

Security-First AI Platform

- On-prem or Cloud
- Ready to use and build
- Designed for Governance



Solution Overview: End-to-end AI Platform

Security First AI Platform

No Risks	Managed Risks
<p>Local AI Services</p>  <p>@PRAGATIX AI Suite</p>	<p>AI Services Inspect and Control</p>  <p>@PRAGATIX AI Firewall</p>
<p>For customer that don't want to take any risk of using Public AI services.</p>	<p>For customers that are willing to use Public AI services but want to manage the risks.</p>
<p>Enterprise AI service to use and build.</p>	<p>Built on AI TRiSM principles.</p>


Pragatix AI Suite





Secure AI services, providing organizations with ready-to-use AI capabilities


- ☑ **Enterprise Ready:** Plug and play with configurable UI
- ☑ **Deployment:** Available as an on-premises, air gapped or private cloud solution.
- ☑ **Access control:** Generate answers based on source data access.
- ☑ **Grounding:** Data connectors to most important sources, such as files, sites, emails, and meetings.
- ☑ **AI router-** Route prompts to cloud and on-prem multi-model services


AI Suite Modules

 **RAG Knowledge Assistant**
Generate answers from all company-connected sources and pre-trained knowledge.


 **Smart Search**
Search all your content beyond Keyword Matching. Understand intent and context.


 **Log analysis**
Ingest logs, classify and structure data, visualize, and apply real-time anomaly detection.


 **Data Extraction**
Capture, classify, and extract information from unstructured or semi-structured documents for IDP- Intelligent Document Processing.


 **Data Classification**
Automatically classify data based on existing data.

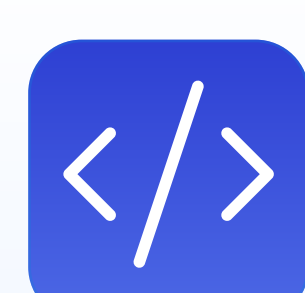
 **Anomaly Detection**
Identify anomalies in data, such as logs

 **Data Analysis**
Perform complex data analysis on Excel and databases using natural language.

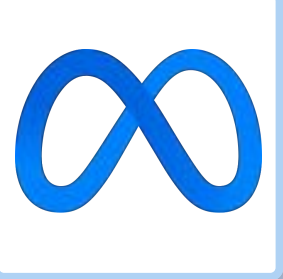

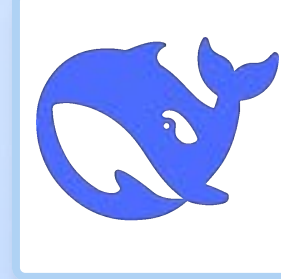
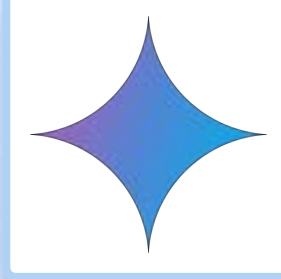
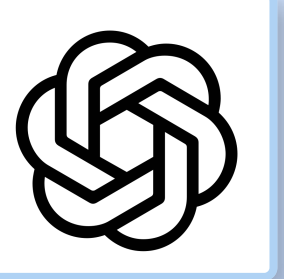


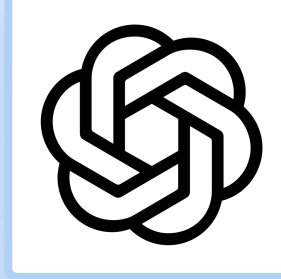
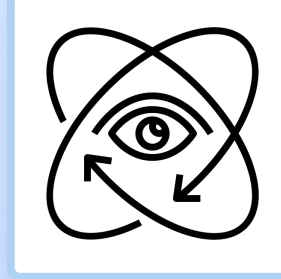

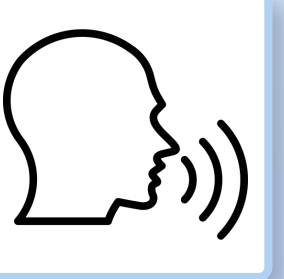
 **Workflow builder**
Build workflow using no-code drag and drop, calling AI Agents and other AI services

 **Document Translation**
Translate documents preserving original layout and formatting.

 **AI Agents**
Run AI agents to plan and perform tasks using tools like Python code, internet search, and managing files. MCP interface

 **AI Code Assistant**
Code completion, error detection, code generation, and answering questions from the company codebase.

