JFrog Exposes Enterprise AI Blind Spots, Driving Centralized Software Supply Chain Governance

New Shadow AI Detection capability enables transparency and risk management, guarding against uncontrolled use of AI models and API calls

Sunnyvale, Calif. and Berlin, Germany – November 13, 2025 — JFrog Ltd (Nasdaq: FROG), the Liquid Software company, today announced an expansion of its AI governance capabilities within the JFrog Software Supply Chain Platform with the introduction of Shadow AI Detection. The new capability, introduced at JFrog swampUP Europe, is designed to equip enterprises with the visibility and control needed to govern and secure the entire AI supply chain, guarding against the uncontrolled use of AI models and APIs, known as Shadow AI, which can introduce significant security and compliance risks.

"Recognizing and mitigating the risks of shadow AI is becoming a critical priority for CIOs and CISOs who must strike a balance between innovating while maintaining security. Organizations should follow proven software development practices by creating developer-friendly workflows with strong security and robust governance," said Yuval Fernbach, VP and CTO, JFrog ML. "The addition of Shadow AI Detection capabilities is intended to strengthen JFrog's leadership in securing the AI supply chain 360-degrees, helping companies utilize AI safely and responsibly."

Delivering Transparency for Better Governance of AI Models and APIs

The rapid integration of AI across development pipelines has created a major governance challenge for organizations. For example, developers and data science teams frequently integrate AI models and services directly from providers such as Anthropic, OpenAI, and Google without organizational oversight. This ungoverned activity, often referred to as Shadow AI, creates dangerous blind spots that leave enterprises vulnerable to compliance violations, data leaks, and supply chain attacks.

JFrog's new Shadow AI Detection helps automatically detect and create an inventory of all internal AI models and external API gateways used across the organization to access data from either approved or ad-hoc third-party sources. Once discovered, these newly visible models and services can be governed centrally, empowering teams to:

- **Enforce security and compliance policies** across all AI assets.
- **Establish defined paths for authorized users** to access and utilize third-party AI services, ensuring controlled and fully auditable interactions.
- **Track and monitor usage** of external AI models and APIs such as OpenAI or Gemini.

Meeting the Global AI Compliance Imperative

The need for a full audit trail of AI activity is becoming an imperative due to emerging global regulations and security risks. JFrog's new AI detection capabilities are intended to enable enterprises to uphold compliance and security in line with key frameworks such as the US Transparency in Frontier AI Act, EU Cyber Resilience Act, EU AI Act, Germany's BSI Guidelines, the EU's NIS2, and the Guidelines and Companion Guide for Securing AI Systems. Collectively, these regulations aim to deliver provenance, accountability, and establish resilience across the AI and software supply chain by:

- Ensuring responsible AI development
- Enforcing rigorous risk management and reporting standards
- Mandating visibility into software components
- Securing AI systems from design to deployment

JFrog Shadow AI Detection is available as part of JFrog AI Catalog, with a GA release planned in 2025. For more information on the entire JFrog Software Supply Chain Platform visit https://jfrog.com/.

###

Like this Story? Share this on X: Our new #ShadowAI Detection capabilities give companies visibility & control over unmanaged #AI models and #API usage, bringing enterprise-grade #governance to the entire AI #softwaresupplychain. https://bit.ly/3LAfuLE #DevGovOps #DevSecOps #AIsecurity #AIGovernance

About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps and MLOps platform, is on a mission to create a world of software delivered without friction from developer to production. 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 that is available, traceable, and tamper-proof. Integrated security features also help identify, protect, and remediate against threats and vulnerabilities. JFrog’s hybrid, universal, multi-cloud platform is available as both SaaS services across major cloud service providers and self-hosted. Millions of users and 7K+ customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation. Learn more at www.jfrog.com or 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 the expected performance of Shadow AI Detection, including but not limited to compliance and security related to key regulatory frameworks in a rapidly changing regulatory environment.

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, Director, Global Communications, siobhanL@jfrog.com

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