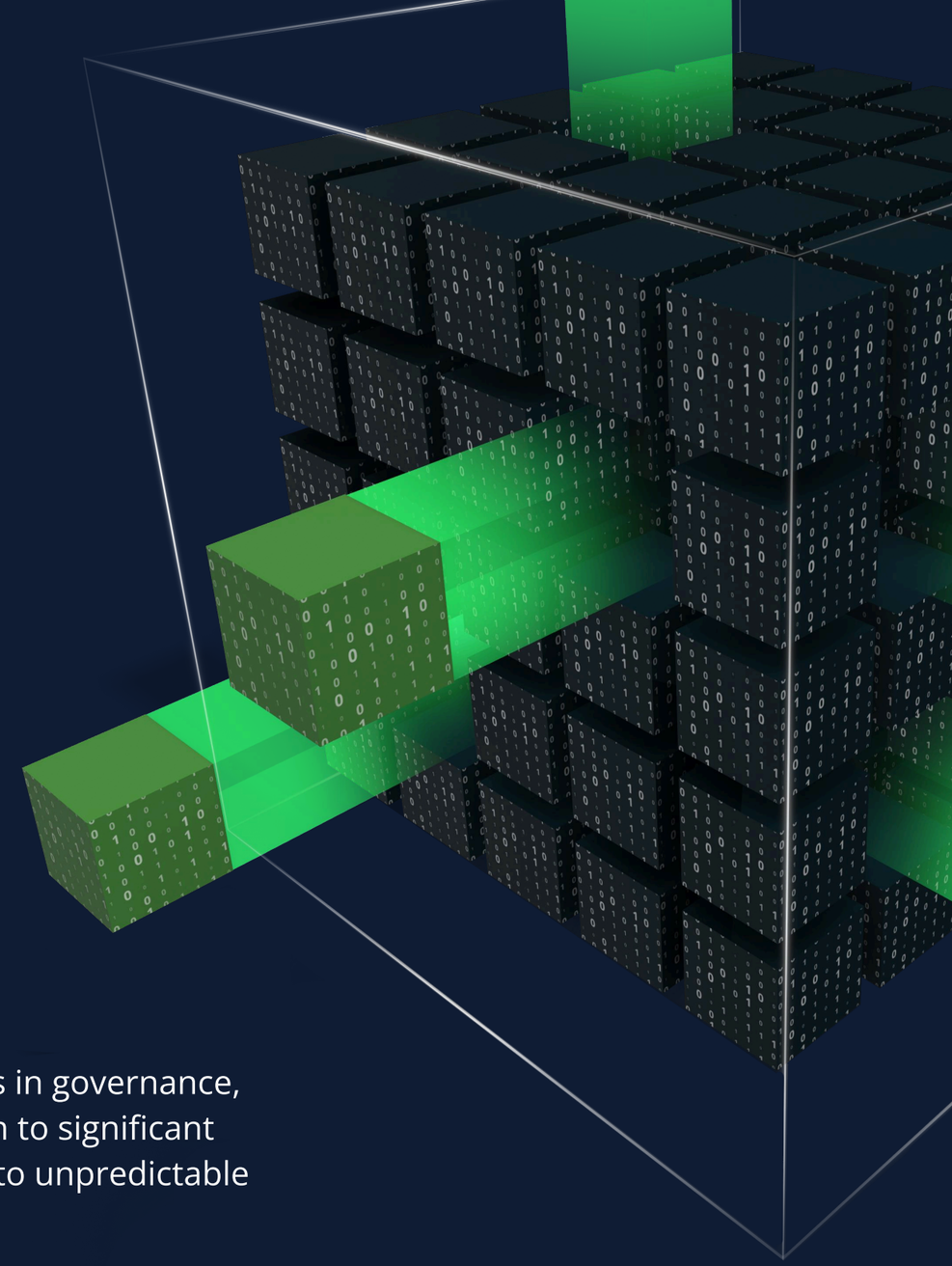
The JFrog Trusted AI 2026 Playbook



From Chaos to Control: A Concrete Plan for a Unified, Secure AI Foundation

As AI adoption accelerates, critical blind spots are created across the organization. These gaps in governance, security, and management allow unvetted AI assets to grow rapidly, exposing the organization to significant risks. Without a unified strategy, organizations often lose control over their AI assets, leading to unpredictable outcomes and major governance gaps.

