AI Bill of Materials

Securing the AI supply chain

The Challenge

The way we build applications is changing. The rise of AI native applications and the use of AI generated code have introduced a new frontier for software security. This adds a fresh layer of complexity to the existing challenges of software supply chain security.

Government regulations and industry standards now require a detailed inventory of all software components, but traditional methods of creating a Software Bill of Materials (SBoM) are not equipped to handle the unique nature of AI components used in your code creating a critical gap, as vulnerabilities can be hidden within AI components, leaving your applications and users at risk.

The Solution

Mend.io's AIBoM is designed specifically for the AI native age. It goes beyond a traditional SBoM by providing unmatched visibility into what makes up your software, including components. Mend.io's AIBoM automatically scans and analyzes human written and AI generated code, open source libraries, and proprietary components to create a comprehensive, machine-readable inventory. It's an essential tool for security teams who need to ensure the integrity of their applications in a world where AI is a fundamental part of the development process.

How Mend.io's AIBoM Works

Mend.io's platform generates an AIBoM in industry standard SPDX and CycloneDX format, providing a machine-readable inventory of all software components and their dependencies, including those from AI components.

With Mend.io's AIBoM you can...

- Pinpoint all components, whether they are explicitly in your code or called by your code.
- Document and track each component, including direct and transitive libraries, to understand the full dependency tree.
- Automatically update your bill of materials when components change, providing continuous visibility.
- Quickly find security vulnerabilities in both human-written and AI generated code.
- Get a clear path to remediate vulnerable components, ensuring updates are backward-compatible and won't break the build.
- Import third-party SBoMs from other tools, creating a unified and holistic view of all your software assets, regardless of their source.

Mend.io's AIBoM provides...

Component and license identification

Run thousands of attacks—before and in production—using prebuilt or custom tests across prompt injection, hallucination, off-topic, and social engineering.

Continuous coverage

Ensure all components, including those used in AI-powered applications, are up to date.

Risk prioritization and remediation

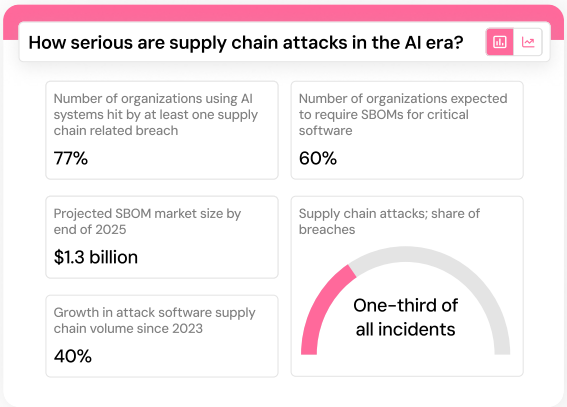
Prioritize and remediate risks in both open-source and AI components based on their potential impact, whether they originate from open-source libraries or AI models.

Regulatory compliance and transparency

Meet regulatory and industry requirements for security and transparency in AI-native applications.

Model Trust and Integrity

Ensure the AI model is trustworthy from its origin. By verifying a model's lineage, you can prevent threats like model poisoning and confirm the integrity of its data and components.



Why Mend AI?

AI Component Detection & Inventory: Comprehensive visibility into AI models, frameworks, agents, RAGs, MCPs, and shadow AI, with an AI-BoM for full dependency mapping.

AI Component Risk Insights: Contextualized insights on model licensing, vulnerabilities, and malicious components to help prioritize and mitigate risk.

System Prompt Hardening: Automatically detect and assess system prompts, compare against best practices, and apply improvements to reduce misuse risks.

AI Red Teaming: Leverage prebuilt or custom tests to uncover behavioral risks like data exfiltration, prompt injection, hallucinations, and unsafe outputs.

Proactive Governance: Enforce policies and workflows to manage AI security and compliance risk throughout the software development lifecycle.

Trusted by the world's leading companies, Mend.io offers the first AI native application security platform designed to help organizations proactively secure AI generated code and AI components, empowering them to manage application risk effectively in modern software development.

Learn more at www.mend.io