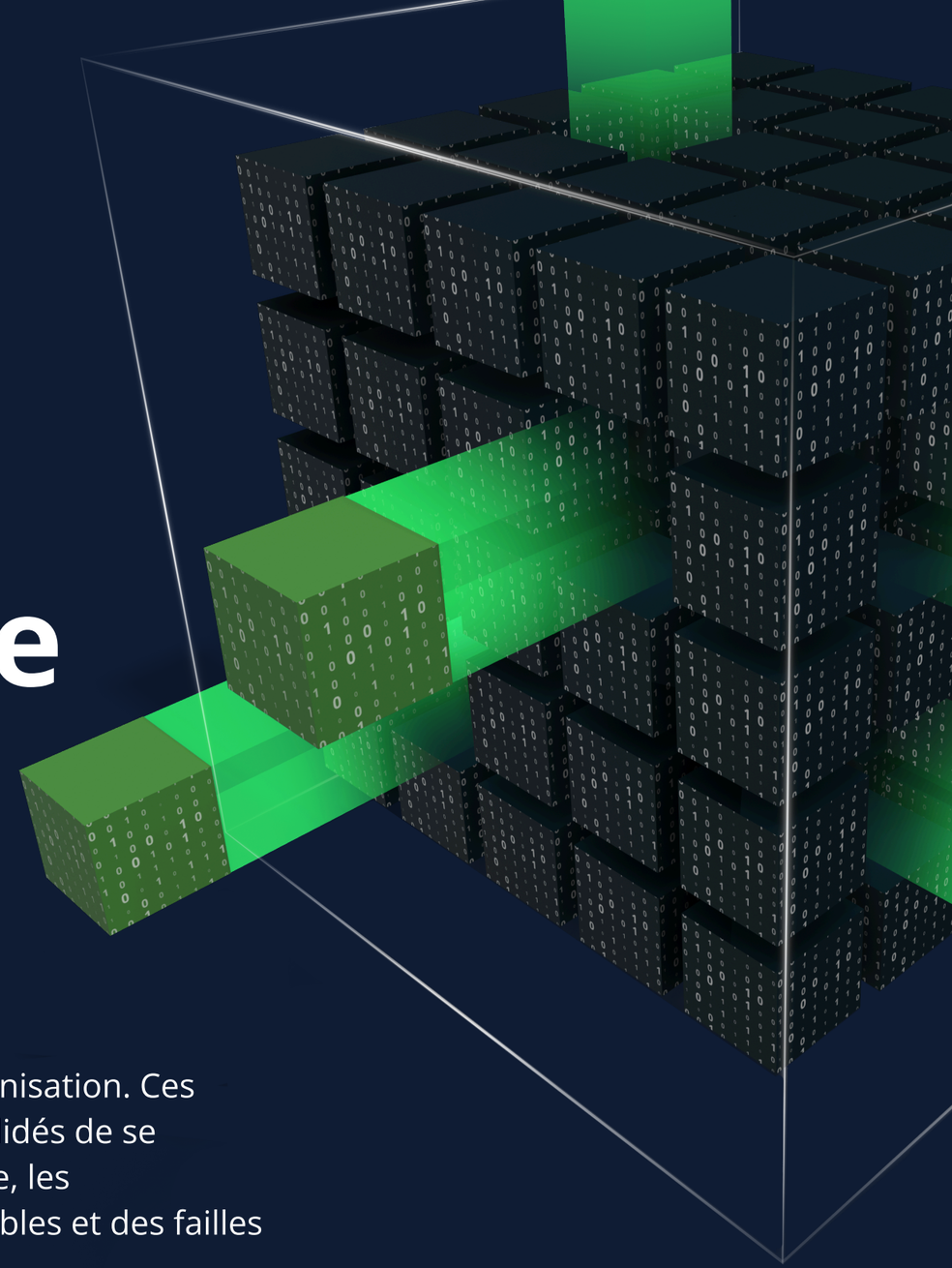


Playbook JFrog 2026 pour une IA de confiance

Du chaos au contrôle : un plan concret pour une base IA unifiée et sécurisée

À mesure que l'adoption de l'IA s'accélère, des angles morts critiques apparaissent dans l'organisation. Ces lacunes en matière de gouvernance, de sécurité et de gestion permettent aux actifs IA non validés de se multiplier rapidement, exposant l'organisation à des risques importants. Sans stratégie unifiée, les organisations perdent souvent le contrôle de leurs actifs IA, entraînant des résultats imprévisibles et des failles majeures de gouvernance.

