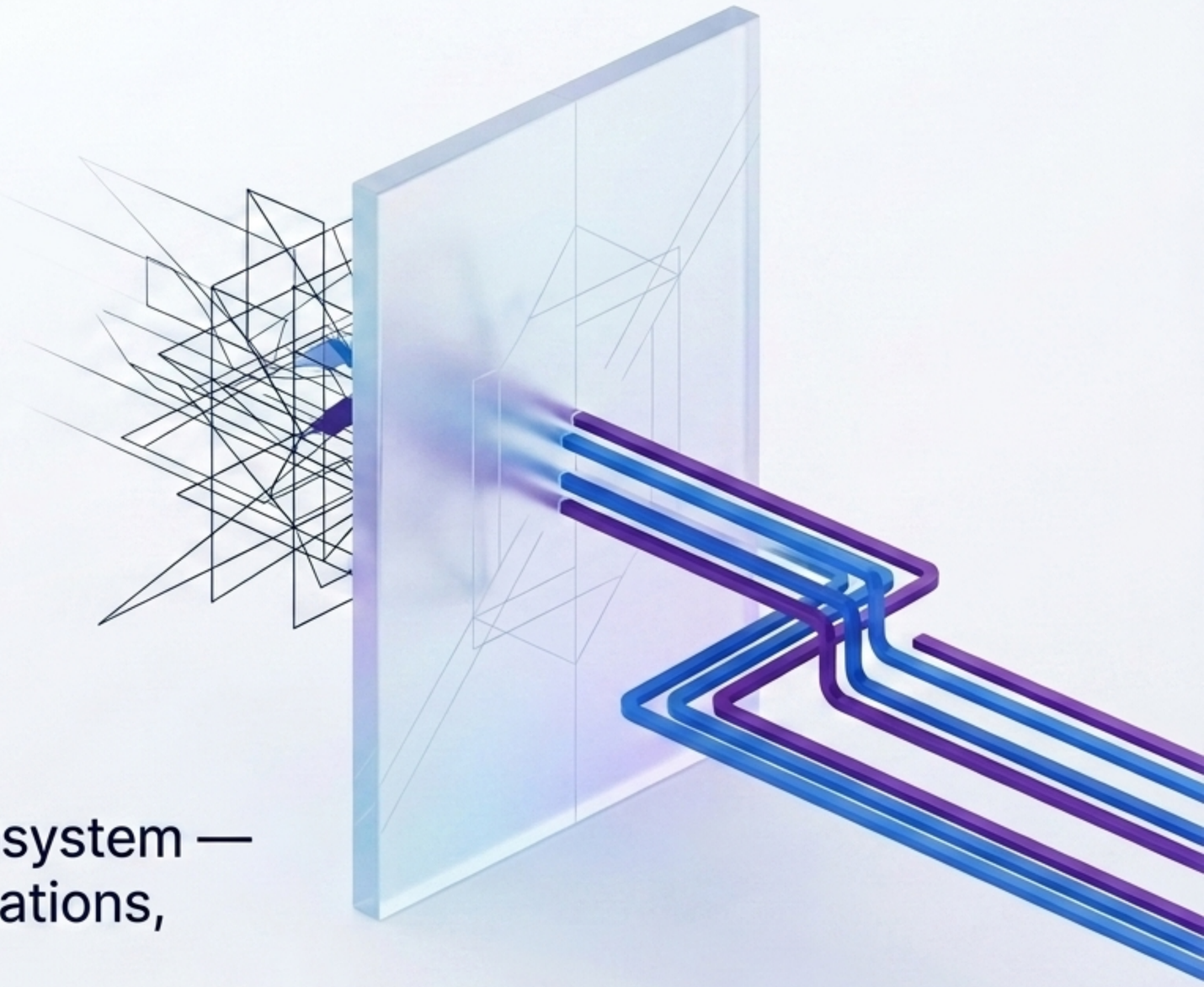
Defenix
Intelligent Defence Unmatched Resilience

DefenGPT AI Security Platform



Complete control over your AI ecosystem — covering SaaS, homegrown applications, endpoints, and developer IDEs.

Comprehensive AI security for people, agents, models, and data

Public AI Tools

Governance for ChatGPT, Copilot, Gemini, Claude, and other public AI services used daily by employees.

AI Agents

Discovery and control for homegrown, embedded, and developer tool agents across all environments.

