

SECURITY FIRST AI PLATFORM

Empower users with responsible and secure AI for generating insights from your company's data.



Company Overview



Security and Governance

- ✓ Externally Funded
- ✓ Founded 2013

✓ hundreds of customers, including 25 Fortune 500



Pragatix

- Generative AI



SphereShield

- Collaboration



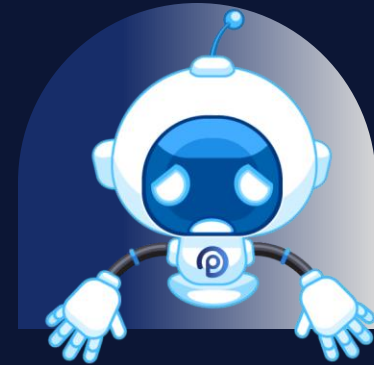
Deployment Presence worldwide

India, Denmark, Korea, Hong Kong, South Africa, Indonesia, Italy, Norway, New Zeland, Switzerland, **USA**, Germany, Russia, Belgium, Global, Sweden, Phillipines, Turkey, Spain, Serbia, Slovenia



THE PROBLEMS

AI models and applications aren't innately reliable and secure.



— SECURITY— Data leakage

- ▶ Connecting AI models to company data can lead to data privacy violations



— GOVERNANCE — Misuse

- ▶ Employees rely on AI for business operations. can lead to Business Financial or reputational harm



Usage control and data protection concerns limit companies from leveraging Generative AI.

1 in 3 enterprises prohibit using public Generative AI (2023)

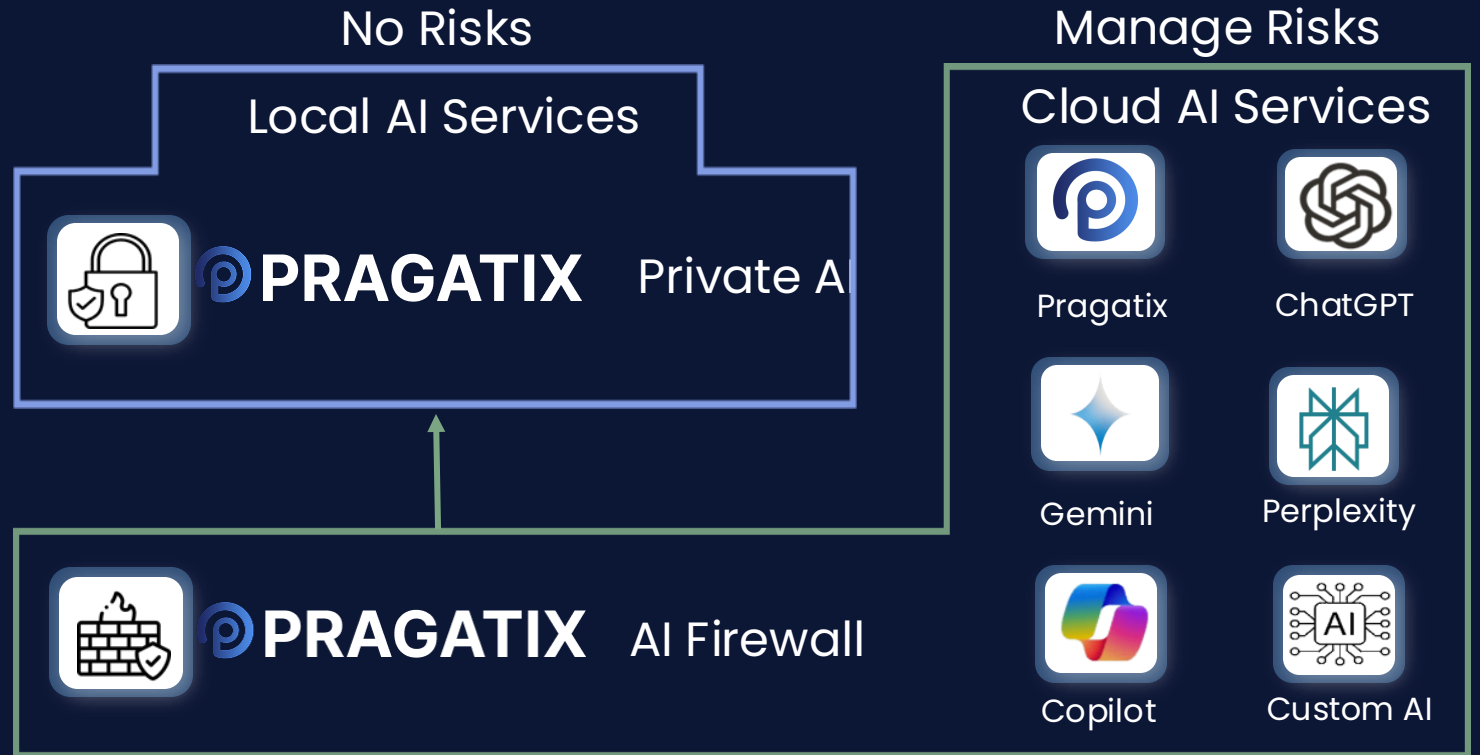
Gartner 2024: "AI governance" is the term most frequently searched by Gartner customers.

