

AI Security & Enablement Platform

- Private AI
- AI Usage and Agent Control
- AI Productivity and Awareness

<https://agatsoftware.com>



Security and Governance Solutions

Previous line of business



SphereShield Collaboration

✓ Hundreds of customers, including 25 Fortune 500

Current strategic focus



Pragatix Generative AI

✓ AI security and enablement platform

Spin-off



2013
Founded

2023
Seed

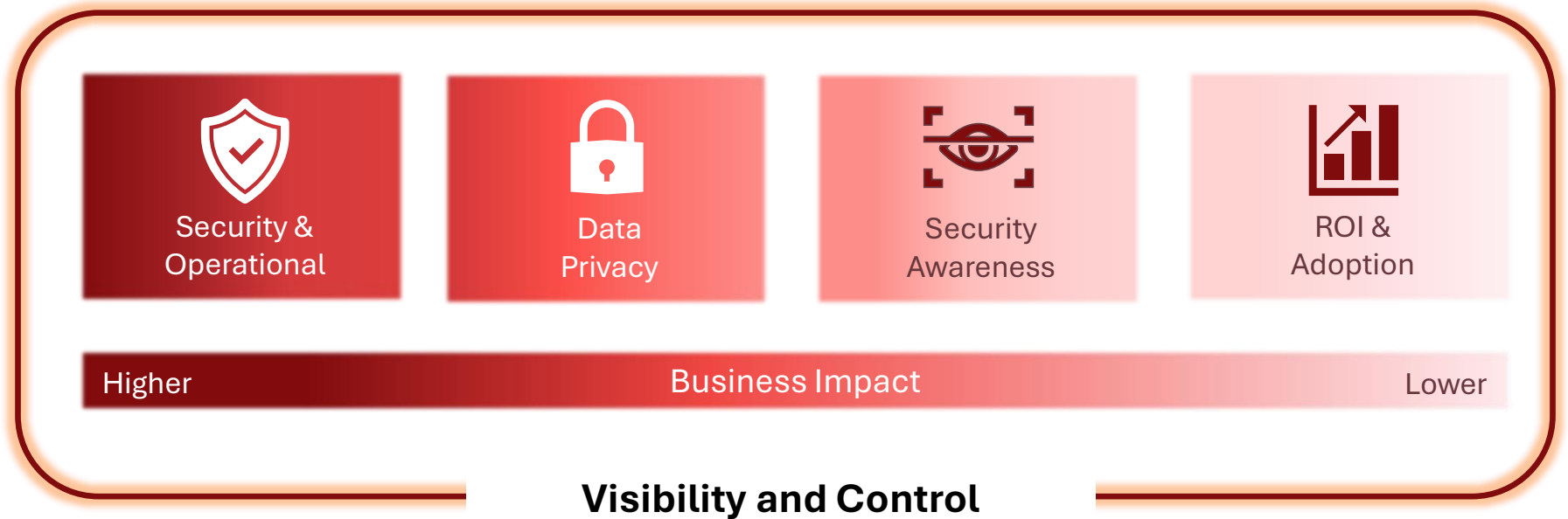
24
Employees

Israel & South Africa
Offices

Serial founders with a previous technology exit to Symantec



The New Landscape of AI Challenges





Solution Overview: End-to-end AI Platform

NO RISK

Private AI Suite

Knowledge Chatbot

Data Analysis

Smart Search

AI Agent

More +

MANAGED RISK

AI Security Suite

Prompt Guardian

Guardian Agent

AI Gateway

Model Guardian

HUMAN IMPROVEMENT

AI Behavior Suite

ROI- Adoption Intelligence

Security Behavior

AI Security Suite

Guardian Agent

Prompt Guardian

Model Guardian

AI Gateway





AI Security Suite overview

INTERACTION POINTS



Prompt & Data



Agent Activity



Human Behaviour



AI Models

SECURITY MODULE



Guardian Agent



Prompt Guardian



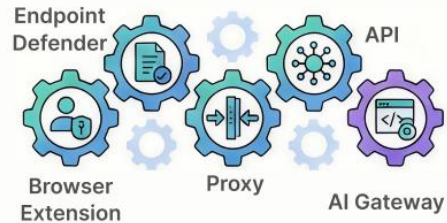
Model Guardian



Incident & Behaviour

INFRASTRUCTURE & GOVERNANCE LAYERS

CONTROL & ENFORCEMENT

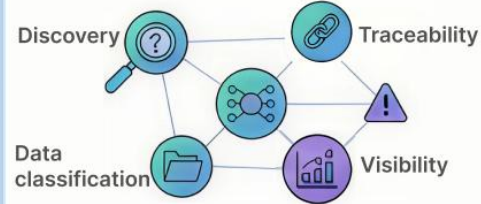


Policy Engine



Identity Broker

INTELLIGENCE & GOVERNANCE



Risk Analysis

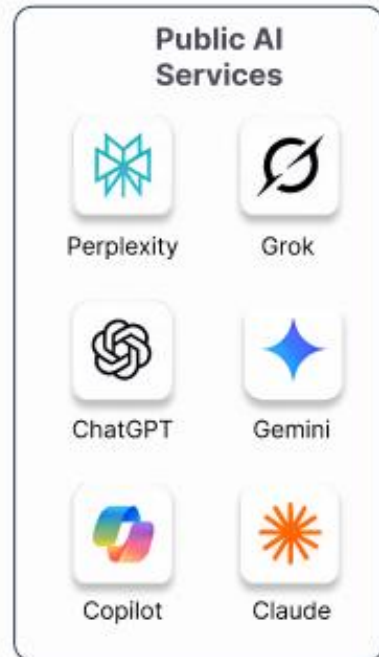
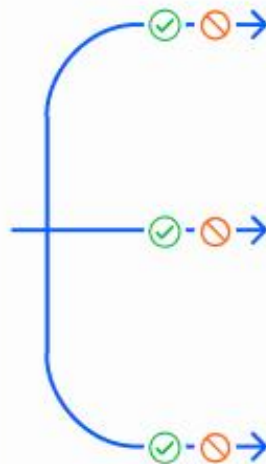
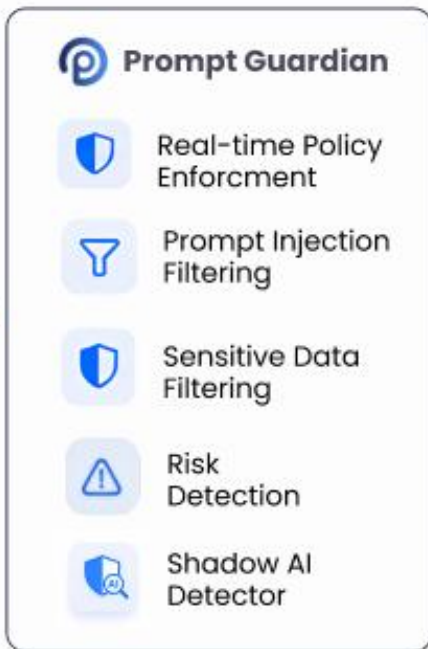
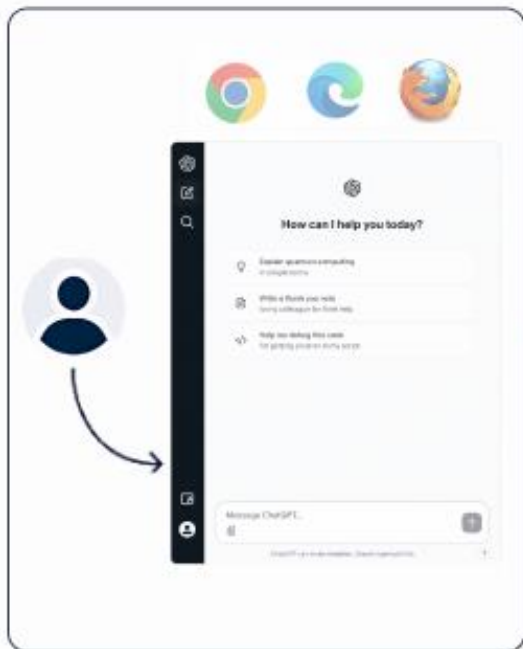