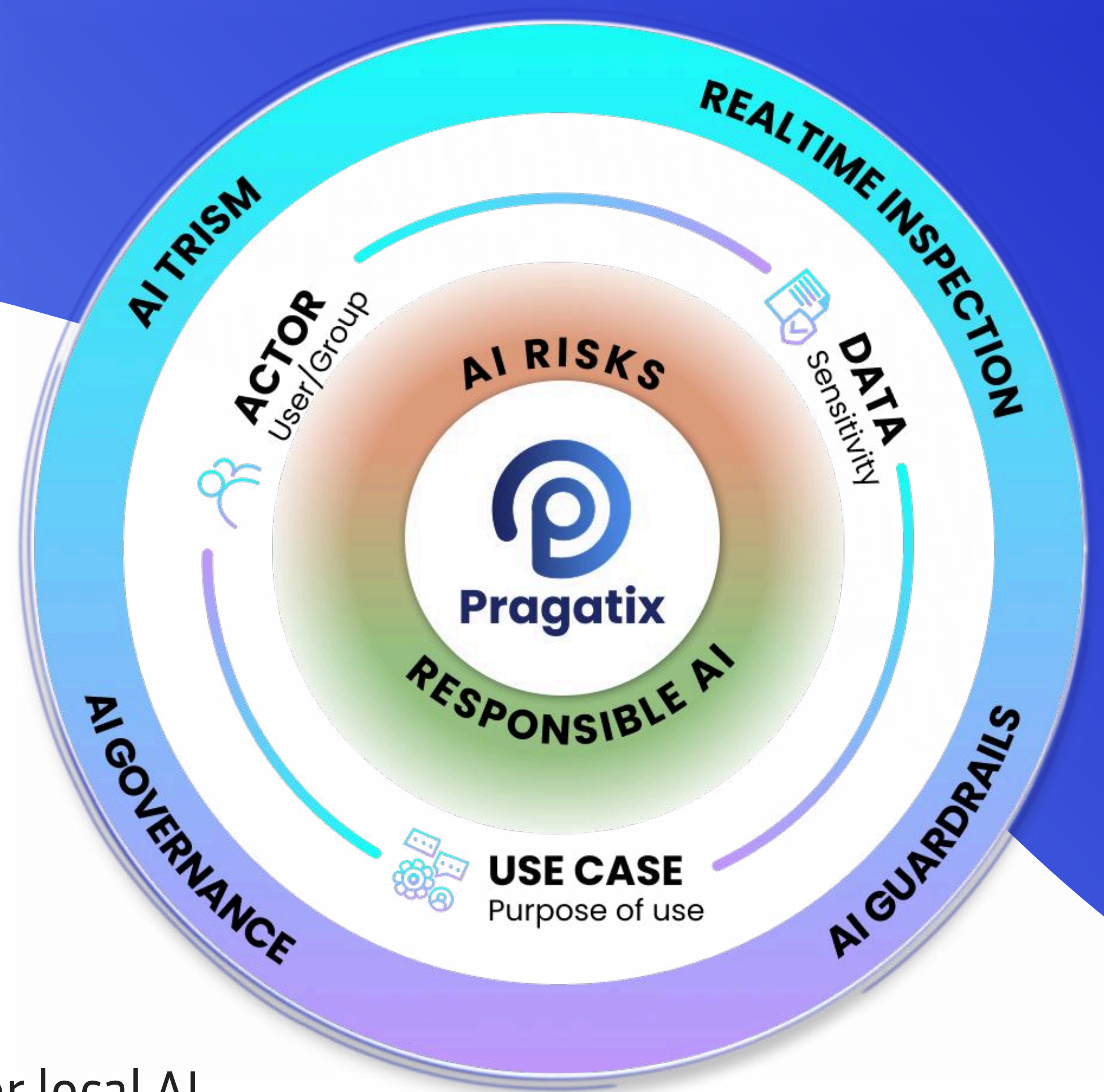
Multi-model Support

On-prem LLM Models						(Optional) Cloud LLM Services		Multi - Model		
										
Llama	Mistral AI	DeepSeek	Gemini	OSS	AI21	AWS Bedrock	OpenAI	Vision	Video	Speech

Pragatix AI Firewall





Mitigate AI risks by enforcing guardrails with Proxy real-time inspection and control .

- ☑ **AI Oversight Anywhere:** Inspection of both external AI services such as ChatGPT and internal AI services of Pragatix and homegrown AI.
- ☑ **Proactive Risk Prevention:** Blocks AI-specific threats like prompt injection, jailbreaks, hallucinations, and toxic content .
- ☑ **Real-time Inspection:** Real-time insight into AI usage, uncovering shadow AI and transparency for audits and reporting.
- ☑ **Deployment:** choose from proxy based, browser extension, or API.
- ☑ **Public AI Support:** Support for online AI like ChatGPT, Gemini, Copilot or local AI.



AI Firewall Capabilities

Delivers the Gartner principles of AI TRiSM – Trust, Risk, and Security Management

 SECURITY Safeguarding Data & Preventing Threats	 RISK MANAGEMENT Mitigating AI-Specific Risks	 TRUST Ensuring Responsible & Reliable AI Outputs	 GOVERNANCE Oversight, Visibility & Compliance
Sensitive Data Protection (DLP): Prevent PII, PHI, and IPp from leaving your environment.	Risk Classification & Rules: Define and manage risky AI activities using natural language policies.	Output Validation: Ensure results are accurate, aligned, and reliable.	AI Agent Activities: Visibility and control on what agents do.
Data Taxonomy & Classification: Identify activities, topics, and sensitivity levels.	Hallucination Reduction: Validate AI outputs against policy and fact-checking rules.	Governance Policies: Enforce responsible usage by role, group, or workflow.	Shadow AI Detection: Discover and audit unsanctioned AI usage.
