# DeepKeep

# THE AI SECURITY PLATFORM

**AUTOMATED 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

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.

PII / Personal Data
Enabled

Adversarial
Disabled

On/Off Topic
Disabled

Toxicity
Enabled

Denial of Service
Enabled

Hallucination
Disabled

Fairness

Online Monitoring

Under Attack

## 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.

Risk Matrix

## 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.

Analysis
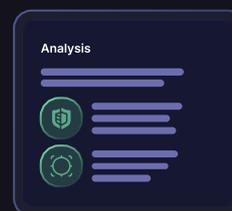
## SECURING AI AGENTS

**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.

1 Vulnerabilities
4 Agents
1 Tools

Tools

Tool Details

MCP Servers

## WHY DEEPKEEP?

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

AICPA
SOC2

ISO
27001
Certified

UNITED REGISTRAR OF SYSTEMS
URS
ISO 9001

GDPR

European Innovation Council

Co-funded by the European Union

Google Cloud Partner