Les principes pour découvrir ces angles morts sont les mêmes pour les logiciels et l'IA, mais les enjeux sont plus élevés. Ce manuel fournit un plan concret en 5 piliers pour combler le fossé entre DevOps, SecOps et MLOps et étendre votre confiance existante à l'ensemble du cycle de vie de l'IA/ML.

1. **CONSOLIDER** LA CHAÎNE D'OUTILS IA FRAGMENTÉE

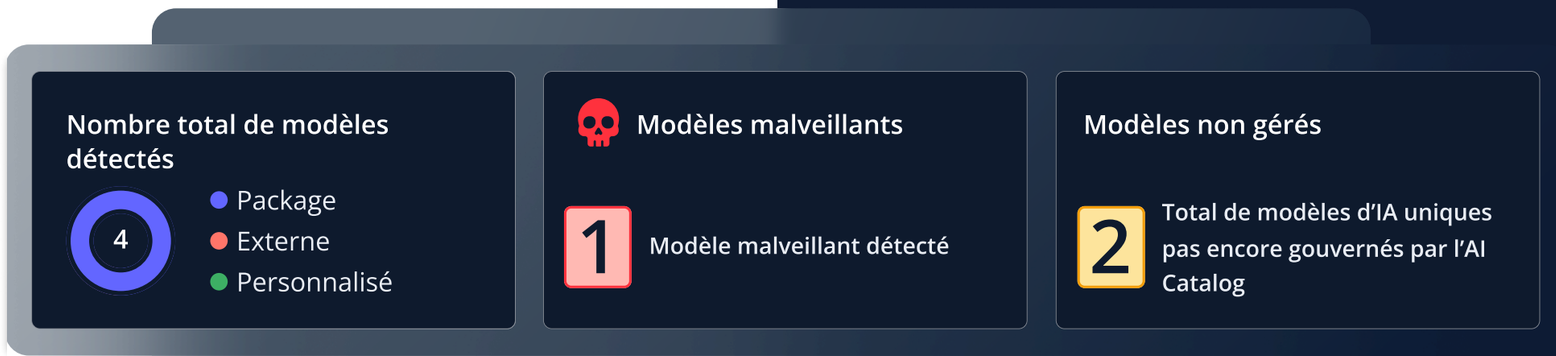
Le problème :
les équipes IA/ML sont submergées par les intégrations entre des outils fragmentés. Vos modèles, vos données, vos binaires logiciels et votre code sont dispersés dans différents systèmes, créant des angles morts de conformité, une surcharge opérationnelle et des retards constants dans les projets.

Le plan :
établir une source unique de vérité. Unifiez tous vos artefacts IA et logiciels en mettant en place un registre central pour vos modèles, conteneurs, applications logicielles, packages Python et ensembles de données. Ce système doit pouvoir servir de proxy pour les dépôts publics (comme Hugging Face) et héberger vos modèles développés en interne ainsi que vos logiciels.

2. **DÉTECTER** LES ACTIFS D'IA CACHÉS ET NON GÉRÉS

Le problème:
on ne peut pas gouverner ce que l'on ne voit pas. L'IA fantôme est omniprésente : seulement environ 50 % des organisations déclarent avoir une « forte visibilité » sur l'utilisation de l'IA par les développeurs1. Chaque modèle ou point de terminaison d'API non validé crée des zones d'ombre et de nouveaux risques de sécurité.

Le plan:
mettez en place un catalogue centralisé pour découvrir et inventorier tous vos actifs d'IA. Ce catalogue doit servir de plaque tournante centrale pour trouver, examiner et étiqueter toutes les API externes, les modèles open source et les modèles développés en interne, rendant l'invisible visible.



Action	Statut	Nom du modèle	Type de modèle	Fournisseur	Licence	Artefacts
Gérer	Non géré	MustER/vgg16_light	Package	Hugging Face	Apache-2.0	1
Gérer	Non géré	DeepSeek-AI/DeepSeek-R1	Package	Hugging Face	MIT	12
Gérer	Partiellement géré	Qwen/Qwen3-VL-8B-Insrtuct	Package	Hugging Face	Apache-2.0	5
Gérer	Géré	OpenAI/gpt-oss-20b	Package	Hugging Face	Apache-2.0	3

[1]Rapport EY.

3. **CENTRALISER** LA VISIBILITÉ ET LA GOUVERNANCE

Le problème:
sans point de contrôle central, il est impossible d’appliquer des politiques. C’est pourquoi 63 % des entreprises ne disposent pas de politiques efficaces de gouvernance de l'IA2. Cette approche fragmentée crée des goulots d’étranglement en matière de sécurité et entrave la conformité aux réglementations régionales sur l’IA, en constante évolution.

