JFrog Unveils First Runtime Security Solution to Deliver Complete Software Integrity and Lineage from Code to Cloud

Complete software lifecycle security enables organizations to simultaneously shift left & right, helping developers save time with quick threat detection and risk remediation

Sunnyvale, Calif. and Austin, TX – JFrog swampUP – September 10, 2024 — JFrog Ltd. ("JFrog") (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today announced the addition of JFrog Runtime to its suite of security capabilities, empowering enterprises to seamlessly integrate security into every step of the development process, from writing source code to deploying binaries into production. The JFrog Platform streamlines collaboration between developers and security teams, automating DevSecOps tasks to save time and strengthen security for modern, cloud-native application development. It equips teams to monitor Kubernetes clusters in real time, enabling them to identify, prioritize, and quickly address security incidents based on actual risk. Additionally, it helps ensure image integrity and helps meet compliance requirements effectively.

"As organizations increasingly shift left to combat today's growing threat landscape, the disconnect among siloed tools places additional strain on developers, security, and MLOps teams," said Asaf Karas, CTO of JFrog Security. "Companies can alleviate this burden by adopting a unified platform that provides end-to-end visibility, remediation, and traceability across the development and security processes. By empowering DevOps, Data Scientists, and Platform engineers with an integrated solution that spans from secure model scanning and curation on the left to JFrog Runtime on the right, organizations can significantly enhance the delivery of trusted software at scale."

A recent IDC survey sponsored by JFrog found that organizations spend an average of $542 per week per developer on security-related or DevSecOps tasks, equating to $1.89 million annually. Developers want to focus on coding, while security teams prioritize risk mitigation. JFrog Runtime empowers users to track and manage packages from various origins, organize repositories by environment types, and activate JFrog Xray policies, ultimately fortifying security from code to runtime. As part of the JFrog Platform, Runtime also addresses the visibility and alignment gaps among teams, optimizing version control and package development, while ensuring R&D, DevOps, and security teams can collaborate effectively and efficiently, saving developers hours of valuable time.

"Runtime security is critical for our customers as it ensures that their applications remain protected while in operation. With the increasing complexity of cloud

environments and the rise of containerized applications, real-time visibility into potential vulnerabilities is essential," said Paul Goldman, CEO, iTMethods. "JFrog Runtime will help enhance our customers' security posture by allowing them to rapidly detect and respond to threats, thus safeguarding their data and maintaining trust in their cloud services."

Industry research shows that one in five applications contain runtime exposure, with 20 percent of all applications having high, critical, or apocalyptic issues during the execution stage. By automating security for fast-moving, dynamic applications like those that run in containers, JFrog Runtime security addresses the unique visibility and insight needs of cloud-native environments.

Key features and benefits of JFrog Runtime include:

- **Real-Time Vulnerability Visibility:** Gain real-time insights into vulnerabilities within your runtime environment.
- **Accelerated Triage with Advanced Prioritization:** Streamline the identification and prioritization of security incidents based on their business impact.
- **Reduced Risk Through Exposure Management:** Quickly identify the source and ownership of vulnerable packages, enabling faster risk mitigation.
- **Protection for Cloud-Based Workloads:** Aid in safeguarding applications with continuous monitoring for post-deployment threats such as malware attacks and privilege escalation.
- **Comprehensive Analytics for Kubernetes clusters:** Enable continuous runtime evaluation of workloads and containers for real-time vulnerability detection and alignment to the corresponding processes and files within JFrog Artifactory.
- **Centralized Incident Awareness:** Maintain a consolidated view of your runtime environment to facilitate accurate incident identification and response.

"A platform that unifies security across the software supply chain from development to production can provide critical visibility and traceability that developers and DevSecOps teams need to manage and remediate risks effectively," said Katie Norton, research manager, DevSecOps and Software Supply Chain Security at IDC. "JFrog's addition of runtime security supports a shift-left and shift-right strategy, fostering comprehensive protection and streamlined processes that lessen the strain on development and security teams."

JFrog Runtime complements JFrog's already robust suite of advanced security capabilities including:

- **AI/ML Model Curation:** JFrog Curation helps defend your software supply chain by enabling early detection and blocking of malicious ML Models retrieved from

open-source repositories like Hugging Face before they even enter your organization. JFrog's universal, scalable security platform also natively proxies Hugging Face allowing developers to access open source AI/ML models while simultaneously detecting malicious models, block their use if needed, and enforcing license compliance to enable safer use of AI.

- **Secure OSS Catalog:** The JFrog open-source software (OSS) package catalog provides a "search engine for software packages" using the JFrog UI or via API. Backed by both public and JFrog data, the OSS Catalog gives users quick insight into the security and risk metadata associated with all OSS packages.

For additional information on JFrog Runtime and the entire suite of JFrog security solutions visit https://jfrog.com/runtime. You can also read this blog and register to join JFrog security experts for a webinar deep diving into JFrog Runtime capabilities on October 2 and 15, 2024 at a time that works best for you.

###

Like this story? Post this on X (formerly Twitter): .@jfrog unveils industry's first Runtime solution that integrates #security at every development stage, from source code to production. Learn more: https://jfrog.co/3THB7Lp #SoftwareSupplyChain #DevSecOps #SDLC

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 our expectations with respect to the runtime security product to its suite of security capabilities to integrate security into the development process.

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:
jfrog@bocacommunications.com

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