

AI Titans Unite at JFrog swampUP 2026 to Define the Future of the Software Supply Chain

Software and security visionaries from Anthropic, Cursor, Google-Wiz, Microsoft, NVIDIA, and more unite to chart the future of trusted software and AI delivery at scale

SUNNYVALE, Calif. – August 12, 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 the all-star speaker lineup for swampUP 2026 – the premier user conference for teams building, securing, and governing trusted software in the AI era – taking place September 1-3 at The Glasshouse in New York City. [Register here.](#)

“Where else can you bring the leaders shaping AI together with the security and software experts delivering it at scale? That’s the power of JFrog swampUP,” said Shlomi Ben Haim, Co-Founder and CEO of JFrog. “As development shifts from human-paced to machine-generated, the software supply chain is being redefined, speed and trust can't be compromised. We’re honored to welcome this extraordinary lineup of speakers and bring their vision together with the real-world best practices, experience, and innovation of our customers and community. Together, we’re here to shape what’s next.”

Every enterprise is adding AI to their software supply chain, which is increasing the attack surface for bad actors. [JFrog research shows](#) attackers are no longer just breaching traditional defenses; they are actively weaponizing the trusted models, registries, and agentic tools fueling today's AI-enabled development. Additionally, 97% of organizations claim AI governance while 53% are still pulling models from public registries where malicious payloads have been found. The gap between perceived security and operational reality has never been wider.

The Leaders and Builders Driving the Next Era of AI & Security Innovation

To help attendees navigate the rapidly shifting landscape of software supply chain security and governance in the agentic AI era, the 2026 swampUP speaker lineup brings together an extraordinary cross-section of security leaders, enterprise architects, and AI pioneers from the organizations defining what trusted, intelligent software delivery looks like in the AI era:

- **Anthropic’s Jason Clinton, Deputy CISO**, will bring a security leadership perspective to the growing risks and governance challenges created as AI reshapes how software is built and delivered.

- **AT&T's VP of Global Software & Product Delivery, [Rinat Zilberstein](#)**, will join **Shlomi Ben Haim, JFrog Co-Founder and CEO**, to discuss how global enterprises must approach software supply chain security in the frontier AI era.
- **Chainguard's** product leaders will join **JFrog's VP of AppSec, Eyal Dyment**, to demonstrate how a self-healing software supply chain, anchored on a single source of truth, enables automated, machine-speed vulnerability detection and fixes in minutes.
- **Cursor's Field CISO, [David Pan](#)**, and **JFrog's Co-Founder and CTO, Yoav Landman**, will explain why having a system of record is essential to secure and govern every package, model, AI asset, and release at scale – regardless of tools or pipelines.
- **Microsoft Software Global Black Belt, [Daniel Meppiel](#)**, and JFrog's Yonatan Arbel, will unveil strategies for securing the "*Agent Software Supply Chain*" – because when agents build your software, they need to be governed too.
- **Moderne's CEO, [Jonathan Schneider](#)**, **Echo Security CTO, [Eylam Milner](#)**, **CTO for Broadcom's Tanzu Division, [James Watters](#)**, and **Chainguard's Field CTO, [Behn Williams](#)**, will join JFrog's Chief Strategy Officer, Gal Marder, on stage to discuss where remediation is headed as frontier AI models outpace traditional security cycles.
- **NVIDIA's Developer Experience Leader, [Krishna Nadiminti](#)**, will explore how to translate SBOM data into actionable risk signals and build trusted supply chains for AI agent skills.
- **TEAM8's Partner and CISO in Residence, [Tim Brown](#)**, **former CISO of SolarWinds**, will join a fireside chat drawing on firsthand experience and learnings from one of history's biggest software supply chain attacks to help attendees better understand threat models to help prevent the next AI-driven attack.

Unmatched Value Add for swampUP Attendees

swampUP 2026 pairs a world-class speaker lineup with hands-on experiences designed to deliver immediate, practical value for business, IT, and developer audiences through:

- **New Product Introductions & JFrog Executive Keynotes:** Shlomi Ben Haim, Co-Founder and CEO, Yoav Landman, Co-Founder and CTO, and other leaders from across JFrog's DevOps, Security, AI/ML and DevGovOps business, will take the stage to provide key insights grounded in customer data, JFrog Security Research, and JFrog Platform usage on the "Agentic Software Supply Chain" surge.
- **Hands-on Training with Certification:** Training Day labs and masterclasses, led by industry experts and emphasizing real-world experience, equip attendees with practical skills across the JFrog Platform and the broader DevOps toolchain.

- **Breakout Sessions for Every Experience Level:** Multi-track sessions on AI/ML model management, agent governance and security, DevSecOps, and Cloud-Native architecture, designed for executives, engineers, security teams, and AI/ML practitioners alike.
- **Community Gala & Networking:** An unforgettable evening at the [Intrepid Museum](#) in New York City, offering uninterrupted time to connect with peers from across the global software community, featuring keynote speaker [Carey Lohrenz](#), the first female F-14 Tomcat Fighter Pilot in the U.S. Navy, sharing hard-won lessons on leading through uncertainty and making critical decisions when the stakes are highest.

Registration is now open, and the full agenda is available at <https://swampup.jfrog.com/>. For more information on reasons to attend swampUP 2026 visit <https://swampup.jfrog.com/jyt/> or follow JFrog on [LinkedIn](#) and X @jfrog.

###

Like this Story? Share this on X: Join Anthropic, [@Cursor_ai](#), [@Microsoft](#), #wiz, [@googlecloud](#), [@chainguard_dev](#), [@ATT](#), [@nvidiaAIDev](#) & more at #swampUP 2026, Sept 1–3 NYC. Register: <https://swampup.jfrog.com> #DevSecOps #AI #SoftwareSupplyChain #DevGovOps #security

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