LockThreat

Govern and Secure Every AI in Your Enterprise

Runtime AI governance and security that detects, decides, and acts on risk in milliseconds across every tool, model, and agent deployed



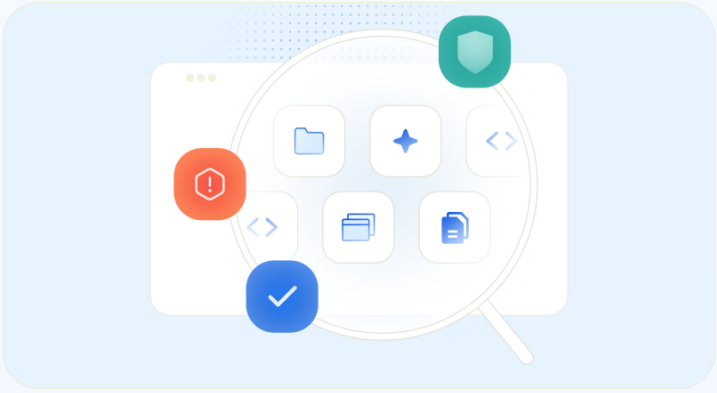
Every enterprise is deploying AI. Most have no governance around it. Shadow AI is spreading. Employees are sharing sensitive data with public models. AI agents are making autonomous decisions. And regulations like the EU AI Act are already here.

Five stages. One continuous operating model.

Discover

Shadow AI Detection

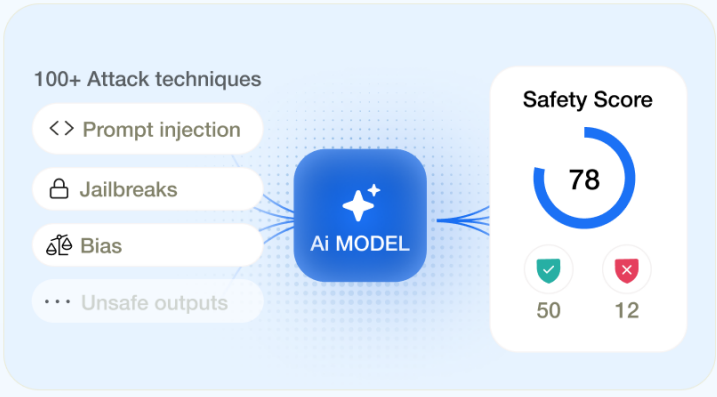
Scans your cloud environments, endpoints, and network to find every AI asset in your organization: approved tools, unapproved tools, downloaded models, and shadow AI deployments. Continuous inventory, not a one-time scan. You cannot govern what you cannot see.



Probe

AI Red Teaming

Runs automated adversarial attacks against your AI models before they go live. Tests for prompt injection, jailbreaks, bias, and unsafe outputs using 100+ attack techniques. Gives you a safety score and a clear approve-or-block decision. Find the weaknesses before production does.



Turn the page for the remaining AI Governance & Security capabilities.

This brochure covers only the AI capabilities of the LockThreat Enterprise GRC platform. To learn about the full platform, visit www.lockthreat.com

Protect

AI Application Firewall

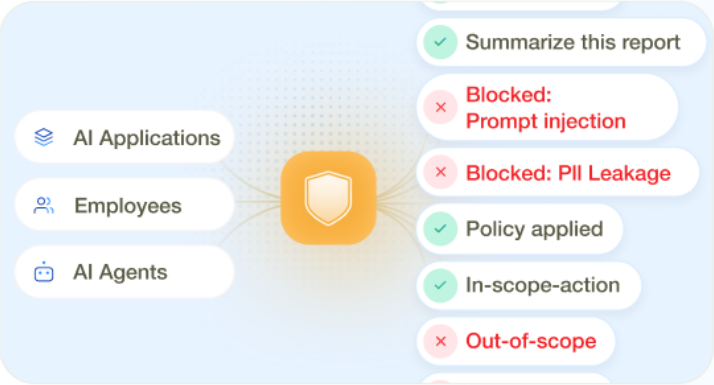
Monitors every prompt in real time for custom AI applications and integrations. Blocks prompt injection, Personally Identifiable Information (PII) leakage, and harmful outputs before they reach the end user. Median response time under 9 ms.

Employee AI Protection

Prevents employees from sharing sensitive data, PII, or Protected Health Information (PHI) with public AI tools like ChatGPT, Gemini, or Claude. Enforces your AI usage policies at the browser level with zero friction.

Agentic AI Security

Governs autonomous AI agents embedded in platforms like Salesforce Agentforce, SAP Joule, and Microsoft Copilot. These agents can access enterprise data, invoke APIs, trigger workflows, and make operational decisions without human oversight. LockThreat monitors agent behavior at runtime, detects policy violations and unauthorized actions, and blocks unsafe execution before damage is done.



Optimize

AI Token Governance

Tracks token consumption per model, per team, and per project. Detects waste, misuse and anomalies. Sets budgets and rate limits. Customers have saved 40 to 50 percent on token costs by eliminating unnecessary consumption.

Govern

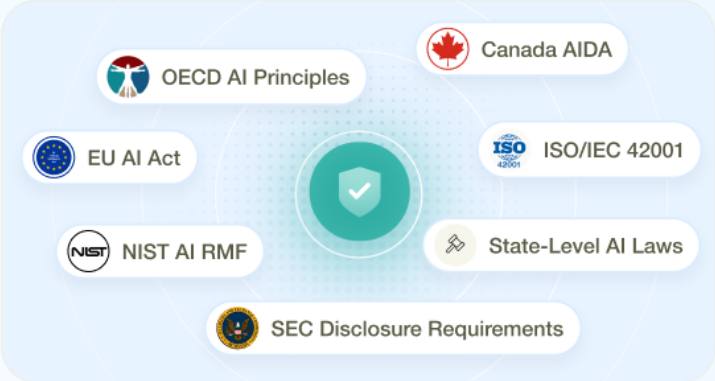
Framework and Regulatory Alignment

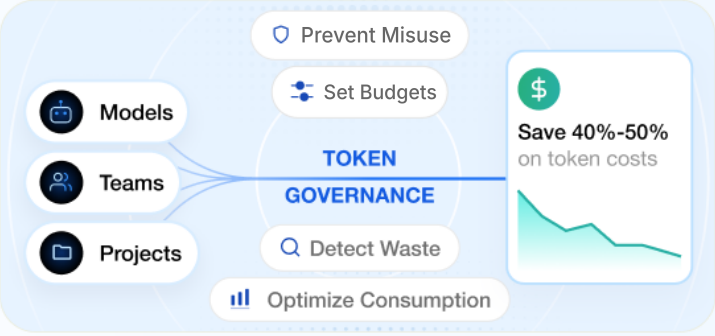
Maps your AI controls to every applicable framework simultaneously: EU AI Act, NIST AI Risk Management Framework (RMF), ISO/IEC 42001, Canada's AI and Data Act (AIDA), OECD AI Principles, SEC disclosure requirements, state-level AI laws, and many others.

Continuous AI Compliance Monitoring

Continuously monitors your deployed AI applications against the control thresholds you define, including hallucination rates, PII redaction, toxicity, and bias. When any threshold is breached, the platform flags it as a control gap linked directly to the relevant regulatory requirement.

One control library. Many frameworks.
Evidence collected automatically.





LockThreat

Full AI Governance and Security

LockThreat delivers full AI governance and security in one enterprise platform. No bolt-ons. No separate tools. No gaps between your GRC program and your AI landscape.

SEE IT IN ACTION