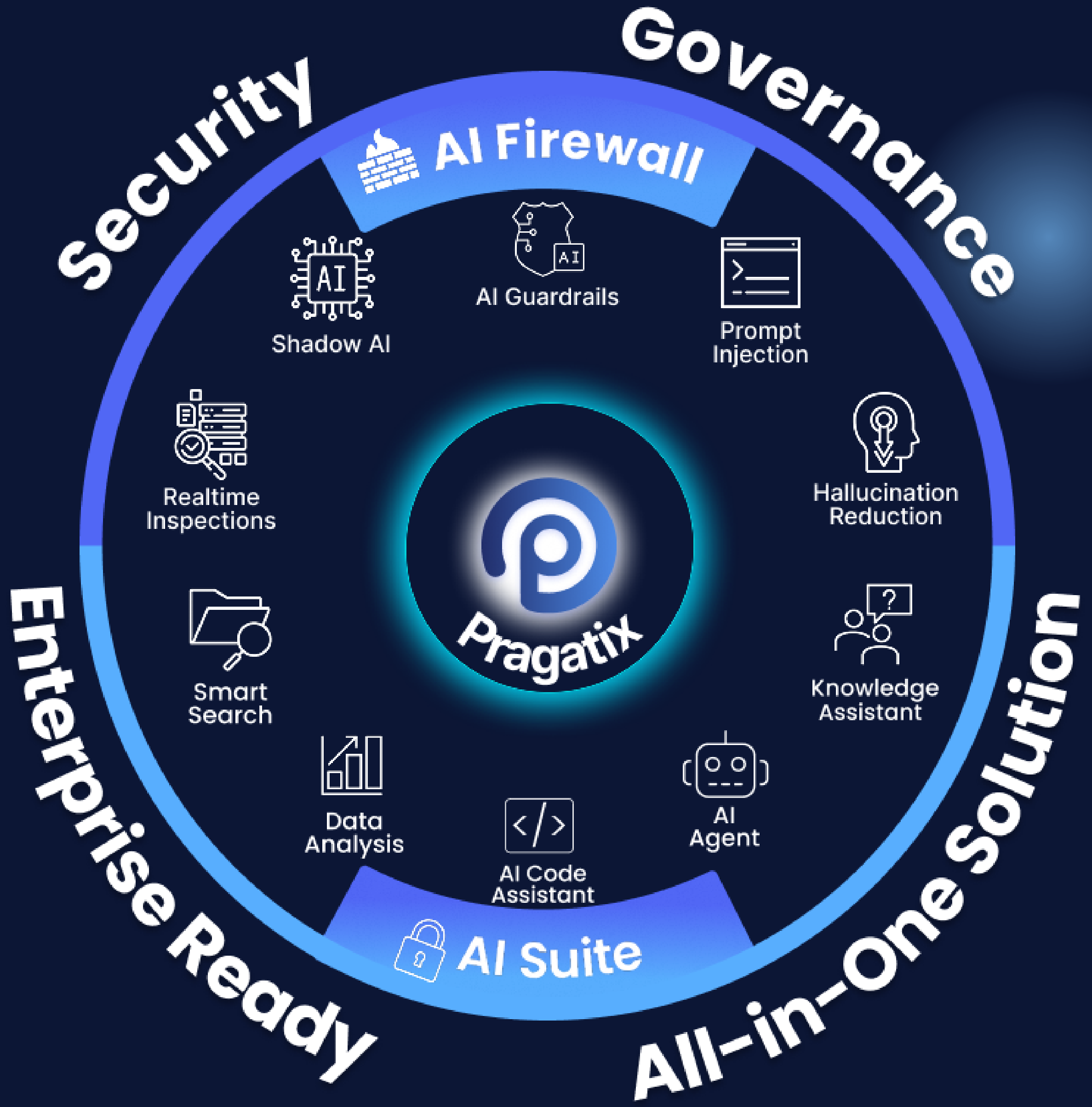
PRAGATIX
By AGAT Software

SECURITY FIRST AI PLATFORM

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

AGAT

Https://agatsoftware.com



Company Overview

AGAT

Security and Governance

Previous line of business

SphereShield
Collaboration

- ✓ Hundreds of customers, including 25 Fortune 500

Spin-off

Current Strategic Focus Shift

Pragatix
Generative AI

Serial founders with a previous technology exit to Symantec.

AT&T
KPMG
LISD
BTБ
MUFG
Shell
OPTUS
VISA
RBC
Belfius
ROLLS ROYCE
Swiss Re
BMO
T
AAA
ING
RENAULT
Fidelity
FedEx
orano
CREDIT SUISSE
Chevron Phillips
BAE SYSTEMS
afni
GENERAL DYNAMICS
kaspersky
SITECORE
BANCA D'ITALIA
NORTHERN TRUST
Weightmans
Applied
L3HARRIS
leidos
LITERA
Morgan Lewis
GLENCORE
Amundi
World Learning
Cascadia HEALTH
groupe mutuel
PIRELLI
vodafone
ACACIA
Scotiabank

Founded in 2013

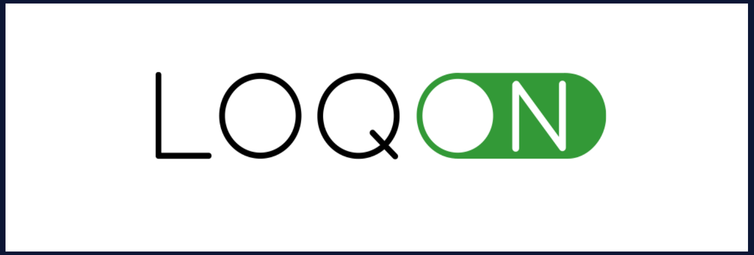
Seed - March 2023

24 Employees

Offices in Israel & South Africa

Pragatix Customer Logos

Peterson
DELIVERING A WORLD OF GOOD TASTE
EST. 1947



Gemeente
Bunschoten

The Problem

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

A lack of **visibility and control** over the use of public AI service by employees creates significant security and business risks.

