



THE AI SECURITY PLATFORM



AI RED TEAMING



AGENTIC AI SECURITY



AI FIREWALL



AI LENS



MODEL SCANNING



EMPOWERING SECURE AI ADOPTION

AI adoption and usage must be done in trustworthy, explainable, private, and secure manners for both the enterprise and its customers. These characteristics could be compromised by mistakes or malicious activity.

DeepKeep delivers end-to-end AI security and trustworthiness across the full AI lifecycle. Built with GenAI at its core, the platform protects both LLM and computer vision systems, keeping pace with AI's rapid innovation.

Cybersecurity teams worldwide use DeepKeep's cloud agnostic, native multilingual platform to secure AI agents, employee AI use, and homegrown AI applications:

AI FIREWALL

Monitor & stop threats originating from AI interactions.

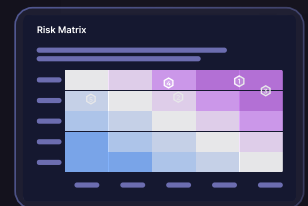
Apply a runtime AI firewall across every app, user or agent interaction. Inspect prompts and evaluate model responses before they're seen or acted on. Apply context-aware guardrails that reflect your compliance standards and data handling policies.



AI RED TEAMING

Adaptive red teaming for your AI agents, apps and models.

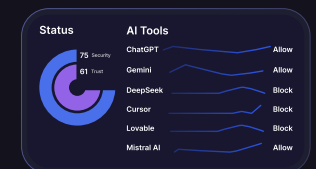
Steer real-time testing with Vibe AI Red Teaming, adapting direction as the system responds to uncover security and trust vulnerabilities that scripted approaches miss. Use Automated AI Red Teaming for continuous, broad coverage at scale.



AI LENS: DISCOVERY & USAGE CONTROL

Discovery and access control for how employees and developers interact with AI systems across the enterprise.

Identify shadow AI across the organization through multiple enforcement points to gain visibility into AI tools used by employees and developers. Enforce access control policies to ensure consistent governance aligned with risk tolerance.



AI AGENT SCANNER

Attack surface visibility across your AI agent pipeline.

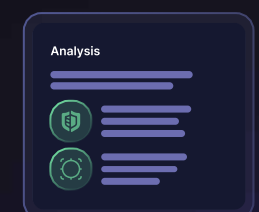
AI Agent Scanner inspects your agent end to end - mapping every LLM, tool, and integration - to uncover exploitable weaknesses including prompt injection and tool misuse. You get a visual attack surface map and a prioritized remediation playbook to harden agents before they go live.



MODEL SCANNING

Ensure your AI model is secure and safe to use.

Static and dynamic scanning of first-party and open-source models to detect malware, vulnerabilities, and hidden threats - giving you full visibility and control over model integrity before and after deployment.



WHY DEEPCKEEP?

-  **End-to-End Security**
-  **Native Multilingual Coverage**
-  **Context-Aware**
-  **SaaS / On-Prem & Air-Gapped Deployments**

