging Face posed the threat of code execution by threat actors, which could lead to data breaches, system compromise, or other malicious actions.

For a deeper look at the integration between the JFrog Platform and Qwak and how it works, read this blog or view this video. You can also register to join JFrog and Qwak for an informative webinar detailing best practices for introducing model use and development

[1] "*Machine Learning Life-Cycle Tools and Technologies," by Kathy Lange, Research Director, AI Software* *https://www.idc.com/getdoc.jsp?containerId=IDC_P40729*

into secure software supply chain and development processes, on Tuesday, April 2, 2024 at 9 a.m. PST/5 p.m. UTC.

###

Like this story? Post this on X (formerly Twitter): .@jfrog extends #MLops reach through platform integration with @Qwak_ai to unlock greater #ML #security and innovation across the #SoftwareSupplyChain. Learn more: https://jfrog.co/48sCi5O #DevOps #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 Qwak, a fully managed ML Platform to streamline, accelerate, and scale the secure delivery of ML applications 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.

Media Contact:

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

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