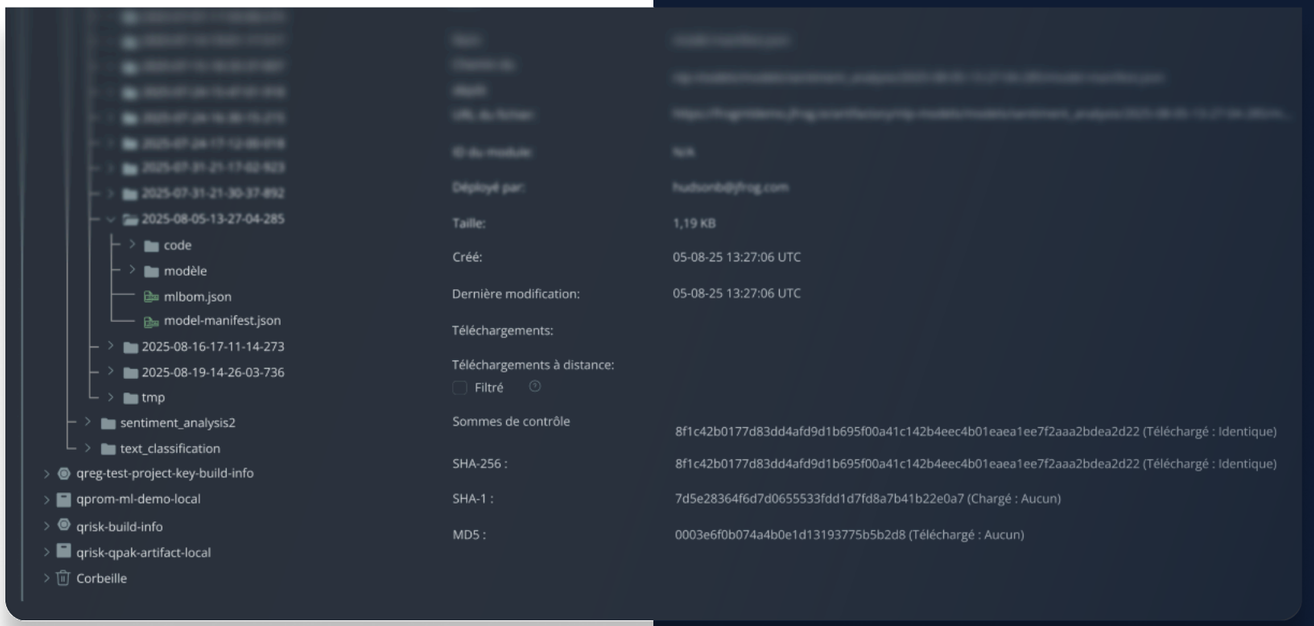
Le plan:
utiliser votre AI Catalog comme point d’entrée unique pour gouverner tous les modèles. Il s’agit d’appliquer vos politiques de sécurité et de conformité aux modèles d’IA. Vos équipes peuvent ainsi sélectionner, valider et déployer des modèles adaptés et préapprouvés en toute confiance, pour tous les cas d’utilisation, depuis un hub central.

[2]Rapport IBM.

4. **RÉDUIRE** LES RISQUES GRÂCE À L'AI-BOM

Le problème:
un modèle d'IA n'est pas un simple fichier. Il repose sur un réseau complexe de code, de données et de « dépendances critiques ». Les modèles malveillants représentent une menace croissante : des centaines ont été identifiés dans des dépôts open source comme Hugging Face, constituant un risque direct pour votre chaîne d'approvisionnement.

