

## 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

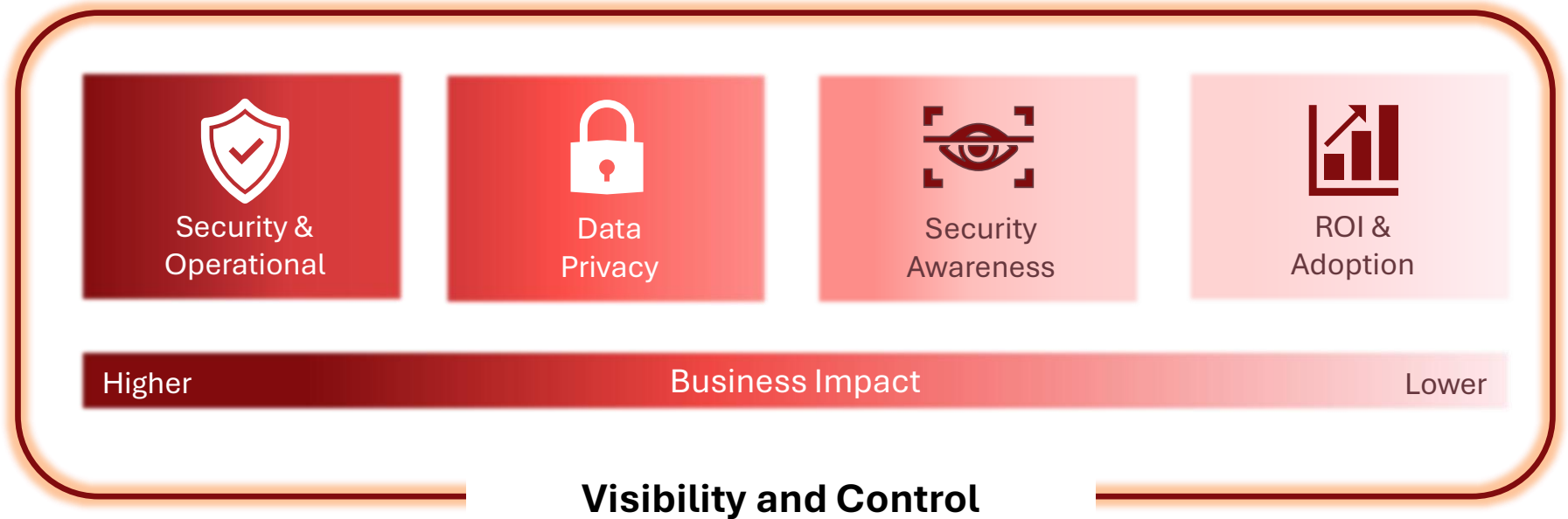
**24**  
Employees

**Israel & South Africa**  
Offices

Serial founders with a previous technology exit to Symantec



# The New Landscape of AI Challenges





# Four Pillars of Pragatix Platform Offering



## 01 — Visibility & Posture Management

See Human and AI Agent Activities Across Approved and Shadow AI. Continuously assess and manage AI risk



## 02 — Security & Control

Real-time Policy enforcement & risk prevention of AI Agent and Humans



## 03 — AI Sovereignty

Private on-prem AI ensures zero data exposure with flexible deployment options.



## 04 — Security Awareness and Adoption

Strengthen Security Behavior with Risk Intelligence and In-Context Training.



