Mend AI

Security for AI Assets

The Challenge

The use of AI technology in software development is exploding, and security teams are scrambling to catch up. Open source AI libraries, such as those stored in Hugging Face, offer developers quick and easy access to pre-trained models and data sets—and offer bad actors an opportunity to inject malicious models into the AI ecosystem. AI introduces security and legal risks into the application development landscape that traditional AppSec tools are not equipped to address.

Security teams need visibility and control over which AI models are being used in their applications. In addition to cybersecurity concerns, there are legal and compliance risks associated with the use of both AI models and AI-generated code that must be accounted for.

The Mend.io Solution

Mend AI gives security teams clear visibility into the AI models being used in their applications by providing coverage for all 350k+ AI models indexed in Hugging Face. Mend AI provides the licensing of each AI model found so compliance teams can ensure their organization is protected from legal risk. Visibility will continue to grow as frameworks for indexing AI vulnerabilities emerge and are added to our reporting.

It's still early days for both AI itself and AI security solutions. Knowing what's in your codebase is valuable, but we won't stop there.

The Road Ahead

Mend AI is in active development in collaboration with our customers. Upcoming features include:

- **AI code snippet detection:** Mend AI's snippet detection spotlights AI-generated code snippets used in your application and accurately identifies the precise AI tool, such as GitHub Co-pilot and AWS Code Whisperer, used to generate it.
- **AI-BOM:** Gain increased transparency into your applications with Mend.io's advanced bill of materials support for AI models, which provides a holistic view of the direct, transitive, and artificial intelligence components and dependencies used in your software.
- **Gender bias detection:** Mend AI uses advanced algorithms to uncover gender biases found in AI models, deflecting potential legal issues and fostering inclusion.

Key Benefits

Visibility

Know which AI models and associated open source licenses are in your codebase. Mend AI detects all 350k+ AI models indexed in Hugging Face.

Insights

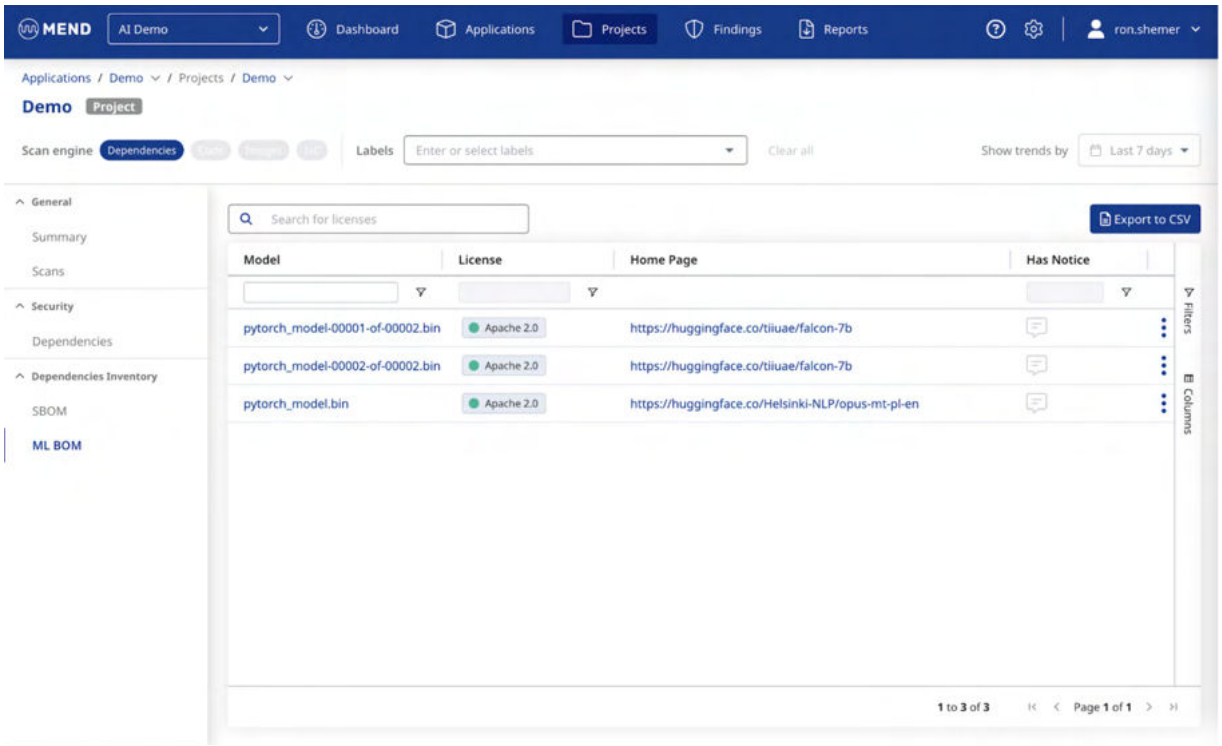
Protect your AI-enhanced applications against security and legal risks. Mend AI gives you control by providing detailed license, version, and security information for each AI model found in your application.

Innovation

Mend AI expands the capabilities of our gold-standard software composition analysis tool, Mend SCA, to cover the AI portion of the modern software supply chain.

Matching the pace of AI development

Mend AI plays such a pivotal role in addressing a critical, emerging, and growing need for our customers using AI models and AI-generated code that we are including these essential capabilities as part of Mend SCA. As AI development and AI security frameworks mature, we'll continue to keep you covered.



About Mend.io

Trusted by the world's leading companies, including IBM, Google, and Capital One, Mend.io's enterprise suite of application security tools is designed to help you build and manage a mature, proactive AppSec program.

Mend understands the different AppSec requirements of developers and security teams. Unlike other AppSec solutions that force everyone to use a single tool, Mend helps them work in harmony by giving each team different, but complementary, tools—enabling them to stop chasing vulnerabilities and start proactively managing application risk.

Learn more at