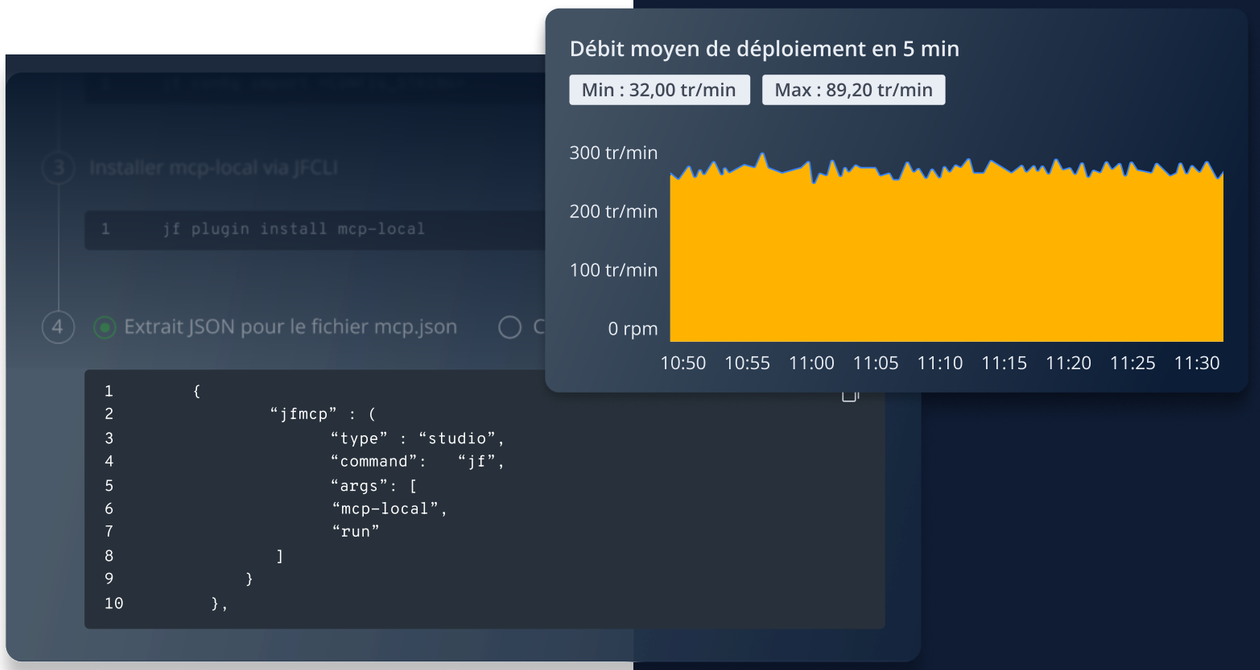
Le plan:
adopter une approche de chaîne d'approvisionnement gouvernée pour vos pipelines IA. Sécurisez les modèles et leurs dépendances de manière proactive en générant un AI-BOM (nomenclature logicielle). Cela vous permet de centraliser le contrôle pour gérer l'accès aux modèles, suivre leur utilisation et garantir que toutes les initiatives IA sont sécurisées et conformes.



5. SIMPLIFIER L’ACCÈS ET LE PASSAGE EN PRODUCTION

Le problème:
Même avec des modèles sécurisés et approuvés, le chemin vers la production est souvent bloqué par des transferts manuels, des surcharges opérationnelles et des goulots d’étranglement de processus. Cette friction freine l’innovation et empêche les équipes d’expédier rapidement les modèles.

Le plan:
Créer un chemin clair et rapide pour passer les modèles en production. En utilisant une passerelle IA sécurisée pour servir les modèles, vous pouvez rationaliser et automatiser le chemin du développement à la production. Cela inclut l’activation du déploiement en un clic pour les modèles autorisés et la connexion sécurisée à des fournisseurs externes (comme OpenAI, Anthropic, etc.), éliminant efficacement les goulots d’étranglement que sont la sécurité et les opérations.

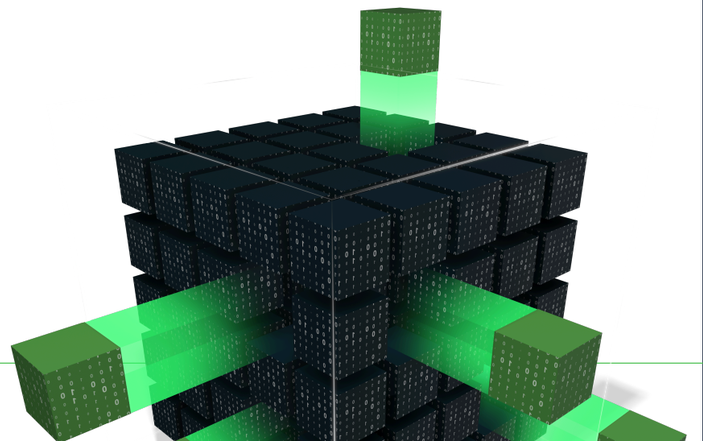


DU PLAN À LA PLATEFORME

Maintenant que vous disposez du plan en 5 piliers pour passer du chaos au contrôle de l'IA, il est temps de le mettre en œuvre au sein de votre organisation.

Besoin d'accompagnement ? Envie de découvrir comment intégrer le JFrog AI Catalog comme hub centralisé pour toutes vos initiatives en IA/ML ?

Discutons-en



À PROPOS DE JFROG

JFrog permet à des milliers d'organisations DevOps dans le monde de créer, de sécuriser, de distribuer et de connecter tout type d'artefact logiciel à tout environnement grâce à la plateforme JFrog universelle, hybride et multicloud.

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