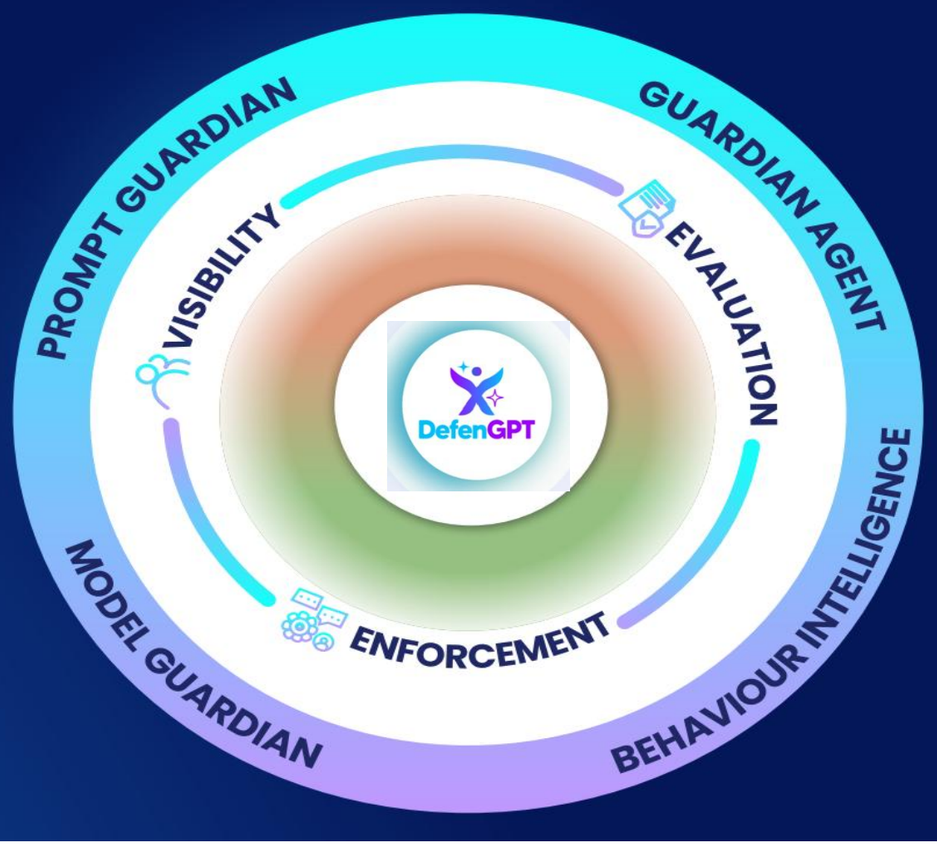
DefenGPT

AI Security Platform

- Unified activity control across Human, AI agents, Data and models.
- Homegrown, SaaS, embedded, and endpoint coverage.



Product Overview

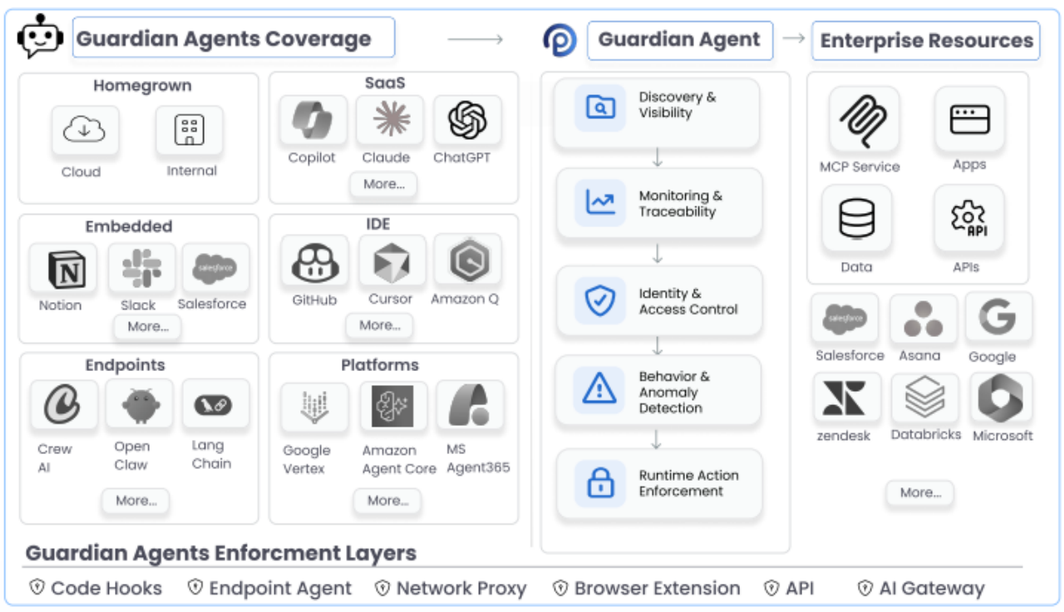
DefenGPT AI Security Platform is an AI Security Platform that provides end-to-end protection and AI usage visibility across human and AI agent interactions. Using a combination of proxy, browser extension, and API integration, it enforces policies in real time across homegrown agents and third-party AI services across cloud and endpoints. The platform enables AI agent monitoring and control, alongside data privacy and AI sovereignty, with governance of prompts and behavior, while also evaluating the risks of using models within internal AI applications .

