

SECURITY FIRST AI PLATFORM

- On-Prem or Cloud.
- Ready to Use and Build.
- Designed for Governance



[Http://agatsoftware.com](http://agatsoftware.com)



Company Overview



Security and Governance

Previous line of business



SphereShield Collaboration

- ✓ Hundreds of customers, including 25 Fortune 500

Current Strategic Focus Shift



Pragatix Generative AI

With over a decade of compliance & security expertise, AGAT delivers Pragatix AI Platform with governance & security at its core.



Founded in 2013

Seed - March 2023-

24 Employees

Offices in Israel & South Africa



The Problem



Enterprises with sensitive data can't adopt AI because of **data exposure and Governance risks using public AI services.**



Companies are looking for AI services to be under their full control or at least have **visibility and control** over public AI usage.

Solution Overview: End-to-end AI Platform



 **PRAGATIX**

Security First AI Platform

No Risks

Local AI Services



 **PRAGATIX** AI Suite

Managed Risks

AI Services Inspect and Control



 **PRAGATIX** AI Firewall

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.

Enterprise AI service to use and build

Built on AI TRiSM principles

PRAGATIX AI Firewall



Gemini



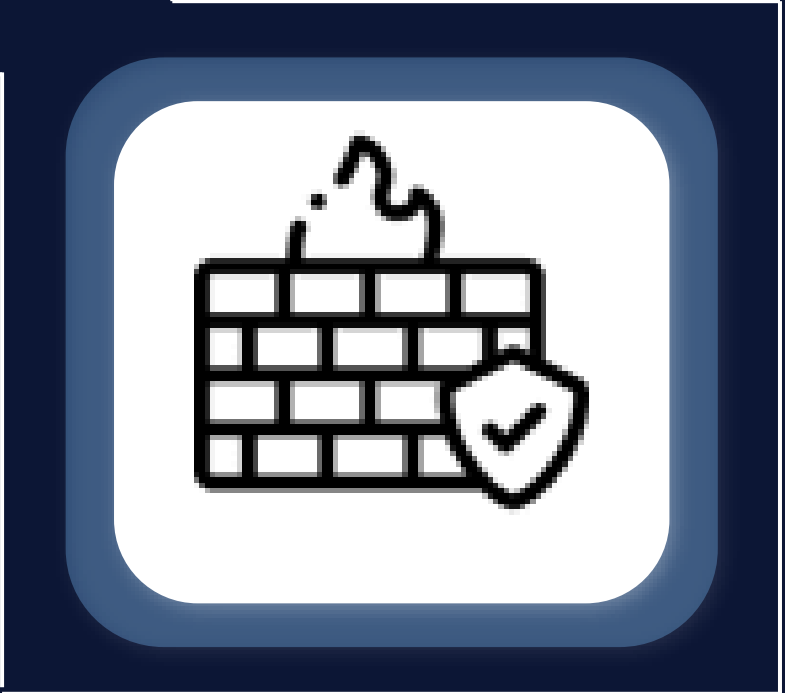
ChatGPT



Copilot



Custom AI

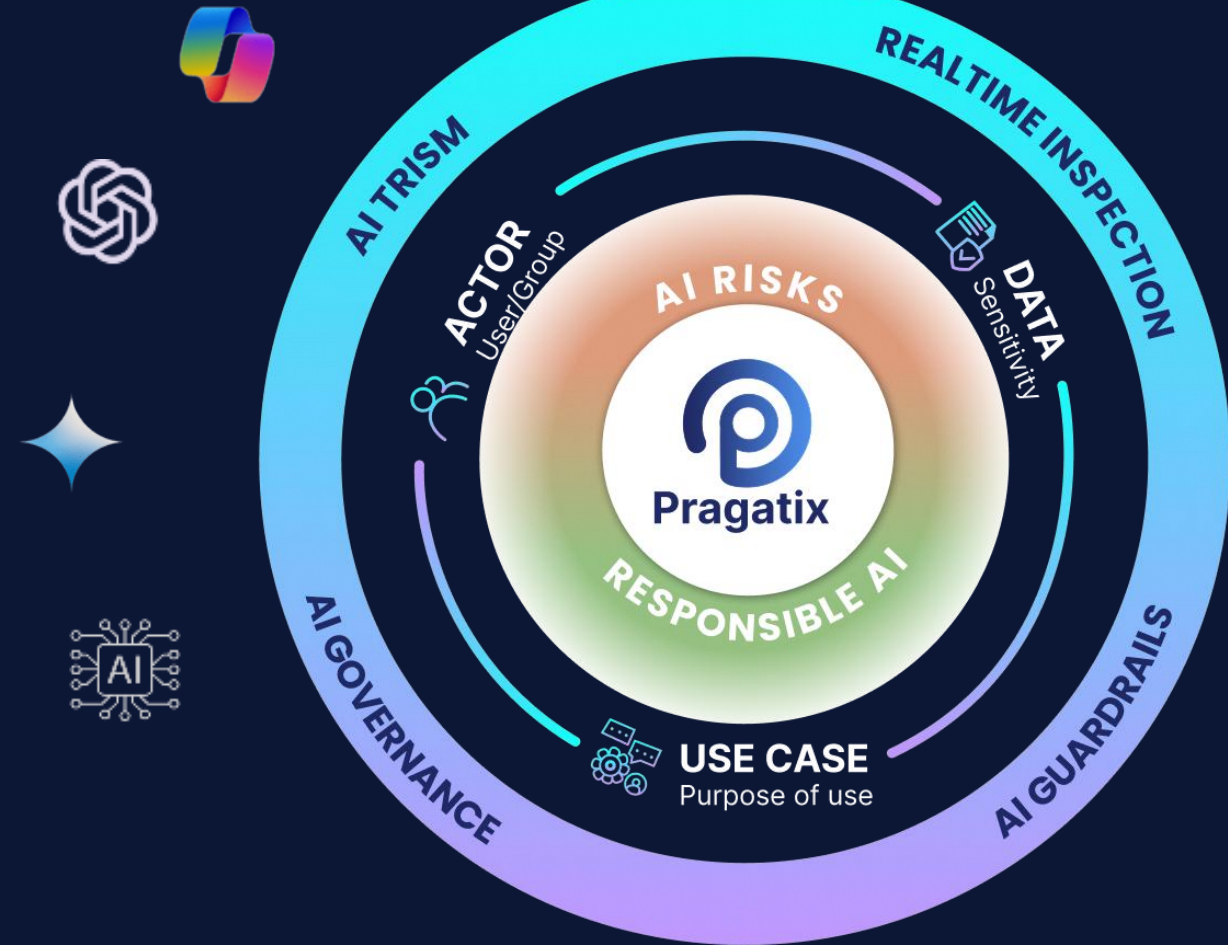




Pragatix AI Firewall



- AI Governance for on-prem and public service like ChatGPT
- Mitigating AI risks with visibility and control of AI usage



