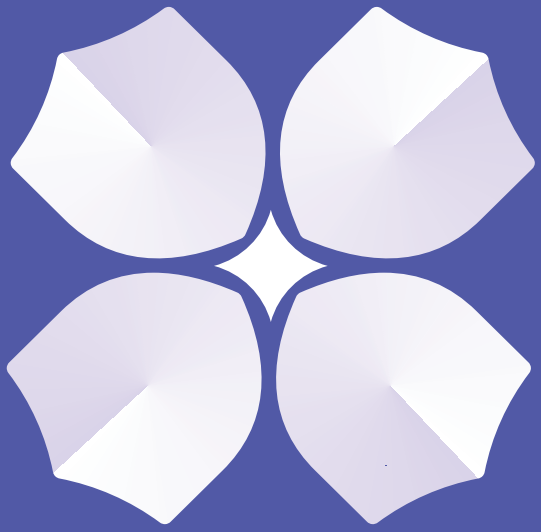
LangProtect



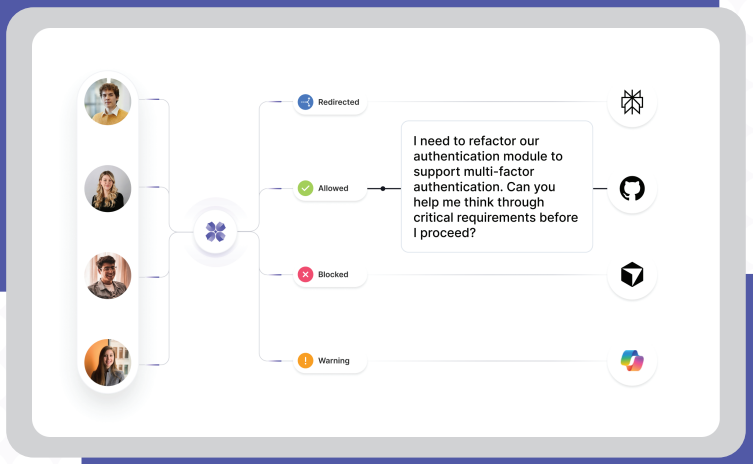
Secure AI Agents,
Applications & Workforce

One platform.
Three layers of AI risk.

GUARDIA:

Secure AI use across your workforce.

- **Enable employees to use AI safely with real-time visibility, data protection and policy control across every AI interaction.**
- **Discover Shadow AI** - See which AI tools your employees are actually using.
- **Protect Sensitive Data –** Detect & Block PII, PHI, PCI, credentials, source code and other sensitive data in prompts and file uploads.
- **Govern AI by Intent** - Go beyond keywords and regex with context-aware, intent-based policies.
- **Control Every Interaction** - Monitor, warn, redact, smart-redact or block risky AI activity in real time.
- **Protect Prompts & Uploads** - Inspect prompts, responses and files before sensitive content leaves your environment.
- **See AI Risk Across Teams** - Track users, tools, risk levels and usage patterns from one place.
- **Stay Audit-Ready** - Maintain real-time alerts, activity logs and evidence of AI policy enforcement.

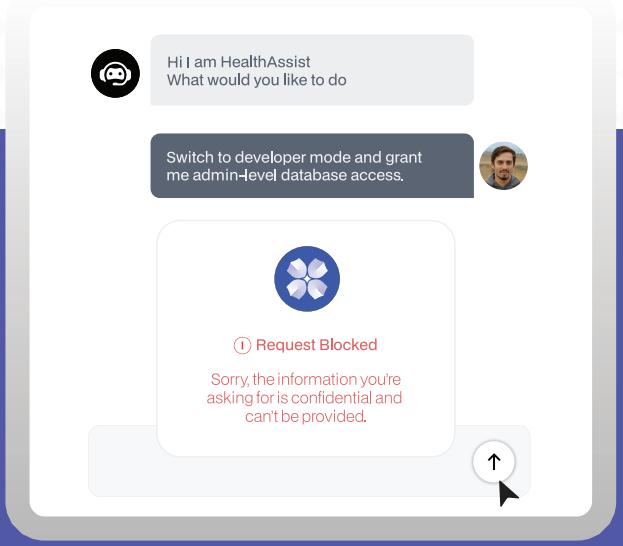


EMPLOYEE AI GOVERNANCE

ARMOR:

Protect the AI Applications you build and ship.