The principles for uncovering these blind spots are the same for software and AI, but the stakes are higher. This playbook provides a concrete 5-pillar plan to bridge the gap between DevOps, SecOps, and MLOps and extend your existing trust to the entire AI/ML lifecycle.

1. **CONSOLIDATE** THE FRAGMENTED AI TOOLCHAIN

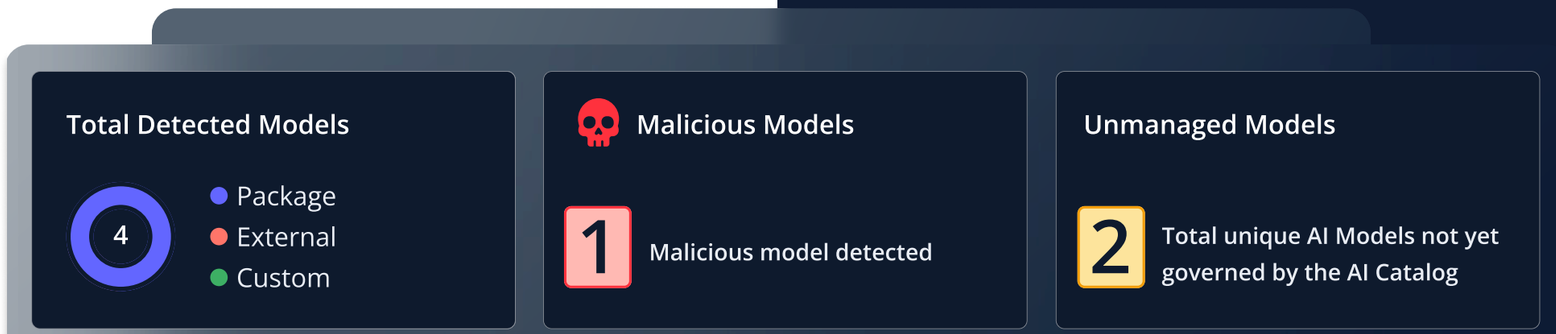
The Problem:
AI/ML teams are drowning in integrations between fragmented tools. Your models, data, software binaries, and code are scattered across different systems, creating compliance blind spots, operational overhead, and constant project delays.

The Plan:
Establish a single source of truth. Unify all your AI and software artifacts by implementing a central registry for your models, containers, software applications, Python packages, and datasets. This system must be able to proxy public repositories (like Hugging Face) and host your internally-developed models together with your software.

2. **DETECT** HIDDEN AND UNMANAGED AI ASSETS

The Problem:
You cannot govern what you cannot see. Shadow AI is rampant, with only about 50% of organizations reporting that they have “high visibility” into developers’ AI usage[1]. Every unvetted model or API endpoint creates AI blind spots and new security risks.

The Plan:
Implement a centralized catalog to discover and inventory all AI assets. This catalog must act as the central hub to find, review, and tag all external APIs, open-source models, and internally-developed models, making the invisible visible.