Solution Overview



For customers that don't want to take any risk of using Public AI services.

For customers that are willing to use Public AI services but want to manage the risks.



PRAGATIX AI Firewall



Gemini



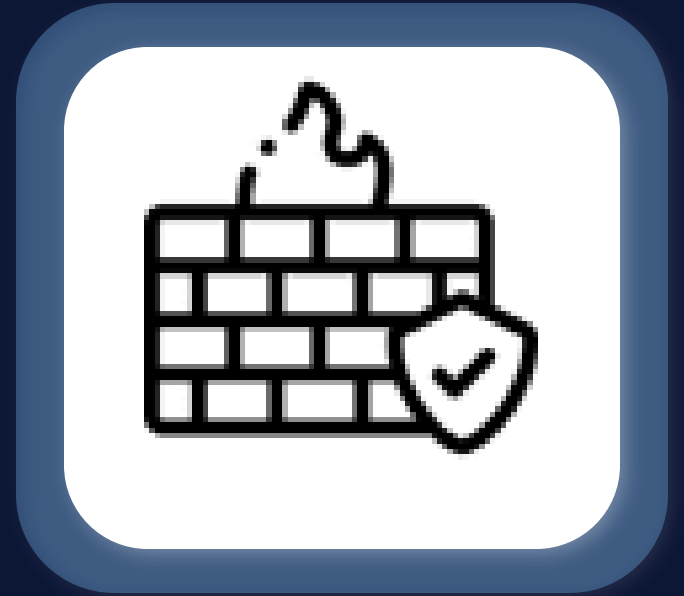
ChatGPT



Copilot



Custom AI

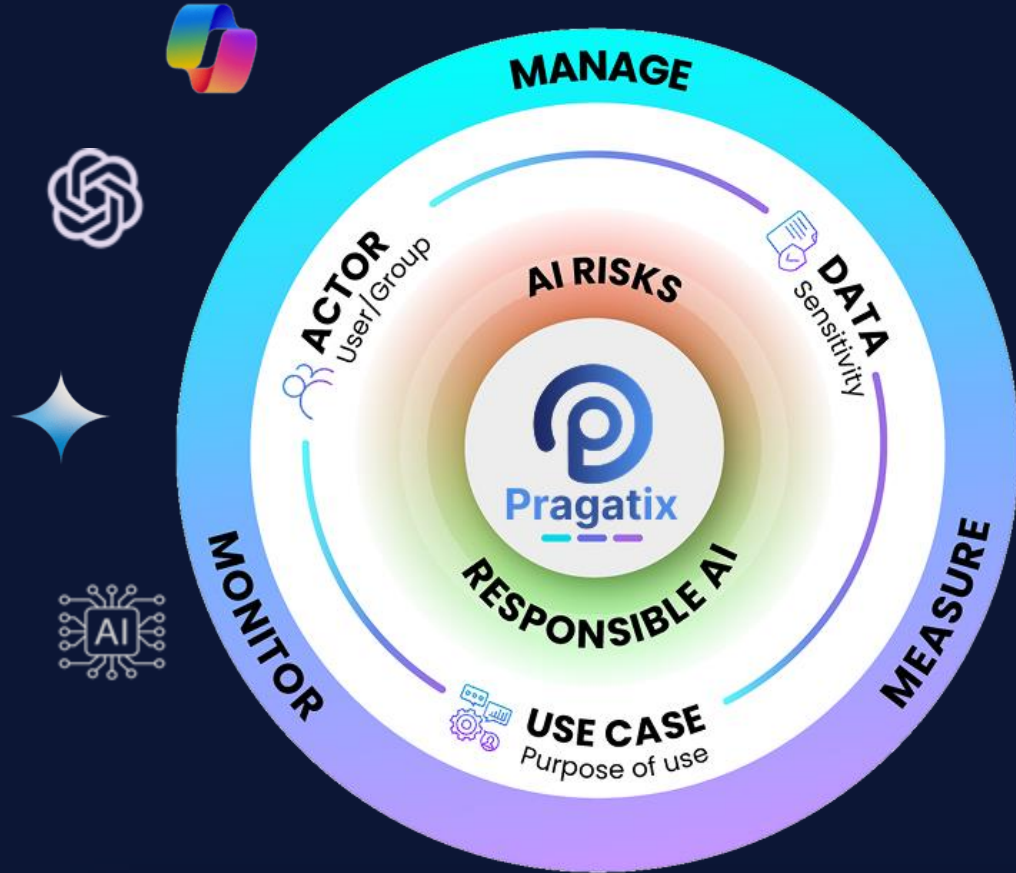




Pragatix AI Firewall



AI Governance for on-prem and public service like ChatGPT



Monitor - Audit and monitoring shadow and official AI usage



Measure - risk based on defined company policies.



Manage- Control risks by defining rules blocking/allowing AI usage.



Compliance – Maintain compliance with regulations like EU AI ACT and NIST AI RMF.



Define Responsible AI for your company.

Mitigating AI risks with visibility and control of AI usage

AI Firewall




Responsible AI by Safeguard and Monitoring Risks


Firewall modules

 Auditing

Monitor and measure usage.

 Data Classification

Data Classification