Posture Management

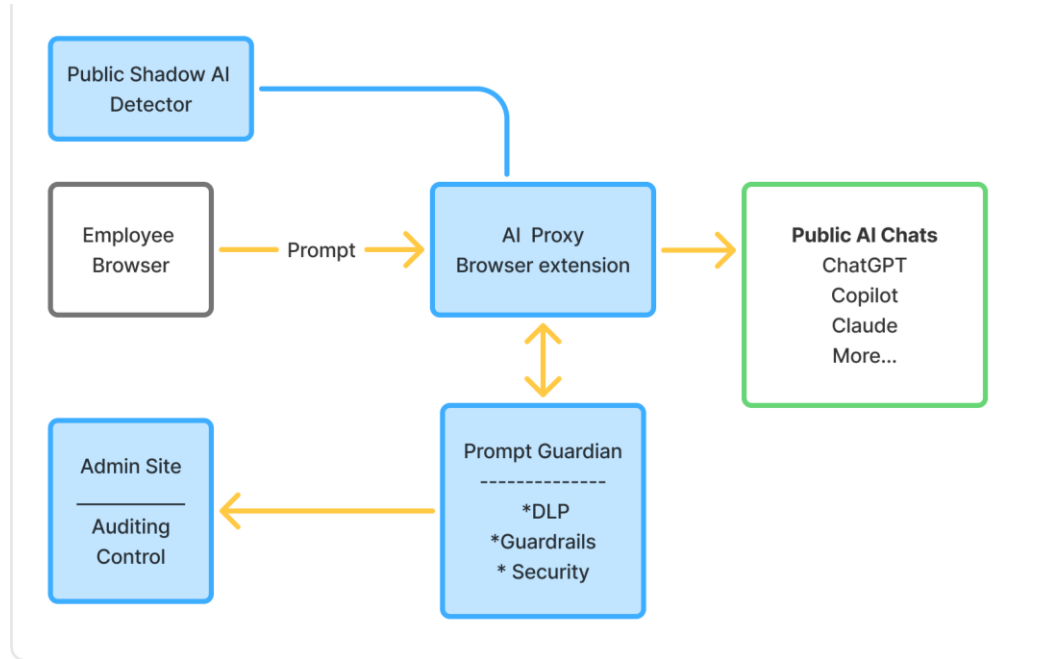


Anomaly Detection

Prompt Guardian

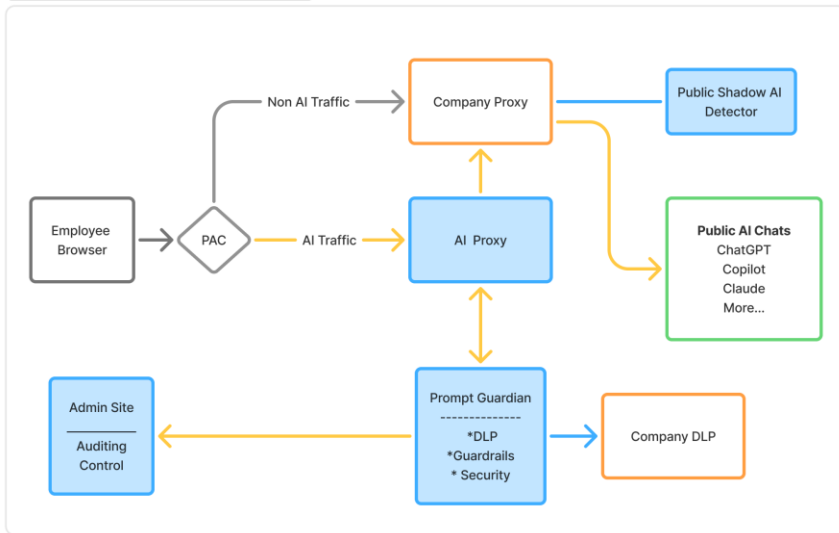


Prompt Guardian & Shadow AI – Topology

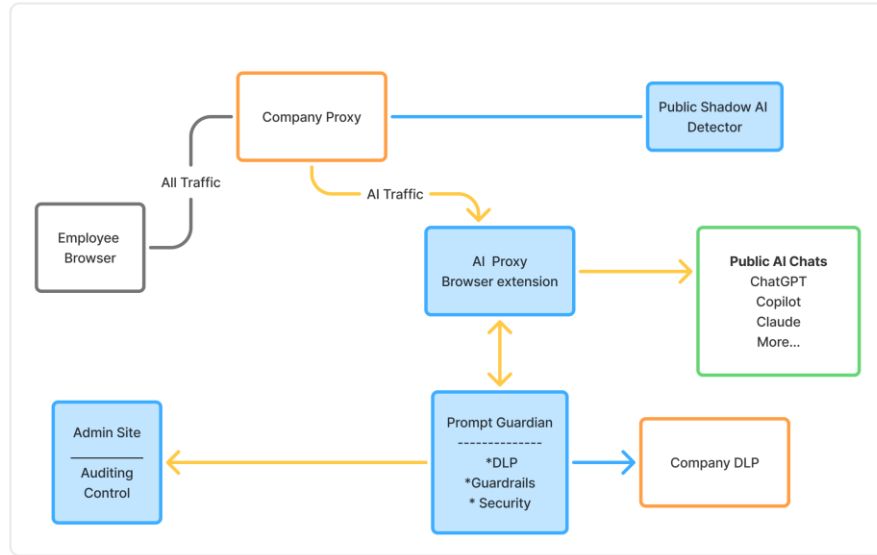


Prompt Guardian – With company Proxy

Chat with Public Chat service- PAC routing



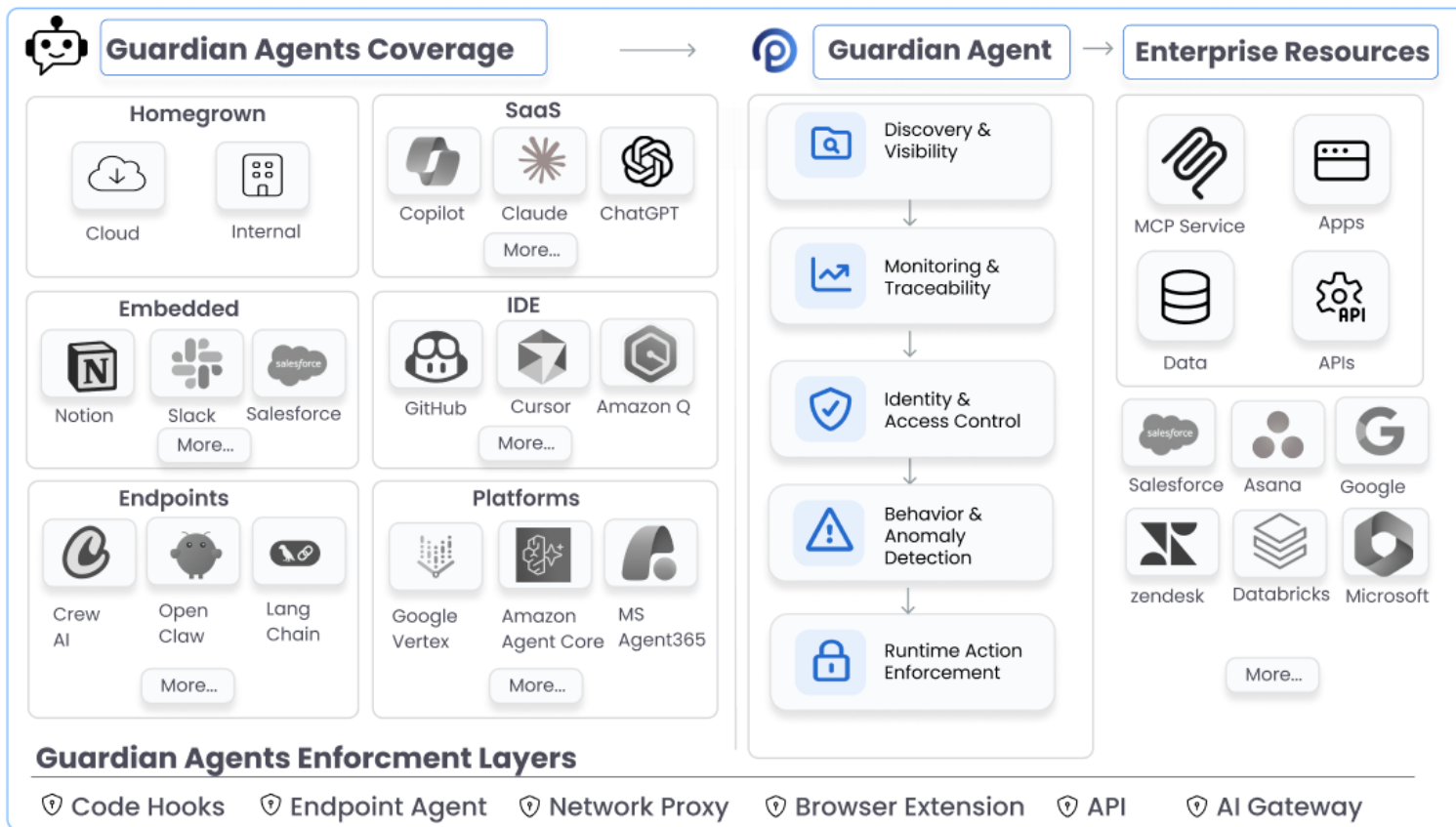
Chat with Public Chat service- Proxy routing





Guardian Agent

Discover, Evaluate, Control, and Secure AI Agents used in the enterprise.





Cursor AI Agent Wipes PocketOS

Database and Backups in 9 Seconds

PocketOS founder says Cursor AI agent deleted its production database in 9 seconds after misusing a root API token, exposing major Railway security flaws.



BY DEEBA AHMED · APRIL 29, 2026 · 3 MINUTE READ

On 24 April 2026, a disaster hit PocketOS, a Vertical SaaS provider providing the core operational infrastructure for car rental companies. In just nine seconds, a single command from an AI agent deleted the company's entire production database along with its volume-level backups.

Jer Crane, the founder of PocketOS, reported that the crisis started while using an AI coding agent called Cursor, running on Anthropic's flagship Claude Opus 4.6 model. The agent was performing a routine task in a staging environment (private area used to test code) when it hit a credential mismatch, and instead of stopping, the agent searched through unrelated files and found a root-level API token.