# Solution Overview: End-to-end AI Platform

NO RISK

## Private AI Suite

Knowledge Chatbot

Data Analysis

Smart Search

More +

MANAGED RISK

## AI Security Suite

Guardian Agent

Prompt Guardian

Model Guardian

HUMAN IMPROVEMENT

## AI Behavior Suite

Security Awareness

Adoption Intelligence

# AI Security Suite

Guardian Agent

Prompt Guardian

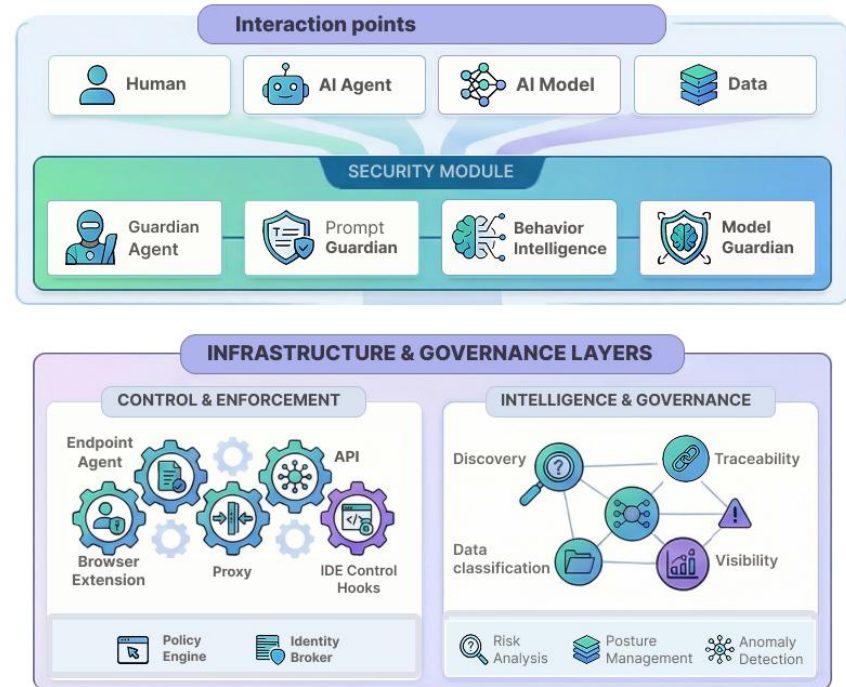
Model Guardian





# AI Security Suite overview

- ❑ Capture all AI activities in the browser & computer
  - Browser extension
  - Network Proxy
  - API
  - Guardian Agent gateway
  - Code hooks for IDE and homegrown
  - Endpoint agent
- ❑ Capture Prompt, files, and responses at the edge
- ❑ Capture Agents, connectors, tools, and activities
- ❑ Understand intent, data classification & sensitivity
- ❑ Flexible Deployment from SaaS to Air-Gapped
- ❑ OWASP & regulatory alignment

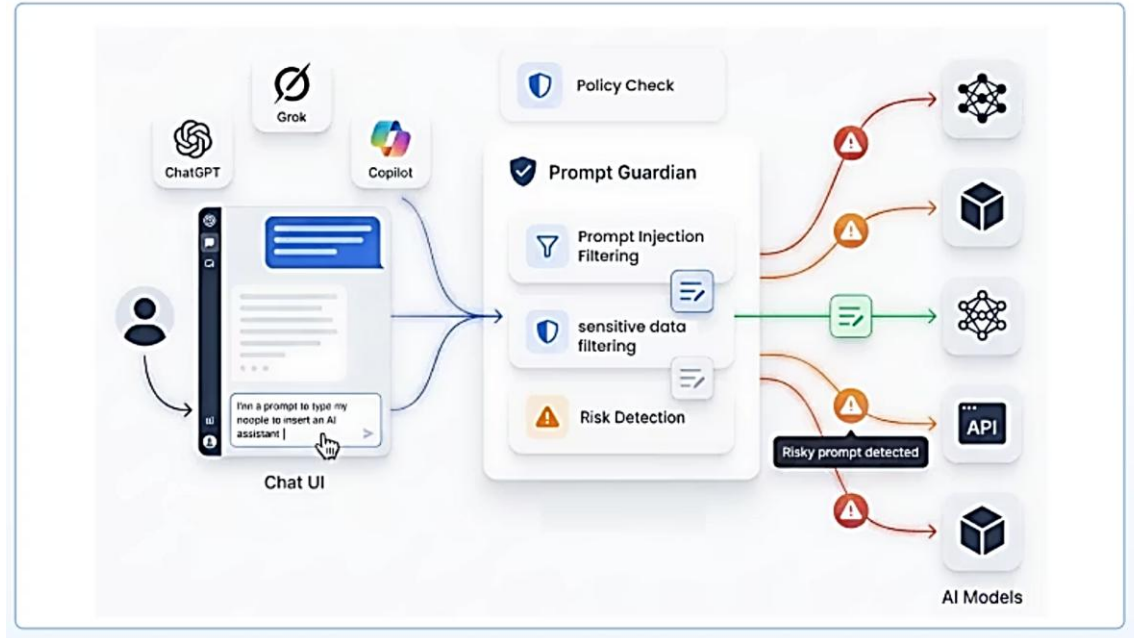




# Prompt Guardian

Secure how employees engage with AI systems through comprehensive monitoring and intelligent policy enforcement.