Usage classification

 Policies

Define risks and actions for AI usage

AI Firewall for Risk Management and Prevention



AI GOVERNANCE FEATURES



AUDITING

- | Record every question/answer
- | Automatic usage classification by topics
- | Identify usage risk levels per user



DATA CLASSIFICATION

- | AI Usage detection and classification
- | Classification of data and Q&A
- | Company Data Sensitivity level
- | Questions and answers topics
- | Questions and answers categories
 - ▶ Regular expression
 - ▶ Natural language AI
 - ▶ System rules (PII, HIPPA, Finance, Self-harm, Sexual , Violence etc)
 - ▶ Content Sensitivity classification



AI POLICIES

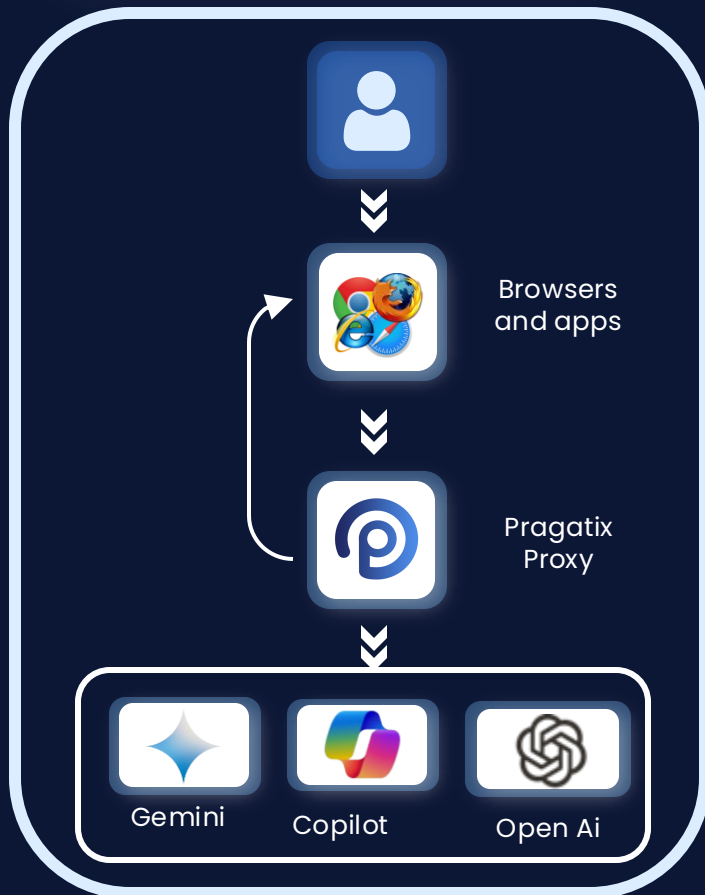
- | Define risk-based company AI usage policies
- | Permitted / Forbidden Access
- | Inspect and apply rules based on source data and Q&A content.
- | Set rules per user/ group
- | Define action – Block/Allow
- | Use data classification for policy risk