AI Models

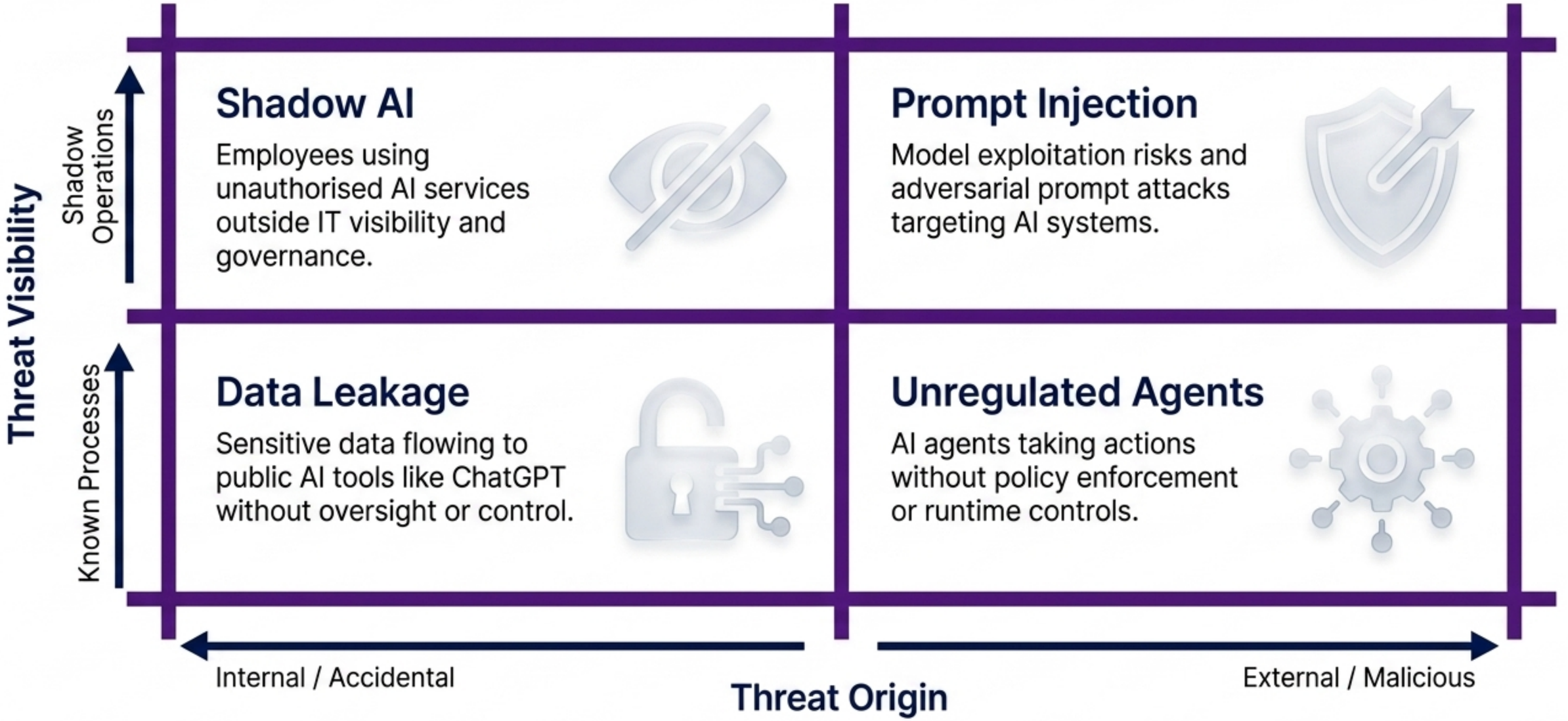
Risk, provenance, and compliance assessments for internal and external models.