Key Capabilities

Guardian Agent

Govern autonomous AI agents and their actions across enterprise systems.

- **Discovery & Visibility:** Inventory all agents with workflows, ownership, and dependencies.
- **Monitoring & Traceability:** Track actions with full audit trails.
- **Identity & Access Control:** Govern permissions, tools, and system access.
- **Behavior & Anomaly Detection:** Ensure alignment and detect misuse.
- **Runtime Action Enforcement:** Block, remediate, and adapt in real time.



Prompt Guardian

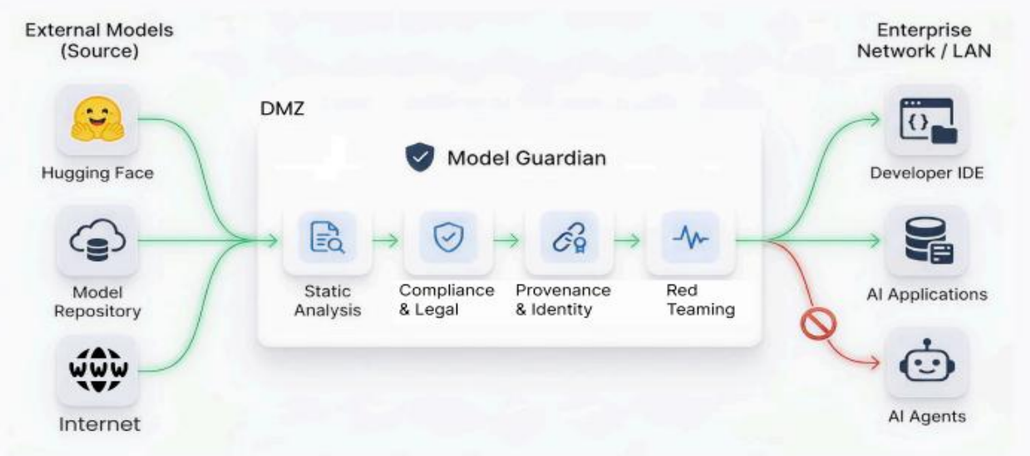
Control how users and agents interact with AI systems.

- **Shadow AI Usage Discovery:** Identify and manage unsanctioned AI tools.
- **Prompt Inspection & Protection:** Prevent prompt injection and data leakage.
- **Risk-Based Enforcement:** Apply contextual policies on usage.
- **Usage Visibility & Audit:** Monitor and log all interactions.

Model Guardian

Evaluate and secure AI models used in the enterprise.

- **Risk & Trust Assessment :** Evaluate models before internal use.
- **Vulnerability Testing & Red Teaming :** Identify jailbreaks, weaknesses, and abuse risks.
- **Governance & Compliance :** Approve and control model usage.



Security Awareness

See every AI interaction — who, what, when, and how risky.

- **Human Risk :** Identify risky employee interactions with AI chat services and agents.
- **AI Agent Risk :** Detect and control what AI agents can do.
- **In-context training :** Real-time, in-context security awareness guidance.

AI Gateway

Control and track AI consumption

- **Control and monitor AI** usage across applications
- **Route AI traffic** through a governed access layer
- **Track usage**, costs, and provider activity
- **Enforce policies** across AI APIs and services

Flexible Deployments

- ☑ SaaS
- ☑ On-premises
- ☑ Private Cloud
- ☑ Air Gapped

From visibility to enforcement

Most Risky AI Agent Behavior (Risk Score)

AI Agent	Connected Tool	Risk Score	Activity Type
ChatGPT	Gmail	9.3	Unauthorized
Copliot	Salesforce	9.3	Exporting data
Claude	Asana	8.7	Delete tasks
Cursor	GItHub	8.5	Code changes
AI Agent	AWS Console	8.0	Infrastructure
ChatGPT	Google Drive	8.5	Data extraction

Explore more of DefenGPT

Private AI Suite
On premise AI capabilities - Click here

Adoption Intelligence
Measure AI to boost productivity - Click here

Try DefenGPT **AI Security Platform** for **FREE** today… Click Here

Defenix
Intelligent Defence Unmatched Resilience

Sales@Defenix.AI

Website: www.defenix.ai