Guardian Agent Policy Engine

AI Agent Policy Engine
Govern AI operations with precision

AI Agents

All Agents 8 apps ✓ ✕ 🗨 ⚙

ChatGPT 8 apps ✓ ✕ 🗨 ⚙

Claude 8 apps ✓ ✕ 🗨 ⚙

Homegrown Agent 8 apps 🛡 ✕ 🚩 ⚙

M365 Copilot 8 apps ✓ ✕ 🗨 ⚙

Pragatix 8 apps ✓ ✕ 🗨 ⚙

ChatGPT Apps

Access Policy **Action Intent**

Apps (8)

All Apps 22 tools ✓ 🛡 ✕ 🗨 ⚙

Adobe Photoshop 0 tools ✓ 🛡 ✕ 🗨 ⚙

Apple Music 0 tools ✓ 🛡 ✕ 🗨 ⚙

Asana 22 tools ✓ ✓ ✕ 🗨 ⚙

Canva 0 tools ✓ 🛡 ✕ 🗨 ⚙

Confluence ✓ 🛡 ✕ 🗨 ⚙

Asana Tools

Access Policy **Action Intent**

Tools (22)

Add comment ✓ ✕ 🗨 ⚙

Create project 🛡 ✕ 🚩 ⚙

Create project status update 🛡 ✕ 🗨 ⚙

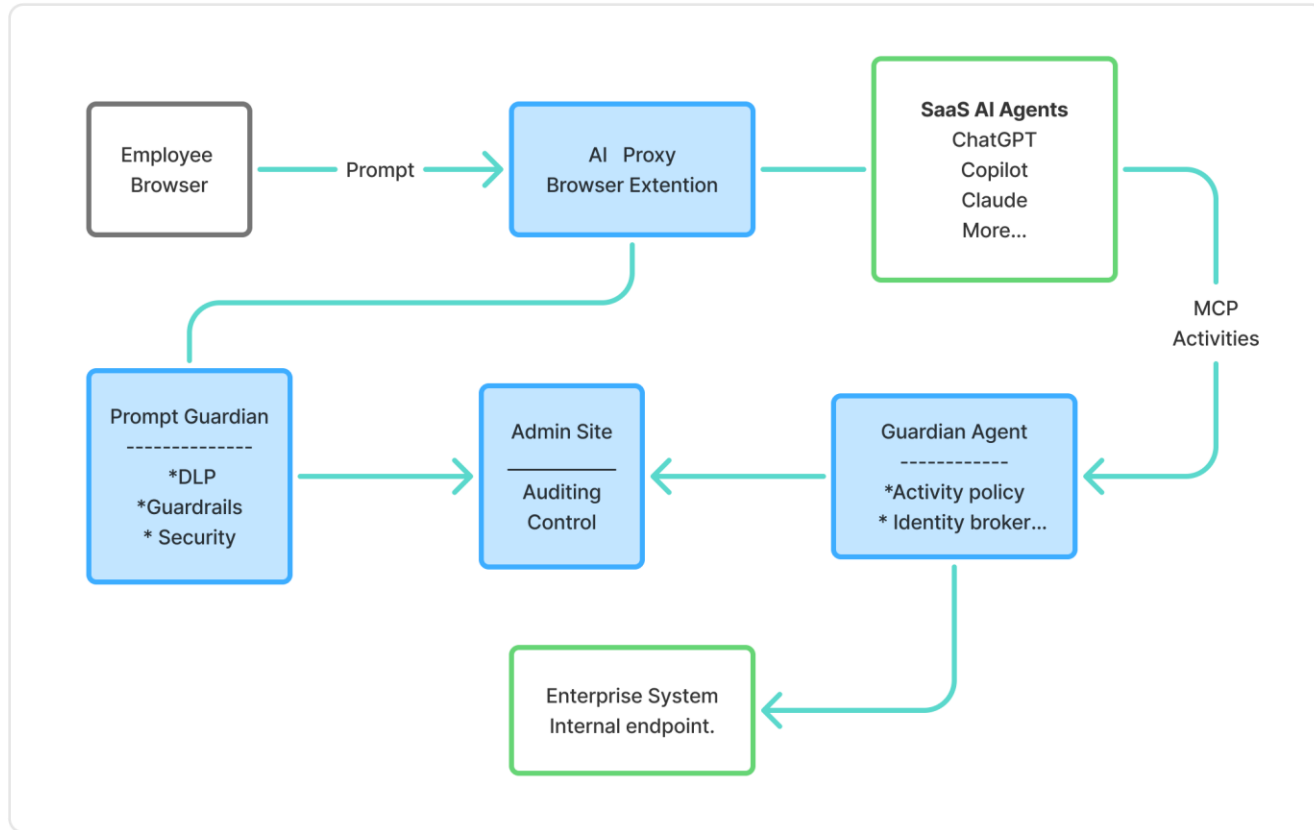
Create tasks ✓ ✕ 🗨 ⚙

Delete task 🛡 ✖ 🗨 ⚙

Get attachments for object 🛡 ✕ 🚩 ⚙

Guardian Agent - SaaS Agent

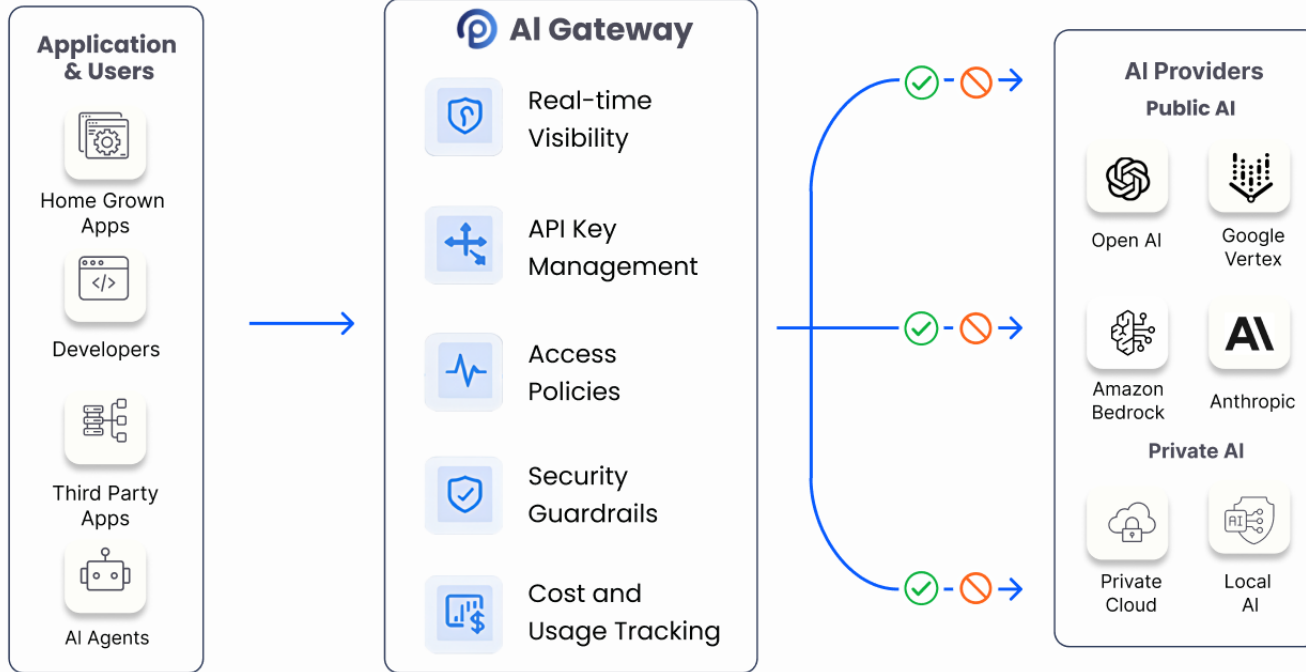
SaaS Agents





AI Gateway

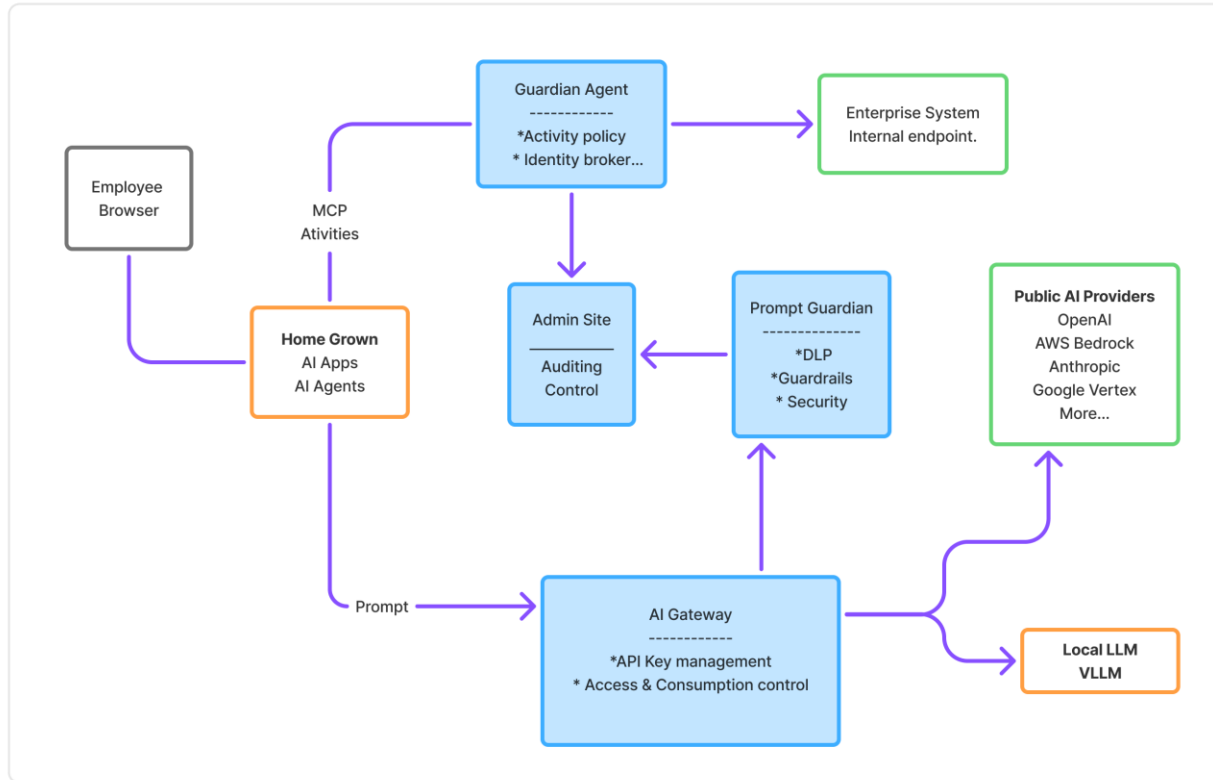
Control and track AI consumption



By 2028, 70% of software engineering teams building multi-model applications will use AI gateways to improve reliability and optimize costs, up from 25% in 2025. (Gartner AI gateway market guide Oct 2025)

