Deepkeep

END-TO-END AI SECURITY & TRUSTWORTHINESS

AI Security Platform

Keeping you on the right side of AI

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.

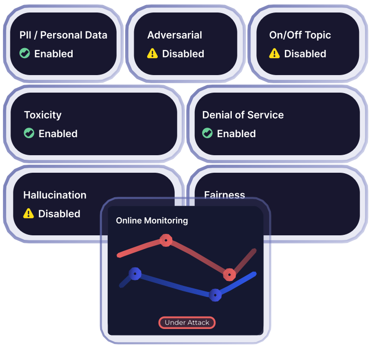
Cybersecurity teams worldwide use DeepKeep's cloud agnostic, native multilingual solution to secure AI agents, employee AI use, and homegrown AI applications.

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.

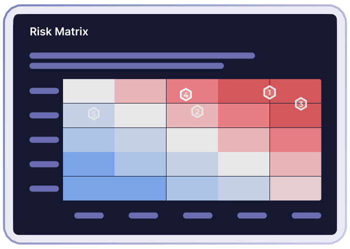
From prompt injection and jailbreaking to data leaks and toxic outputs, apply context-aware guardrails that reflect your compliance standards and data handling policies.



AUTOMATED AI RED TEAMING

Context-based evaluations of your AI model.

White box or black box model and application testing, tailored to your specific use case, identifies flaws and vulnerabilities, suggesting mitigations to secure and ensure your apps and agents act according to policy.



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.

SECURING AI AGENTS

Establish AI agent visibility and tackle risks.

Identify and mitigate risks in AI agent behavior before they escalate. Monitor activity, tackle excessive agency, enforce MCP server and tool usage, trace data flows, and assess how agents interact with systems and make decisions - keeping you ahead of incidents.

WHY DEEPKEEP?

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

AICPA SOC2

Information Security Management System ISO 27001 Certified

UNITED REGISTRAR OF SYSTEMS URS ISO 9001

DeepKeep
www.deepkeep.ai

Derech Menachem Begin 121
Tel Aviv, Israel

European Innovation Council

Co-funded by the European Union

hub:raum tech incubator of T