MANIFEST

Summer 2025

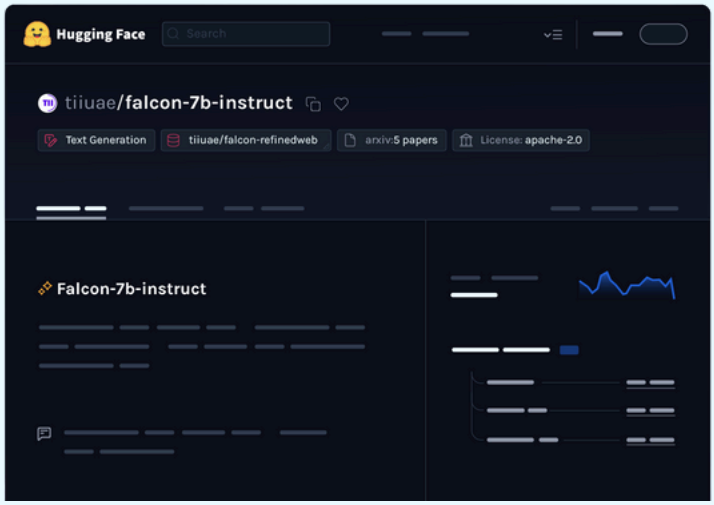
Manifest AI Risk Overview

Assess AI risk across models, datasets, licenses, and dependencies.

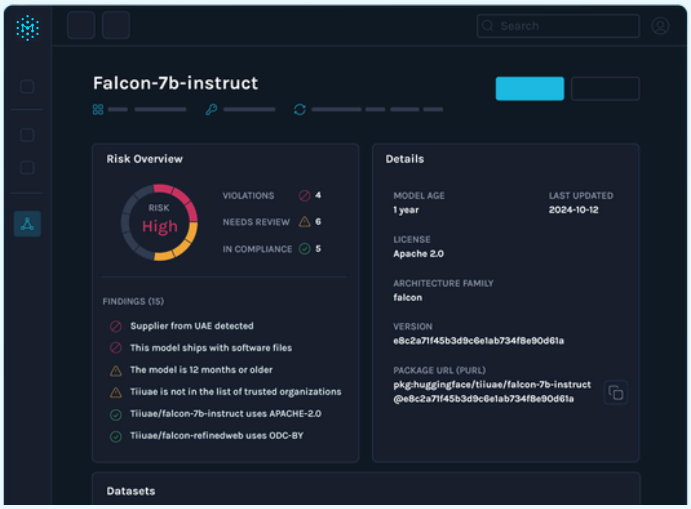
Manifest empowers private and public sector organizations to operate critical systems and applications with confidence. We detect and manage hidden software supply chain and AI risks at scale.

Manifest AI Risk gives you full visibility into the AI models and data powering your software, so you can govern AI use at every level. AI Risk continuously monitors both open-weight and custom models to enable AI governance policy enforcement, risk reduction, and ensure responsible AI development.

Bringing Visibility to AI



Open-weight AI reference sites often obscure security details, creating challenges in verifying the integrity of models.



Manifest AI Risk gives you visibility into models, datasets, and dependencies, with automated assessments to manage AI risk without slowing development.

THE GOVERNANCE CHALLENGE

As AI adoption accelerates, so do the risks; spanning outdated models, blackbox training data, non-compliant licenses, and geopolitical concerns. AI risk encompasses threats from integrating AI into software, including high-risk licenses, undocumented datasets, restricted or unmaintained models, shadow AI, and third-party dependencies.

Ultimately, these mirror the longstanding challenges of the software supply chain.

