SOLUTION SHEET

JFrog AI CATALOG

One Secure Supply Chain for Software and AI

JFrog AI Catalog governs every AI asset your developers and coding agents consume as native artifacts inside the same system of record that controls your software.

THE CHALLENGE

Unchecked AI Assets Are Already in Your Supply Chain

Developers and coding agents are continuously pulling AI assets, bypassing every approval and review process you have in place. Every unvetted asset is a threat in waiting: malicious models, compromised MCP servers, and skills with access they shouldn't have.

THE SOLUTION

Govern Every AI Asset in Your Agentic Supply Chain

JFrog AI Catalog governs every AI asset entering your supply chain, from the assets powering your coding agents to those shipping in your builds. Any AI asset that fail your organizational policies is proactively blocked.

End the AI Governance Silo

Govern software and AI through a **single system of record** with shared permissions control, policies, and audit trail. Retire the patchwork of disjointed point solutions.

Block Threats at the Gate

Enforce your policies at the point of request with **proactive blocking**. Stop risky AI before it reaches your coding agents or builds, not after the breach.

Future-Ready Coverage

Manage models, MCP servers, skills, and plugins as **first-class artifacts** in one platform. Coverage that scales with every new AI asset type as it emerges.

Connect to Any AI Source. Trust Every Asset.

- Cover every AI source: in-house, commercial, open-source, and public registries.
- Bring every model, MCP server, agent skill, and plugin under one governance layer.
- Ensure developers and coding agents can use only pre-approved AI assets.

CAPABILITIES

Shadow AI Detection

- Detect every unmanaged AI asset and external service across your agentic software supply chain.
- Block malicious or non-compliant assets and allow safe ones, on the spot.

Centralized AI Registry

- Manage models, MCP servers, agent skills, and plugins as native artifacts in one registry.
- Trace every AI asset to its source, version, and the release it's shipped in.

Automated Policy Enforcement

- Define security, compliance, and operational policies once, and apply them continuously.
- Allow only AI assets that match your policies. Block everything that doesn't.

Secure AI Gateway

- Route every model, MCP server, and skill connection through a centralized secure gateway.
- Connect approved AI assets natively to coding agents like Cursor and Claude Code.
- Monitor deployments and usage patterns, track performance for operational insights.

v1.0230402

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.

LEGAL STATEMENT

www.jfrog.com
www.x.com/jfrog
www.facebook.com/artifrog/
www.linkedin.com/company/jfrog-ltd

Learn more and book your personalized demo at https://jfrog.com/ai-catalog/demo/