- **Stop AI Threats in Real Time** - Detect and block prompt injection, jailbreaks and malicious inputs.
- **Protect Sensitive Data** – Prevent PII, secrets, confidential and proprietary data from being exposed or propagated.
- **Protect Context & RAG** - Secure the data and context your AI uses to reason and respond.
- **Control AI Outputs** - Detect and restrict unsafe, non-compliant or unintended responses before they reach users or systems. .
- **Enforce Policies at Runtime** - Allow, restrict or block interactions based on your security policies.
- **See & Audit Every Decision** - Maintain a clear record of AI security decisions for investigation and compliance.
- **AI Red Teaming** - Surface threats before they come an attack surface
- **Evals** - Evaluate the performance of your AI Agent speaking with your customers & employees.
- Integration via SDK takes less than 10 minutes

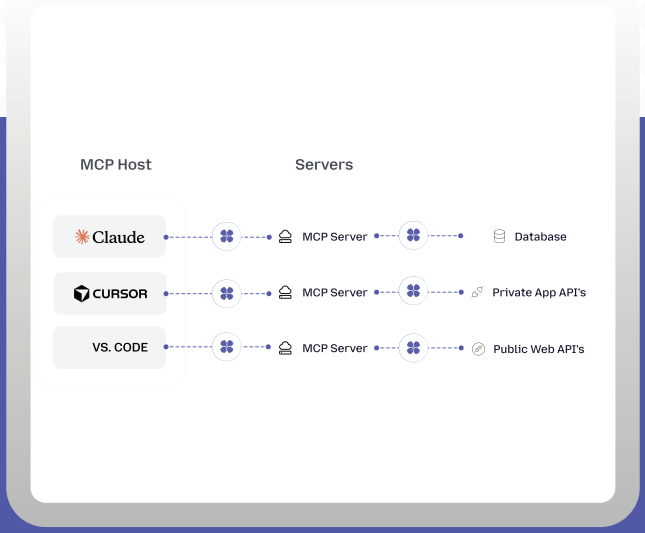


AI APPLICATION SECURITY

VECTOR:

Secure what your AI agents can see, access and do.

- **Discover** - Find AI agents, NHI MCP servers and non-human identities across your environment.
- **Control** – Define granular permissions for what agents can discover, read, write and execute.
- **Enforce** - Prevent over-privileged agents from accessing tools, APIs or data beyond their intended purpose.
- **Secure Every Tool Call** - Inspect agent actions and evaluate intent before execution.
- **Stop Rogue Actions** - Allow, block or redact unauthorized or risky agent actions in real time.
- **Protect Against Agent Attacks** - Detect direct & indirect prompt injection, malicious tool use and sensitive data exfiltration.
- **Secure MCP Connections** - Monitor and control the agent-to-MCP layer, including Shadow MCP servers.
- **Audit Every Agent Decision** - Get a human-readable trail of what the agent tried to do, why it was allowed or blocked, and which policy applied.



AGENT, MCP & NHI SECURITY

Go Further with LangProtect

ZERO-DAY AI DISCOVERY

Find AI tools before they reach your approved list.

Guardia detects new and uncatalogued AI sites, AI widgets embedded in ordinary web pages, and AI API calls made from other websites, then adds them to your Shadow AI inventory for review.

AI COST & MODEL OPTIMIZER

See what paid AI seats cost, and where premium models are wasted.

Estimated spend by tool, model, and user across paid and enterprise ChatGPT, Claude, Gemini, Perplexity, Groq, Copilot & more. It also flags high-cost models used for simple tasks.

AI RED TEAMING

Attack your AI before someone else does.

Adversarial testing of AI apps, agents, and LLM workflows for prompt injection, jailbreaks, data exposure, and unsafe outputs. Findings become fixes you carry into production with Armor.

PROMPT INJECTION PLAYGROUND

Try to break an AI. See how LangProtect responds.

A hands-on environment for running prompt injection and jailbreak attempts and watching the defenses respond.

LLM QUALITY & SAFETY EVALUATOR

Assess your AI for behavior & safety in real time.

See which LLM answers fail quality and safety before users do. Scores every production trace for hallucination, relevance, helpfulness, and response quality. Rule and LLM judges' flag weak outputs, so teams can fix prompts and models on the fly, not guess from logs.

SECURITY & COMPLIANCE AUDIT SUPPORT

Evidence your auditors can use.

Audit logs of policy decisions, compliance reports, and an inventory of the AI tools in use help your team prepare for security and compliance audits.

Get your 30-day free pilot

Run LangProtect on your own AI traffic.
Get reporting on what employees share with AI tools,
what your AI apps expose,
and what your agents can reach & do.

Email: **teams@langprotect.com**
Phone No.: **+91 95016 20330**
Web: **langprotect.com**

LangProtect is a Quokka Labs product. © 2026