AI Native AppSec Platform: Mend AI

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

Built natively into Mend.io’s AI Native AppSec Platform, Mend AI 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, security teams gain the visibility and control they need to effortlessly expand security coverage, curb AI sprawl, and ensure compliance.

With Mend AI, 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

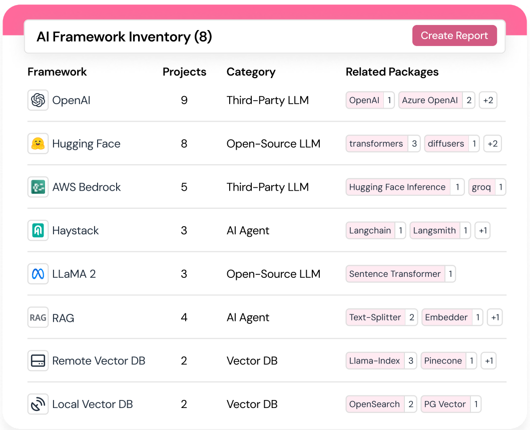
Harden system prompts to proactively assess and control AI prompt risks by identifying threats based on their content, structure, or potential for misuse.

AI Behavioral Risk Coverage (Red-teaming)

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

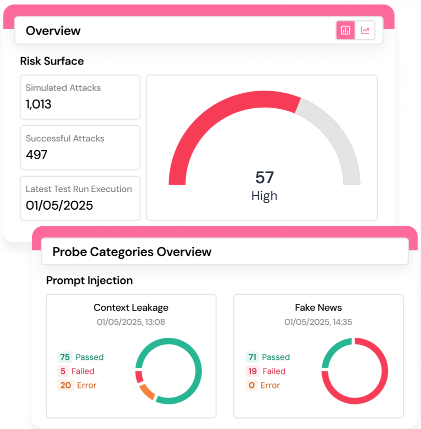
Proactive Policies and Governance

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



AI Framework Inventory (8)

Framework	Projects	Category	Related Packages
OpenAI	9	Third-Party LLM	OpenAI 1 Azure OpenAI 2 +2
Hugging Face	8	Open-Source LLM	transformers 3 diffusers 1 +2
AWS Bedrock	5	Third-Party LLM	Hugging Face Inference 1 groq 1
Haystack	3	AI Agent	Langchain 1 Langsmith 1 +1
LLaMA 2	3	Open-Source LLM	Sentence Transformer 1
RAG	4	AI Agent	Text-Splitter 2 Embedder 1 +1
Remote Vector DB	2	Vector DB	Llama-Index 3 Pinecone 1 +1
Local Vector DB	2	Vector DB	OpenSearch 2 PG Vector 1



Overview

Risk Surface

Simulated Attacks: 1,013

Successful Attacks: 497

Latest Test Run Execution: 01/05/2025

Probe Categories Overview

Prompt Injection

Context Leakage
01/05/2025, 13:08
75 Passed
5 Failed
20 Error

Fake News
01/05/2025, 14:35
71 Passed
19 Failed
0 Error

Why Mend.io's AI Native AppSec Platform?

Gain full visibility & control: Understand your entire AppSec landscape—including AI components, code, dependencies, and containers—with a comprehensive, continuous inventory.

Focus on what matters: Get actionable, contextual insights into AI risks, from licensing and vulnerabilities to malicious models, and prioritize remediation within your broader AppSec strategy.

Manage risk holistically: Mitigate AI and AppSec risks from one source of truth. Govern AI components throughout the SDLC with Mend.io's policy engine and automation workflows.

Deploy fast, at scale: Implement Mend.io's AI Native AppSec Platform for thousands of developers in less than an hour, across all applications in development.

Lower developer burden: Increase adoption with a security solution your developers will actually use. Scan, remediate, and govern directly in developers' workspace—no tool switching required.