

JFrog Partners with Wiz to Close the Gap on AI-Era Threats, Keeping Global Businesses Secure

The leader in software supply chain security collaborates with the leading cloud and AI security platform to deliver a single source of truth from code to cloud to runtime – giving teams the visibility and speed to remediate threats before attackers exploit them

SUNNYVALE, Calif. and NEW YORK — swampUP 2026 — September 2, 2026 — [JFrog Ltd](#) (Nasdaq: FROG), creators of the [JFrog Software Supply Chain Platform](#), the system of record for trusted software artifacts, binaries, and AI assets, today announced a new integration with [Wiz](#), now part of [Google Cloud](#), that closes a critical gap in AI-Era security: shrinking the time between risk detection and verified code fixes. The JFrog Platform serves as the single source of truth for all software artifacts - from build to production - while the Wiz cloud and AI security platform adds instant cloud runtime visibility. Together, [the integration](#) enables security and engineering teams with a unified view of what's running, where it came from, whether it's trusted, and how to fix it – enabling teams to keep pace with frontier AI models that move faster than most organizations can respond.

"Today's enterprise security teams are caught between two sources of information: AppSec teams see what was built but lose visibility once software ships. Cloud security teams see what is running but lack the supply chain context to understand the real risks," said Gal Marder, Chief Strategy Officer, JFrog. "Our partnership and integration with Wiz solves this by delivering a unified view from build to production – so teams can move from detection to remediation in hours vs. days."

In the Frontier AI era, the threat landscape has shifted fundamentally. Attackers now weaponize vulnerabilities faster than defenders can respond – the median time to exploit is now under a day, according to [recent Forrester research](#). Yet Mean Time to Remediate (MTTR) – already a critical metric – has become even more consequential. Previously, teams measured remediation in days; now, the difference between hours and days can determine whether an organization is breached. The bottleneck is no longer detection – it is manual investigation. AppSec teams see what was built and scanned; cloud security teams see what is running. That visibility gap forces teams to manually stitch together context across disconnected tools, turning threat response into a weeks-long investigation rather than a hours-long fix.

The JFrog-Wiz integration is designed to close this gap by connecting both halves of the picture in real time. The integration operates through an API-based data workflow. Wiz identifies vulnerable and exposed workloads across cloud environments and JFrog traces each workload back to its source artifact in [JFrog Artifactory](#), enriches it with [JFrog Advanced Security](#) vulnerability findings, Contextual Analysis, and [AppTrust](#) provenance data. Together, security teams get a unified view and full control: what's running, where it came from, whether it's trusted, and how to fix it – without building custom dashboards or manual correlation. The result: teams spend less time reconstructing context and more time remediating.

The JFrog integration with Wiz delivers:

- **Faster risk-to-fix motion:** What previously took days of manual investigation now takes hours. Security teams see Wiz findings and JFrog supply chain context in one unified view on the Wiz Security Graph with no manual correlation required.
- **Continuous compliance instead of periodic audits:** [JFrog AppTrust](#) cryptographic verification confirms every running workload matches what was signed and approved. This creates an environment for continuous compliance validation rather than snapshot-based periodic assessments.
- **Ownership clarity and automatic routing:** Every artifact carries the team, build pipeline, and individual who promoted it. When a threat is identified, ownership routes automatically – no time wasted chasing down who owns the fix.
- **Automatic detection of untrusted deployments:** Untrusted images running from unapproved registries are flagged automatically. Remediation paths trace directly to the build pipeline, with fix availability confirmed against existing Artifactory artifacts.
- **Zero-friction integration:** Based on an API connection, the integration requires no new agents, no cluster instrumentation, and no elevated cloud permissions. Customers running both JFrog Advanced Security and Wiz can operationalize this integration in just minutes.

“We’re happy to collaborate with JFrog to bring cloud runtime visibility and software supply chain context together in one unified view,” said Oron Noah, VP of Product, Extensibility & Partnerships at Wiz. “This integration helps customers spend less time on manual correlation and more time remediating risk.”

The JFrog-Wiz integration is available to customers immediately and ships as part of [JFrog Advanced Security](#). To learn more and see the integration in action visit www.jfrog.com/jfrog-and-wiz.

###

Like this Story? Share this on X: .@JFrog and @Wiz unite to help businesses stay ahead of #AI-driven security threats – giving joint customers a direct path from production alert to code fix. Learn more: <https://jfrog.com/jfrog-and-wiz/> #SoftwareSupplyChain #DevSecOps #swampUP #DevGovOps

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 software delivered 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, 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 Notes Regarding 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 anticipated performance of JFrog’s integration with Wiz.

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 Contact:

Siobhan Lyons, Director, Global Communications, siobhanL@jfrog.com

Investor Contact:

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