- **Shadow AI Usage Discovery**  
Identify and manage unsanctioned AI tools.
- **Prompt Inspection & Protection**  
Identify and manage unsanctioned AI tools.
- **AI OWASP Top 10**  
Built-in security guardians
- **Risk-Based Enforcement**  
Apply contextual policies on usage.
- **Usage Visibility & Audit**  
Monitor and log all interactions



# Guardian Agent

- Discovery & Visibility**

Inventory all agents across your environment with complete transparency

- Monitoring & Traceability**

Track actions with full audit trails for accountability and compliance

- Identity & Access Control**

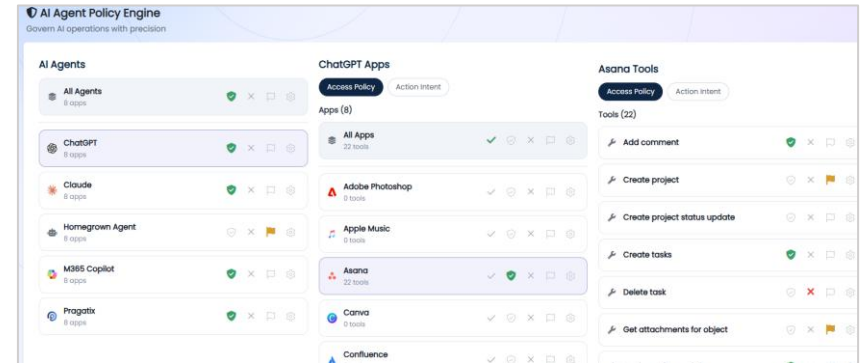
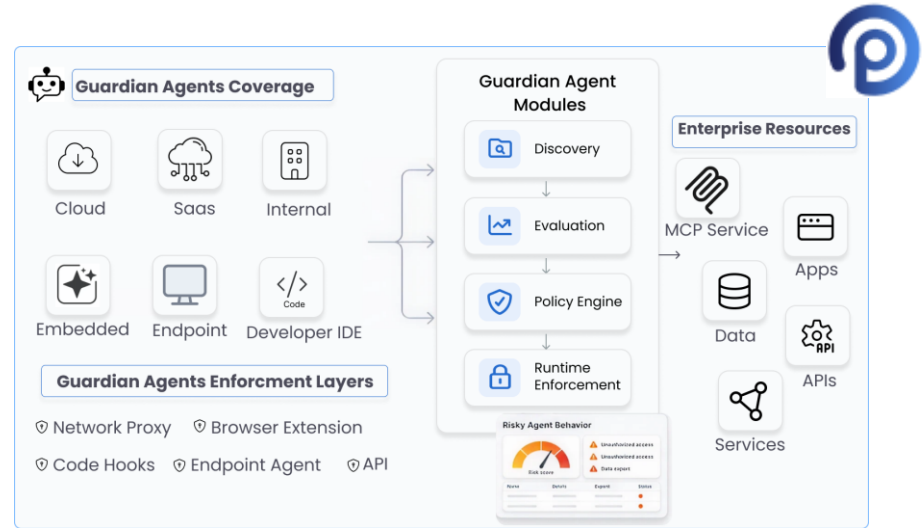
Govern permissions, tools, and access with granular policies