GLOBAL REGULATIONS

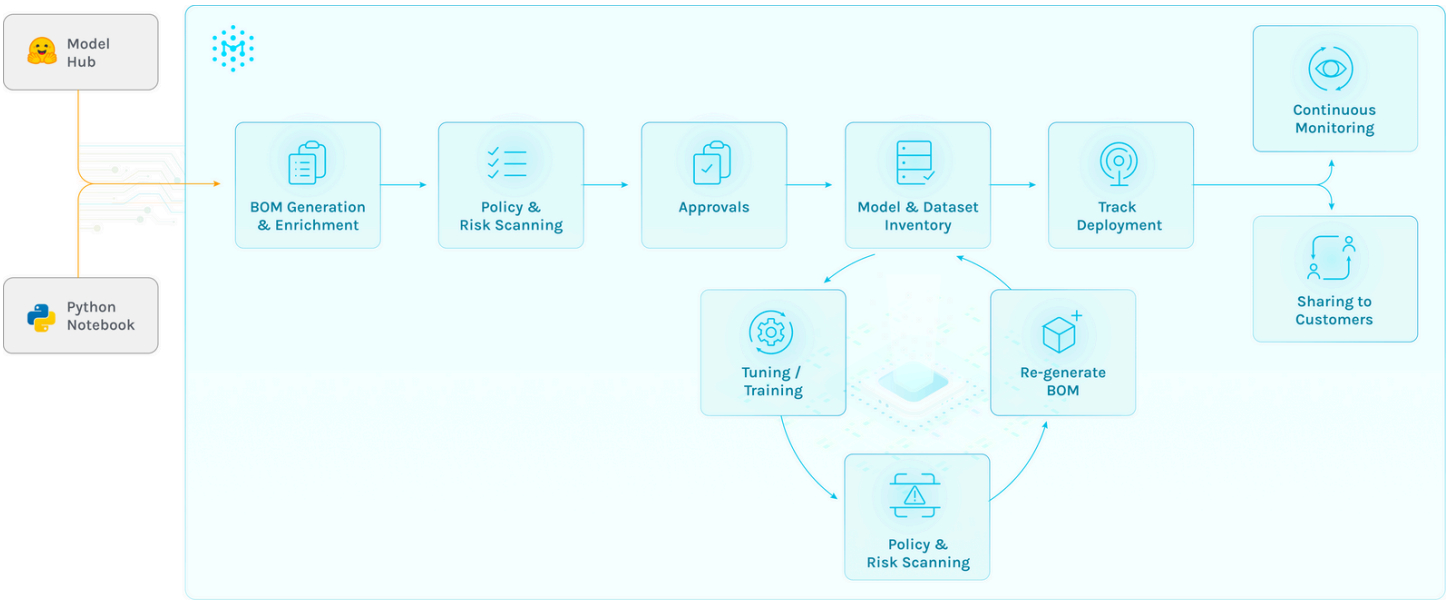
Since 2022, the momentum for AI regulation has surged, with governments and industry watchdogs worldwide intensifying their oversight to rein in risks and shape the future of AI.

Regulations top of mind for Manifest customers:

- EU AI Act
- EU NIS 2
- NIST 800-218
- UNECE R155
- OWASP SAMM
- ISO/SAE 21434
- Executive Order 14028
- Executive Order 14144
- OMB M-22-18
- FDA Cybersecurity Guidance

Learn more at manifestcyber.com/ai-risk.

HOW IT WORKS



Manifest AI Risk generates AI SBOMs and continuously analyzes AI models for risk through three key methods:

- Direct analysis of open-source models from Hugging Face
- Ingestion of third-party AI SBOMs in CycloneDX or SPDX formats
- Monitoring of developer Python notebooks throughout the model tuning process

Each model is assessed against your organization's AI Risk Policies and assigned a risk rating (High to Low). Based on this evaluation, models are categorized as Approved, Forbidden, or placed in a Review queue. The Manifest Python plugin enables ongoing monitoring of custom model development, ensuring complete visibility and policy compliance.

KEY FEATURES

- **Configure Policies:** Ensure AI model development aligns with your organization's governance policies.
- **Explore AI Risk**: Evaluate open-weight models from Hugging Face for risks related to undocumented training data, alignment with internal policies, and potential licensing or usage restrictions.
- **Enforce Policies:** Detect models in source code and python notebooks, and trigger alerts and enforcement actions for developers and security teams for models that violate internal policies.
- **Track and Inventory Models:** Keep track of all AI models in use, open-weight or custom tuned.
- **Scan Source Code:** Detect AI models embedded in source code by scanning the CI/CD pipeline and GitHub repositories.

Start your trial of Manifest AI Risk

Ready to bring visibility and governance at scale to your AI supply chain? Sign up for a trial and start assessing AI risk throughout the entire development lifecycle.

https://bit.ly/3Tk6efo

OUR ACCREDITATIONS

FedRAMP High

GDPR

DOD Impact Level 5

SOC 2 TYPE 2

NIST 800-171 Compliant