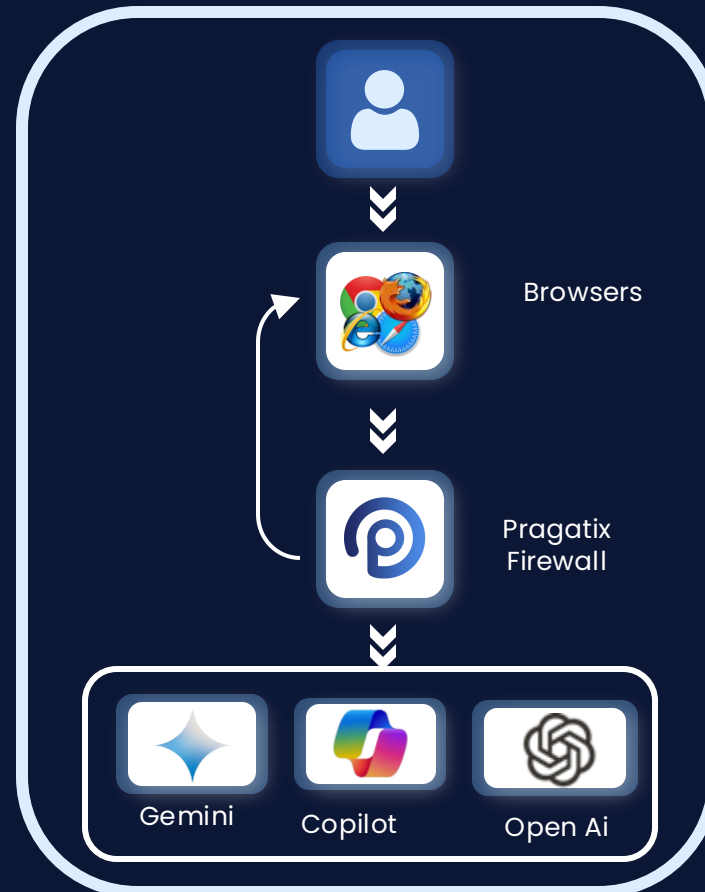
Pragatix Firewall Dataflow Topologies

Network Proxy

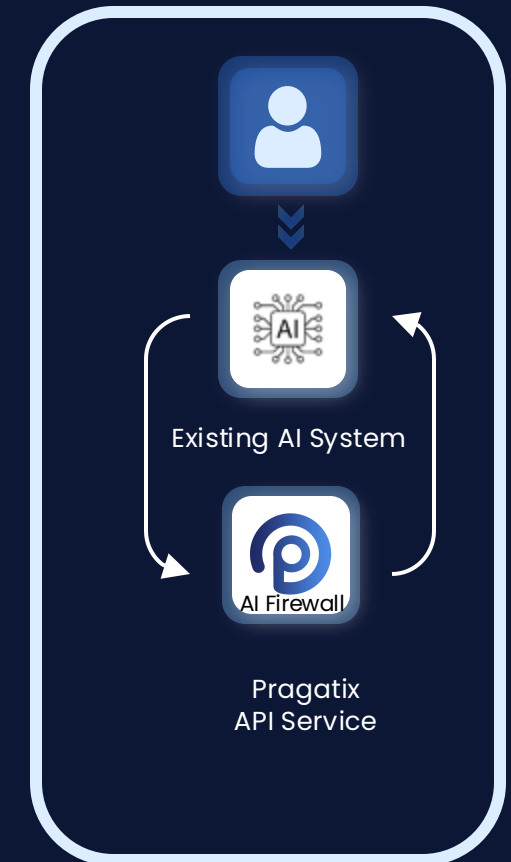


Forward traffic to Pragatix Proxy
Captures all browsers and applications

Browser Extension



Service API



Connect your AI system with
restAPI



Pragatix Firewall Supported services



ChatGPT (Web/ app)
by OpenAI



CoPilot (Web/ App / Teams /