Solution Overview: End-to-end AI Platform

PRAGATIX

Security First AI Platform

No Risks

Local AI Services

PRAGATIX AI Suite

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

Enterprise AI service to use and build

Managed Risks

AI Services Inspect and Control

PRAGATIX AI Firewall

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

Real-time Proxy control

PRAGATIX
AI Firewall

Gemini

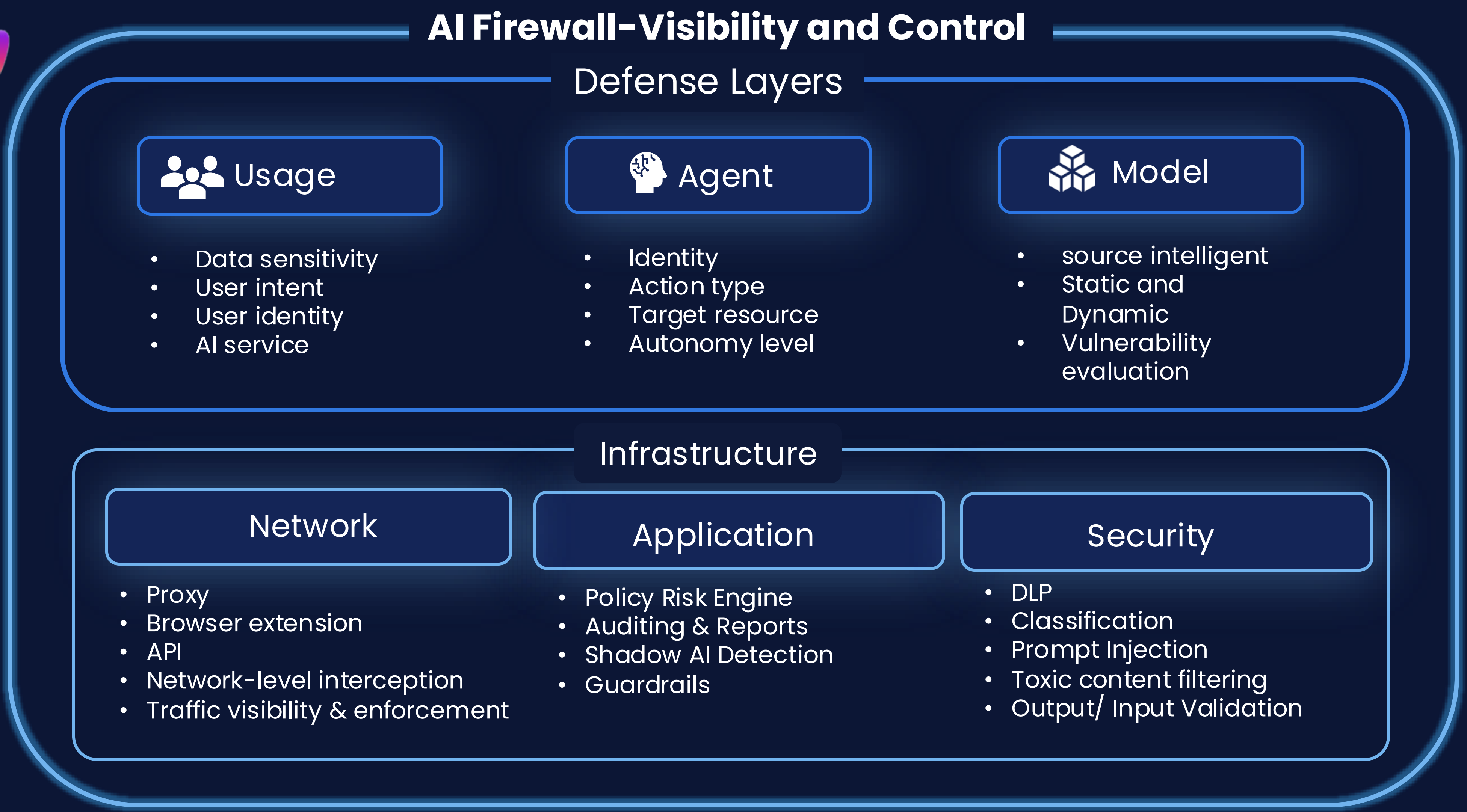
ChatGPT

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



AI Firewall-Visibility and Control

Defense Layers

Usage

- Data sensitivity
- User intent
- User identity
- AI service

Agent

- Identity
- Action type
- Target resource
- Autonomy level

Model

- source intelligent
- Static and Dynamic
- Vulnerability evaluation

Infrastructure

Network

- Proxy
- Browser extension
- API
- Network-level interception
- Traffic visibility & enforcement

Application

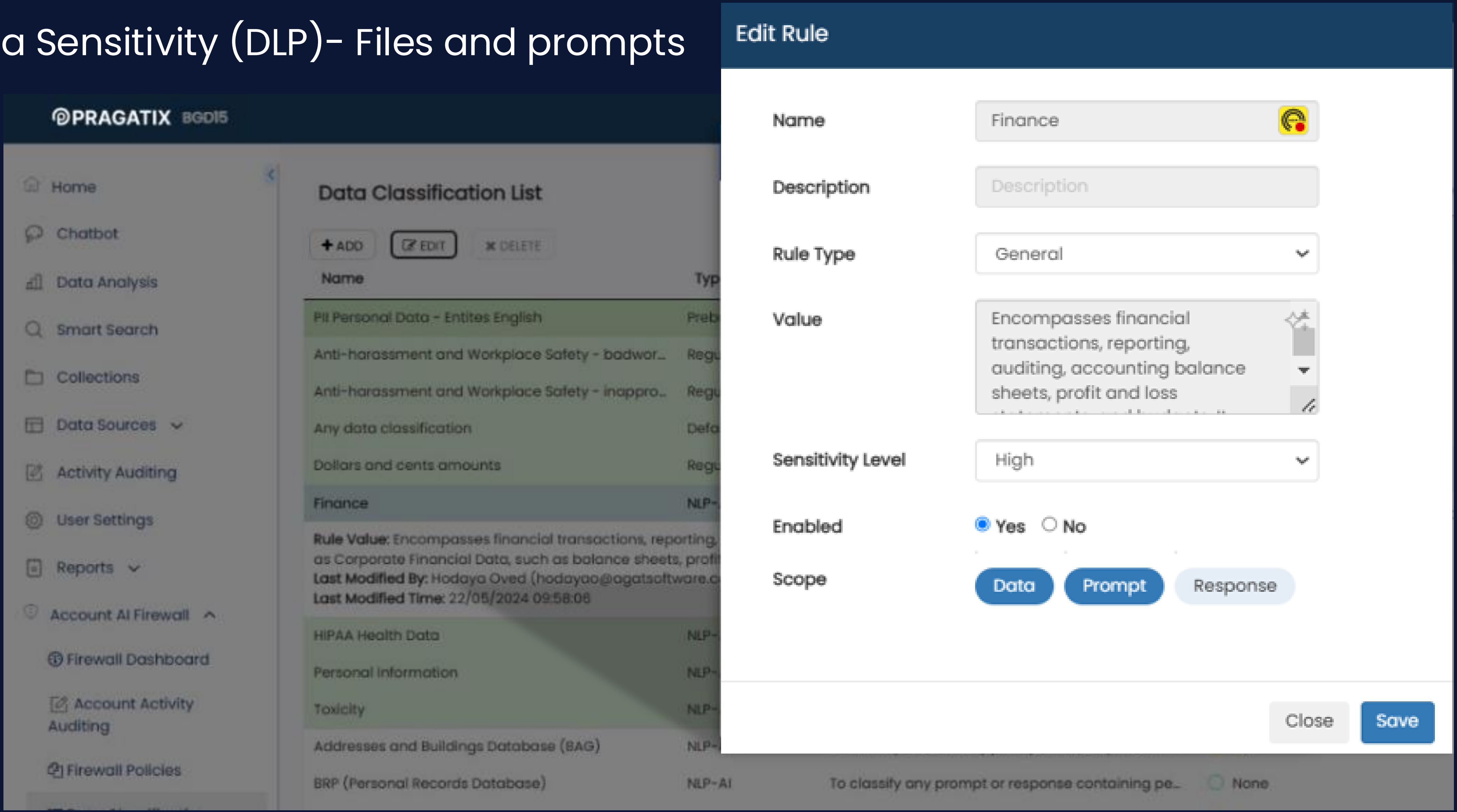
- Policy Risk Engine
- Auditing & Reports
- Shadow AI Detection
- Guardrails

Security

- DLP
- Classification
- Prompt Injection
- Toxic content filtering
- Output/ Input Validation

Data classification

Data Sensitivity (DLP)- Files and prompts



Data Classification List

Name	Typ		
PII Personal Data - Entites English	Preb		
Anti-harassment and Workplace Safety - badwor...	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	To classify any prompt or response containing pe...	○ None

