LangProtect

End-to-End AI Security & Governance Platform

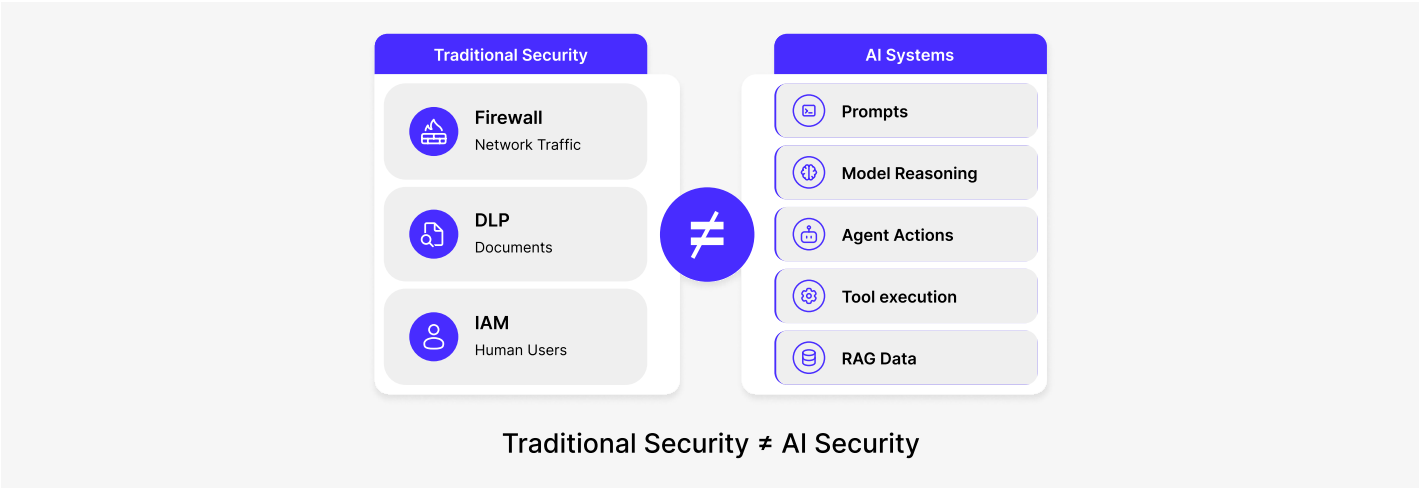
Protect every prompt. Control every agent. Govern every AI interaction.
Enterprise-ready AI security

LangProtect is an enterprise AI security platform that delivers real-time visibility, protection, and governance across LLM applications, autonomous agents, and employee AI usage. It secures AI interactions across enterprise systems, shadow tools, and AI workflows with sub-50ms latency and no vendor lock-in.

Enterprise AI adoption is rapidly expanding—from copilots and RAG systems to multi-agent workflows—introducing new risks such as prompt injection, sensitive data leakage, shadow AI usage, and uncontrolled agent actions.

Traditional security tools were not built for AI environments, creating a growing AI security gap.

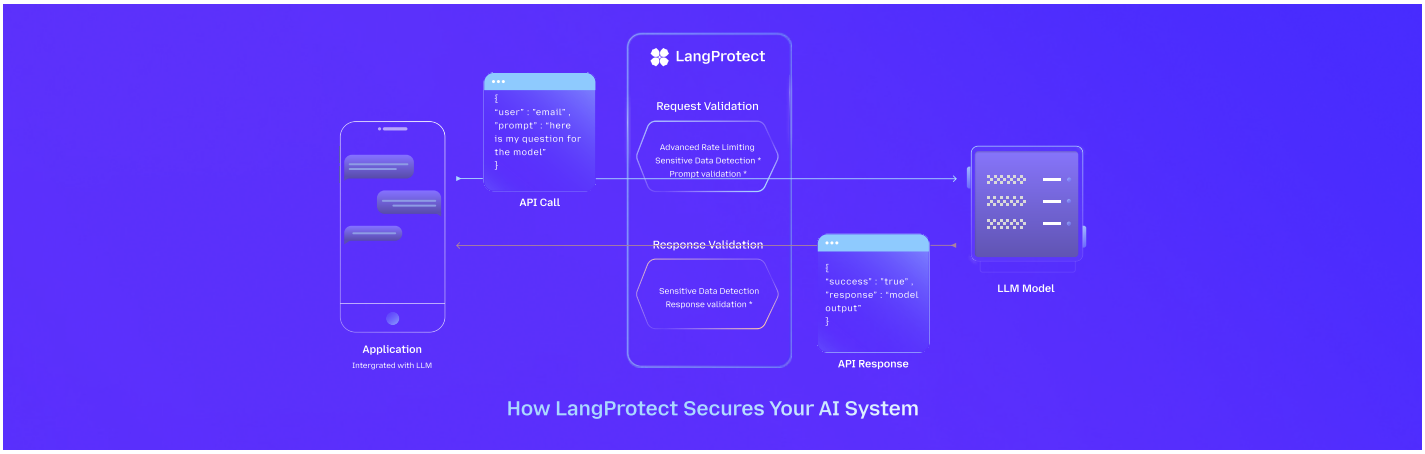
LangProtect provides AI-native runtime protection, centralized visibility, and policy-driven governance to secure AI interactions across the enterprise.



Core Problem Solved

Uncontrolled AI adoption exposes enterprises to prompt injection attacks, data leakage of sensitive information (PII, PHI, and intellectual property), jailbreak exploits, and widespread shadow AI usage. In many organizations, less than 10% of high-risk AI vulnerabilities are visible to security teams.