Firewall TRiSM modules



Security

DLP, Classification, Prompt Injection



Risk Management

Toxic content filtering, hallucination reduction



Trust

Output Validation, Policy Enforcement



Governance

Oversight, visibility, Shadow AI, Control



Data classification

Data Sensitivity (DLP)- Files and prompts

The screenshot shows the PRAGATIX Data Classification List interface. The left sidebar contains navigation options: Home, Chatbot, Data Analysis, Smart Search, Collections, Data Sources, Activity Auditing, User Settings, Reports, Account AI Firewall, Firewall Dashboard, Account Activity Auditing, and Firewall Policies. The main area displays a table of classification rules. The 'Finance' rule is selected, and its details are shown in an 'Edit Rule' modal window.

Name	Type
PII Personal Data - Entites English	Preb...
Anti-harassment and Workplace Safety - bodwor...	Regu...
Anti-harassment and Workplace Safety - inappro...	Regu...
Any data classification	Defa...
Dollars and cents amounts	Regu...
Finance	NLP-
HIPAA Health Data	NLP-
Personal Information	NLP-
Toxicity	NLP-
Addresses and Buildings Database (BAG)	NLP-
BRP (Personal Records Database)	NLP-AI

Edit Rule

Name: Finance

Description: Description

Rule Type: General

Value: Encompasses financial transactions, reporting, auditing, accounting balance sheets, profit and loss

Sensitivity Level: High

Enabled: Yes No

Scope: Data Prompt Response

Buttons: Close, Save

Rule Value: Encompasses financial transactions, reporting, as Corporate Financial Data, such as balance sheets, profit
Last Modified By: Hodaya Oved (hodayao@ogatsoftware.c...
Last Modified Time: 22/05/2024 09:58:08

To classify any prompt or response containing pe... None

Usage classification



User intent – what is the AI used for

The screenshot displays a web application interface for managing usage classifications. A modal window titled "Edit Rule" is open, allowing the user to edit the "Financial Forecasting" rule. The modal contains the following fields:

- Name:** Financial Forecasting
- Description:** Financial Forecasting
- Rule Type:** General (selected from a dropdown menu)
- Value:** Involves questions about budgeting and financial analysis aimed at predicting future financial performance. It includes tasks such as projecting revenue growth, estimating future expenses, forecasting cash flow, and anticipating market trends using data from past.
- Enabled:** Yes No

At the bottom of the modal are "Close" and "Save" buttons. The background shows a "Usage Classification List" table with the following data:

Name	Created By	Enabled
Any usage	system	Yes
Code Quality Improvement	system	Yes
Customer Service	Yoav Crombie	No
Data Analysis	system	Yes
Financial Forecasting	system	Yes
HR Recruitment	system	No
Legal Advice	system	Yes
Marketing Content	system	Yes
Price Inquiry	system	No
Programming	system	Yes
Support Service	system	Yes
Text Improvement	system	Yes
Costs Inquiry	Yoav Crombie	Yes
Employee Screening	Yoav Crombie	Yes
Ethical Misuse	Reuvain Aarons	Yes

At the bottom of the page, it indicates "Showing 1 to 15 of 20 entries" and "1 row selected". Navigation buttons for "Previous", "1", "2", and "Next" are visible.



Which AI Services are used

Manage AI Usage - Handle Shadow AI

Monitor and control which AI models are used in production to ensure compliance and prevent misuse.