Rule Value: Encompasses financial transactions, reporting, as Corporate Financial Data, such as balance sheets, profi
Last Modified By: Hodaya Oved (hodayao@agatsoftware.c
Last Modified Time: 22/05/2024 09:58:06

Edit Rule

Name: Finance

Description: Description

Rule Type: General

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

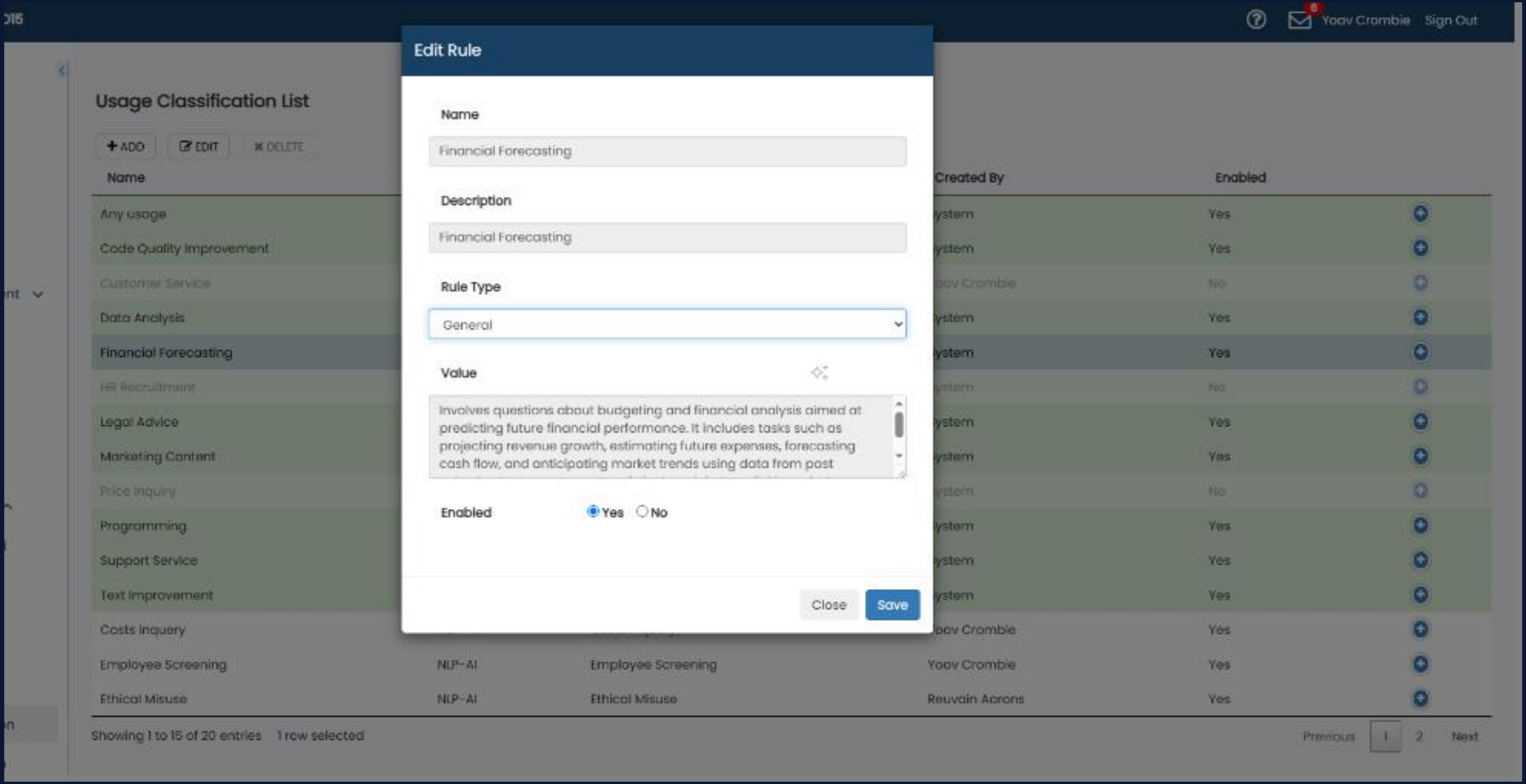
Sensitivity Level: High

Enabled: ● Yes ○ No

Scope: Data Prompt Response

Usage classification

User intent – what is the AI used for



Usage Classification List

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

Showing 1 to 15 of 20 entries 1 row selected

Edit Rule

Name: Financial Forecasting

Description: Financial Forecasting

Rule Type: General

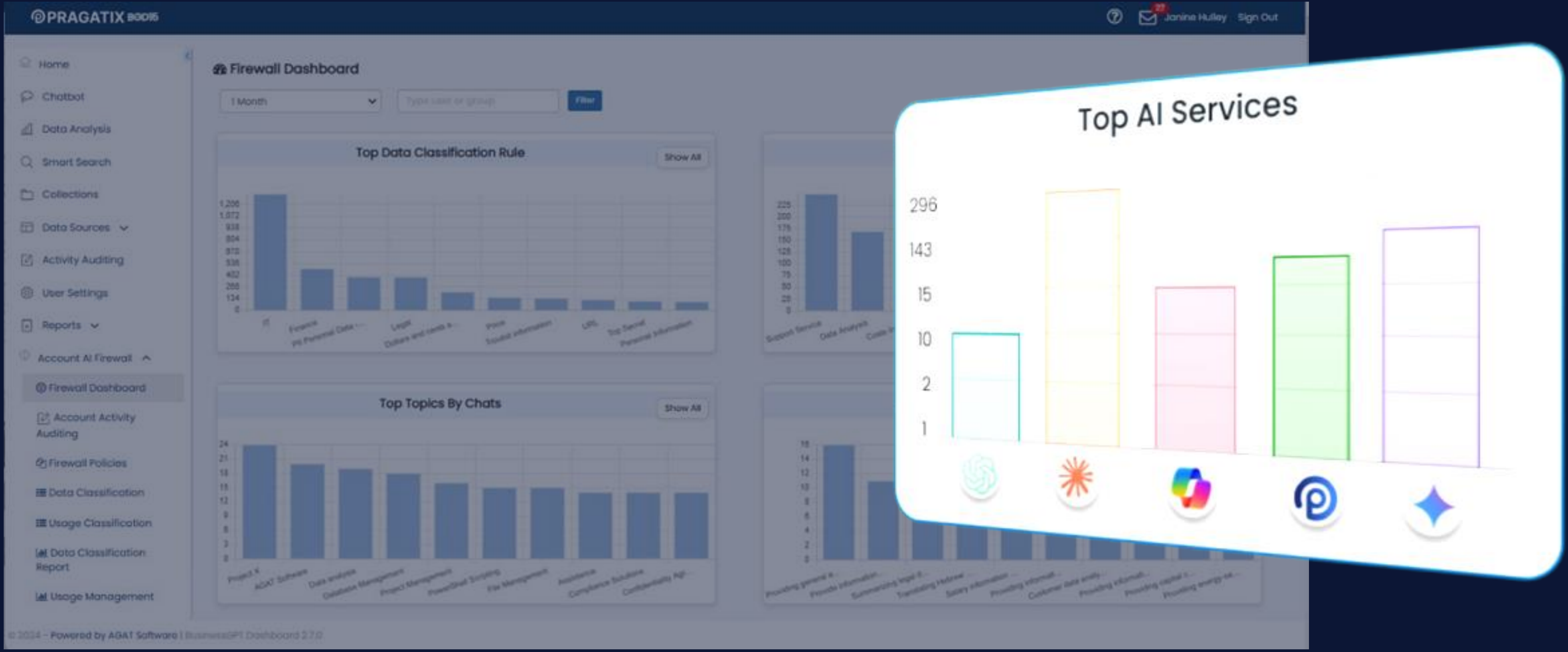
Value: Involves questions about budgeting and financial analysis aimed at predicting future financial performance. It includes tasks such as projecting revenue growth, estimating future expenses, forecasting cash flow, and anticipating market trends using data from past