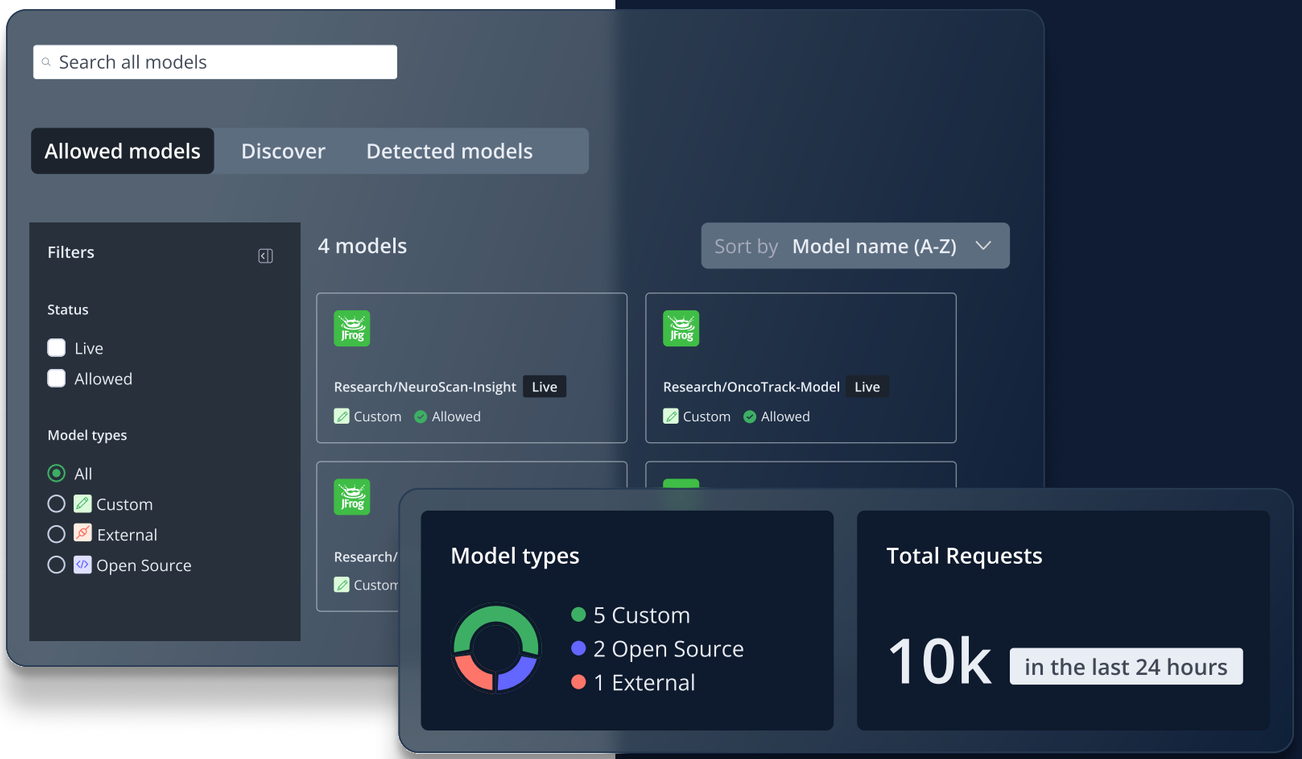
Action	Status	Model name	Model type	Provider	License	Artifacts
Manage	Unmanaged	MustER/vgg16_light	Package	Hugging Face	Apache-2.0	1
Manage	Unmanaged	DeepSeek-AI/DeepSeek-R1	Package	Hugging Face	MIT	12
Manage	Partially Managed	Qwen/Qwen3-VL-8B-Insrtuct	Package	Hugging Face	Apache-2.0	5
Manage	Managed	OpenAI/gpt-oss-20b	Package	Hugging Face	Apache-2.0	3

[1] EY Report.

3. **CENTRALIZE** VISIBILITY AND GOVERNANCE

The Problem:
Without a central point of control, it's impossible to enforce policy. This is why 63% of companies lack effective AI governance policies[2]. This fragmented approach creates security bottlenecks and makes it impossible to comply with evolving regional AI regulations.

The Plan:
Use your AI Catalog as the single gateway to govern all models. This is where you apply your existing security and compliance policies to AI models. This empowers your teams to confidently select, validate, and deploy the right, pre-approved model for any use case, all from one central hub.