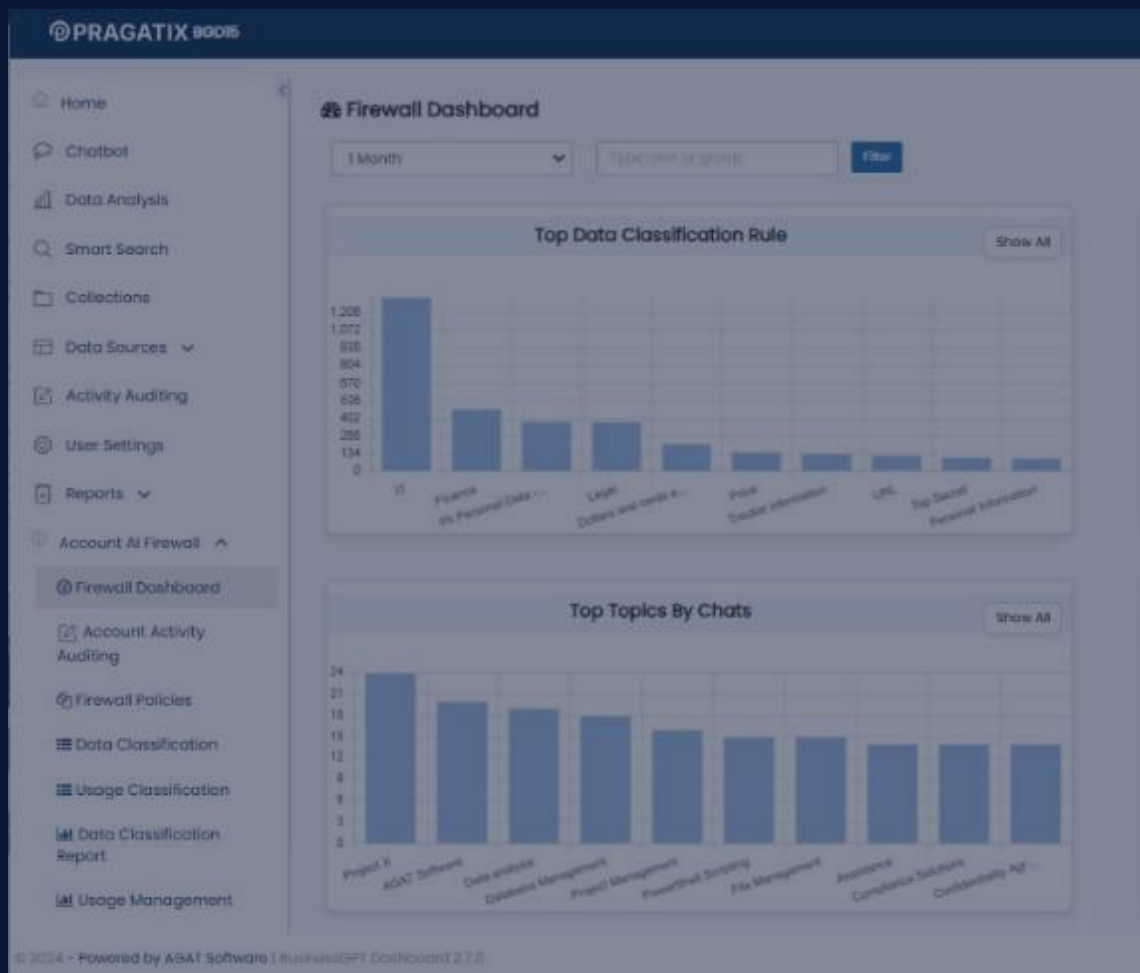




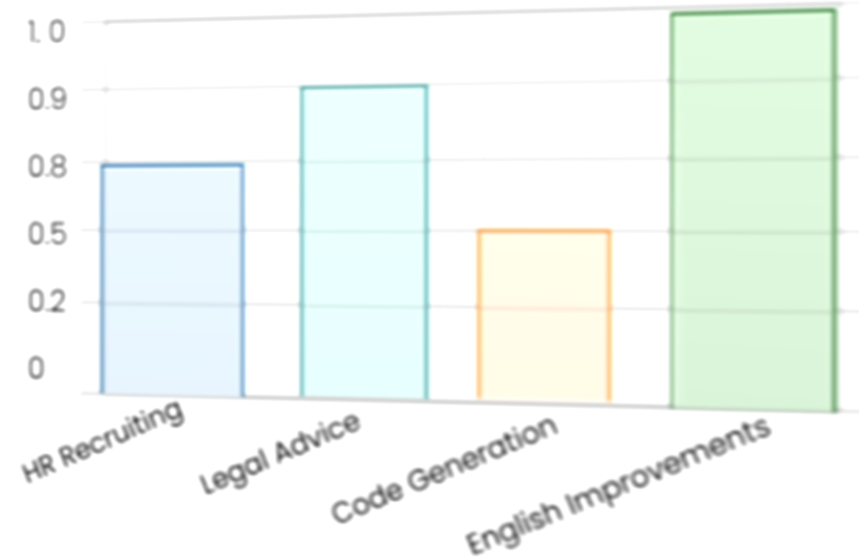
What AI is used for

Audit AI Usage:

Track all AI activity to identify potential risks, security breaches, and biases.



Activity Usage



Account Activity Auditing



Account Activity Auditing

Click here to learn more about Activity Auditing

Advanced search

REANALYZE FILTER CHAT REFRESH

Sensitivity	Usa...	Guardrail Policies	Action	Prompt	AI Ser...
None		No policy	Allowed	רשום בגוף שלישי	
None		No policy	Allowed	אם לאנגלית ורחום בצורת רליס נוסס: ניתן בעת להספיק עיצוב	
None		No policy	Allowed	what should a new employee learn when stat...	
High		No policy	Allowed	in a finance reports what is more used costs ...	
None		No policy	Allowed	what is S/S in the following : I'll mail the S/S to ...	
None		No policy	Allowed	Improve english Hugo from Mirabaud was ha...	
Critical		Top Secret	Blocked	what do you know about project x?	
None		No policy	Allowed	where i can find my 'Personal Access Tokens' ...	
Low		Code writing	Flagged	Help me write a script to copy this table to an...	
None		No policy	Allowed	Where is your API documentation?	
Low		No policy	Allowed	im getting this error after step 2: Msg 1205, Lev...	
Low		No policy	Allowed	im getting this error after step 1: Msg 1205, Lev...	
Low		No policy	Allowed	how can i delete this db on SSMS: BGDB im ge...	
None		No policy	Allowed	what is the blessing for ending the ramadan t...	
Medium		Legal advice for all	Flagged	לפי בחוק הגנת השכר קובע שיש השלים לעובד בני עבודה סא	

Low Code writing Flagged Help me write a script to copy this table to an...

Policy applied Low risk policy Code writing

Prompt Help me write a script to copy this table to another table in a different Db. this is the other table: SELECT TOP (200

- Data classification:
 - Name: IT (NLP-AI) Description: Information Technology Sensitivity Level: Low Details
- Usage classification:
 - Name: Data Analysis (NLP-AI) Details
 - Name: Programming (NLP-AI) Details
- Specific usage:
 - Writing database copy script

Response Instructions No instructions

Response To copy the data from the '[GW_AI_MODELS]' table (in your current DB) to '[BGDBGateway].[dbo].[SupportedMc

Response Data sources Document image

User email agi@agatsoftware.com

Chat Name Copy Table Script

Chat Context

Chat topics SQL Scripting, Database Querying, Data Transfer, Table Operations, Database Management

Firewall type Chrome Extention

Chat AI service Chat GPT

AI Model Type

Chat Mode

Prompt id 13111

BusinessGPT Dashboard 2.10.0 | Gateway status

AGI- Virtual Assistant 31/03/2025 11:51:16

Yoav Cromble 31/03/2025 08:58:03

Yoav Cromble 31/03/2025 08:41:41

Guardrail Policy



Block Prompts that violate Firewall Policies

Edit Guardrail Policy

Policy details:

Name: Legal advice for all Enabled: Yes No

Description: Prevent legal use of AI

Policy risk & action:

Risk Level: High Firewall Action: Flag

Policy conditions:

Identity Type: Group Identity Value: Everyone

Scope	Name	Rule Type	Classification Type	Value
Usage Classification	Legal Advice	General	AI	Provides insights and strategies c...
- Select -	- Sele			

[+ New Usage Rule](#) [+ New Data Rule](#)

Close Save

ChatGPT 3.5

You: What is the salary of Yoav?

ChatGPT: Your question was blocked due to policy: Salary

Pragatix AI Firewall

Your question was blocked due to policy: Salary

There was an error generating a response

Regenerate

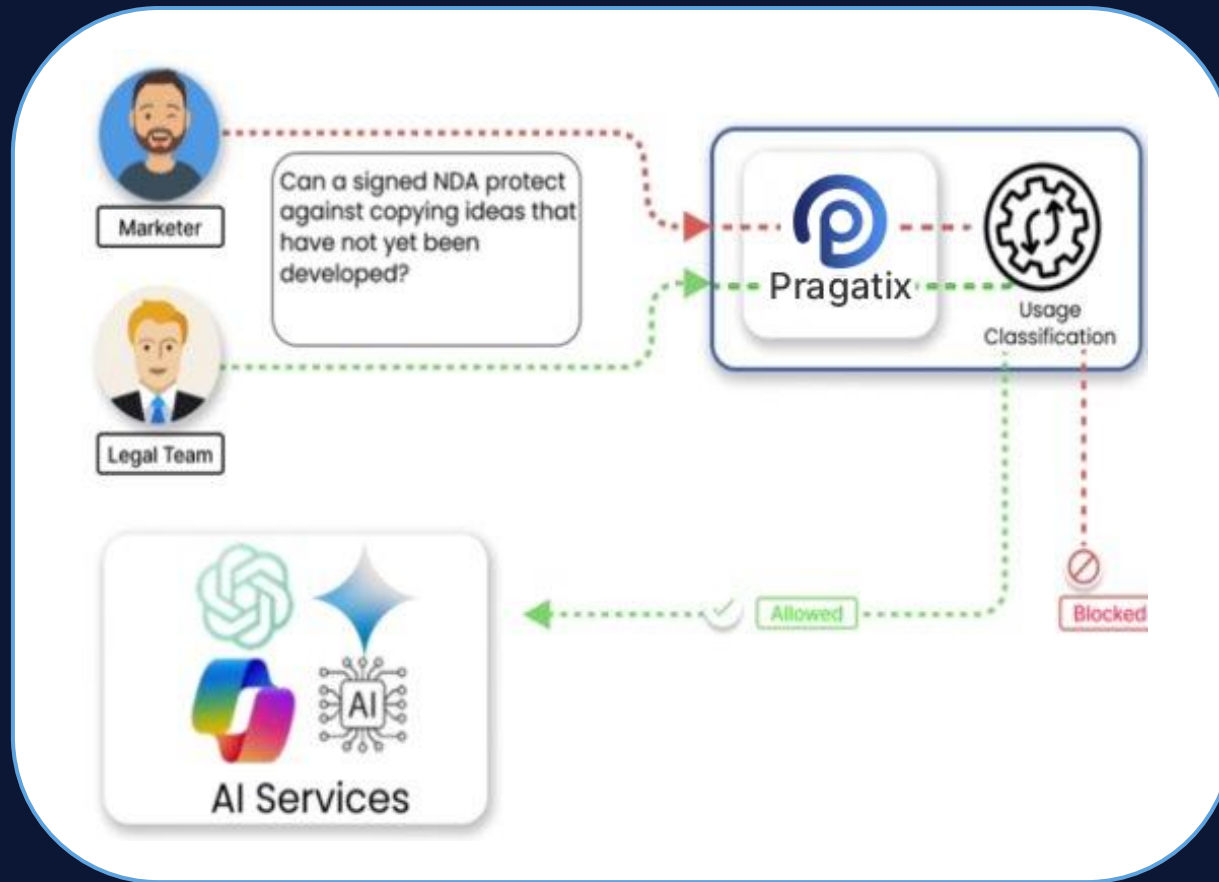
ChatGPT can make mistakes. Consider checking important information.



Guardrails – Who can do what?

Set policies:

Define rules to govern AI usage, specifying what AI can be used for, and establishing control over prompts and responses..



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

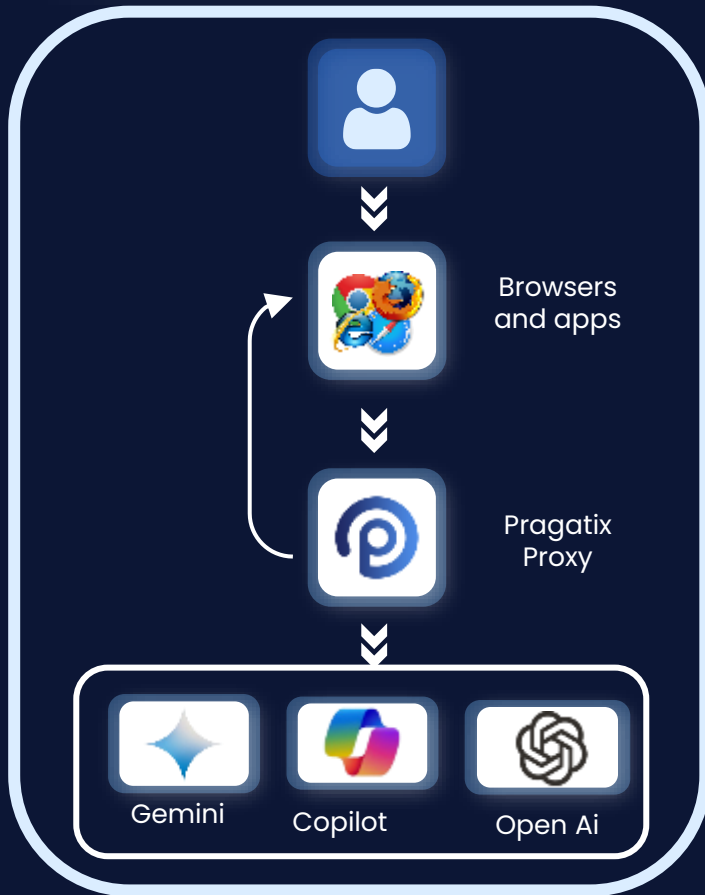


Deep Seek

Pragatix Firewall Dataflow Topologies

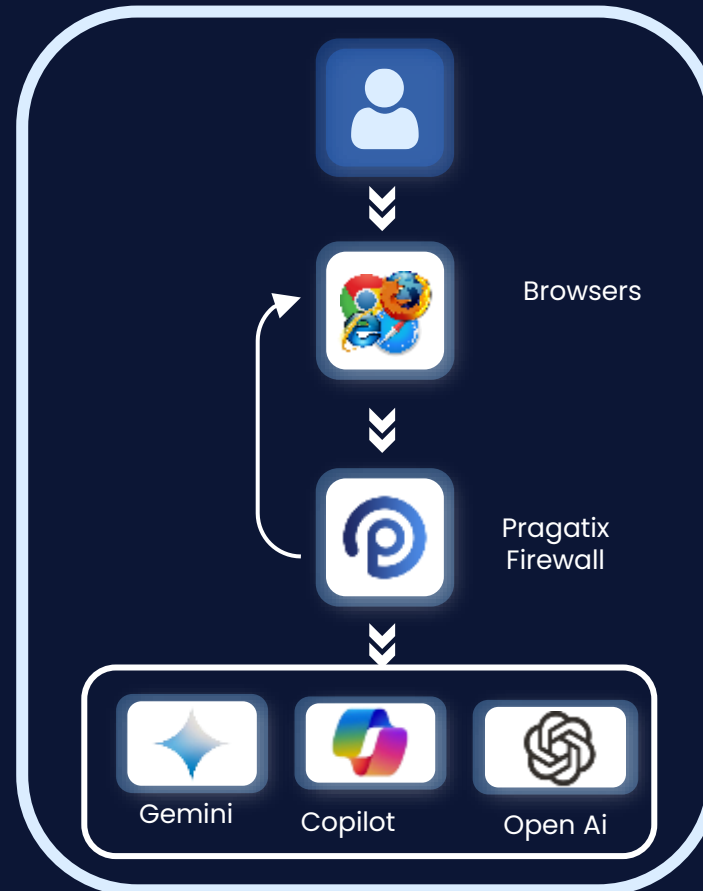


Network Proxy

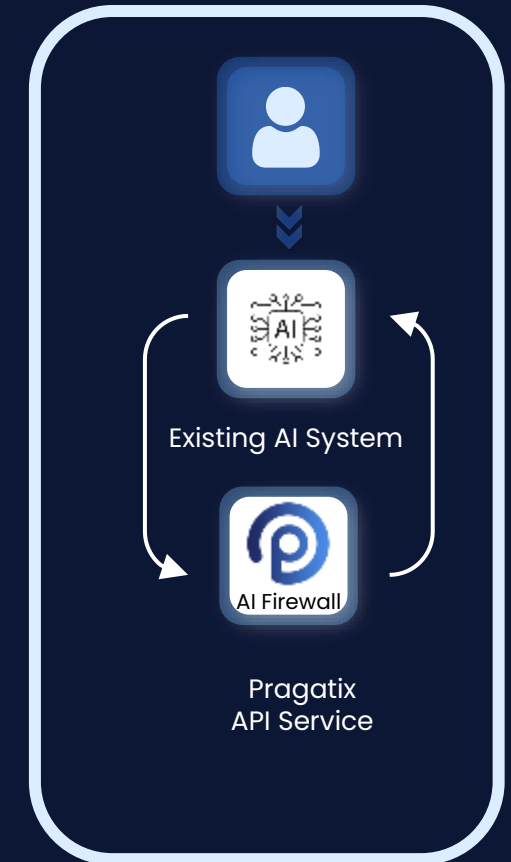


Forward traffic to Pragatix Proxy
Captures all browsers and applications

Browser Extension



Service API



Connect your AI system with
restAPI

PRAGATIX AI Suite



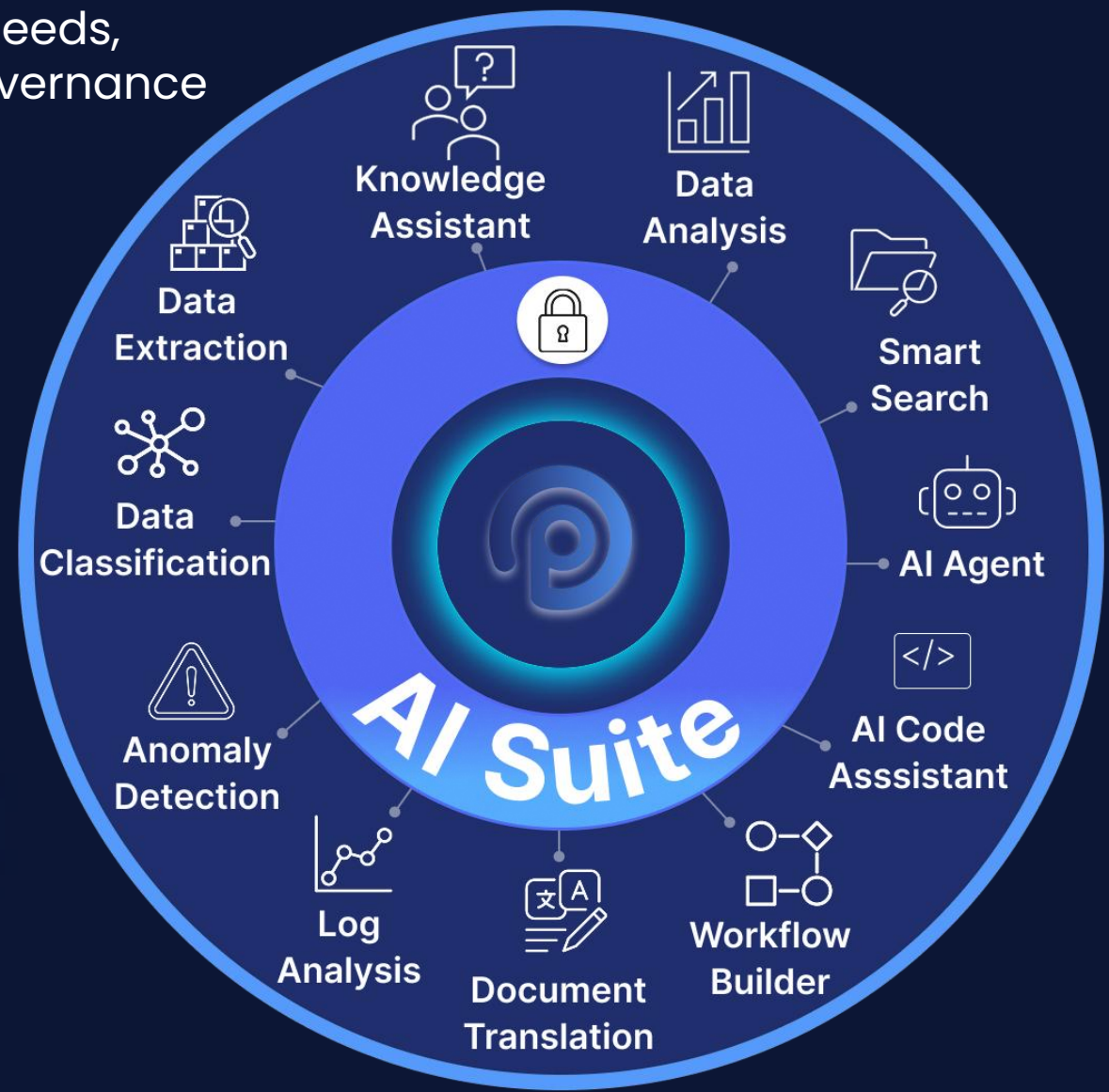


Pragatix Private AI Suite Core Modules

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

- Deployment On-premise, Air gapped and cloud VPC
- Grounding with Company Data
- Sync and Control Data Permission
- Enterprise Ready and Build
- Build with Security and Governance First Design

ZERO DATA EXPOSURE





Multi-model Support

LLM Model



Llama



AI21



Claude



Deep
Seek



Mistral
AI



GPT

Model Host



Fireworks



AWS
Bedrock



OpenAI



Private
cloud



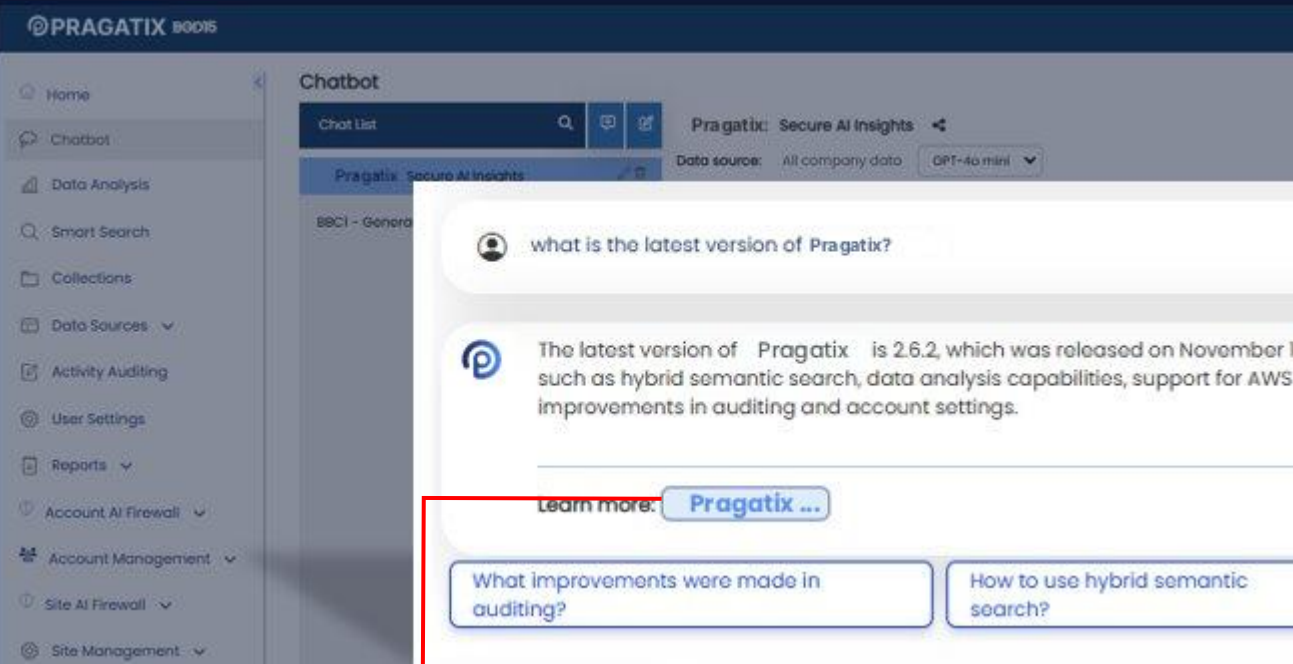
On
prem



Knowledge ASSISTANT

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

Admin can create domain expert chatbot with instructions on how to answer and how to ask.



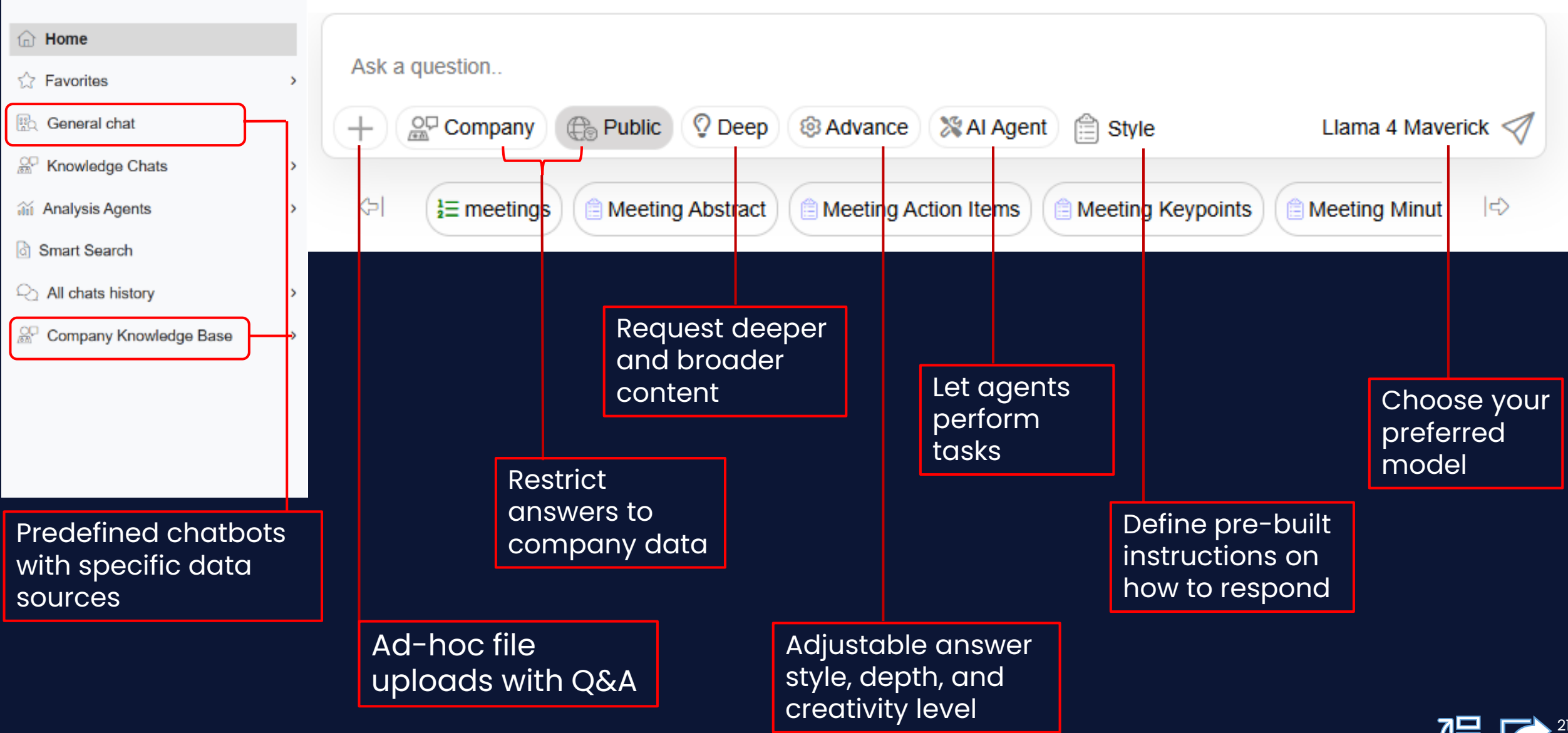
Grounding-company source



Pragatix Lite Mode



Pragatix AI Suite Chatbot Features



Data Analysis- Powered by AI Agents



Analyse data by asking questions in Natural Language

Ask in natural language

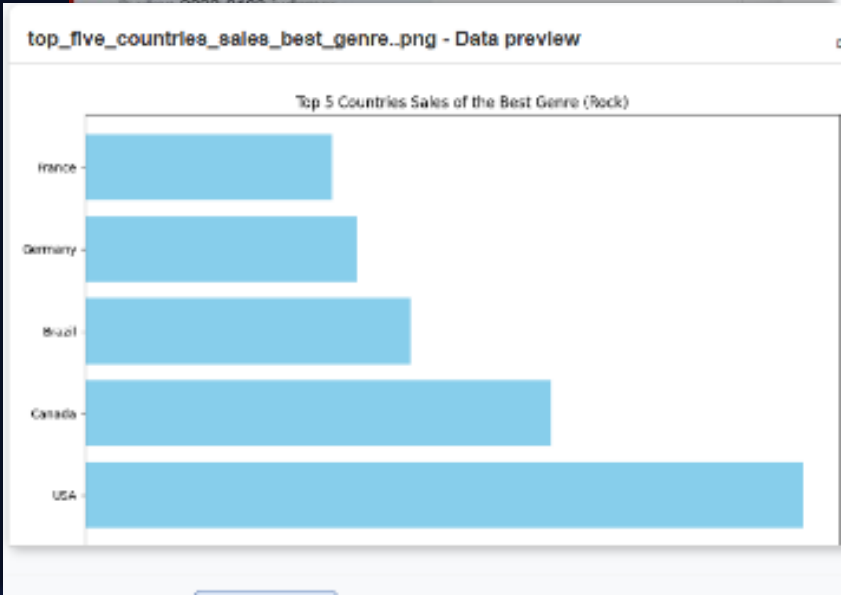
Home | Analysis chat history | most profitable genre | Data Analysis | 31/03/2025 14:29

Generate a report showing the most profitable genre in each country based on sales

View planning and steps

The file contains 24 rows, summarizing the most profitable genre for various countries based on total sales. For example, Argentina's most profitable genre is Latin with total sales of 91.06, while Brazil's is Rock with total sales of 691.02.

The 'most_profitable_genre_by_country.csv' file addresses your question by providing a clear overview of the most profitable music genres in different countries based on sales data. You can download it using the button below.



most_profitable_genre_by_country.csv - Data preview

Country	Genre	TotalSales
Argentina	Latin	91.06
Australia	Rock	170.28
Austria	Rock	203.4
Belgium	Rock	209.88
Brazil	Rock	691.02
Canada	Rock	989.03
Chile	Latin	91.06
Czech Republic	Rock	226.02
Denmark	Rock	219.78
Finland	Rock	159.29



Company Data Smart Search



Comprehensive search:

Retrieve company content search results through an AI and Keyword search.

