JFrog Launches AI Catalog to Secure and Govern AI Model Delivery

New AI Catalog Extends the JFrog Platform to Discover, Govern, and Deploy AI Models, including the Open-Source NVIDIA Nemotron Models, with Speed, Security, and Compliance

Sunnyvale and Napa, Calif. – JFrog swampUP – September 9, 2025 — JFrog Ltd (Nasdaq: FROG), the Liquid Software company and creators of the award-winning JFrog Software Supply Chain Platform, today unveiled an enhanced AI model catalog for securing, governing, consuming, and deploying AI and ML models, whether open source, self-built, or external across the enterprise: the JFrog AI Catalog. Available immediately, the new offering allows organizations to securely build specialized agentic solutions and integrate AI services into their software supply chain, while maintaining full visibility, control, and compliance, accelerating the path from AI inception to production. It also provides direct access to AI open models, including NVIDIA Nemotron models, a family of open-source AI models, with publicly available open weights, datasets, and recipes that provide leading efficiency and accuracy.

“One of the biggest challenges for organizations adopting AI is ensuring governance and security to deliver Trusted AI,” said Yuval Fernbach, VP & CTO, JFrog ML. “Building on our Secure Model Registry, the new AI Catalog provides a centralized hub to access and govern AI/ML models – whether internal, from open-source repositories like Hugging Face, or from external API providers like NVIDIA NIM and Anthropic. By integrating seamlessly with the ecosystem, the JFrog AI Catalog gives organizations complete visibility, compliance, and control over model usage, helping them innovate faster while delivering Trusted AI in today’s complex regulatory environment.”

Secure, Scalable AI in the JFrog Software Supply Chain Platform

Gartner research indicates “a significant challenge for data science and AI leaders is overseeing and governing the activities of dispersed DSML teams while optimizing collaboration with centralized resources. Enhanced AI governance and management capabilities, linked across data sources and other assets, are now must-have capabilities.”(1) The JFrog AI Catalog serves as a central repository for locating and managing AI models, datasets, and related resources. It enables organizations to manage the AI model lifecycle with enterprise-grade security and governance, reducing operational complexity while aiming to allow consistent compliance across software development workflows.

(1) Gartner Magic Quadrant for Data Science and Machine Learning Platforms, by Afraz Jaffri, Maryam Hassanlou, Tong Zhang, Deepak Seth, Yogesh Bhatt, May 2025.

JFrog's AI Catalog provides companies with a single source of truth and centralized hub for:

- **End-to-End Model Governance:** Easily track model usage, and access with clear policies and permission controls, including enforcement on a per-project basis.
- **Continuous Security and Compliance and Visibility:** Ongoing model scanning and evidence tracking using JFrog Xray to ensure secure, compliant AI model usage, including model lineage visibility.
- **Robust Discoverability:** Search and explore models based on tags, projects, and use cases with detailed model cards and metadata.
- **Building Specialized AI Agents:** Access to NVIDIA Nemotron models, which provide full transparency with open weights, datasets, and recipes, making building specialized AI agents accessible for anyone using the JFrog Platform.
- **Streamlined Deployment:** One-click model deployment, to your own runtime or using connections to external AI providers such as OpenAI and Anthropic.

With the JFrog AI Catalog, teams can:

- **Discover Secure Models:** Provide developers and data scientists with easy access to curated AI models from external APIs, open-source repositories, and internally developed models, increasing productivity and collaboration while enforcing security with integrated scanning and evidence tracking.
- **Govern Model Usage:** Centrally manage model access and track usage, aiming to allow secure and compliant AI model usage across the organization according to different project policies.
- **Consume and Deploy Models:** Securely connect to external model providers (OpenAI, Anthropic, AWS, Google, and others) or deploy secure, containerized models – such as NVIDIA NIM – internally. One-click deployment provides simplicity for streamlining the path to AI in production while maintaining visibility into deployment and usage patterns.

"Enterprises face increasing demands for secure, transparent AI model management to maintain compliance and accelerate innovation," said Adel El Hallak, Senior Director of Product, NVIDIA. "By providing direct access to NVIDIA Nemotron models and NIM microservices, within the JFrog AI Catalog, organizations can deploy and govern open-source AI solutions with greater visibility and control, supporting secure, sovereign AI initiatives across their workflows."

Designed to help organizations keep pace with the rapid evolution of AI while maintaining top-level security and governance, the JFrog AI Catalog streamlines the path from model discovery to production without adding unnecessary complexity. The JFrog AI Catalog is available immediately for customers of JFrog Curation, delivering 360-degree visibility and scalable management of all traditional and AI artifacts. For more information read this blog, visit https://jfrog.com/ai-catalog/, or register for the *"AppTrust, AI Catalog and more"* webinar on October 9 at 9 AM PT.

###

Like this Story? Share this on X: New from @JFrog: The AI Model Catalog. Discover, govern, and deploy AI models across your org with the same security, compliance, and DevSecOps workflows you trust from JFrog. Future-proof your AI development: http://bit.ly/4nCyOWv #SoftwareSupplyChain #DevOps #DevSecOps #cybersecurity #AI #DeveloperTools #MLOps

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. Learn more at www.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 anticipated performance of the JFrog AI Catalog.

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, 2024, 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

Final PR & Social Graphic: