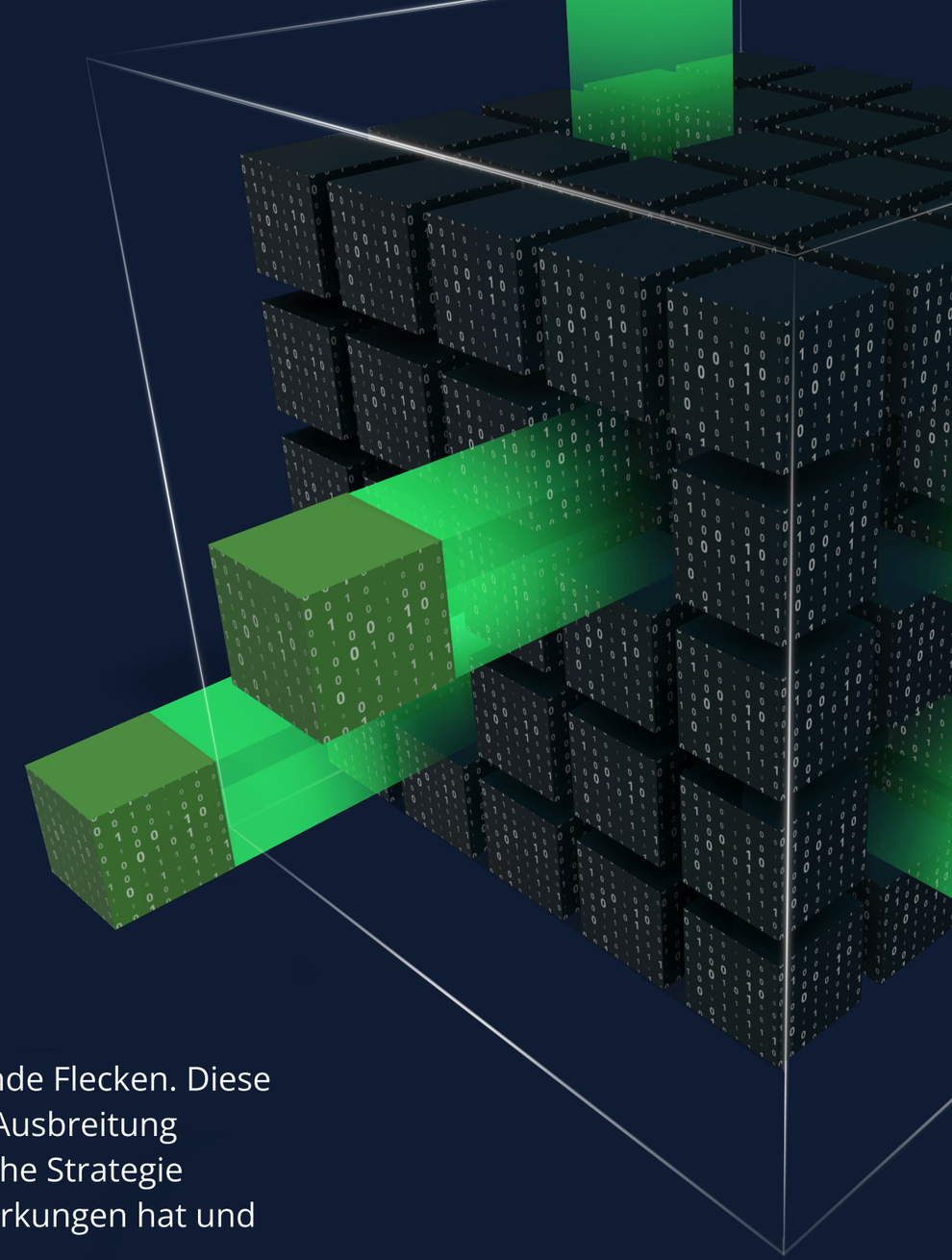


Das JFrog Trusted AI 2026 Playbook

Vom Chaos zur Kontrolle: Ein konkreter Plan für eine einheitliche und sichere Grundlage zur Nutzung von KI

Mit der zunehmenden Verbreitung von KI entstehen im gesamten Unternehmen kritische blinde Flecken. Diese Lücken in den Bereichen Governance, Sicherheit und Management begünstigen die schnelle Ausbreitung ungeprüfter KI-Assets und setzen Unternehmen erheblichen Risiken aus. Ohne eine einheitliche Strategie verlieren Unternehmen schnell die Kontrolle über ihre KI-Assets, was unvorhersehbare Auswirkungen hat und zu erheblichen Governance-Lücken führt.

Die Prinzipien zur Aufdeckung dieser blinden Flecken sind für Software und KI dieselben, allerdings mit deutlich höheren Risiken. Dieses Playbook bietet einen konkreten 5-Säulen-Plan, um die Lücke zwischen DevOps, SecOps und MLOps zu schließen und Ihr bestehendes Vertrauen auf den gesamten KI/ML-Lebenszyklus auszudehnen.

1. **KONSOLIDIEREN SIE** DIE FRAGMENTIERTE KI-TOOLCHAIN

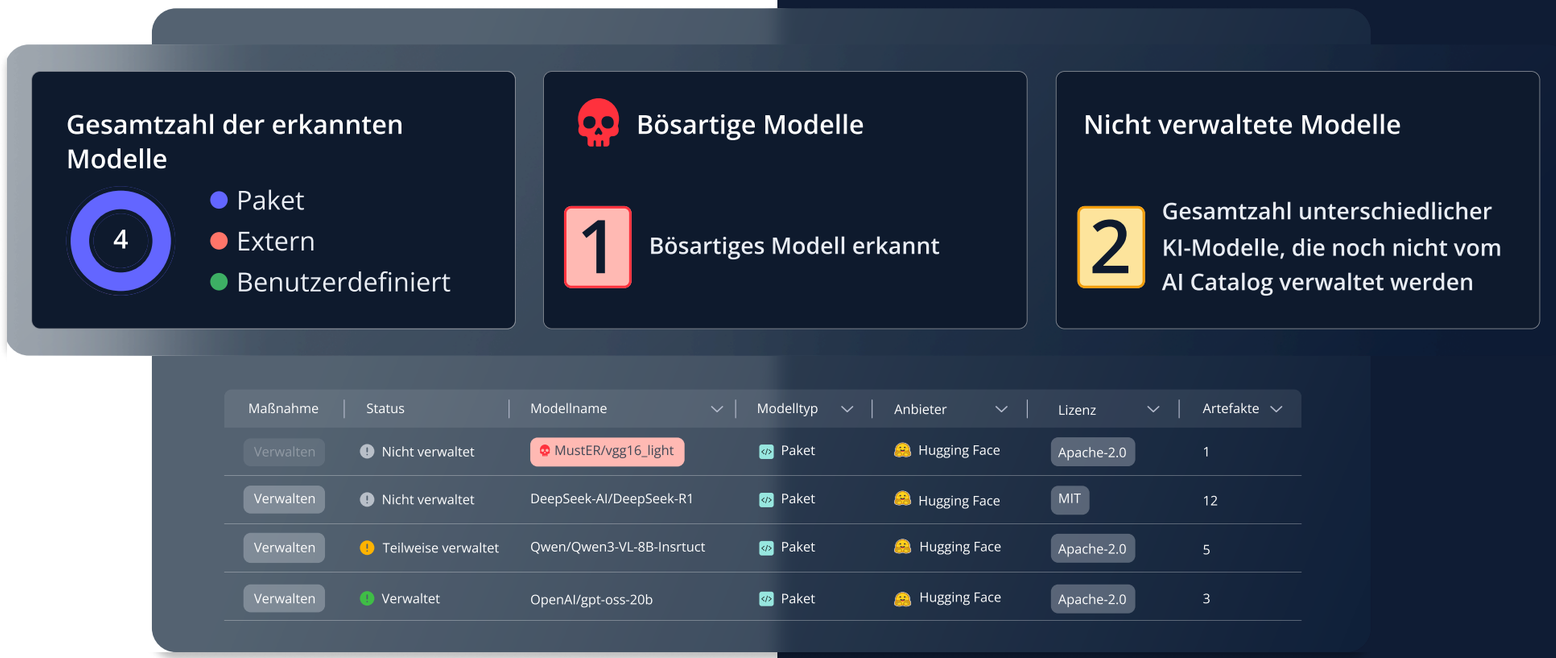
Das Problem:
KI/ML-Teams kämpfen mit einer Vielzahl an Integrationen zwischen fragmentierten Tools. Ihre Modelle, Daten, Software-Binärdateien und Code sind über verschiedene Systeme verteilt, was blinde Flecken bei der Compliance, zusätzlichen Betriebsaufwand und ständige Projektverzögerungen zur Folge hat.