Endpoints & IDEs

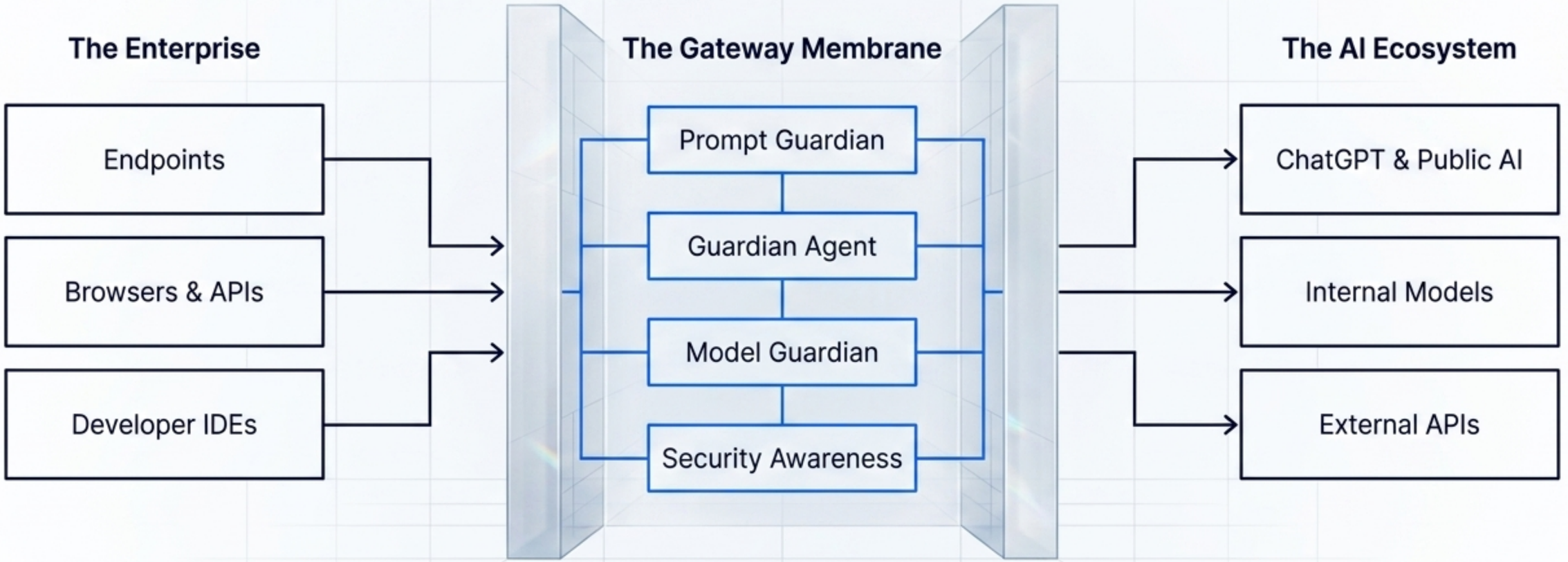
Full monitoring and governance for browsers, APIs, endpoints, and developer environments.

