



SOLUTION SHEET — Capability Spotlight

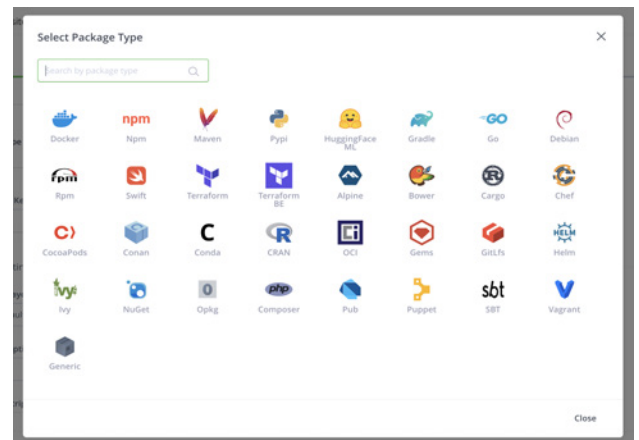
ML Model Management

Create a single system of record for ML models that brings ML/AI development in line with your existing secure SSC.



OVERVIEW

More development organizations are building and leveraging ML/AI models for use in software applications. However, a lack of standardized best practices on how to incorporate MLOps into the broader software supply chain has led ML model development to largely occur in isolation from the rest of software development. Further, the use of open source models poses similar challenges to using OSS packages - security, availability, versioning, etc. - particularly as the open source model ecosystem is still relatively new and the threat landscape uncertain.



ML Model Management with JFrog is an industry-first solution allowing organizations to bring development and security of AI/ML models alongside their other software components for a unified view of the software assets they're building and releasing. It delivers the same best practices organizations have benefited from for secure package management with JFrog to model management - control, availability, visibility, security, traceability/auditing.

BENEFITS



Manage ALL your Software Artifacts in One Place

Store and manage models alongside the other components that make up modern software applications for better visibility and insight into the status of your software and its development.



Bring DevOps Best Practices to ML Development

The DevOps practices developed over a decade of experience with OS package management, pipeline automation, and quality/feedback loops can now be applied to ML model management.



Ensure Integrity and Security of ML Models

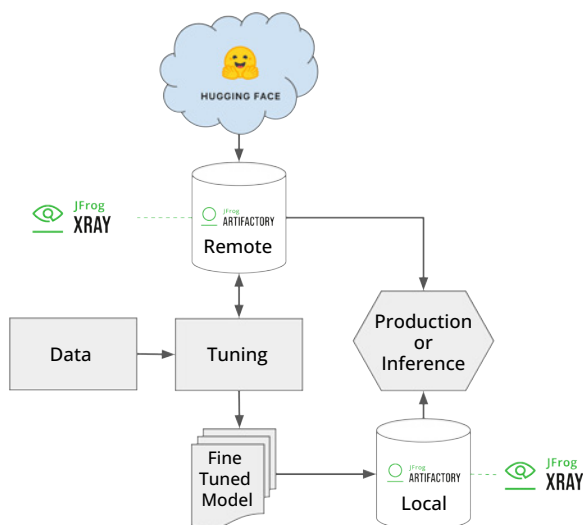
Manage your models in a system that introduces important controls including RBAC, versioning, license and security scanning so that ML, Security, and DevOps teams feel confident in the models used and be ready for the inevitable regulation to come.



A Single Platform for DevOps, SecOps, and MLOps

Consolidate disparate tools and eliminate point solutions with a single system of truth that can manage ML Models and the technologies that package them into applications used by consumers. Seamlessly combine workflows of ML Engineers and DevOps teams without needing to change the way either party works.

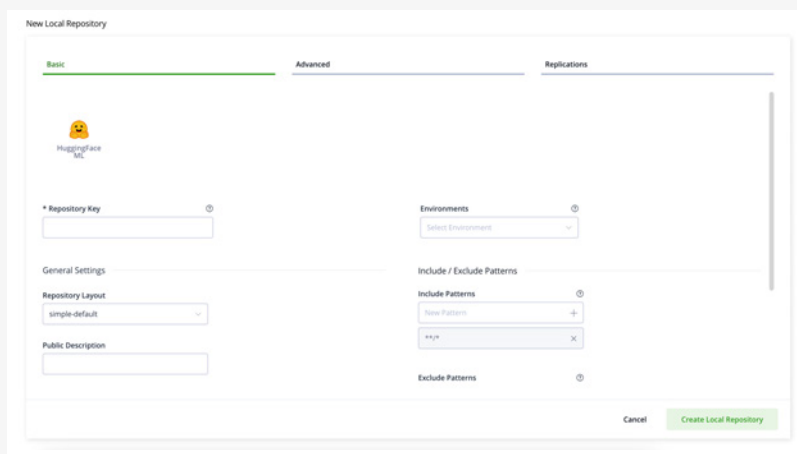
KEY CAPABILITIES



- Secure ML model registry
- Store and manage proprietary and modified OSS models
- Simplified, intuitive ML versioning
- Proxy Hugging Face for always available open source models
- Detect malicious models and enforce license compliance
- Standardize MLOps processes across teams
- Integrated with ML tools such as Jupyter Notebooks and Amazon SageMaker

SIMPLIFYING MODEL VERSIONING

Model versioning can be a frustrating process with many considerations when taking models from Data Science to Production. Git approaches create a version with every commit, but lack context and become untenable as more people get involved. JFrog leverages a name and timestamp-based versioning approach paired with an advanced file system to ensure all stakeholders use the right version, at the right place, and the right time.



v0.0170124

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.



<https://jfrog.com/r/m/>

LEGAL STATEMENT

Copyright © 2024 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.



www.jfrog.com



www.twitter.com/jfrog



www.facebook.com/artifrog



www.youtube.com/@JFrogInc



www.linkedin.com/company/jfrog-ltd