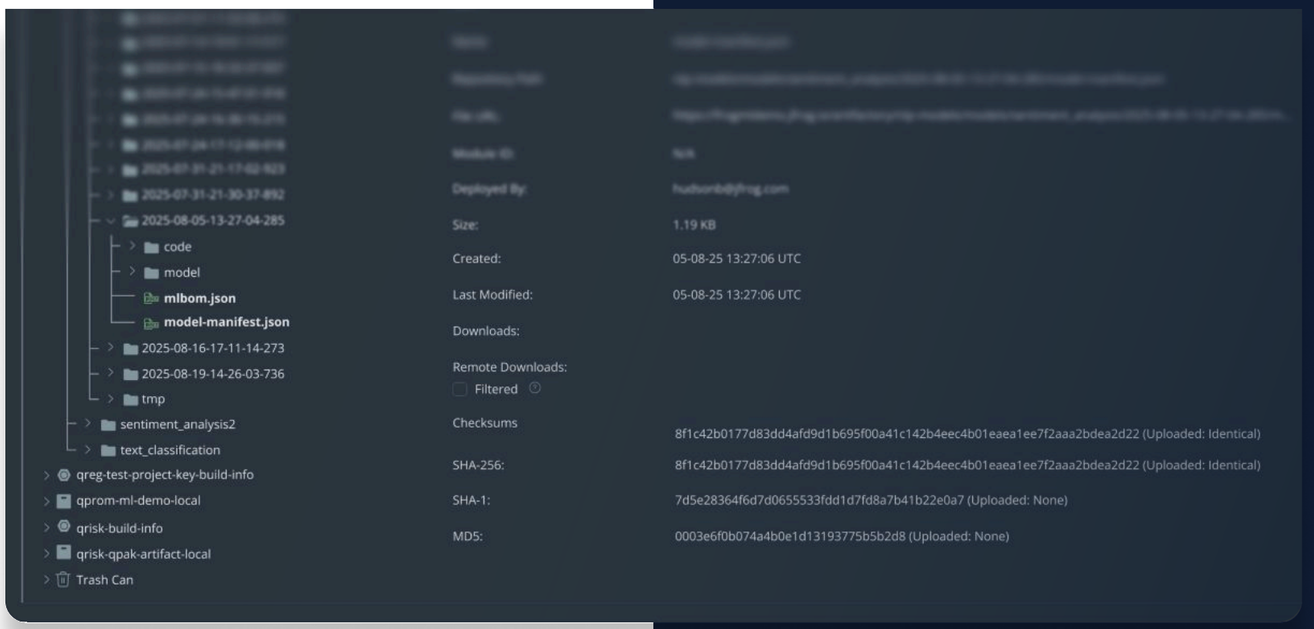


[2]IBM Report.

4. **REDUCE** RISK THROUGH AI-BOM

The Problem:
An AI model is not a single file. It comes with a complex web of code, data, and "critical dependencies". Malicious models are a growing threat, with hundreds identified in open-source repositories like Hugging Face, posing a direct risk to your supply chain.

The Plan:
Apply a governed supply chain approach to your AI pipelines. Proactively secure models and their dependencies by generating an AI-BOM (Bill of Materials). This allows you to centralize your control to manage model access, track usage, and ensure all AI initiatives are secure and compliant.



5. **SIMPLIFY** ACCESS AND PATH TO PRODUCTION

The Problem:
Even with secure, approved models, the path to production is often blocked by manual handoffs, operational overhead, and process bottlenecks. This friction stalls innovation and prevents teams from shipping models quickly.

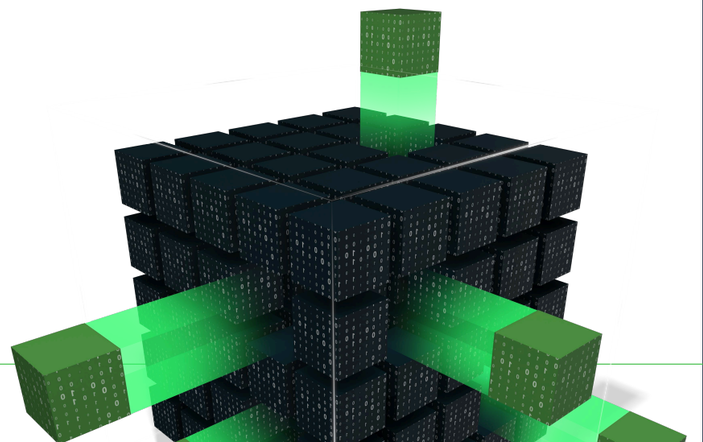
The Plan:
Create a clear, fast path to get models into production. By using a secure AI gateway to serve models, you can streamline and automate the path from development to production. This includes enabling one-click deployment for allowed models and securely connecting to external providers (like OpenAI, Anthropic, etc.), effectively removing security and operations as a bottleneck.

FROM PLAN TO PLATFORM

Now that you have the 5-pillar plan to move from AI chaos to control, it's time to implement it within your organization.

Need support? Curious about how to integrate the JFrog AI Catalog as your centralized hub for all your AI/ML initiatives?

Let's Chat



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