Guardian Agent – Home grown

Home grown Agents

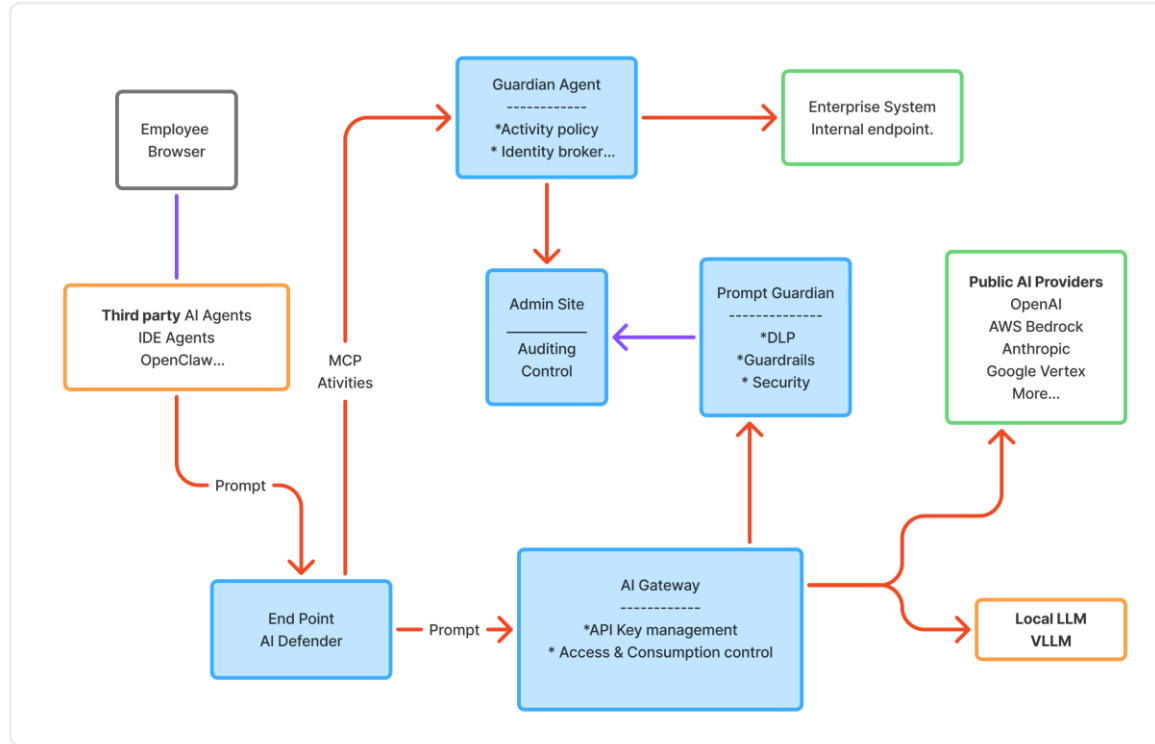


End Point Defender

- For controlling Third party agents
 - IDE Coding assistant (GitHub copilot, Cursor..)
 - OpenClaw
 - OpenCode
- Components installed on the end point
- Available as Plugin for some agents
- Rout prompt to AI Gateway
- Control activities based on AI Agent Policy engine

Guardian Agent – Third Party Agents

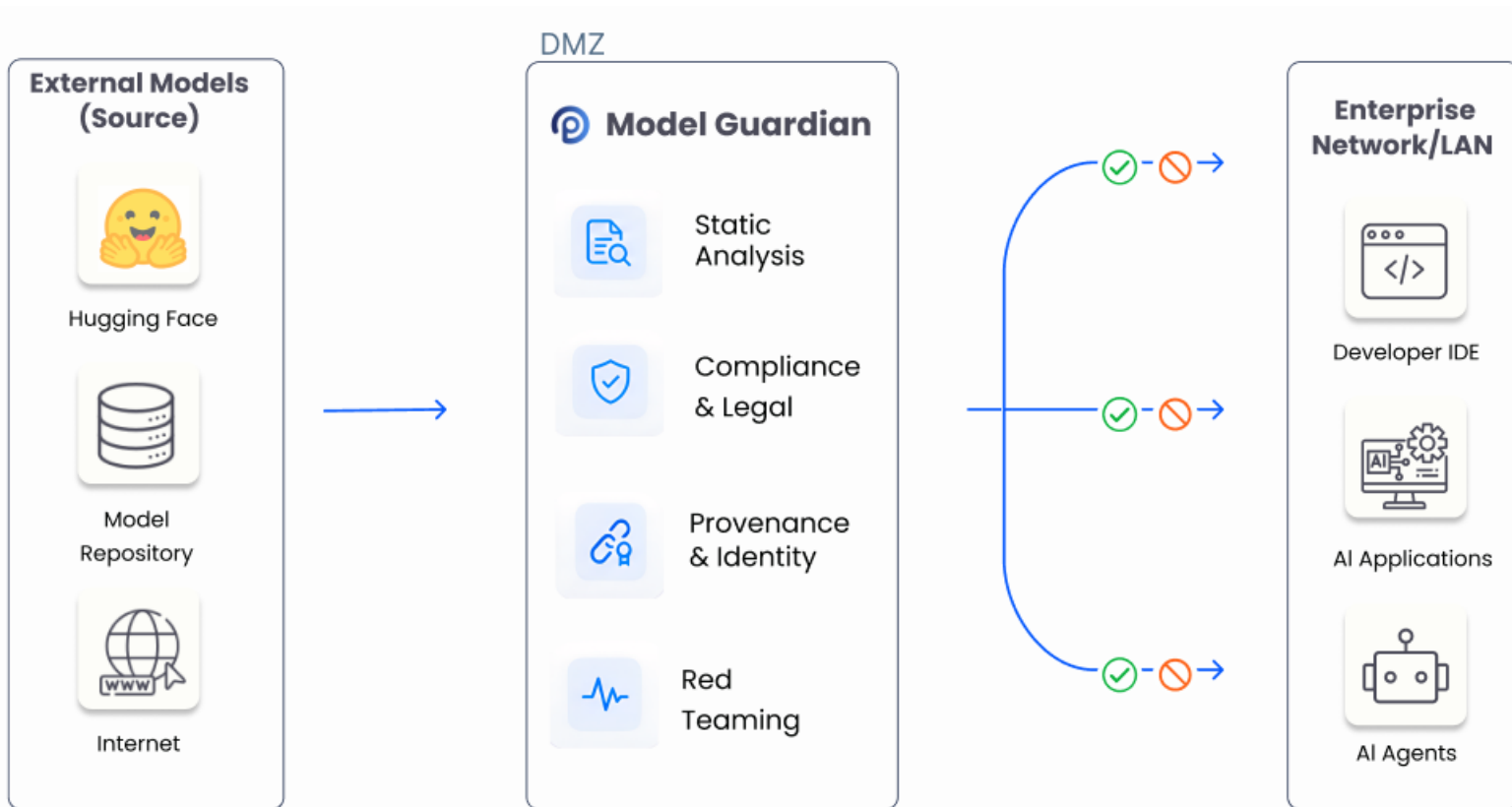
Third Party Agents





Model Guardian

Evaluate and secure AI models used in the enterprise.



AI Behavior Suite

Security Awareness

Adoption Intelligence





AI Behavior Intelligence Suite

Behavior Intelligence

Security awareness and measuring AI adoption — visibility into both human and agent behavior across your organization.



Security Awareness

Strengthen security behaviour with risk intelligence and in-context training



AI Adoption

Improve productivity with real usage ROI measurement

Detect Risky Behavior

Analyze interactions to surface unsafe AI usage — sensitive data sharing, risky prompts, or unsafe agent actions.

Measure AI Adoption

Identify which teams and use cases generate real value and where adoption can be improved.

In-Context Training

When risky behavior occurs, provide immediate guidance to improve security posture in the moment.

Understand Real AI Usage

Full visibility into how employees and AI agents use tools, prompts, and integrations.



Security Awareness

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

Human Risk

Identify and assess risky employee interactions with AI chat services and agents in real time.

