Mend AI Premium

Secure the AI powering your applications

The Challenge

AI is powering business critical applications at an unprecedented pace. Open source AI libraries, like Hugging Face, accelerate development with easy access to pre-trained models and datasets. However, AI also brings unprecedented risks—data exposure, malicious models, and compliance challenges— that bypass detection from traditional AppSec tools, silently expanding your attack surface. Without the right protections, innovation turns into liability.

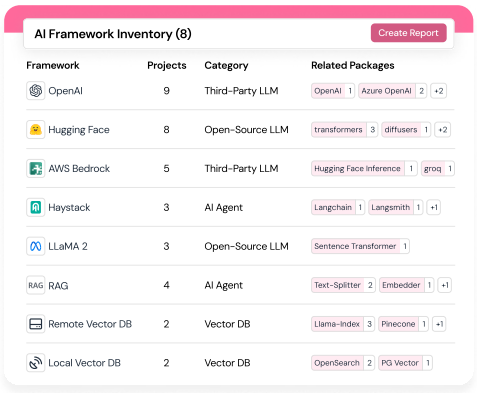
Security teams need a unified approach to manage AI component risks throughout the development lifecycle - from detection and inventory to risk assessment and policy enforcement.

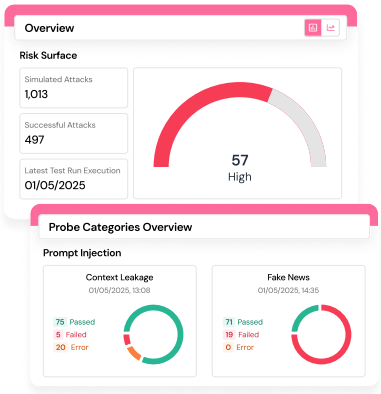
The Solution

Mend AI Premium empowers security teams to proactively address these new risks - without completely reinventing the wheel.

Whether you choose Mend AI Premium as a standalone offering or as an upgrade option for Mend.io's AI Native AppSec Platform, it continuously discovers and inventories AI models and frameworks, identifying and assessing risks within each application's context. Armed with this insight, security teams can effectively measure, prioritize, and remediate AI related threats alongside broader AppSec risks—all within a unified, single source of truth.

With Mend AI Premium, security teams gain the visibility and control they need to effortlessly expand security coverage, curb AI sprawl, and ensure compliance.





With Mend AI Premium, You Gain...

Continuous Inventory and AI-BoM

Comprehensive, holistic visibility into your AI Models and AI Frameworks, including shadow AI components.

AI Component Risk Insights

Actionable, contextualized insights on AI Model risks, such as licensing, security vulnerabilities, and malicious models.

System Prompt Hardening

Harden system prompts to proactively assess and control AI prompt risks by identifying threats based on their content, structure, or potential for misuse

AI Behavioral Risk Coverage (Red-teaming)

Pre-built, customizable tests uncover unique threats like data exfiltration, prompt injection, and hallucinations for conversational AI.

Proactive Policies and Governance

Robust policies and workflows to govern AI components throughout the software development lifecycle.

Mend.io offers the first AI native application security platform, empowering organizations to build and run a proactive AppSec program tuned for AI powered development. The unified platform secures AI generated code and embedded AI components, drives risk reduction through AI powered remediation, automates compliance, and provides a holistic enterprise scale view of risks and clear actions for developers across your entire codebase.

Learn more at www.mend.io