Enabled ● Yes ○ No

Which AI Services are used

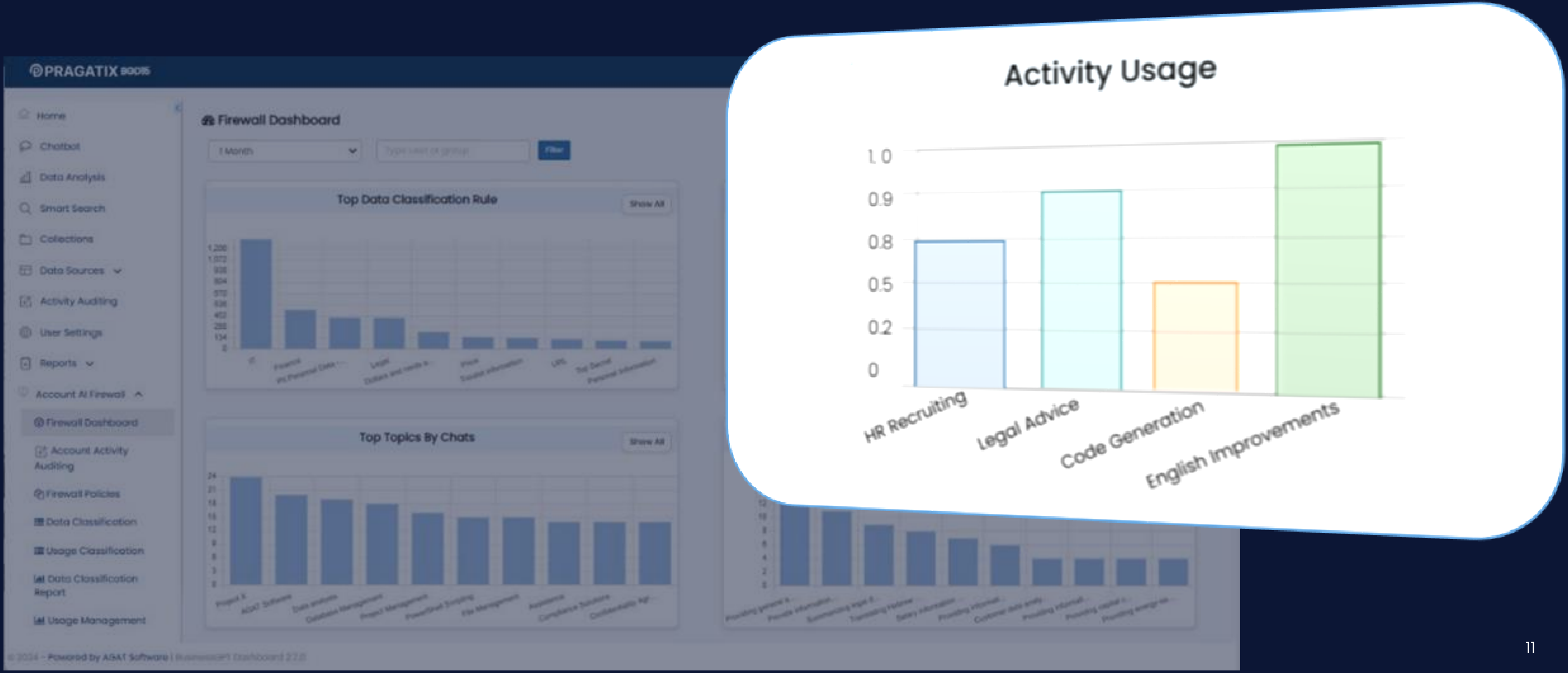
Manage AI Usage - Handle Shadow AI

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

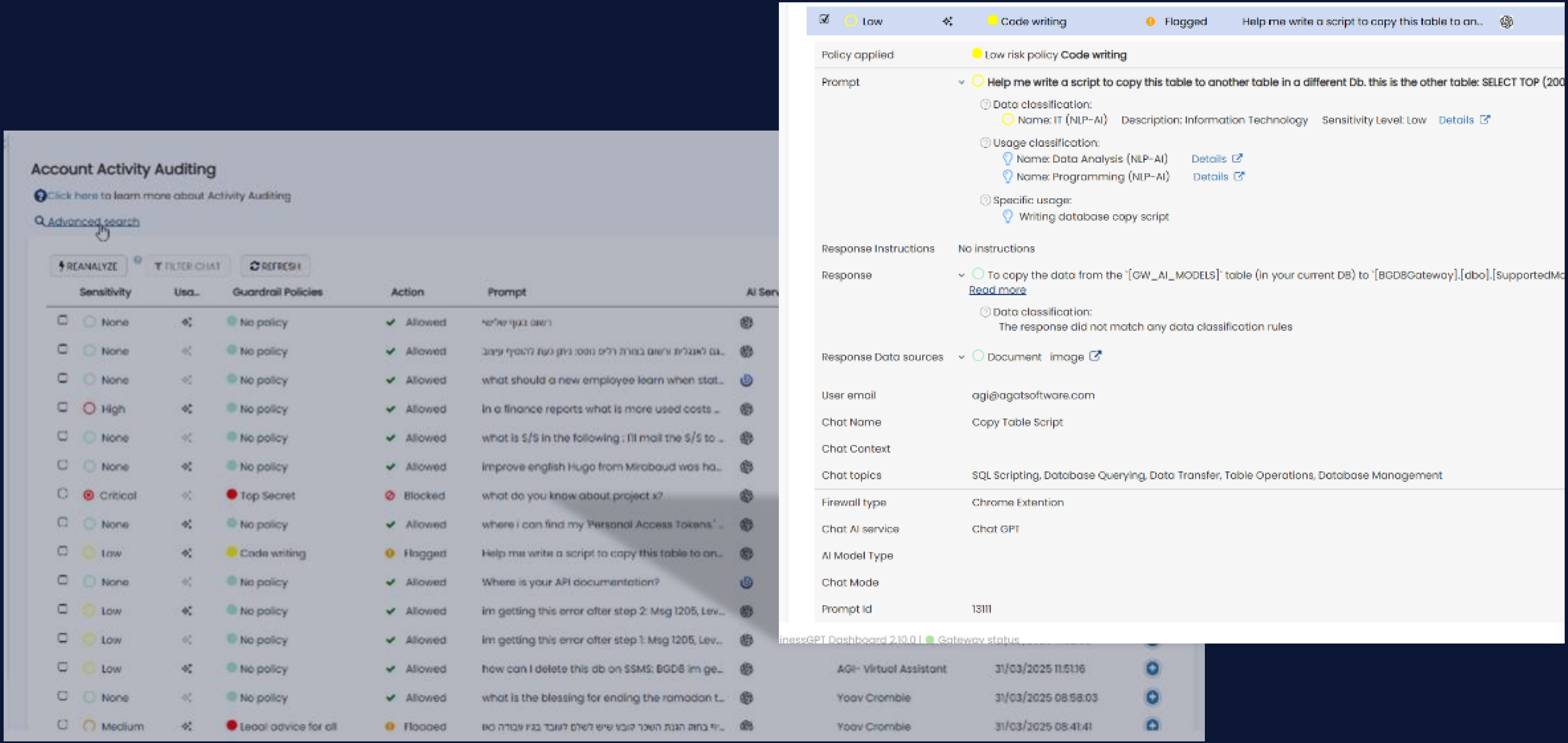


What AI is used for

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



Account Activity Auditing



Account Activity Auditing

Click here to learn more about Activity Auditing

Advanced search

	Sensitivity	Usa..	Guardrail Policies	Action	Prompt	AI Serv			
☐	None		No policy	✓ Allowed	רשום בגוף שלישי				
☐	None		No policy	✓ Allowed	גם לאנגלית ורשום בצורה רליס נוסף: ניתן כעת להוסיף 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..		AGI- Virtual Assistant	31/03/2025 11:51:16	
☐	None		No policy	✓ Allowed	what is the blessing for ending the ramadan t..		Yoav Crombie	31/03/2025 08:58:03	
☐	Medium		Legal advice for all	Flagged	בחוק הגנת השכר קובע שיש לשלם לעובד בגין עבודה אם..		Yoav Crombie	31/03/2025 08:41:41	

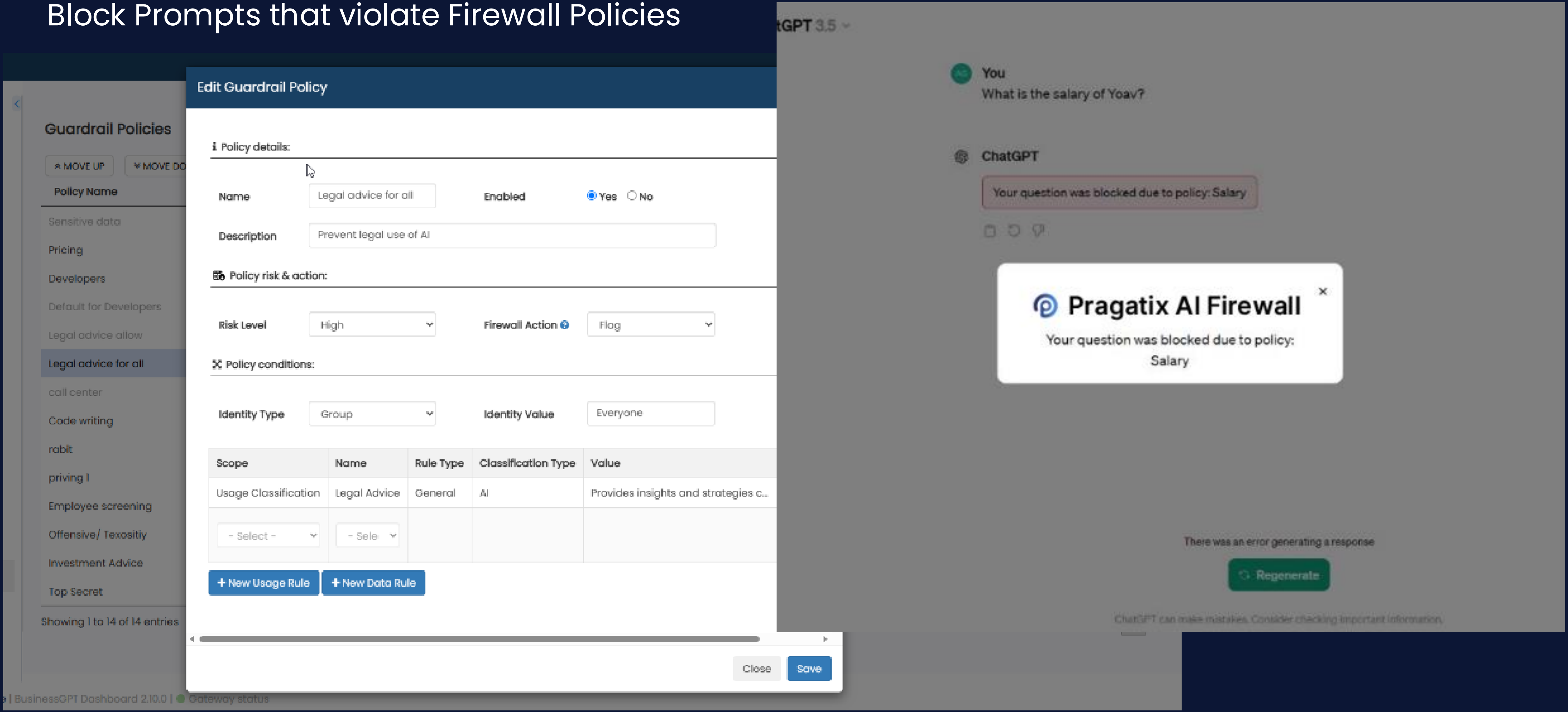
inessGPT Dashboard 2.10.0 | Gateway status

☑	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].[SupportedMo Read more Data classification: The response did not match any data classification rules
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

Guardrail Policy

Block Prompts that violate Firewall Policies



Guardrail Policies

Policy Name
Sensitive data
Pricing
Developers
Default for Developers
Legal advice allow
Legal advice for all
call center
Code writing
rabit
priving I
Employee screening
Offensive/ Texositiy
Investment Advice
Top Secret

Showing 1 to 14 of 14 entries

| BusinessGPT Dashboard 2.10.0 | Gateway status

Edit Guardrail Policy

ℹ 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			

tGPT 3.5

You
What is the salary of Yoav?