Outlook / Word / Excel /
PowerPoint...) by Microsoft



Gemini by Google



Claude
AI by Anthropic



Jamba
By AI21 Labs



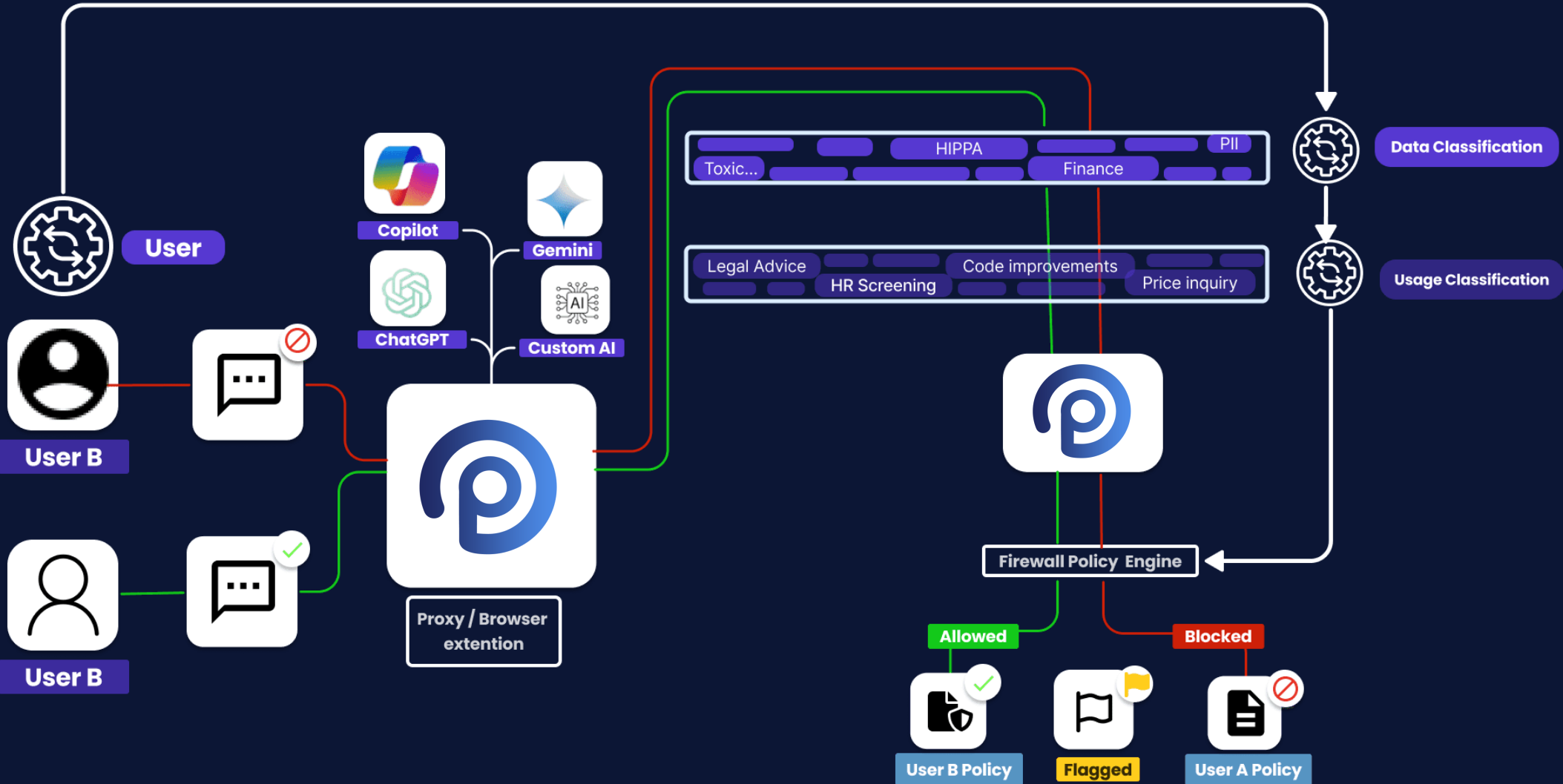
Perplexity
Coming Soon



Deep Seek
Coming Soon



Policy Engine Flow



PRAGATIX Private AI



Pragatix Private AI Capabilities



Generate answers from all company-connected sources and pre-trained knowledge.