DefenGPT AI Security Platform

AI adoption is outpacing governance



Full-spectrum AI coverage via the Intelligent Gateway

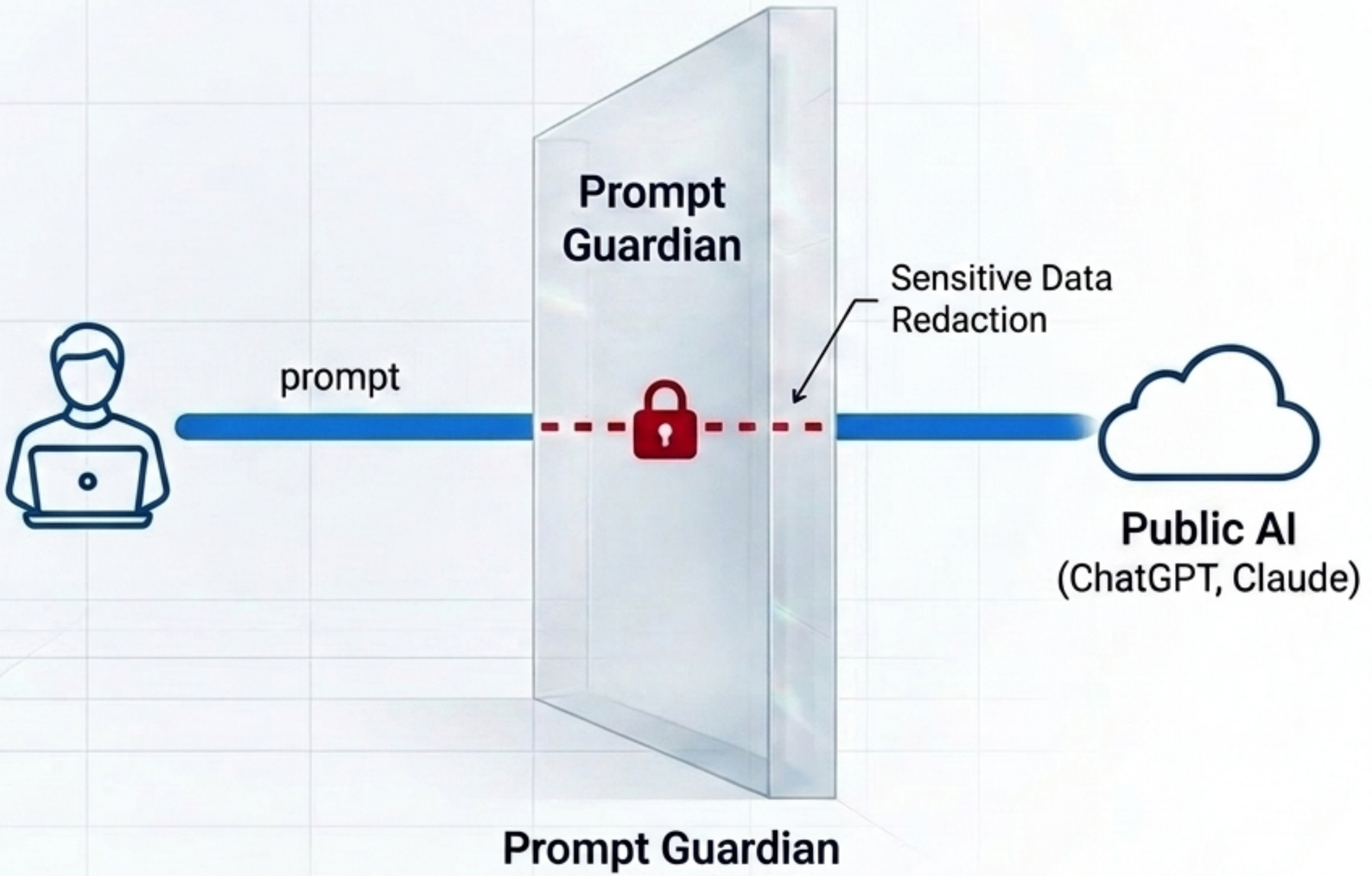


The DefenGPT AI Security Suite provides complete visibility and real-time control across your AI ecosystem, ensuring secure and compliant AI adoption.

DefenGPT AI Security Platform

Key Capabilities

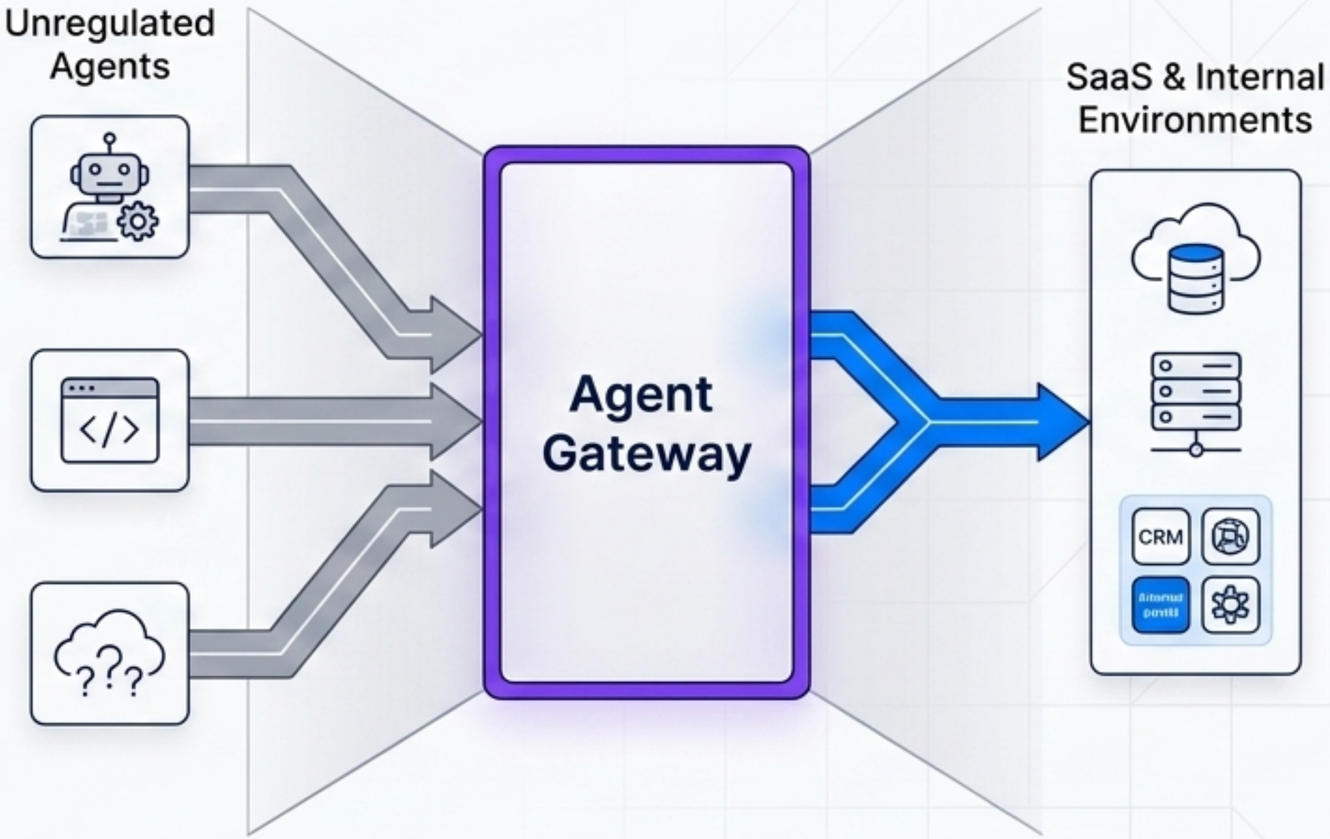
- Inspect prompts and responses in real time.
- Detect and prevent sensitive data exposure.
- Identify and block shadow AI usage.
- Enforce risk-based policies automatically.