ChatGPT
Your question was blocked due to policy: Salary

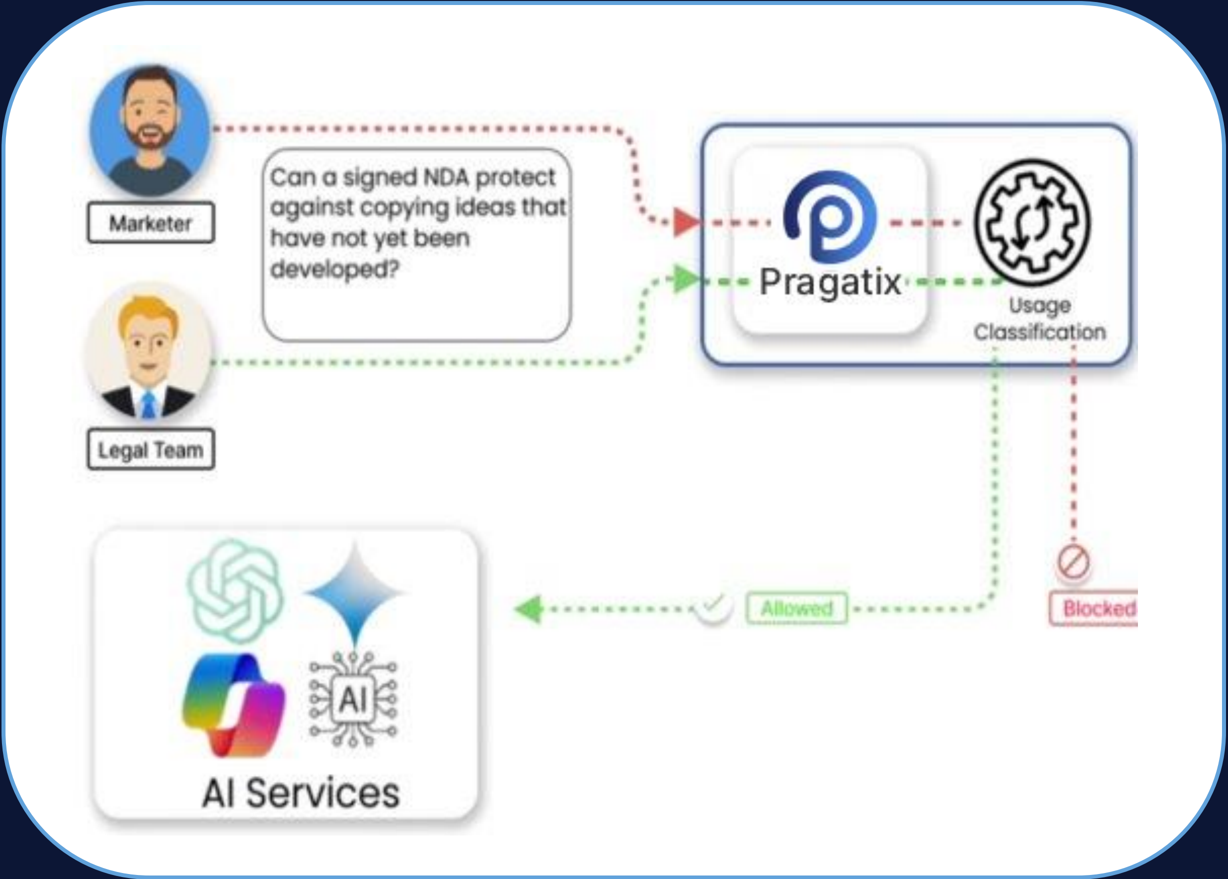
Pragatix AI Firewall
Your question was blocked due to policy: Salary

There was an error generating a response

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..


Marketer
Can a signed NDA protect against copying ideas that have not yet been developed?
Legal Team
Pragatix
Usage Classification
Allowed
Blocked
AI
AI Services

