

# Secure the layer where modern AI risk actually lives

Modern application risk no longer lives in one place. It spans the **code layer**, the **AI layer**, and the **interaction between them**.

Most security tools protect only one.

**Mend.io secures all three.**

## How Mend.io is Different

### Code-to-AI lifecycle coverage

Protect source code, open source dependencies, containers, AI models, prompts, agents, and runtime behavior—together.

### Precision that reduces real risk

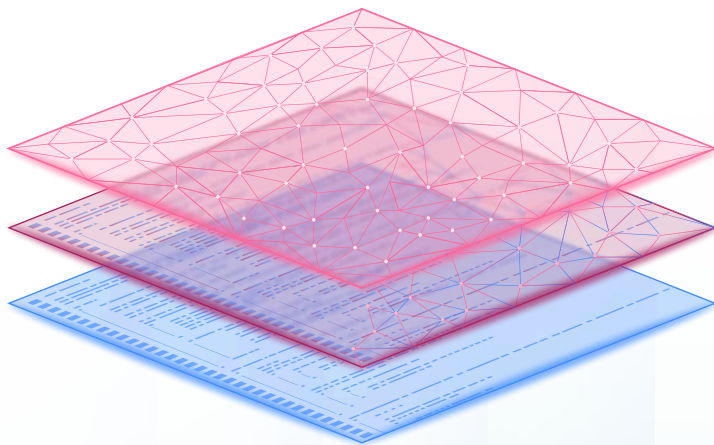
Reachability analysis, exploitability context, and high-accuracy scanning focus teams on what actually matters.

### Automation developers actually adopt

Fix risks directly inside pull requests, pipelines, and existing workflows.

### Continuous protection across the AI lifecycle

Discovery powers red teaming. Red teaming strengthens guardrails. Guardrails reinforce prompts.



## What Mend.io Secures

### The AI Layer

Bring visibility and governance to modern AI usage:

- ✓ AI-BOM inventory of models, prompts, and agents
- ✓ Shadow AI discovery
- ✓ AI component risk insights
- ✓ System prompt detection and hardening

**Outcome:** Understand where AI risk enters your environment.

### The Interaction Layer

Secure how AI behaves inside real applications:

- ✓ Prompt injection testing
- ✓ Data leakage simulation
- ✓ Behavioral red teaming
- ✓ Runtime guardrails inside your environment

**Outcome:** Continuously test and protect real-world AI behavior.

### The Code Layer

Secure your software supply chain across:

- ✓ Source code vulnerabilities (SAST)
- ✓ Open source dependencies (SCA)
- ✓ Containers and images
- ✓ License and policy compliance risk

**Outcome:** Reduce exploitable application risk without slowing development.

# The Mend.io Platform

## Mend AppSec

Protect the modern code layer with:

- 🕒 High-accuracy SAST
- 🕒 Reachability-driven SCA
- 🕒 Container risk visibility
- 🕒 Policy enforcement and compliance alignment
- 🕒 AI-powered remediation guidance

**Value:** Move from vulnerability visibility to measurable risk reduction.

## Mend AI

Secure AI systems across their lifecycle with:

- 🕒 AI-BOM and Shadow AI discovery
- 🕒 System Prompt Hardening with AI
- 🕒 weakness scoring
- 🕒 Behavioral red teaming at scale
- 🕒 Runtime guardrails inside your environment

**Value:** Secure how AI behaves—not just what it's built from.

## Mend Renovate

Automate dependency remediation across your supply chain:

- 🕒 Continuous dependency updates
- 🕒 Merge-confidence scoring
- 🕒 Automated remediation pull requests

**Value:** Eliminate vulnerable dependencies before they become incidents.

# How Mend.io Reduces Risk Faster

## Detect

Discover risk across code, dependencies, containers, and AI systems with high-accuracy analysis.

## Prioritize

Focus remediation using reachability and exploitability—not severity alone.

## Remediate

Accelerate fixes with AI-powered remediation and automated dependency updates.

## Protect

Enforce policies, block vulnerable builds, harden prompts, and apply runtime protections continuously.

# The Result

Organizations use Mend.io to:

- 🕒 Reduce exploitable application risk faster
- 🕒 Gain visibility into AI usage across environments
- 🕒 Secure AI behavior in production systems
- 🕒 Automize remediation at scale
- 🕒 Demonstrate posture to leadership, auditors, and regulators

**Secure the code layer. Secure the AI layer. Secure the interaction between them.**

**Mend.io** is a leading application security solution that helps organizations fix less and reduce risk faster. Built for both AI-driven and modern development workflows, **Mend.io** gives teams visibility into all code – human-written, AI-generated, open source, third-party and container components – and helps them prioritize and remediate the risks that matter most.