Smart Search

Chat List

What marketing mat...

What Marketing PPT's ...

What marketing mat...

What marketing mat...

Show me contracts th...

partner contract with ...

h20

what contracts do we...

who are our customer...

h20

powerpoint

de-dsbudes <> AGAT ...

List reports including f...

Maximum Number of Items to Download 7

What

What marketing material do we have for SphereShield for MS Teams?

Download all 7 search results from here

Displaying top 5 results of 7:

Rank	File Name	Type
1	SphereShield for MS Teams presentation transcript.pdf	MicrosoftSharePointFile
2	SphereShield for Microsoft Teams.docx	MicrosoftSharePointFile
3	(OLD) Marketing general description - SphereShield for MS Teams.docx	MicrosoftSharePointFile
4	SphereShield for Microsoft Teams - Short.docx	MicrosoftSharePointFile
5	ms_teams_datasheet_301.pdf	MicrosoftSharePointFile

Showing 1 to 5 of 5 entries

Exact keyword match

ms_teams_datasheet_301.pdf

What marketing material do we have for SphereShield for MS teams?

ms teams datasheet 3.00

3 / 4 | 83%

SphereShield allows users to create granular policies based on external traffic, users, groups and Teams. Scan all the content used in MS Teams including Exchange, OneDrive and SharePoint.

Ethical Wall

SphereShield addresses many important

Contextual semantic match



Pragatix AI Agent Tools



Intelligent Document Processing

Extracts structured content from unstructured data



Powerful Translation

Preserve original formatting and layout



Image Analysis

Identify, classify, and extract insights from images



Image Generation

Create custom images from text prompts



Web Search

Automate web queries and summarize findings from multiple sources in real time.



Speech-to-Text Text-to-Speech

Convert spoken words into text or text into spoken words



AI Suite

AI Code Assistant

AI Code Assistant



Codebase Autocomplete

Automatically completes code, from single lines or full sections, in any language.

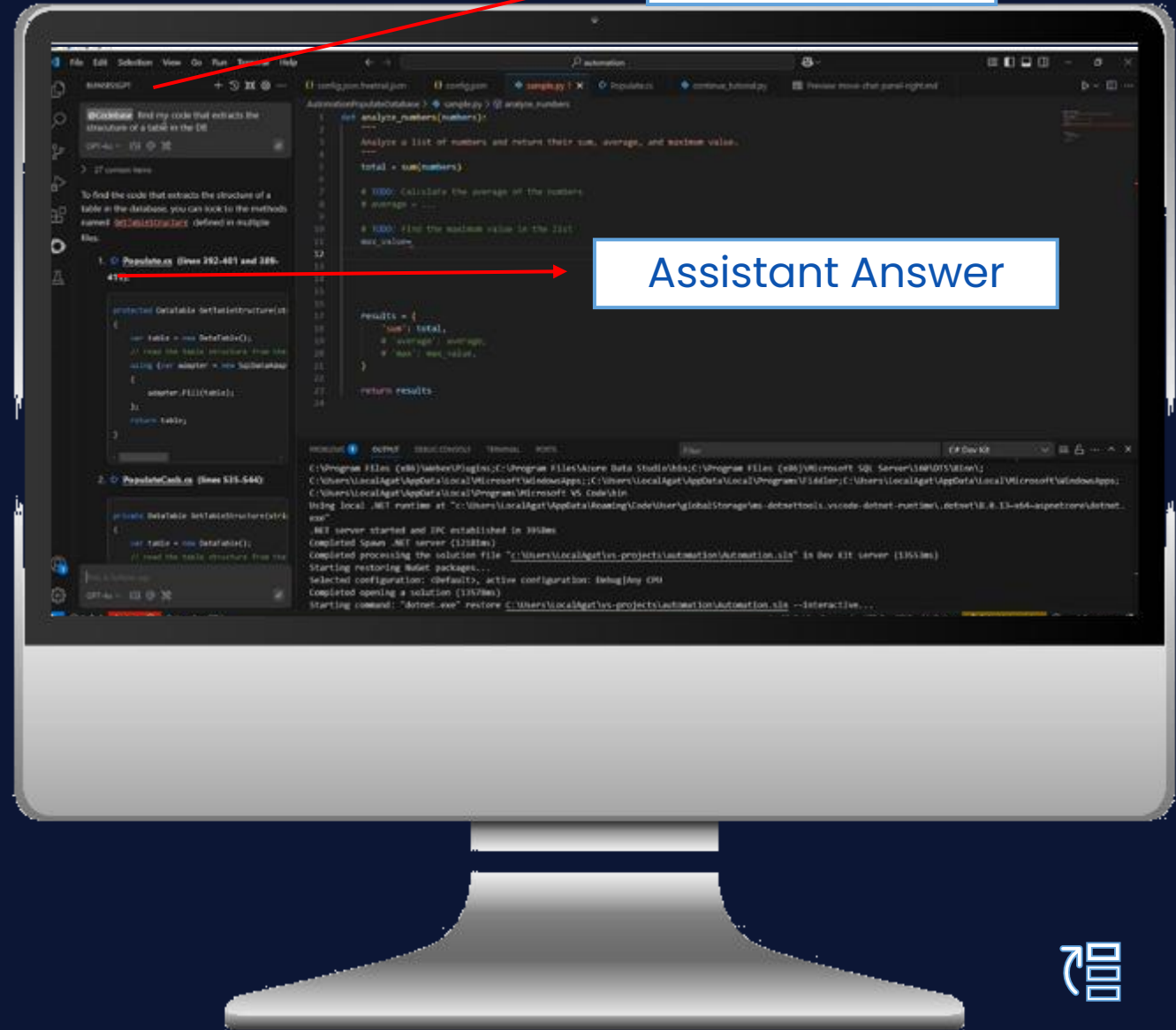


Codebase Q&A

Ask questions about your code and receive answers.

User Question

Assistant Answer





Thank You

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

Visit Us at AGATSoftware.com