Pragatix Firewall Supported services

ChatGPT (web/app)
by OpenAI

Copilot (web/app)
By Microsoft

Gemini
by Google

AI21

Jamba
By AI21 Labs

Claude
AI by Anthropic

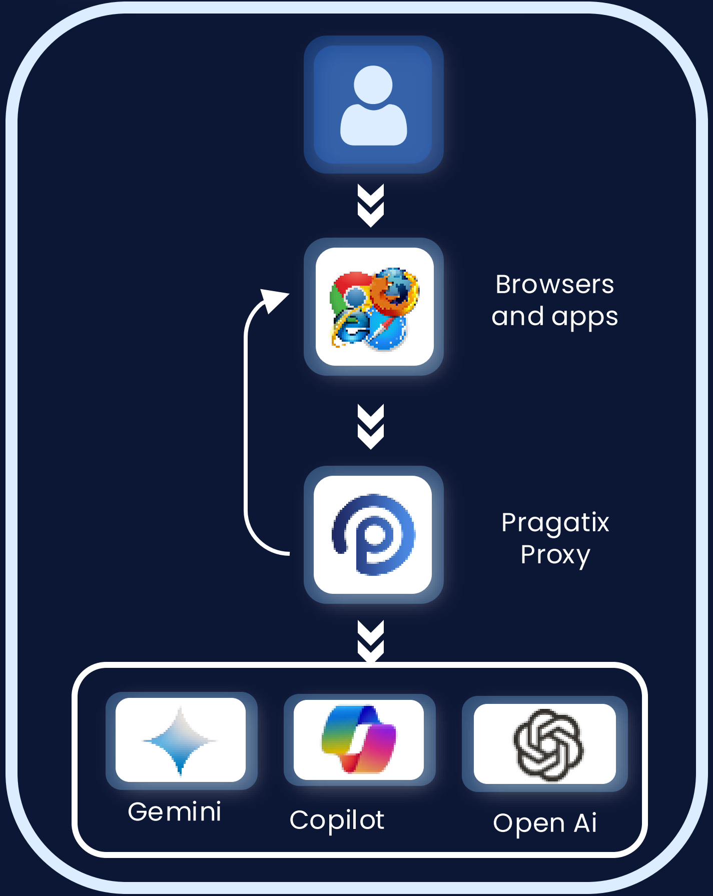
Grok

Perplexity

Deep Seek

Pragatix Firewall Dataflow Topologies

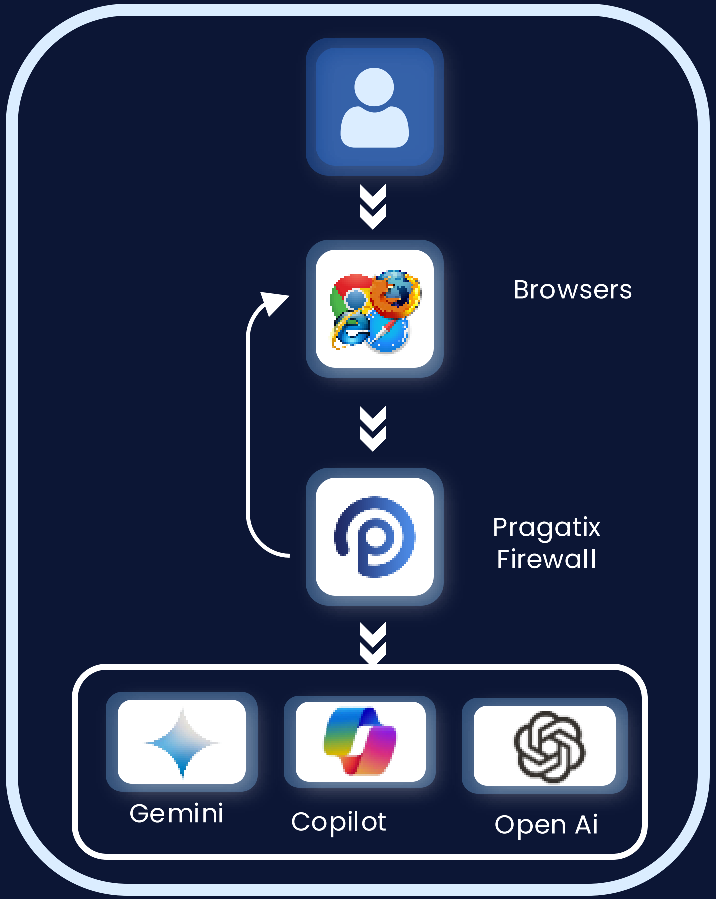
Network Proxy



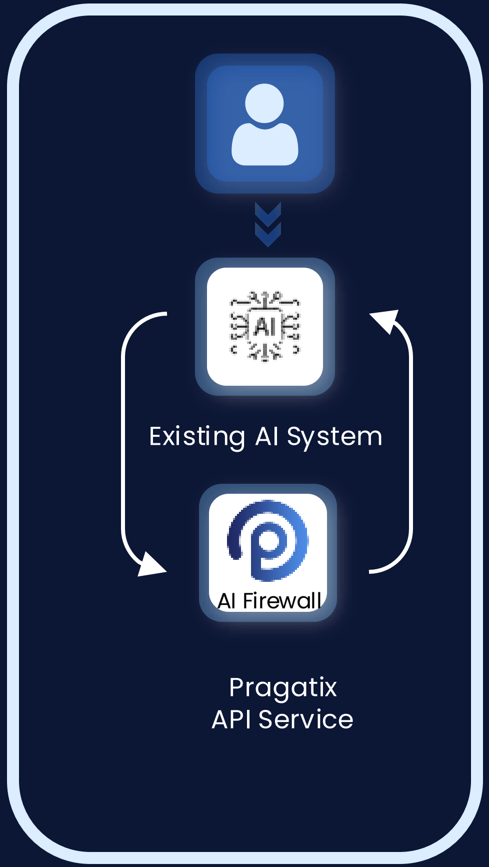