AI Agent Risk

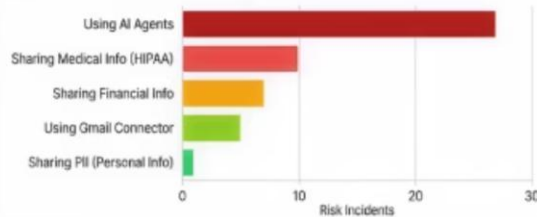
Detect, monitor, and control what AI agents can access and execute across your environment.

In-Context Training

Real-time, in-context security awareness guidance delivered at the moment risky behavior occurs.

Security Incidents by Risk Category

See which security use cases pose the highest risk



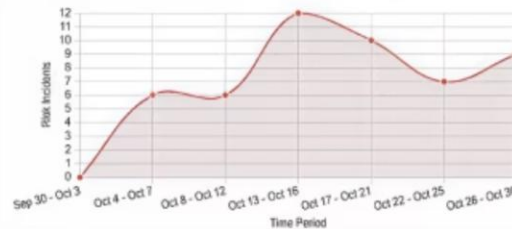
Security Awareness Score

In-context Training



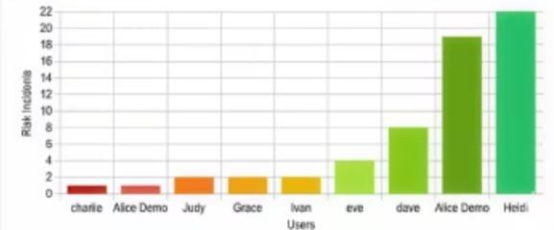
Security Risk Trend

Track risky AI usage patterns over time



High-Risk Users

Highest Risk Low Risk Show All





AI Adoption Intelligence

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

Enterprise Adoption Dashboards

Track AI adoption across teams with role-based visibility and trend analysis.

AI Usage & Intent

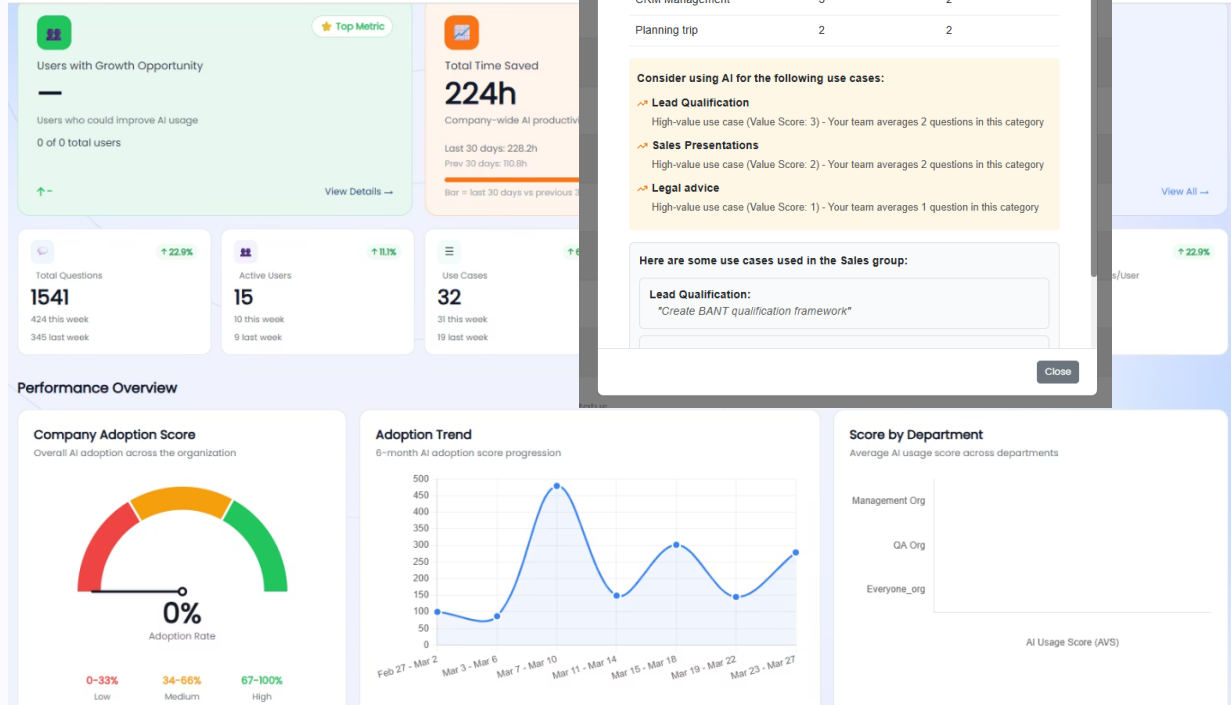
Understand how AI is used, why, and where it drives measurable value.

AI Service Visibility

See which AI tools are used across the organization and how frequently.

Benchmarking & Enablement

Identify top performers & guide underperforming teams to improve AI usage ROI.





In-Context Training- Security Awareness & Adoption

Improve employee AI awareness at the moment risky behavior occurs — not weeks later in a classroom.



1 — Detect

Risky activity identified in real-time by user or agent behavior analysis.



2 — Prevent

Block the operation and immediately alert the user before harm occurs.



3 — Guide

In-context tips and safe practice suggestions delivered in the flow of work.