Prompt Injection & Jailbreak Protection: Stop malicious instructions from bypassing safeguards.	Toxic Content Filtering: Block unsafe, harmful, or policy-violating prompts and responses.	Content Integrity Checks: Maintain tone, safety, and brand alignment.	AI Monitoring & Auditing: Map, log, and analyze AI interactions.
OWASP LLM Threat Coverage: Address top AI risks like insecure output handling .	Business Safeguarding: Prevent reputational or financial harm from unsafe or incorrect AI use.	Policy-Based Enforcement: Translate company rules into automated safeguards.	Usage Mapping: Track who uses AI, how, and how often. .

Book Demo

<https://agatsoftware.com/>

Pragatix Benefits

All-in-one Solution

One-stop shop for all your enterprise AI services and AI governance needs.

Accelerate AI Adoption

Deploy enterprise-ready AI in minutes. No coding required.

Zero Data Exposure

Run AI fully on-premises, private cloud, or even air-gapped.

Full Control & Flexibility

Choose and manage your own AI models (open-source or proprietary) while applying your own governance and access policies.

Secure AI Firewall Protection

Address AI OSWASP risks such as prompt injection, data leakage, and unsafe outputs while gaining visibility on all AI usage.

Enhanced Reporting

Actionable reports for managing adoption and governance.

About AGAT

AGAT is a leading provider of cutting-edge AI solutions. Its flagship product, Pragatix, is an enterprise-ready AI platform that enables rapid adoption of Generative AI while ensuring data privacy and security.

Backed by more than a decade of expertise, AGAT has delivered trusted compliance and security solutions to dozens of highly regulated organizations, including over 25 Fortune 500 companies.

Contact Details

✉ info@agatsoftware.com

☎ www.AGATSoftware.com

🌐 [+972-2-579-9123](tel:+972-2-579-9123)