Forward traffic to Pragatix Proxy

Captures all browsers and applications

Browser Extension



Service API



Connect your AI system with restAPI

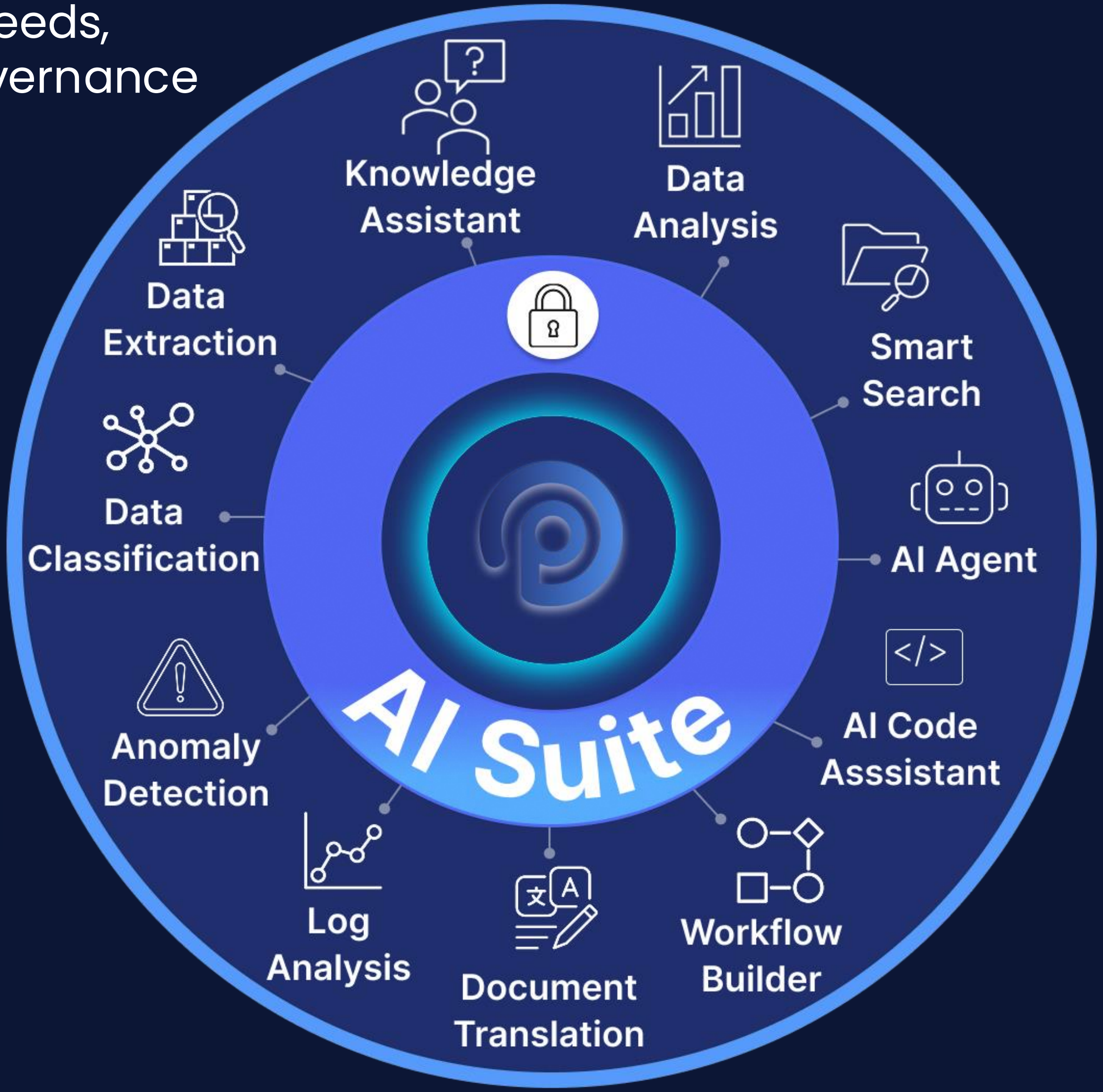
PRAGATIX
AI Suite

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

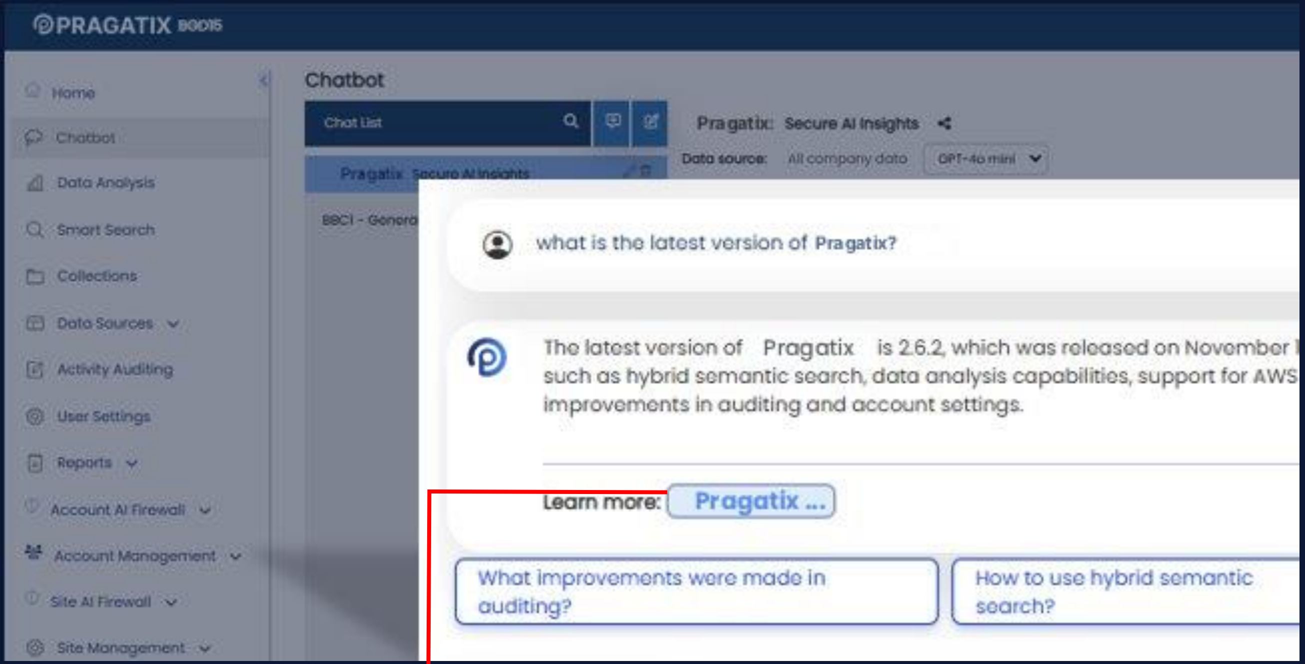
Model Host

- 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.