Answers



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

Insights

Data Analysis

Knowledge Chatbot



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

Discovery

Smart Search



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

Development

AI Code Assistant



Pragatix

AI Agent



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

Execution



Private AI

Multi-model Support

Open Source



Llama

AI21

AI21



Deep
Seek



Mistral
| AI

Cloud Services



AWS
Bedrock



OpenAI



Pragatix – Private AI

End-to-end private AI solution



Secure on-prem/ Self-hosted Cloud.

Data does not leave company control.



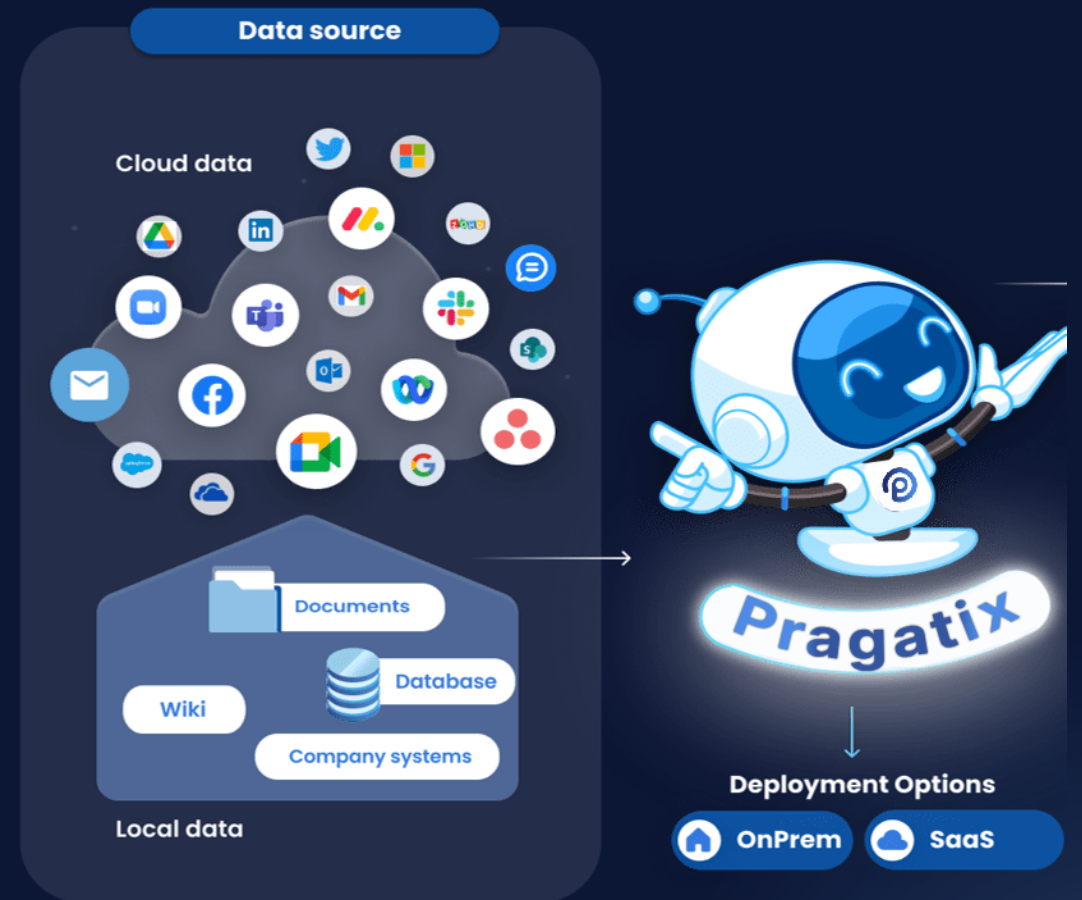
Sync and Control Data Permission

Ensures responses align with users' existing access in CRM, document management, and other source systems.



Grounding with Company Data

Extracts insights from emails, chats, meetings, CRM, websites, and knowledge bases, connecting to key data sources.



Zero Data exposure

Pragatix Private AI Supported Data Sources



Microsoft:
Teams chats,
Team channels,
Teams meeting
transcripts, One
Drive, SharePoint,
Email (Exchange
/Outlook), Planner.



Google:
Meeting
transcripts,
Drive, Gmail.



Slack:
Channels,
Chats.