Runtime policy enforcement for autonomous systems via Guardian Agent

Key Capabilities

- Discover all AI agents and tools in use across SaaS and internal environments.
- Control access and permissions.
- Monitor behaviour and detect anomalies.
- Enforce runtime policies across all agents via the AI Gateway.



Centralised traffic routing and model risk evaluation

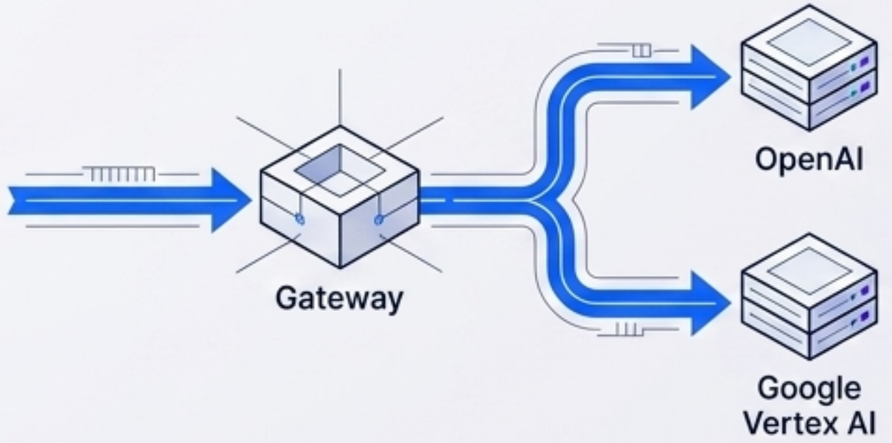
Model Guardian

Risk Engine

- Assess model risks and trustworthiness using source intelligence.
- Conduct static analysis and dynamic red teaming for vulnerability assessments.
- Validate model provenance and compliance.

