JFrog Positioned as a Leader in the First Gartner® Magic Quadrant™ for Software Supply Chain Security

JFrog places highest for ability to execute; reinforcing the market need for a holistic, unified software supply chain solution to secure all artifacts and AI assets

SUNNYVALE, Calif. – June 22, 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 it has been named a Leader in the Gartner® Magic Quadrant™ for Software Supply Chain Security, positioned the highest for Ability to Execute amongst any other vendor in the report.

This is the first time Gartner has published a Magic Quadrant for this segment – a complimentary copy of the full report is available here.

"Software engineering is evolving into software supply chain engineering. Developers and security teams now carry a responsibility that extends well beyond the application: not only to build software, but to build software that can be trusted in a hybrid world of human and AI agents. It is a structural shift, not a trend," said Shlomi Ben Haim, CEO of JFrog. "The AI era is accelerating software creation faster than any organization can audit. Enterprises ship more code, from more sources, and the demand for autonomous flow is growing more than ever. This movement leads to a Tsunami of binaries and a flood of vulnerabilities that make the software supply chain the primary target for attacks. While this is Gartner's first Magic Quadrant for this category, it's a market JFrog has been building for years. We understood early that speed without trust is a liability. Having a holistic platform – that automates software flow with security, governance, and velocity operating as one – is what enterprises need, and it's what we built."

Closing the AI Governance Gap in Software Supply Chains

Gartner identified software supply chain attacks among the top four critical security threats where attackers currently hold the advantage[1]. The threat is no longer focused on the volume of code, but rather, the speed of the "CVE Blitz" – adversarial symmetry – and this

[1] *Gartner, Press Release: Gartner Identifies Four Critical Threats Requiring Urgent Improvements from Cybersecurity Leaders, NATIONAL HARBOR, MD, June 2, 2026.*

risk is only accelerating with AI. The JFrog 2026 Software Supply Chain Security State of the Union report found:

- Attackers are actively targeting AI models, agentic tools, and developer workflows – not just finished applications.
- A majority of organizations still source AI models from untrusted repositories, creating a governance gap that existing tools were not built to close.
- Malicious packages reached record levels, with 177,000 new malicious packages detected.
- Malicious npm packages surged 451% year-over-year.

These findings highlight a fundamental shift: scanning finished code is necessary but no longer sufficient. Security has to be built into the supply chain itself – at every stage, for every artifact type, including AI.

Delivering Trusted Software in the AI Era Must Be Structural

JFrog is recognized in this inaugural report for its differentiated approach to software supply chain security. Unlike competitors, JFrog embeds trust, governance, and security directly into the software delivery process. Rather than adding another point solution to an already fragmented ecosystem, the JFrog Software Supply Chain Platform brings together software composition analysis, OSS license compliance and third-party governance, continuous threat intelligence, end-to-end SBOM lifecycle management, third-party reputation analysis, and binary artifact management to help enterprises secure the full lifecycle of software and AI assets. Available as SaaS, on-premises, or in hybrid environments, JFrog is designed for the operational realities of the enterprise that need security and compliance without compromising developer velocity or slowing innovation.

Innovations in the Gartner evaluation of the JFrog Platform include:

- **JFrog Curation:** Malicious packages, vulnerable dependencies, and non-compliant components are increasingly entering software environments before anyone notices – and regulations like DORA are raising the stakes for organizations that can't demonstrate control over what enters their software supply chain. JFrog Curation is designed to stop risky open-source components at the door and guides developers to pre-vetted package versions, before a bad dependency becomes everyone's problem.
- **JFrog AI Catalog and MCP Server:** As AI-generated code and agent-based development accelerate, most enterprises have no visibility into which AI models and agent skills are entering their environments – and no controls to stop the ones

they shouldn't trust. JFrog AI Catalog and MCP Server apply the same security standards and trust layer enterprises already use JFrog to enforce.

- **JFrog AppTrust:** Security and compliance teams are under growing pressure to prove that policies were actually enforced – not just written down – yet most still rely on manual approvals, and disconnected evidence trails that fall apart under audit scrutiny. JFrog AppTrust replaces that with immutable evidence and automated policy gates across the software supply chain, so teams can demonstrate continuous enforcement without spreadsheets or last-minute fire drills.
- **Expanded SBOM Evidence:** Customers, auditors, and regulators are no longer satisfied knowing what software an organization uses – they want proof that known vulnerabilities were assessed, that risk decisions were documented, and that nothing was ignored. Expanded SBOM evidence capabilities, including VEX support aligned to CycloneDX and SPDX 3.0, are built to give organizations the verifiable documentation trail they need to answer those questions with facts, not explanations.

Together, these capabilities enable organizations to maintain security, compliance, and velocity in the AI era across increasingly complex and distributed software supply chains. To read the full Gartner Magic Quadrant for Software Supply Chain Security, visit https://jfrog.com/gartner-magic-quadrant/. To learn more about JFrog's vision and approach to software supply chain security read this blog.

###

Share on X: *@JFrog has been named a Leader in the inaugural Gartner® Magic Quadrant™ for Software Supply Chain Security – and placed the highest on the Ability to Execute axis of any vendor evaluated. Learn why: https://bit.ly/4grCARU #SoftwareSupplyChain #DevSecOps #AI #governance #DevGovOps*

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from JFrog.

About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps, DevGovOps and MLOps 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.

Media Contact:

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

Investor Contact:

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