Zoom:
Meeting
transcripts.



Webex:
Spaces, Direct
messages,
Meeting
transcripts.



CRM & Tasks
Planner,
Monday,
Asana

Coming soon:



Discord



Google Sheets



Unique Selling Proposition (USP)



Problem solved

No Visibility and Governance for public AI service



Approach

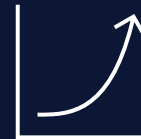
Pragatix analyses public AI services (ChatGPT, Copilot) usage in real-time.



Technology

To support public or external AI services, a network proxy is required.

Over many years, AGAT has developed a field-proven proxy handling advanced protocols and including extensive filtering capabilities.



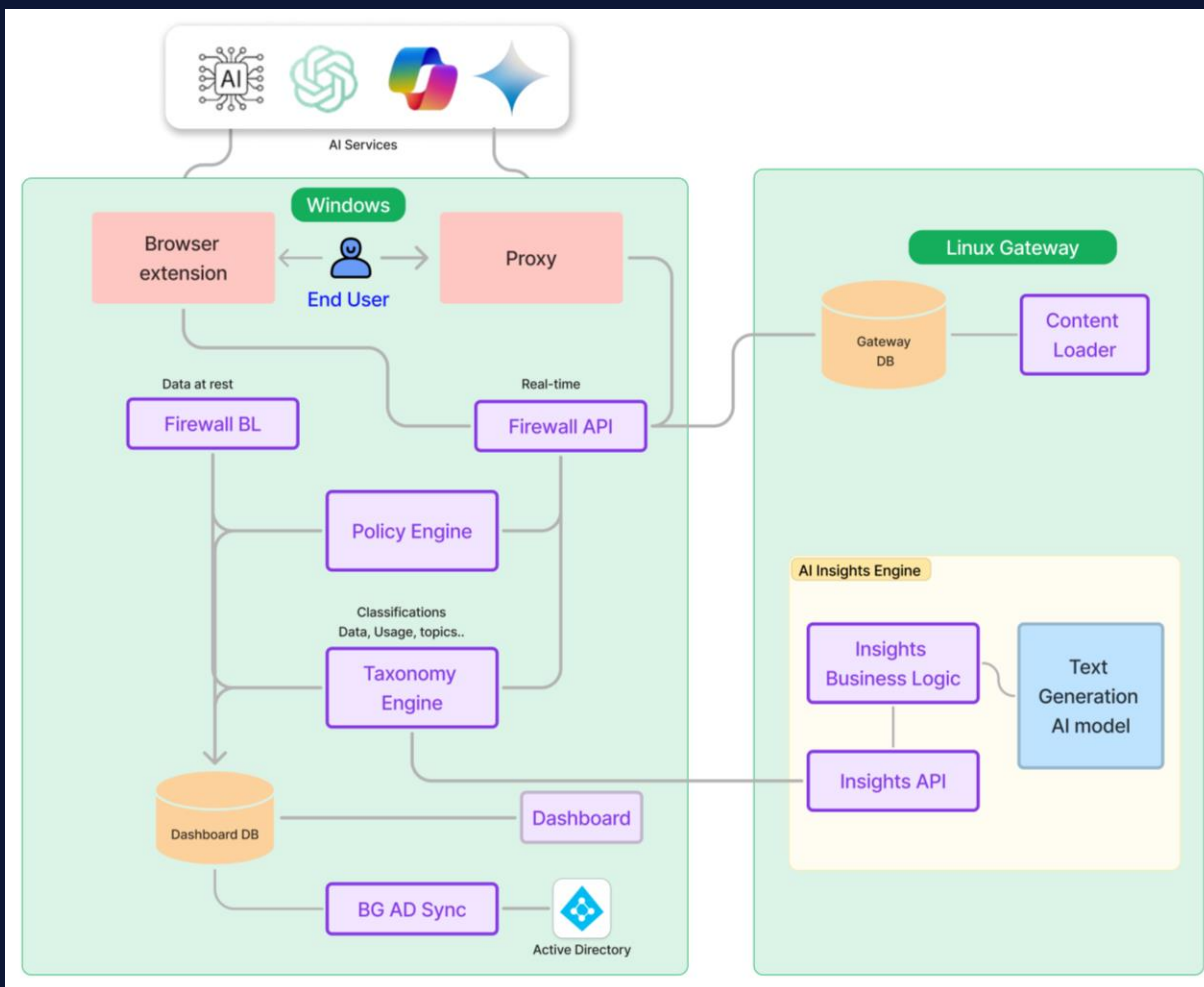
Experience

Experience in Compliance, Large data analysis and Global secure deployments.