AI Gateway

Traffic Control

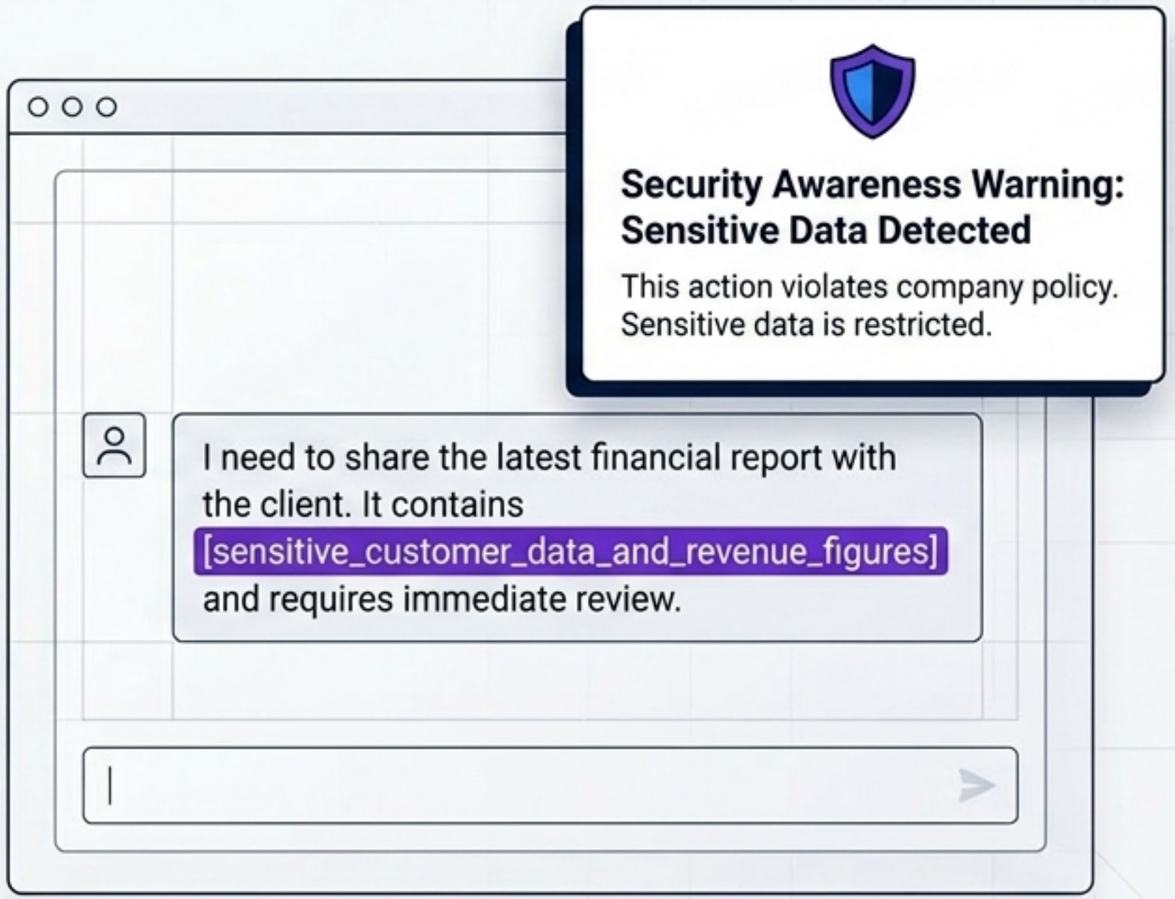


- Centralise all AI usage and route traffic through a governed access layer.
- Track usage, costs, and provider activity (e.g., OpenAI, Google Vertex AI).
- Enforce policies across AI APIs and services.

Real-time behavioural monitoring and in-context training

Enhance Human & Agent Behaviour

- Gain visibility into AI usage to detect risky users and agents.
- Detect risky prompts and actions immediately.
- Deliver in-context alerts and guidance inside the employee's existing workflow.
- Provide real-time training for users to enable safe innovation.



The AI Security Suite in action

Stage 1

Monitors & Controls

- Browser extensions
- Network proxies
- API integrations
- Agent gateways
- Endpoint and IDE controls

Stage 2

Stage 3

This Enables

- Comprehensive visibility into AI usage
- Data classification and intent detection
- Real-time blocking, warnings, or redactions
- Audit trails for compliance and governance

Flexible deployment built for enterprise AI risk

Speed & Agility

Maximum Air-Gapped Control

SaaS

Fully managed cloud deployment with rapid onboarding.

Private Cloud

Dedicated cloud environment for enhanced data control.

On-Premises

Air-gapped environments for maximum security and compliance.

Secure your AI journey without compromising innovation

Take control of your AI adoption. Protect your organisation with complete visibility, real-time control, and enterprise-grade governance across every AI touchpoint.

Defenix

Intelligent Defence Unmatched Resilience

For More Info ..
Contact : Sales@defenix.ai

Book a Demo

View Datasheet

Global Presence: London, UK | Toronto, Canada | Abu Dhabi, UAE | Mumbai, India | Kampala, Uganda