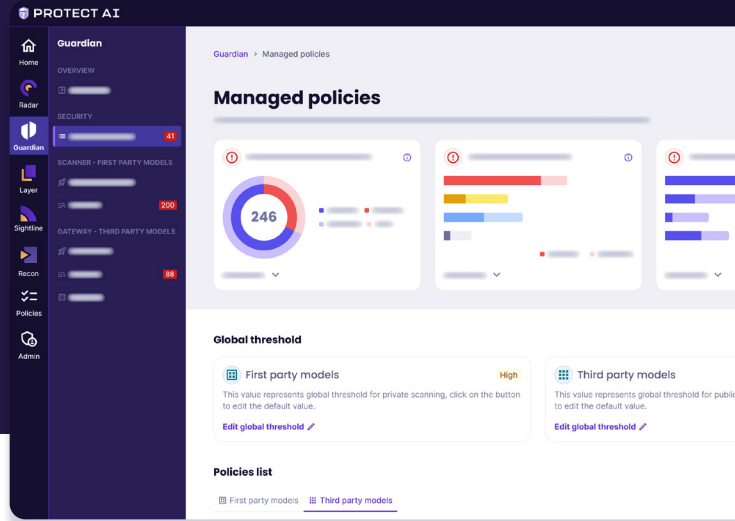


# The Platform for AI and ML Security

Protect AI delivers the broadest and most comprehensive platform to secure your AI. It enables you to see, know, and manage security risks to defend against unique AI security threats, and embrace MLSecOps for a safer AI-powered world.



## Addressing Unique AI Security Risks



### TECHNOLOGY

The AI supply chain is complex, introducing unique technical risks and vulnerabilities that put your business at risk.



### OPERATIONS

Without adequate oversight and controls, AI systems might behave unpredictably, inaccurately 'or' simply fail.



### REGULATION

Organizations must evaluate how AI and ML fit into regulatory structures and take steps to stay compliant.



### REPUTATION

As enterprises turn to AI for their customer-facing workflows, failures can lead to a loss of brand trust.



## The Protect AI Platform

Protect AI is the only vendor neutral, cloud-agnostic MLSecOps platform that helps you to See, Know, and Manage AI Risk end-to-end.

 User, Roles & Group Controls

 SIEM / SOAR Connectors

 AI/ML Vendor Neutral

 Security & Risk Policies

 Global Dashboards

 Deploy Everywhere

### GUARDIAN

First & Third Party Model Security

Enterprise AI Controls

CI/CD Integration

### RECON

Automated and Human Augmented GenAI Red Teaming

Comprehensive Threat Coverage Across 6 Major Risks

No-code Integration

### LAYER

LLM Security

LLM Monitoring & Observability

30+ Unique GenAI Scanners

### RADAR

AI Bill of Materials (AI-BOM)

AI Risk Assessment

AI Governance, Risk & Compliance

# Continuously monitor, manage, and improve the security of your AI systems with the Protect AI platform for AI-SPM

## Get Started with AI Asset Security

Implement Zero Trust for the engine that powers your AI — the Machine Learning Model.



### GUARDIAN

- Enforce the use of secure models through managed policies and a secure gateway
- Continuously scan both first and third party models and artifacts for risks before they are deployed

## Implement Comprehensive GenAI Security at Scale

Defend your LLMs from risk with end-to-end observability and monitoring



### LAYER

- Evaluate LLM inputs and outputs for data leakage, adversarial threats, content moderation, and more
- Gain full visibility into the upstream and downstream actions of the LLM
- Go beyond firewalls to scale LLM usage securely

Rigorously Red Team your LLMs with automated scanning for risks and vulnerabilities



### RECON

- Comprehensively evaluate threat exposure for all GenAI, including prompt injections, jailbreaks, data leakage and more
- Optimize LLM selection and guardrails for safety and security
- Continuously improve the security posture of your GenAI system

## Protect AI is the only platform to enable advanced and comprehensive AI-SPM capabilities

## Gain Full Visibility, Risk Assessment, and Management of the AI Lifecycle

Ensure continuous assessment, management, and discovery of risk across AI entities



### RADAR

- Inventory all AI entities and dependencies, including datasets, models, pipelines and applications, via an AI-BOM
- Enforce policies to ensure your AI remains compliant with AI regulation

**BOOK A DEMO AT [PROTECTAI.COM](https://protectai.com) »**



## Join the community



### MLSECOPS

Learn best practices in MLSecOps, listen to podcasts with thought leaders, and connect with our thriving community.



### HUNTR

Join the hunt in the world's first AI Bug Bounty Platform—huntr is the place to start your journey into AI threat research.



### OPEN SOURCE

Contribute code or issues, discover documentation, and get started with AI security with our Apache 2.0 licensed Open Source projects for AI Security.