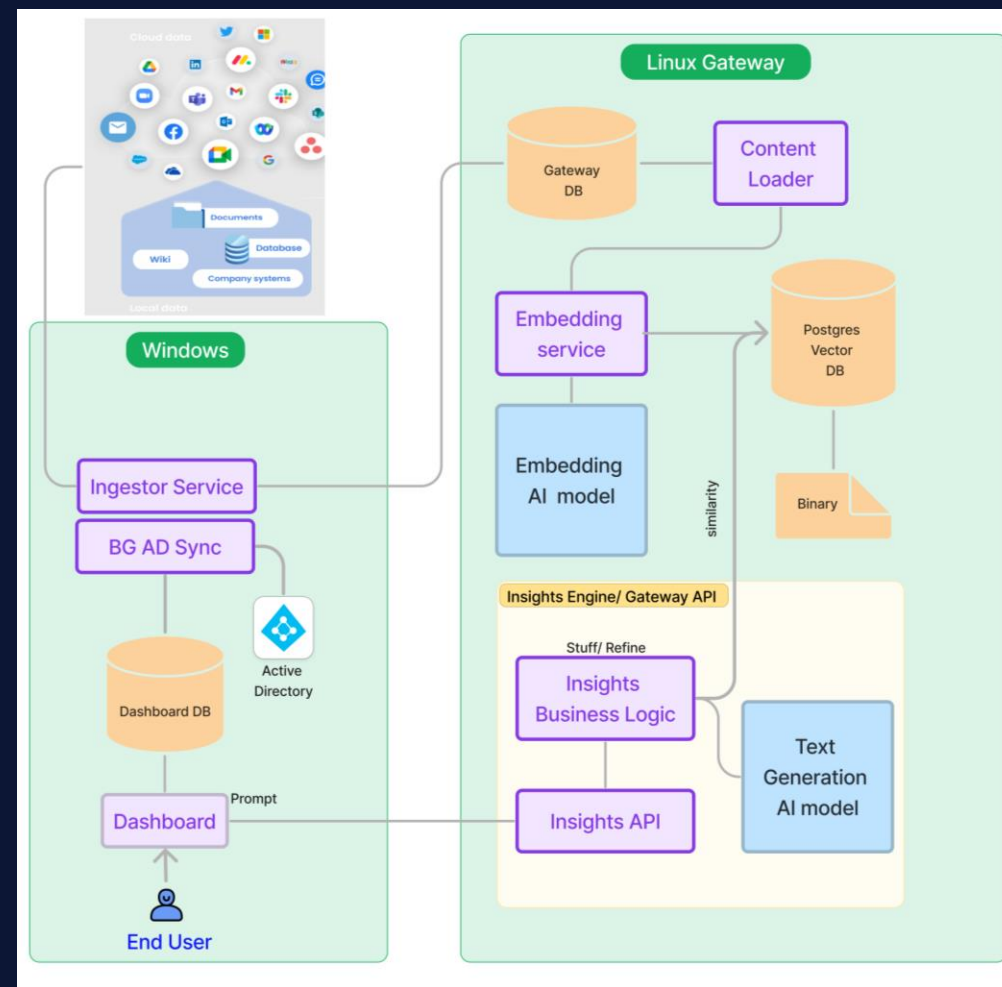


Pragatix Topologies

AI Firewall



Private AI



Benefits of Pragtaix



Control AI usage across platforms:

ChatGPT, Gemini, Copilot, Internal and external AI systems



Secure sensitive data by regulations

PII, HIPPA, Finance



Mitigate OWASP risks:

Prompt injection, Prompt leak, Jailbreak, DDoS.



Manage AI Usage:

Users, Content, Activity



Handle risks:

Reputational damage, IP lost, Financial Business Loss



Meet industry standards:

NIST AI RMF and ISO standards.



Implement AI Governance

Internal Policies



Meet industry standards:

NIST AI RMF (Risk Management Framework) and ISO 42001 (Artificial intelligence Management system)



Start your AI Business Journey



Contact Details:
www.agatsoftware.ai