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 Solution

Mend AI gives security teams clear visibility into the AI models being used in their applications, allowing them to identify and address potential security and compliance risks. It analyzes over 350,000 pre-trained models to help uncover licensing concerns and versioning challenges. With Mend AI, development and security teams can focus on innovation and building secure AI-powered applications with confidence.

Mend AI adds key features and benefits to Mend SCA, including:

Comprehensive Pre-Trained Model Indexing - Mend AI ensures complete coverage of all 350k+ AI models indexed in Hugging Face, to give clear visibility into the AI Models used in your applications.

Dependency Protection - Mend AI delivers detailed AI model versioning and update information for every AI model used in your applications - protecting against outdated dependencies with AI Models.

License Compliance - Mend AI equips your security teams with the license details of each AI model used in your applications, instilling safeguards against license types not approved by your organization.

AI-BoM - Mend.io's AI-BoM (bill of materials) provides a holistic view of the artificial intelligence components and dependencies used in your software, promoting full transparency of AI models and their dependencies.

It's still early days for both AI itself and AI security solutions. Knowing what's in your code base is valuable, but we won't stop there. Mend AI is under active development in collaboration with our customers.

Why Mend AI?

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

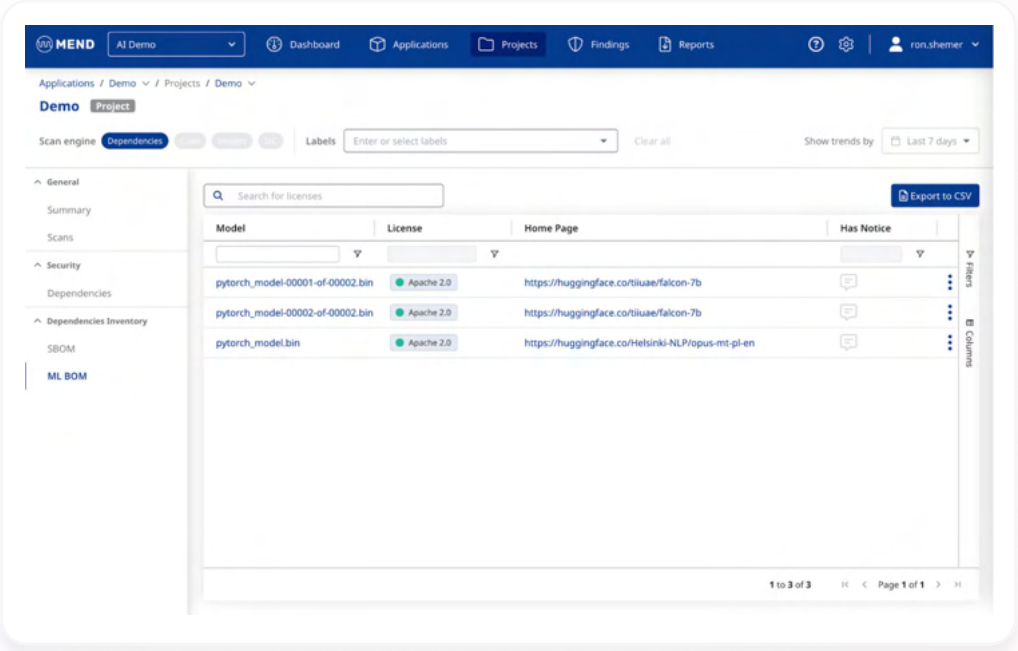
Protect your AI-enhanced applications against security and legal risks. Mend AI gives you control by providing detailed license, version, and security information for each AI model found in your application.

No added costs

The full set of Mend AI features is included with every Mend SCA license. There's no need to buy an extra product to protect AI assets.

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