JFrog
AI CATALOG
SOLUTION SHEET

The Trusted Source for Enterprise AI

Where AI Innovation Meets Enterprise Control

Centralized Governance

Gain end-to-end visibility over your entire AI ecosystem.

Simple Access

Consolidate all allowed AI assets into a single hub.

Secure Delivery

Streamline the path to trusted impactful AI in production.

THE CHALLENGE

Uncontrolled AI usage creates misuse risks and delivery chaos.

Widely dispersed AI access and usage creates governance blind spots, magnifies compliance risks, and causes manual, error-prone production bottlenecks.

THE SOLUTION

Accelerate AI innovation with enterprise-grade control and trust.

JFrog AI Catalog establishes a single source of truth to govern every enterprise AI component. It provides the confidence and stability required to accelerate innovation securely.

THE RESULT

Proven Results in Rapid, Trusted Delivery.

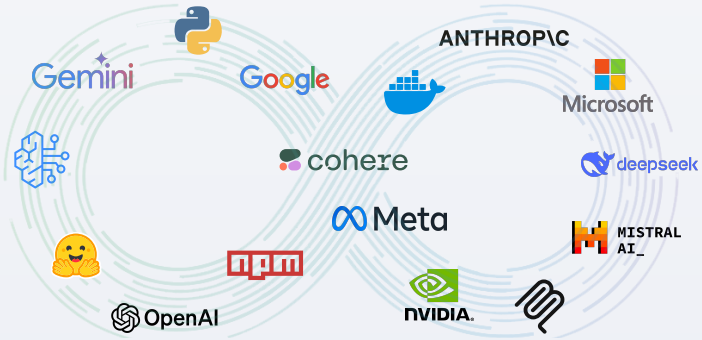
Over 7,000 of the world's most demanding organizations, including the majority of the Fortune 100, rely on the JFrog Platform to secure their software supply chain. The same trusted framework for security and governance is also purpose-built for your AI usage. This gives you a unified platform to control your AI development end-to-end.

NVIDIA AIRBUS AMERICAN EXPRESS Tripadvisor Google

Unmatched Integration & Ecosystem Freedom:

JFrog AI Catalog provides simple and secure access to the evolving AI ecosystem

- Access a broad range of AI models and MCP servers, from in-house creations to diverse commercial and open-source assets, ensuring ecosystem flexibility.
- Achieve controlled ecosystem freedom by bringing all AI workloads under centralized governance within your organization's secure software supply chain.
- Ensure AI/ML teams innovate with approved and secure AI components verified by continuous scanning and policy enforcement.



Innovate without compromising governance, security, and compliance

- Centralize governance over your entire AI landscape, precisely controlling which assets are allowed for use.
- Apply granular access and permissions, defining who can use each AI asset.
- Ensure continuous security with automated scanning and complete audit-ready tracking.

Discover and access all AI assets from a centralized, trusted source

- Easily browse and search for models and MCP servers to streamline discovery and boost productivity.
- Effortlessly review all relevant model and MCP server details for immediate, actionable evaluation.

Detect and eliminate Shadow AI

- Expose every unmanaged AI model or API call across your enterprise.
- Apply centralized governance for unmanaged AI assets under a unified registry.
- Automatically identify and block the usage of non-compliant or malicious AI assets.

Deploy and connect any AI asset

- Use the secure AI Gateway for one-click deployment of approved models and fast, secure connections to any external API.
- Single-line MCP server configuration for increased productivity.
- Monitor deployments and usage patterns, tracking performance for operational insights.

Talk to a JFrog Expert

Help Center

v1.0220620

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