JFrog Unveils World's First DevOps-Centric Security Solution to Control the Entire Software Supply Chain

JFrog Advanced Security Unifies Developer, Security, and Operations Teams with Enterprise-wide Automation and Control of the Software Delivery Flow

Sunnyvale, Calif. – October 18, 2022 — JFrog Ltd. ("JFrog") (NASDAQ: FROG), the Liquid Software company and creators of the JFrog DevOps Platform, today released JFrog Advanced Security – the world's first binary-focused, DevSecOps solution providing holistic security coverage from any source to any destination. Natively integrated with JFrog's Artifactory binary repository and JFrog Xray's software composition analysis tool, JFrog Advanced Security capabilities offer users a full platform experience and coverage for software supply chain security at scale.

Research indicates cybercrimes cost the global economy 6 trillion dollars in 2021 and this figure is expected to increase to 10.5 trillion dollars by 2025.[1] The biggest threat vector in today's cybersecurity attacks is open source code, as bad actors look to exploit "weak links" in a company's software supply chain such as critical vulnerabilities, misconfigured services, or leaked secrets. At the same time, developers, security leaders, and operations teams are juggling a myriad of disparate security point solutions, which collectively deliver an incomplete view of their software ecosystem. JFrog Advanced Security is designed to provide visibility and control of a company's software supply chain using a single, unified platform and intuitive UI, which helps dramatically reduce overhead, and quickly identify malicious code that commonly compromises development, deployment, and runtime processes.

"The depth of security and remediation solutions vendors provide is limited by the data they own, protect, and analyze. JFrog functions as a single source of record for companies' binaries at the heart of our customers' software supply chain. This means JFrog is uniquely positioned to provide security solutions from the inside out, with comprehensive and holistic solutions," said Shlomi Ben Haim, co-founder and CEO of JFrog. "This is required in a world where every developer has become the target, and every DevOps team knows the only way the entire supply chain can be secured is through binaries. Our customers asked us to provide end-to-end coverage and control, and we're excited and proud to launch the most advanced security solution we've ever introduced as part of our DevOps platform."

Security teams will do whatever it takes to secure the business, while developers want to create quality software vs. spending all day fixing vulnerabilities. Both sides are investing in fortifying the business, but collaboration between the two teams and a clear picture of software package dependencies can be hindered by disparate systems, varying or redundant information and inconsistent reporting.

---

[1] "Resilience Requires a Modern Path to Board-Level Cyber, Privacy and Data Risk Governance," *Nasdaq Center for Board Excellence 'Risk & Cyber Oversight' Insights Council*, by *Rajesh De, Chris Hetner, Steve Roycroft, and Dominique Shelton Leipzig*, Oct. 2022.

"Many of today's enterprise software security solutions fall short because they only focus on source code and what happens before that software is in production," said Asaf Karas, CTO, JFrog Security. "However, to truly protect your software supply chain you need to consider both code in development and in production at the binary level. JFrog Advanced Security provides a rich set of binary and source code analysis capabilities spanning from developer to production environments in a single, integrated DevOps platform – helping eliminate complexity, streamline security detection, assessment, and remediation efforts."

By creating an intelligent bridge between developers, security, and operations teams, fueled by a highly-skilled security research team, JFrog Advanced Security is designed to be a single source of truth for guiding critical vulnerability exposure (CVE) detection, assessment, and remediation strategies using:

- **Exposed Secrets Detection:** Uncover "secrets" such as passwords, access tokens and private keys that have been leaked or left exposed in any container stored in JFrog Artifactory to prevent the accidental leak of API keys, internal tokens, or credentials that can put enterprises at risk.
- **Container Contextual Analysis:** This industry-first technology provides the ability to scan containers for the presence of malicious packages or use of vulnerable open-source code inside enterprise applications early in the development process. Container Contextual Analysis can also detail which open source vulnerabilities are actually exploitable in the context of a company's own code, allowing developers to disregard or de-prioritize non-applicable incidents, which helps sharpen focus and remediation efforts.
- **Insecure use of Libraries and Services:** Helps developers to quickly identify whether common open-source software libraries and services are used or configured insecurely, leaving their enterprises susceptible to attack.
- **Vulnerable Infrastructure-as-Code (IaC):** Customers can inspect IaC files stored in their JFrog Artifactory instance to ensure cloud infrastructure deployments are not misconfigured – making them exploitable.
- **Single Scalable Architecture**: The JFrog Platform provides both a legend of artifacts within an organization, augmented by JFrog Advanced Security features for comprehensive control and safeguarding of an entire software portfolio across on prem, cloud, multi-cloud and hybrid deployments extending out to the edge at any scale.
- **Native Integration with Artifactory:** JFrog Artifactory is the core of the JFrog Platform, functioning as a universal binary repository, allowing companies to securely control and manage update flows across the software supply chain at scale.

"As the volume and sophistication of cyberattacks continues to escalate, organizations are challenged to constantly monitor threats and work cross-functionally to resolve them, while using a myriad of disjointed point solutions which can slow them down," said Jim Mercer, Research Director for DevOps and DevSecOps at IDC. "Companies need more of a platform approach to cohesively integrate security into the DevOps workflow to bridge developers,

operations, and security teams to remediate threats across the software supply chain efficiently."

To learn more about JFrog Advanced Security read this blog, visit https://jfrog.com/advanced-security, or join us for an informative product overview webinar, *"Announcing JFrog Advanced Security"* on October 20, 2022, at 9:00 a.m. PST / 12:00 p.m. EST / 6:00 p.m. CEST. Learn more and register here. Interested parties can also see the new JFrog Advanced Security capabilities in action during the swampUP City Tour taking place in New York, London, and Munich between October 18 – 24, and at booth P10 during KubeCon taking place October 24 - 28 in Detroit, MI.

###

Like this story? Tweet this: .@jfrog unveils world's first #devOps-centric #security solution for enterprise-wide visibility and control of the software supply chain. Learn more https://bit.ly/3CDiLSi #devsecops #developers #swampUP 2022

About JFrog

JFrog Ltd. (NASDAQ: FROG) is on a mission to power all the world's software updates, driven by a "Liquid Software" vision to allow the seamless, secure flow of binaries from developers to the edge and connected devices. The JFrog Platform enables software creators to power their entire software supply chain throughout the full binary lifecycle, so they can build, secure, distribute, and connect any source with any production environment. JFrog's hybrid, universal, multi-cloud DevOps platform is available as both self-managed and SaaS services across major cloud service providers. Millions of users and thousands of customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely manage their mission-critical software supply chain. 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 JFrog's Advanced Security technology, statements made by JFrog's Executives, and the ability of Advanced Security to help resolve cybersecurity threats, reduce overhead, identify malicious code, eliminate complexity and streamline security detection, assessment and remediation efforts.

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, 2021, 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