Der Plan:
Schaffen Sie eine Single Source of Truth. Vereinheitlichen Sie alle Ihre KI- und Software-Artefakte, indem Sie eine zentrale Registry für Ihre Modelle, Container, Softwareanwendungen, Python-Pakete und Datensätze implementieren. Dieses System muss in der Lage sein, öffentliche Repositories (wie Hugging Face) als Proxy zu nutzen und Ihre intern entwickelten Modelle zusammen mit Ihrer Software zu hosten.

2. **ERKENNEN SIE** VERSTECKTE UND NICHT VERWALTETE KI-ASSETS

Das Problem:
Was Sie nicht sehen, können Sie nicht kontrollieren. Shadow AI ist weit verbreitet: Nur etwa 50 % der Unternehmen geben an, dass sie eine „hohe Visibility“ in Bezug auf die KI-Nutzung ihrer Entwickler haben1. Jedes nicht geprüfte Modell bzw. jeder ungeprüfte API-Endpunkt erzeugt blinde Flecken bei der KI und schafft neue Sicherheitsrisiken.

Der Plan:
Implementieren Sie einen zentralen Katalog, um alle KI-Assets zu entdecken und zu inventarisieren. Dieser Katalog muss als zentraler Hub fungieren, um alle externen APIs, Open-Source-Modelle und intern entwickelte Modelle zu finden, zu überprüfen und zu taggen – und so Unsichtbares sichtbar zu machen.

