



NEWS RELEASE

# JFrog Closes the Shadow AI Blind Spot: Unveils AI-SEC to Control Every AI Agent, Skill, and Model, from Developer to Production

2026-10-21

*New Local Shadow AI Detection and Bring Your Own LLM Key scanning give security teams oversight of AI assets that pipeline and registry controls never reach*

SUNNYVALE, Calif. & BARCELONA, Spain--(BUSINESS WIRE)-- **swampUP Europe 2026** – [JFrog Ltd.](#) (Nasdaq: FROG), the Liquid Software company and creators of the [JFrog Software Supply Chain Platform](#), the system of record for trusted software artifacts, binaries, and AI assets, today announced advancements in [JFrog AI Security](#), bringing AI asset detection, scanning and policy enforcement together in a single solution for the AI-Driven Software Supply Chain. JFrog is building upon its current Shadow AI Detection capabilities, extending to the developer endpoint. [Local Shadow AI Detection](#) surfaces AI assets running directly on developer machines, where pipeline and registry controls don't reach. JFrog is also introducing New [AI Asset Scanning with Bring Your Own LLM Key](#) (BYOK), which lets customers scan skills, coding agent plugins, and APM packages using their own LLM instance, so they can vet this layer of the AI supply chain on infrastructure they control.

JFrog's new Local Shadow AI Detection and Bring Your Own LLM Key (BYOK) scanning give security teams oversight of AI assets that pipeline and registry controls never reach.

"Developers are already running AI agents organizations can't see. JFrog AI Security brings

them under control," said Shlomi Ben Haim, Co-Founder and CEO, JFrog. "Until now, the conversation around AI agents has focused on what they can build vs. what they can break or who answers for it when that happens. The question is no longer whether agents will touch your supply chain – it's

whether you can prove what they touched. Our customers live in a zero-trust world and can't trust AI agents or developers using AI blindly. JFrog brings detection, scanning, and policy enforcement for the AI-powered software supply chain into one solution."

## Attackers Moved from Code to Instructions

The [JFrog 2026 Software Supply Chain Security State of the Union](#) report tracked malicious AI agent skills, identifying 969 carrying high-impact payloads, alongside 495 malicious AI models on Hugging Face. Existing AppSec tools were built to catch vulnerable code. Agent skills, plugins, and APM packages ship something different: plain-English instructions that an agent reads and acts on.

JFrog's AI Security bridges that gap with three capabilities: [Local Shadow AI Detection](#), which inventories the AI assets in use; [AI Asset Scanning](#), which reads the intent of models, skills, plugins, and APM packages; and [JFrog Agent Guard](#), which enforces policy at the point an agent reaches for any of them. Together, they give security and developer teams a single source of truth for AI assets.

## Shadow AI Detection Now Extends to the Developer Endpoint

Security teams increasingly need to know which AI assets are in use and who introduced them. Developers install skills, plugins, MCP servers, hooks, and other agentic assets through Git, Slack, marketplaces, and zip files, often outside the security teams' review. Each of these assets runs with the developer's own permissions and credentials, and it is not always clear what was installed, who installed it, or whether anyone approved it – which becomes increasingly problematic in an environment that is becoming more and more compliance driven.

JFrog's new Local Shadow AI Detection extends visibility to developers' machines by:

- **Detecting assets as they land:** Deployed through the JFrog Agent Plugin on the developer workstation via mobile device management (MDM) or agent harness settings, it finds skills, plugins, and MCP servers, regardless of which repository or marketplace they came from.
- **Scanning on the local device:** Deterministic scanning runs on the workstation itself, and only metadata and a risk assessment go back to the JFrog Platform.
- **Creating a baseline:** Every asset is cross-referenced against source data in the JFrog Platform to understand what is approved for use, enabling security teams to move forward with confidence.

With [JFrog AI Security](#), platform engineering and security teams finally have comprehensive visibility and policy enforcement through a single system of record.

## AI Asset Scanning with BYOK

The new [AI Asset Scanning Bring Your Own LLM Key](#) (BYOK) capabilities use semantic scanning with the customer's own private LLM account helping customers to:

- **Keep control of their data:** Prompts and skills go directly from the JFrog Platform to the customer's model endpoint, with nothing routed through a JFrog-hosted gateway.
- **Leveraging existing LLM contracts:** Customers using their own key can scan and be billed through their own provider, leveraging existing investments. For JFrog's self-hosted customers, BYOK is the only way to run AI Asset Scanning.

"Security teams need visibility that starts at the developer's machine – before an asset ever reaches a coding agent or is shared through Artifactory. Regulated customers need scanning that points at their own models," said Yuval Fernbach, Vice President & CTO, JFrog AI Security. "Local Shadow AI Detection

and AI Asset Scanner address both needs in a single solution: JFrog AI Security."

JFrog AI Security, including Local Shadow AI Detection and AI Asset Scanning, is available now to JFrog Unified Security and Ultimate Security customers. Initial releases of JFrog AI Asset Scanning BYOK supports: Anthropic's Opus 4.8, OpenAI's GPT 5.6 Sol, and Google's Gemini 3.1 Pro. To learn more about Local Shadow AI Detection, visit <https://jfrog.com/ai-security/> or check out this [product demo](#).

***Like this Story? Share this on X:*** AI agents don't just write software, they follow instructions. JFrog Research uncovered 969 AI agent skills carrying high-impact malicious payloads. Attackers aren't breaking in, they're being invited. @JFrog AI Security puts every model, skill, plugin, and MCP server under one system of record, from laptop to production. Learn more: <https://jfrog.co/4zIDm3r> #AISecurity #AgentSecOps #DevGovOps #DevSecOps #softwaresupplychain #AIGovernance

## About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps, DevGovOps, and AgentSecOps platform, is on a mission to create a world of trusted software delivery without friction from development to production. Driven by a "Liquid Software" vision, the JFrog Platform is a software supply chain system of record that is designed to power organizations as they build, manage, govern, and distribute secure software with speed and scale. Holistic security features help identify, protect, and remediate against threats and vulnerabilities. The universal, hybrid, multi-cloud JFrog Platform is available as both SaaS services across major cloud service providers and self-hosted. Millions of users and approximately 6,600 organizations worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation in the AI era. Learn more at <https://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 our expectations with respect to the performance of JFrog AI Security, including Local Shadow AI Detection and AI Asset Scanning BYOK.

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, 2025, 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 Contacts:

EMEA: Nicholas Shiers, EMEA Communications Manager, [nicholasS@jfrog.com](mailto:nicholasS@jfrog.com)

US: Siobhan Lyons, Director, Global Communications, [siobhanL@jfrog.com](mailto:siobhanL@jfrog.com)

**Investor Contact:** [investors@jfrog.com](mailto:investors@jfrog.com)

Source: JFrog Ltd.