SOLUTION SHEET

Don't Let Shadow AI Break Your Software Supply Chain

Ensure your teams can rapidly adopt Agentic AI and MCP tools without compromising the integrity of your software supply chain.

Unified Visibility

Manage traditional code, binaries, AI models, and MCP servers in a single system of record.

Proactive Security

Gatekeep and curate AI tools and open-source dependencies before they enter the developer ecosystem.

Agentic Speed

Automate governance, contextual scanning, and compliance so developers can build at the speed of the market.

THE CHALLENGE

Your developers aren't waiting for IT approval.

They're already running unvetted MCP servers and AI models to keep pace, creating a shadow supply chain with catastrophic consequences: over-privileged agents, poisoned models, and automated data exfiltration executing at machine speed.

THE SOLUTION

Streamline your supply chain with a single source of truth.

With JFrog Artifactory and JFrog Xray at the core, you can govern your AI supply chain with the same rigor as your traditional software, without slowing down your teams.

THE RESULT

A proven track record of happy customers

"Centralizing our artifact management with JFrog Artifactory has transformed our DevSecOps approach. We now have a single source of truth for all binaries, ensuring consistency and security across every deployment. With JFrog Xray, we've shifted from reactive to proactive vulnerability management. This has not only reduced our security risks but also minimized costly rollbacks, streamlining our development process significantly."

Mr. Hideki Homma, Senior Engineer, Panasonic HVAC

ARTIFACTORY

Standardize on a single source of truth

- **Universal Artifact Management:** Store AI models, datasets, and MCP servers right alongside your standard Docker images, Java, and Python packages.
- **Break the Data Science Silo:** Integrate AI/ML artifacts directly into your CI/CD pipelines.
- **End-to-End Traceability:** Ensure every AI model in production can be instantly traced back to its training version and build parameters.

CURATION

Stop threats before they enter

- **Proactive Digital Border:** Block unvetted or high-risk MCP servers and packages before they reach developers.
- **Eliminate the Shadow Supply Chain:** Stop side-loading of malicious AI tools from unvetted public registries.
- **Enforce License Compliance:** Automatically reject tools with licenses that could jeopardize proprietary algorithms.

XRAY

Automate granular governance

- **Contextual Analysis:** Xray analyzes binaries to determine if a vulnerability is truly exploitable in your environment, reducing false positives by up to 75%.
- **Tool-Level Access Control:** Grant a senior architect the delete_data tool while restricting a junior developer to read_only on the same AI agent.
- **Automated AIBOM & SBOM Generation:** Instantly generate machine-readable inventories to meet emerging regulatory standards like the EU AI Act.

PLATFORM

Scale delivery without drift

- **Immutable Release Bundles:** Ensure the exact code and AI models validated in QA are precisely what executes in production.
- **Peer-to-Peer Distribution:** Push massive AI models and software updates to thousands of global endpoints simultaneously without crashing network infrastructure.
- **High-Velocity Deployment:** Transition from manual weekly releases to confident, automated daily deployments.

The Leading Platform for Software and AI Supply Chain Governance

Request Your Personalized Demo

Help Center

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.

www.jfrog.com

www.x.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd

JFrog