

JFrog Introduces the Software Supply Chain Traffic Controller: One Trusted Path for Every Software Package

Together with industry-leading SASE providers Zscaler, Cloudflare, and Netskope, JFrog enables organizations to control open source consumption at the network edge, ensuring every package and artifact used by developers, AI agents, or non-engineering employees flows through a trusted, governed software supply chain. No bypass. No exceptions.

SUNNYVALE, Calif., August 27, 2026 — [JFrog Ltd.](#) (Nasdaq: [FROG](#)), the Liquid Software company and creators of the [JFrog Software Supply Chain Platform](#), the system of record for software artifacts, binaries, and AI assets, today announced new solutions integrated with Zscaler™, Cloudflare, and Netskope – three of the industry's leading Secure Access Service Edge (SASE) providers – to stop malicious packages at the network level before they reach users' machines. The [JFrog Traffic Controller](#) universally works with SASE solutions and JFrog Curation to deliver network-layer enforcement that automatically reroutes software package download requests through JFrog Artifactory as the single source of truth – ensuring all software developers and AI agents can develop safely at speed, while giving the organization a traffic enforcement solution to prevent bypasses.

[JFrog's 2026 Software Supply Chain Security State of the Union](#) showed a 451% surge in malicious packages year over year, reaching over 171,000 unique instances. Yet only 40% of organizations have malicious package detection capabilities in place, and secrets detection is active in just 28% of enterprises. The categories growing fastest in threat volume seem to be the least covered by today's tooling.

“Open source has powered software innovation for decades, but in today's zero-trust world, simply enabling traffic is no longer enough. Organizations need control over what enters their software supply chain, whether it is requested by a developer, an AI agent, or an automated tool. The answer is not another security alert or another gate that disrupts the developer workflow. It is a universal control point that ensures every package flows through one trusted system of record, where policy can be governed and enforced,” said Shlomi Ben Haim, Co-Founder and CEO, JFrog. “JFrog Traffic Controller extends that enforcement to the network edge, creating one trusted path for software consumption with no exceptions, while developers and AI agents continue working without disruption. We're thrilled to partner with the world's leading security companies to bring this vision to

our customers while staying true to JFrog's universal philosophy - empowering our customers with a freedom of choice without compromising control, security, or speed."

The Threat and the AI Governance Gaps are Getting Worse

Today's threat extends well beyond known malicious packages. AI coding agents like Claude Code, Cursor, Copilot, and Kiro now run directly on developer machines, autonomously pulling dependencies, installing libraries, and invoking build processes with little to no review. Agents – like developers – don't always follow proxy configurations, consult approved package lists, or pause before fetching packages from the default public registries. Therefore, each agent session is a potential unmonitored entry point into the organization's software supply chain.

This risk is amplified as frontier AI models further accelerate attackers' ability to discover and exploit vulnerabilities. The window between disclosure and active exploitation has shrunk to mere hours, making comprehensive visibility into every software component entering the organization the only reliable way to answer, "are we exposed?" before attackers already know the answer.

Gartner recognized these increasing stakes – citing software supply chains as one of [*"four critical and unpredictable threats where attackers hold a significant advantage to successfully exploit weaknesses in targeted organizations."*](#) The coverage gap is real – not just theoretical – and it's structural. AI coding agents, autonomous build tools, and non-engineering employees using AI-powered applications often download dependencies directly from public registries, bypassing every pipeline-level control and leaving no audit trail.

Reroute, Don't Block: How JFrog Closes the Governance Gap

The [JFrog Software Supply Chain Platform](#) helps stop malicious and unwanted packages at the network layer and creates a complete, auditable record of every package entering the organization across companies using Zscaler, Cloudflare, and Netskope simultaneously. Rather than simply blocking out-of-policy requests, JFrog Traffic Controller transparently reroutes outbound package downloads through JFrog Artifactory, where JFrog Curation inspects each package against the configured security, license, and quality policies before it enters the organization. Compliant packages are delivered without interruption while malicious ones are stopped and, when available, a safe approved version is served automatically.