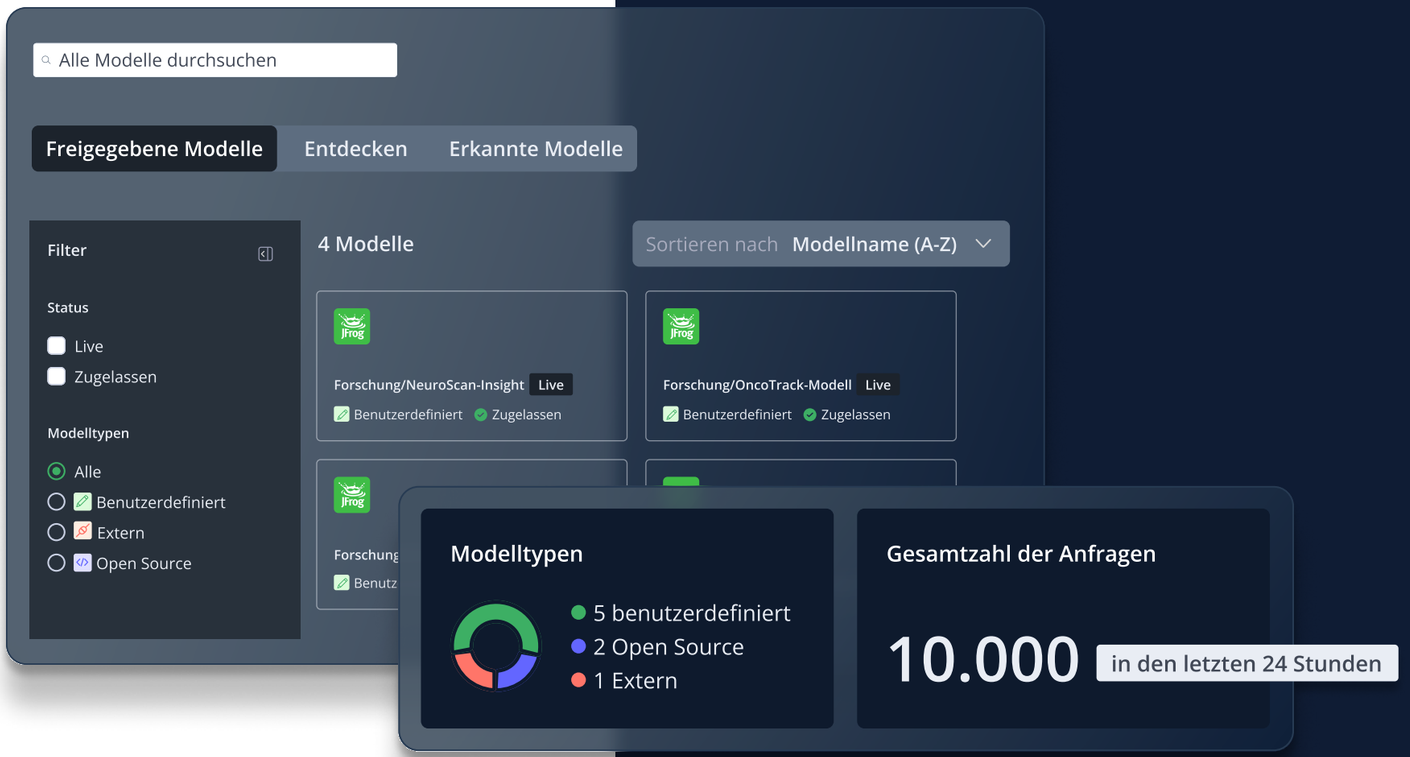


[1]EY-Report.

3. ZENTRALISIEREN SIE VISIBILITY UND GOVERNANCE

Das Problem:
Ohne eine zentrale Kontrollinstanz ist es unmöglich, Richtlinien durchzusetzen. Aus diesem Grund verfügen 63 % der Unternehmen nicht über effektive Richtlinien zur KI-Governance2. Dieser fragmentierte Ansatz führt zu Sicherheitslücken und erschwert die Einhaltung neuer regionaler KI-Regulierungen.

Der Plan:
Nutzen Sie Ihren AI Catalog als zentrale Schnittstelle zur Steuerung aller Modelle. Hier wenden Sie Ihre bestehenden Sicherheits- und Compliance-Richtlinien auf KI-Modelle an. So ermöglichen Sie Ihren Teams, für jeden Anwendungsfall souverän das passende, vorab genehmigte Modell auszuwählen, zu validieren und bereitzustellen – alles über einen zentralen Hub.