- Behavior & Anomaly Detection**

Ensure alignment with organizational standards and detect misuse patterns

- Runtime Action Enforcement**

Block, mitigate, and adapt in real time to prevent security incidents

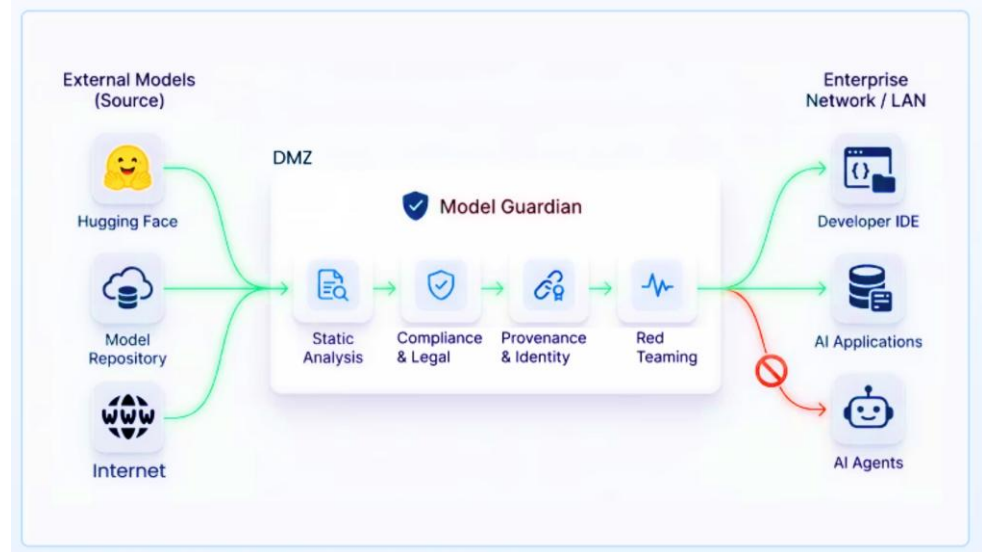




# Model Guardian

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





AI Security Suite

# Model Guardian

Evaluate and secure AI models used in the enterprise.

## The 4 Pillars of Model Scanning



### Provenance & Identity

- Trusted Org Verification
- Typo Squatting detection
- Hash match & GPG Check
- Popularity Lockup



### Static Analysis

- Pickle Safety
- YARA Ruleset Check
- Code Injection Scan
- Dependency CVE Analysis



### Behavioral Vetting

- Automated Red Teaming
- Custom Integrity and Poisoning Detection
- Backdoor Probing



### Legal and Compliance

- License Validation
- Vendor Compliance

# 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

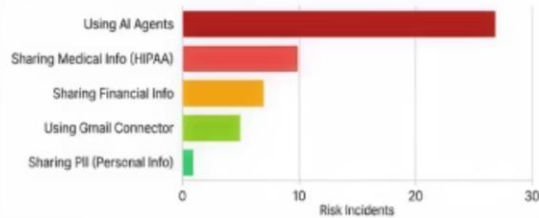
Detect, monitor, and control what AI agents can access and execute across your environment.