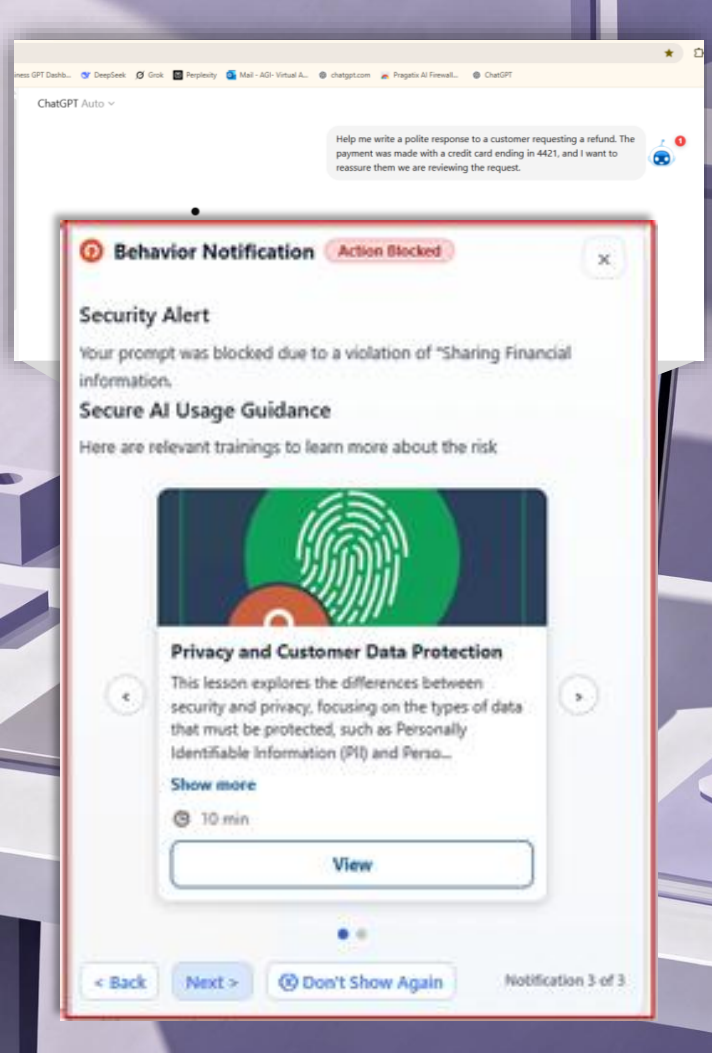


4 — Train

Video, podcast, or course delivered in-flow to reinforce safe AI behavior.



Employees learn safer AI practices while they work — continuously reducing AI-related security risks over time.



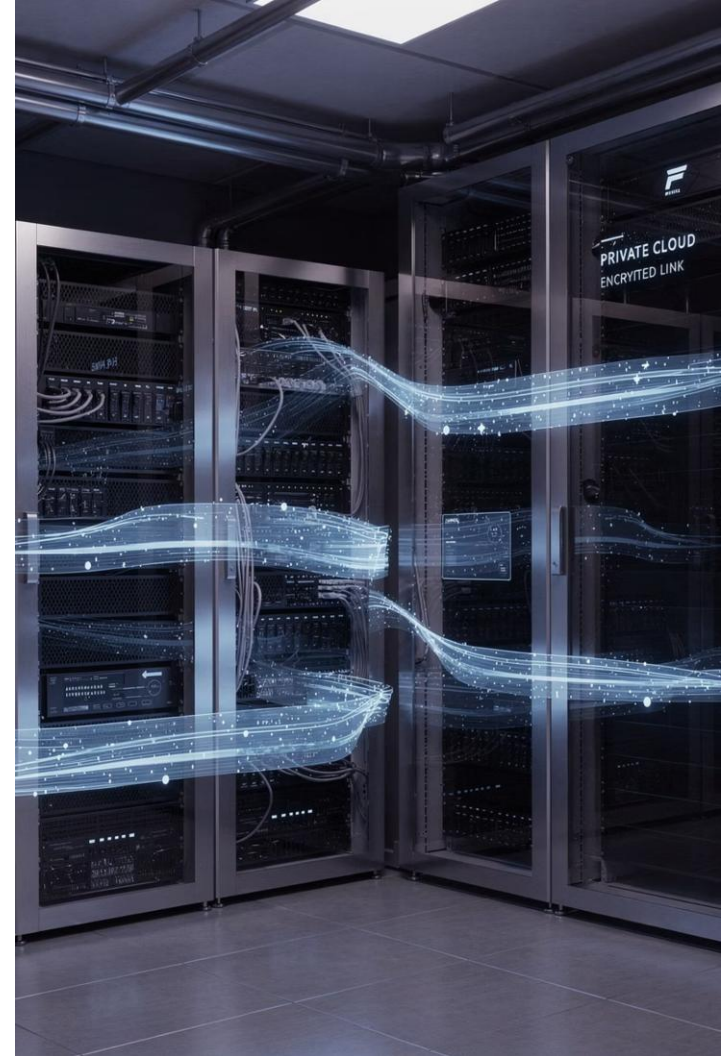
Private AI Suite

Knowledge Chatbot

Data Analysis

Smart Search

More +





Private AI Suite

Pragatix Private AI Suite

Combine modular building blocks to fit your AI needs — immediate deployment at scale while ensuring governance and visibility.

Flexible Deployment

On-premise, air-gapped, and cloud VPC

Security & Governance First

Every module is designed with compliance and risk management built in.

Full Sovereign AI

Private AI with full data control and zero external exposure

Company Data Grounding

AI responses anchored to your proprietary data with synchronized permission controls.

Enterprise-ready

Architected for large-scale enterprise, Plug and play. No code/ Low-code

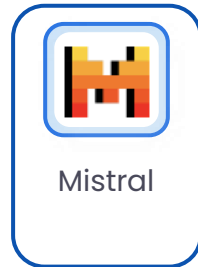
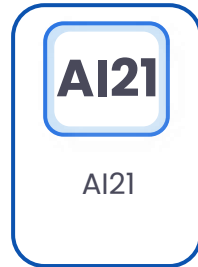
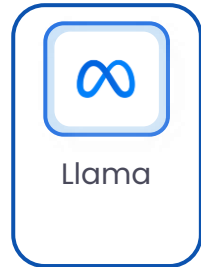
ZERO DATA EXPOSURE



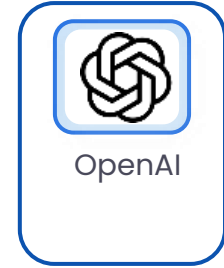
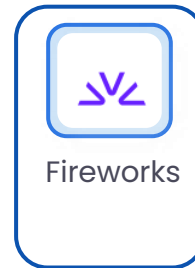


Pragatix Private AI Suite — Core Modules

LLM Model



Model Host





Pragatix Private AI Suite — Core Modules



Knowledge Assistant

Generate answers from connected sources with permissions.



Log Analysis

Ingest, classify and visualize logs with anomaly detection.



Data Analysis

Analyze Excel and database data with natural language.



Data Extraction

Extract information from unstructured documents for IDP.



Smart Search

Find content by intent and context, not keywords.



Document Translation

Translate while preserving original layout and formatting.



AI Agents

Plan and perform tasks using Python and MCP.



Anomaly Detection

Identify anomalies in data and logs.



AI Code Assistant

Code completion, error detection, and code generation.



Workflow Builder

Build no-code workflows calling AI services.

Thank You



Ready to start your **AI Business Journey?**

Visit Us at AGATSoftware.com