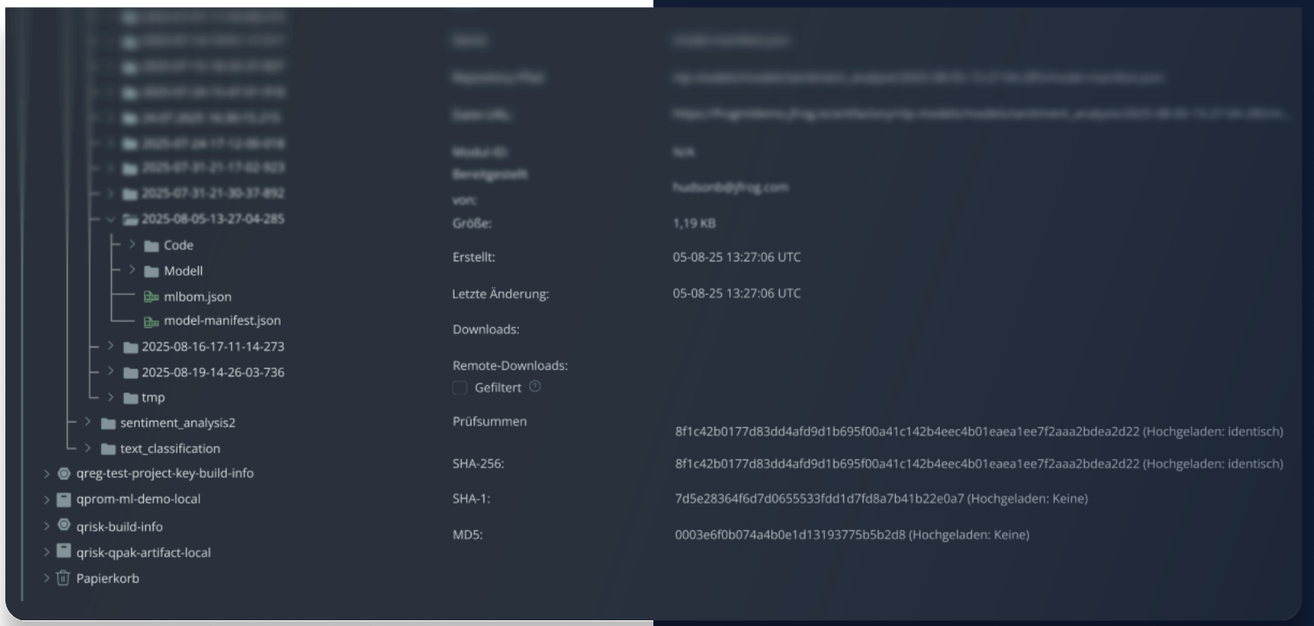


[2]IBM-Report.

4. **REDUZIEREN SIE** DAS RISIKO DURCH EIN AI-BOM

Das Problem:
Ein KI-Modell ist keine einzelne Datei. Es besteht aus einem komplexen Zusammenspiel von Code, Daten und „kritischen Abhängigkeiten“. Die Bedrohung durch bösartige Modelle nimmt zu: Hunderte wurden bereits in Open-Source-Repositories wie Hugging Face identifiziert und stellen ein direktes Risiko für Ihre Lieferkette dar.

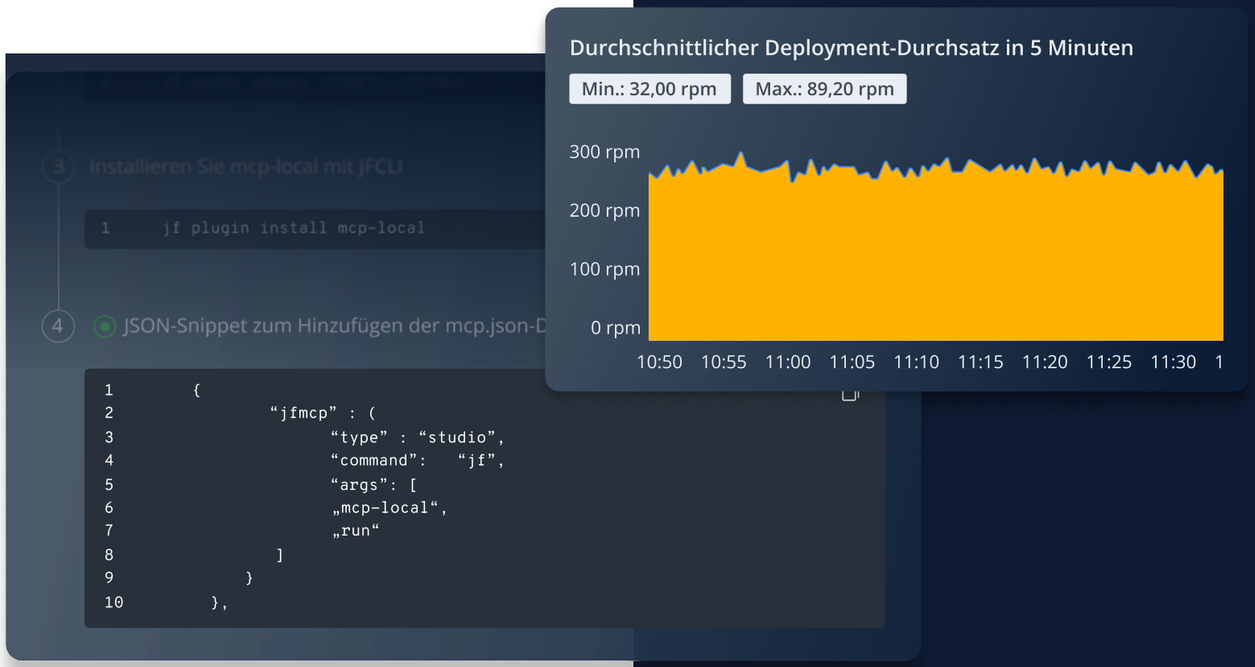
Der Plan:
Wenden Sie einen kontrollierten Lieferkettenansatz auf Ihre KI-Pipelines an. Schützen Sie Modelle und deren Abhängigkeiten proaktiv, indem Sie ein AI-BOM (Bill of Materials) erstellen. So zentralisieren Sie die Kontrolle über den Zugriff auf Modelle, können deren Nutzung nachverfolgen und sicherstellen, dass alle KI-Initiativen sicher und regelkonform sind.