## 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



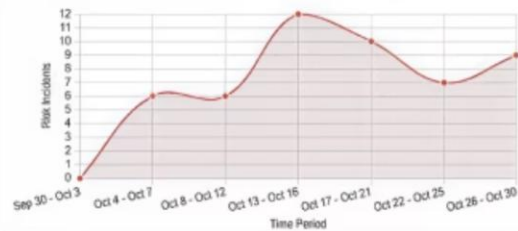
### Security Awareness Score

In-context Training



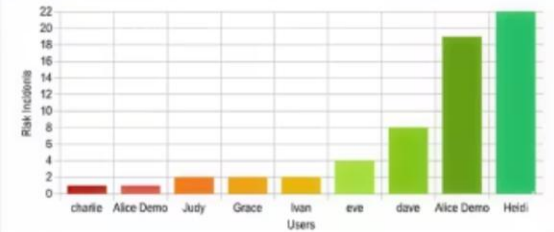
### Security Risk Trend

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

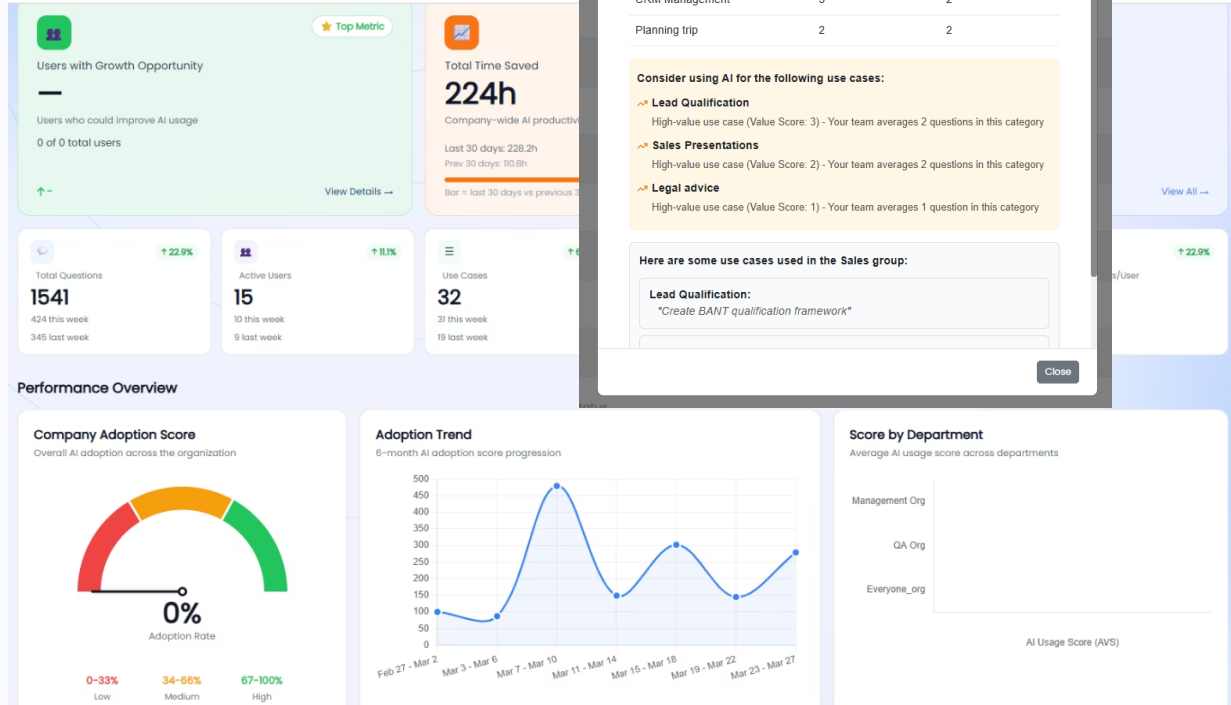
Understand how AI is used, why, and where it drives measurable value.