LangProtect closes this gap by securing AI systems at runtime. The platform detects and neutralizes threats in real time, enforces security policies across AI interactions, and generates audit-ready telemetry to support regulatory compliance frameworks such as HIPAA, GDPR, and PCI DSS.



How LangProtect Works

LangProtect operates as a runtime AI security layer positioned between applications, users, and AI models.
Every interaction with an AI system — including prompts, retrieved context, tool calls, and model outputs — is inspected in real time before execution.

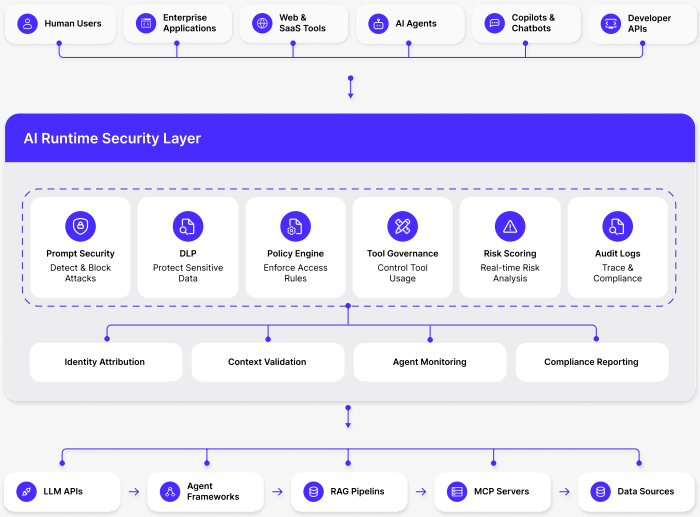
The platform enforces security across four key control points:

- Prompt Inspection – Detect prompt injection, jailbreak attempts, and policy violations.
- Context Validation – Validate RAG data sources and prevent manipulated context.
- Tool Governance – Control agent tool usage and prevent unauthorized actions.
- Response Validation – Detect hallucinations, sensitive data exposure, and unsafe outputs.

All interactions are logged and correlated with user or agent identities to ensure full auditability and governance.

Capability	Description	Key Features
Visibility	Real-time visibility into AI usage across applications, agents, and employee workflows	• Discovery of AI apps, LLM APIs, and RAG pipelines • Prompt, response, and tool monitoring • Multi-agent and MCP server visibility • Identity attribution and risk scoring
Protection	Runtime AI defense preventing misuse, data leakage, and unsafe outputs.	• Prompt injection and jailbreak prevention • Sensitive data detection and DLP protection • RAG context validation • Tool execution and API access control • Browser-level AI interaction protection
Governance	Enforce AI policies, accountability, and compliance.	• Context-aware policy enforcement • User and agent identity tracking • Role-based tool access control • Audit logs, risk dashboards, and SIEM integration

LangProtect Platform Architecture



Target Use Cases

01 **Secure Enterprise AI Adoption**
Prevent data leaks in internal copilots, productivity tools, and enterprise applications.

02 **Shadow AI Detection**
Identify unauthorized AI tools used by employees across browsers and SaaS platforms.

03 **AI Agentic Security**
Monitor and control autonomous agents executing workflows and tool actions.

04 **RAG Pipeline Security**
Prevent manipulated knowledge sources from influencing AI responses.

05 **Developer AI Security**
Protect AI-powered SaaS products and APIs from prompt injection and misuse.

06 **High-Risk Industry Protection**
Healthcare (PHI), Finance (PII), Technology (code/IP).

LangProtect Deployment Options

Cloud Deployment
Multi-cloud support, centralized policy management, minimal infrastructure overhead

On-Premise Deployment
Fully self-hosted, no external data exposure, air-gapped compatibility, data residency alignment.

Identity & Observability Integration
SSO, role-based access control, IAM integration, structured JSON log export, webhook & SOC intergation

Key Differentiators

LangProtect delivers capabilities that traditional security tools cannot provide for AI systems.

01 **AI-Native Security Layer**
Designed to inspect prompts, model reasoning, and agent actions.

02 **Agent Governance**
Monitor and control autonomous multi-agent workflows.

03 **Shadow AI Visibility**
Detect unauthorized AI usage across browsers and SaaS tools.

04 **Tool Execution Security**
Control agent tool usage with parameter validation and policy enforcement.

05 **Flexible Deployment**
Cloud, on-premise, and hybrid deployments.

06 **Low Latency Runtime Protection**
Sub-50ms inspection without impacting application performance.

Business Impact

LangProtect enables organizations to adopt AI securely while reducing operational and compliance risk.

Organizations using LangProtect can:

- Prevent prompt injection and jailbreak attacks
- Reduce sensitive data exposure through LLM interactions
- Eliminate Shadow AI usage across employees
- Secure autonomous agents and tool execution
- Gain complete visibility into enterprise AI activity
- Meet compliance requirements such as GDPR, HIPAA, and SOC 2

Secure AI Adoption Across Your Organization

Govern AI agents and MCP connections with intent-based security to prevent unauthorized execution, data exfiltration, and non-compliant behaviors in real-time.

100,000+
AI Prompts Detected Across teams

100+
AI Tools monitored in real time

20+
Custom Governance Policies Applied

99%
Sensitive Data Coverage

<5ms
Risk Detection In Real Time

BOOK A DEMO TODAY

Certifications

Get Personalize Security Solution for your Industry

Get My Security Solution