5. VEREINFACHEN SIE DEN ZUGRIFF UND DIE BEREITSTELLUNG FÜR DIE PRODUKTION

Das Problem:
Selbst bei sicheren, zugelassenen Modellen wird der Weg in die Produktion oft durch manuelle Übergaben, zusätzlichen Betriebsaufwand und Prozessengpässe blockiert. Diese Ineffizienzen bremsen Innovationen aus und verhindert, dass Teams Modelle schnell bereitstellen können.

Der Plan:
Etablieren Sie einen schnellen und klar definierten Prozess, um Modelle in die Produktionsumgebung zu überführen. Durch den Einsatz eines sicheren KI-Gateways zur Bereitstellung von Modellen können Sie den Weg von der Entwicklung bis zur Produktion rationalisieren und automatisieren. Dazu gehören One-Click-Deployments für zugelassene Modelle sowie die sichere Anbindung zu externen Anbietern (wie OpenAI, Anthropic usw.). So werden Sicherheits- und Betriebsprozesse nicht länger zum Bottleneck.

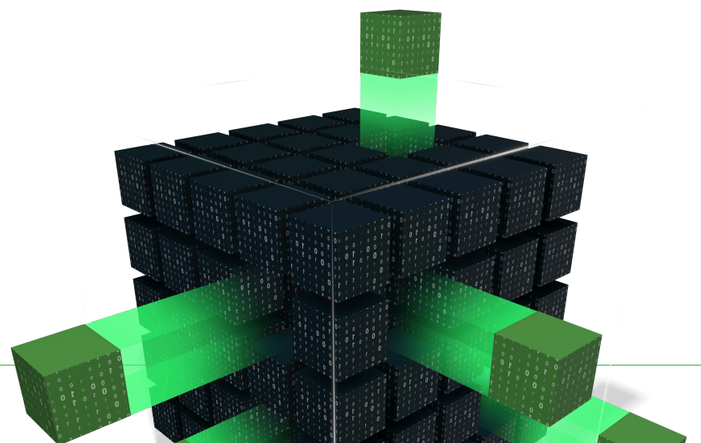


VOM PLAN ZUR PLATTFORM

Sie haben nun einen 5-Säulen-Plan, um das KI-Chaos unter Kontrolle zu bringen. Der nächste Schritt ist die Umsetzung in Ihrem Unternehmen.

Brauchen Sie Unterstützung? Möchten Sie erfahren, wie Sie den JFrog AI Catalog als zentralen Hub für all Ihre KI/ML-Vorhaben integrieren können?

Jetzt Kontakt aufnehmen



ÜBER JFROG

JFrog ermöglicht es Tausenden von DevOps-Unternehmen weltweit, jedes Software-Artefakt mit der universellen, hybriden Multi-Cloud Plattform von JFrog zu erstellen, abzusichern, zu verteilen und mit jeder beliebigen Umgebung zu verbinden.

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