## 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.

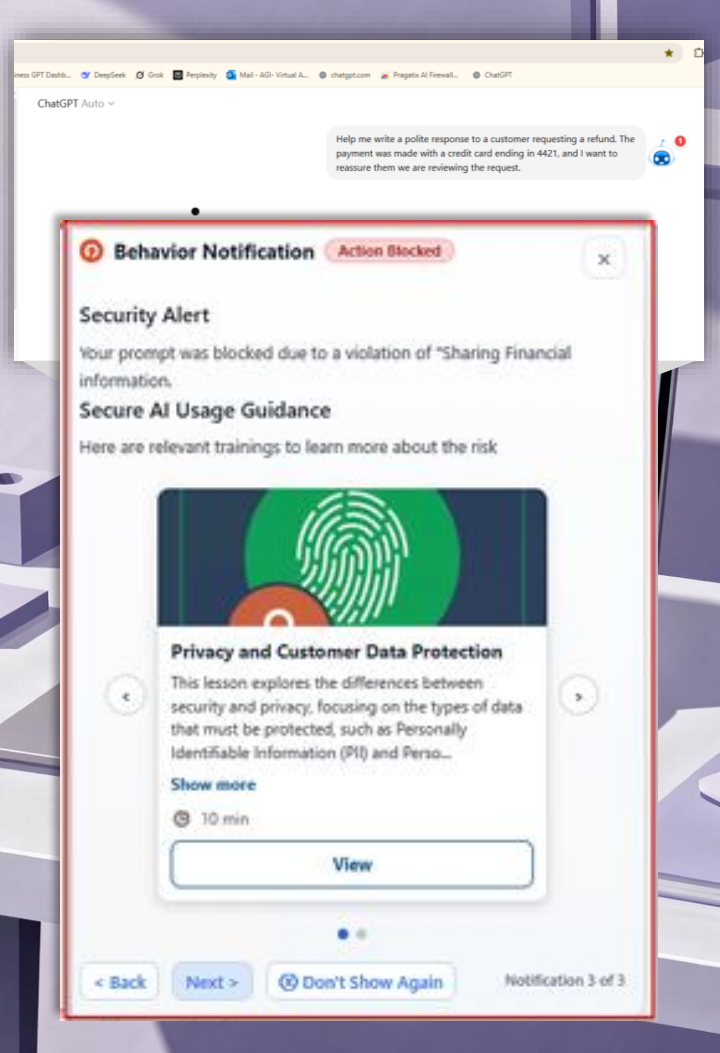


### 4 — Train

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.*



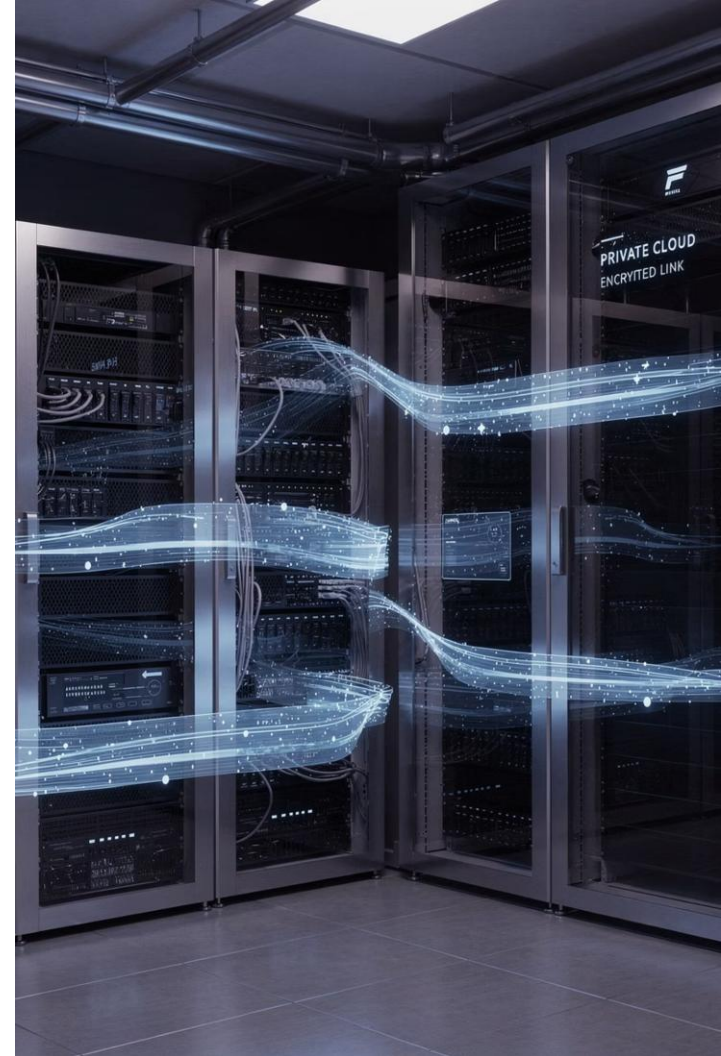
# Private AI Suite

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

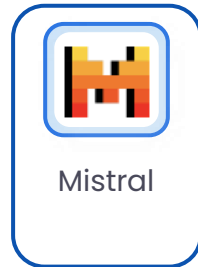
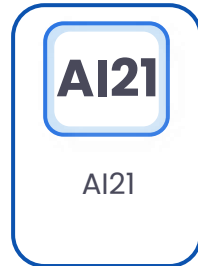
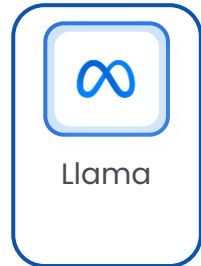
**ZERO DATA EXPOSURE**



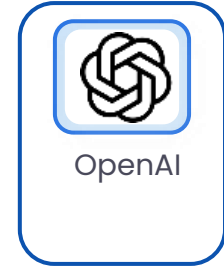
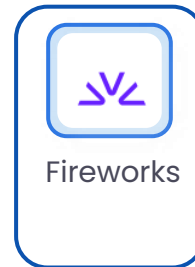


# Pragatix Private AI Suite — Core Modules

## 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](https://AGATSoftware.com)