"By partnering with Cloudflare, Netskope and Zscaler, our Traffic Controller works natively with the security infrastructure our customers already use," said Gal Marder, Chief Strategy Officer, JFrog. "We're making it possible for the entire software security ecosystem to enforce the same standard with zero friction: every package needs to be curated before first use, every transaction on record, no exceptions. That is how the industry builds a supply chain it can actually trust."

When the Pipeline Is Secure, but the Perimeter Is Not

Adyen, a global financial technology platform enabling businesses to accept, process, and settle payments across online, mobile, and in-store channels, consolidated their software supply chain on the JFrog Platform to help scale their enterprise-wide DevSecOps practices. Adyen uses JFrog Curation as a real-time firewall to block malicious open-source packages from entering their software pipelines. This allows developers to safely pull software components without introducing vulnerabilities, while experiencing zero disruption to their workflow.

"JFrog Curation provides a firewall for open-source packages. You instill policies that defend the organization, but the goal isn't to say 'no'," said Supun Vidana Pathirana, DevSecOps Specialist, at Adyen. "It's about how we can help developers continue their work without disrupting their workflow. We enable development; we don't block it."

Initial Gateway Security Solutions Supported

The JFrog Traffic Controller solution is available immediately through JFrog Curation, supporting:

- **Zscaler Internet Access™ (ZIA™):** Identifies and curates the supply chain software package traffic through JFrog.
- **Cloudflare Gateway:** Can be configured to TLS-inspect public registry traffic and apply firewall policies to redirect package requests to JFrog Artifactory.
- **Netskope One SSE:** Applies real-time protection policies to redirect package manager traffic through JFrog, with browser passthrough to preserve the developer experience.

At the heart of the JFrog Platform, Artifactory serves as the system of record for the software supply chain – storing, managing, and governing the binaries and packages that organizations rely on. When combined with JFrog Curation, the JFrog Platform creates a single source of truth – protected by policy-driven controls – that prevents malicious, risky,

or unwanted packages from entering the software supply chain. JFrog Traffic Controller extends this protection to the network edge while preserving customer choice. Traffic Controller is designed as a universal enforcement layer that integrates with leading SASE providers, allowing customers to choose their preferred solution.

"Bringing JFrog's package intelligence into Netskope's real-time protection policies gives joint customers a contextual, policy-driven answer to every package download, facilitating the user and agent build flow rather than a legacy solution which could only block access," said David Willis, Vice President, Technology Alliances, Netskope.

Support for additional SASE partners is expected to follow. Interested parties can learn more at <https://jfrog.com/curation/package-traffic-controller/>, [read this blog](#), view [this demo](#), or register for JFrog swampUP 2026 at the Glasshouse in New York, September 1-3, 2026. Register [here](#). Organizations interested in evaluating JFrog Curation and JFrog Traffic Controller can request a demo at jfrog.com/curation.

###

Like this Story? Share this on X: Your pipeline is locked down. But what about the #AI agent that just pulled a malicious #npm package from outside it? @JFrog + @Zscaler + @Cloudflare + @Netskope just closed that gap with the new JFrog Traffic Controller - stopping malicious #opensource packages at the network edge before they ever touch your pipeline. The perimeter just became part of the pipeline. #SoftwareSupplyChain #DevSecOps #OpenSourceSecurity #security #DevGovOps

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 in the AI era.

About JFrog swampUP 2026

JFrog's annual swampUP event is the premier conference for teams building trusted software in the AI era. Bringing together software developers, security professionals, IT and DevOps leaders, MLOps engineers, and community innovators, swampUP confronts the central challenge of modern software delivery: building, securing, and governing trusted software alongside the AI models and autonomous agents that now ship with it at enterprise scale. Designed to help organizations master

the AI surge with "Trusted Intelligence," the 2026 global JFrog swampUP tour features events in [New York City](#) (September 1-3 at The Glasshouse) and [Barcelona](#) (October 20-22 at The InterContinental). Attendees will experience visionary keynotes, hands-on technical training, and immersive breakout sessions empowering them to engineer trust into their agentic software supply chains without sacrificing speed. Learn more and register at <https://swampup.jfrog.com/>.

Media Contact:

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

Investor Contact:

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