Pragatix: Secure AI Insights

Data source: All company data   GPT-4o mini

what is the latest version of Pragatix?

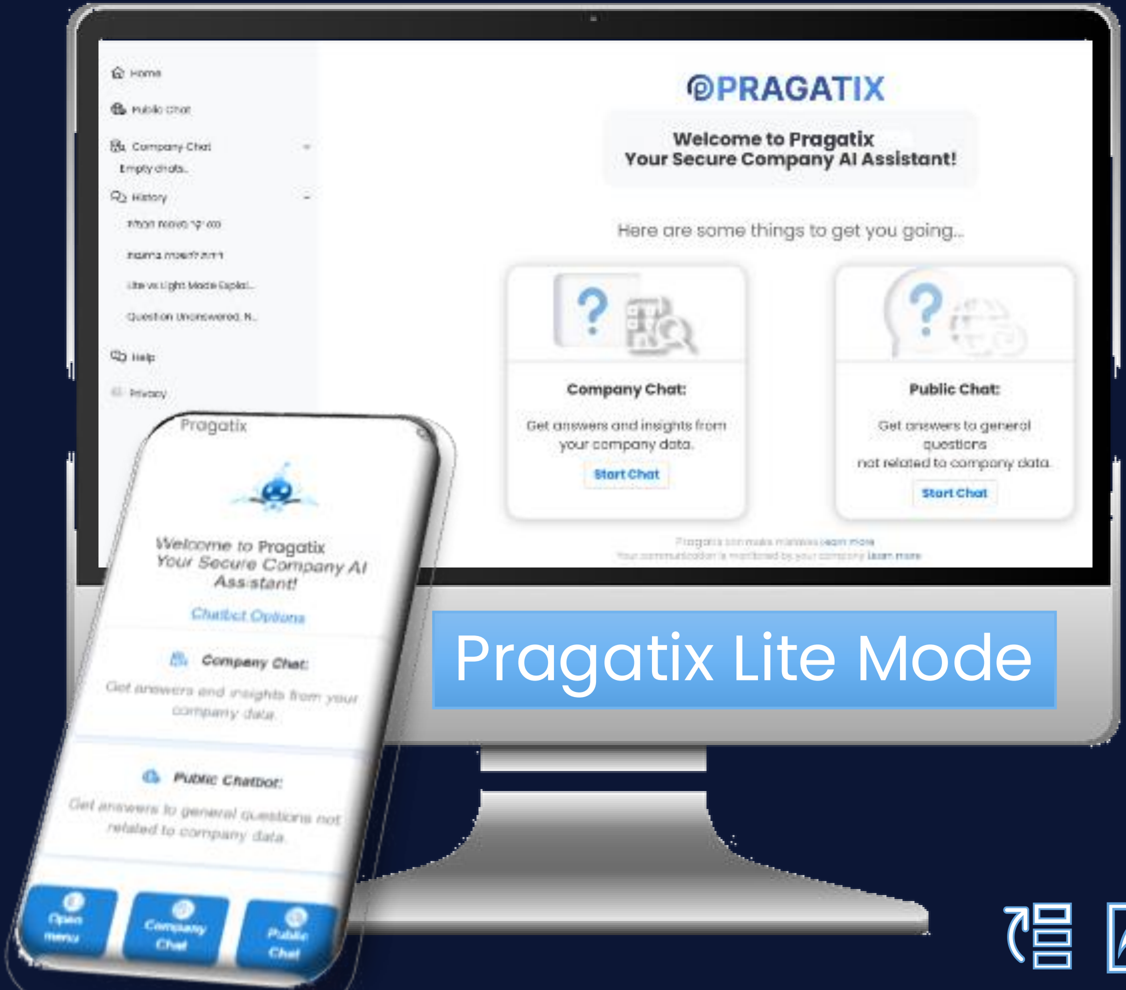
The latest version of Pragatix is 2.6.2, which was released on November
such as hybrid semantic search, data analysis capabilities, support for AWS
improvements in auditing and account settings.

Learn more: Pragatix ...

What improvements were made in auditing?

How to use hybrid semantic search?

Grounding-
company source



PRAGATIX

Welcome to Pragatix
Your Secure Company AI Assistant!

Here are some things to get you going...

Company Chat:
Get answers and insights from your company data.
Start Chat

Public Chat:
Get answers to general questions
not related to company data.
Start Chat

Pragatix

Welcome to Pragatix
Your Secure Company AI Assistant!

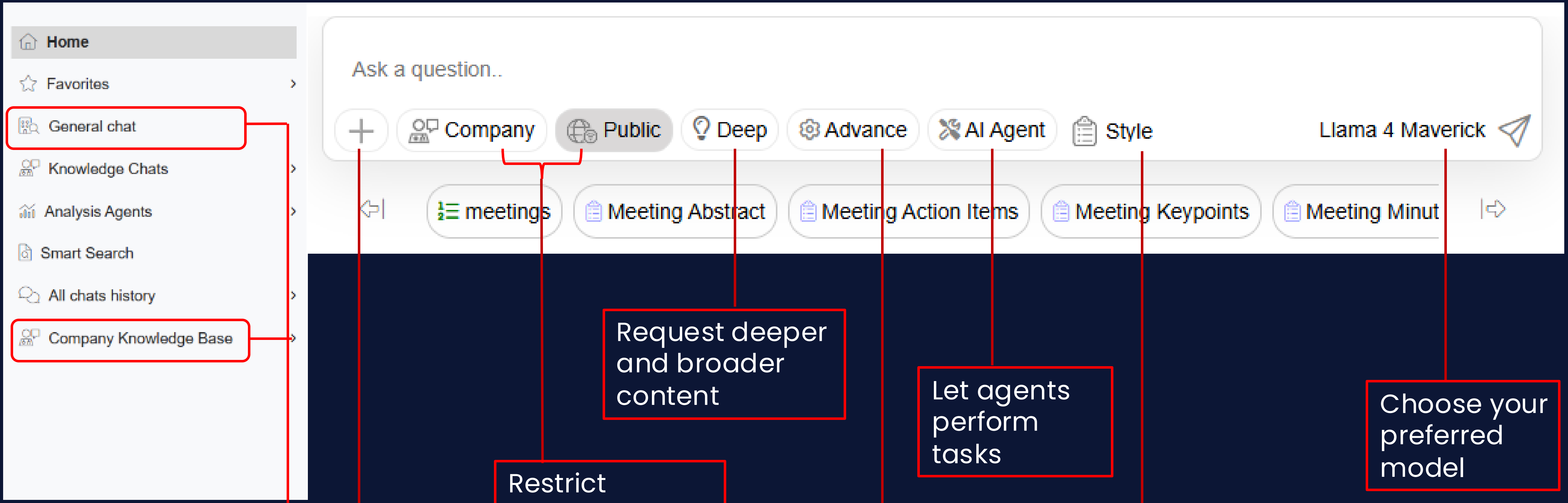
Chatbot Options

Company Chat:
Get answers and insights from your company data.

Public Chatbot:
Get answers to general questions not related to company data.

Pragatix Lite Mode

Pragatix AI Suite Chatbot Features



Predefined chatbots with specific data sources

Ad-hoc file uploads with Q&A

Restrict answers to company data

Request deeper and broader content

Adjustable answer style, depth, and creativity level

Let agents perform tasks

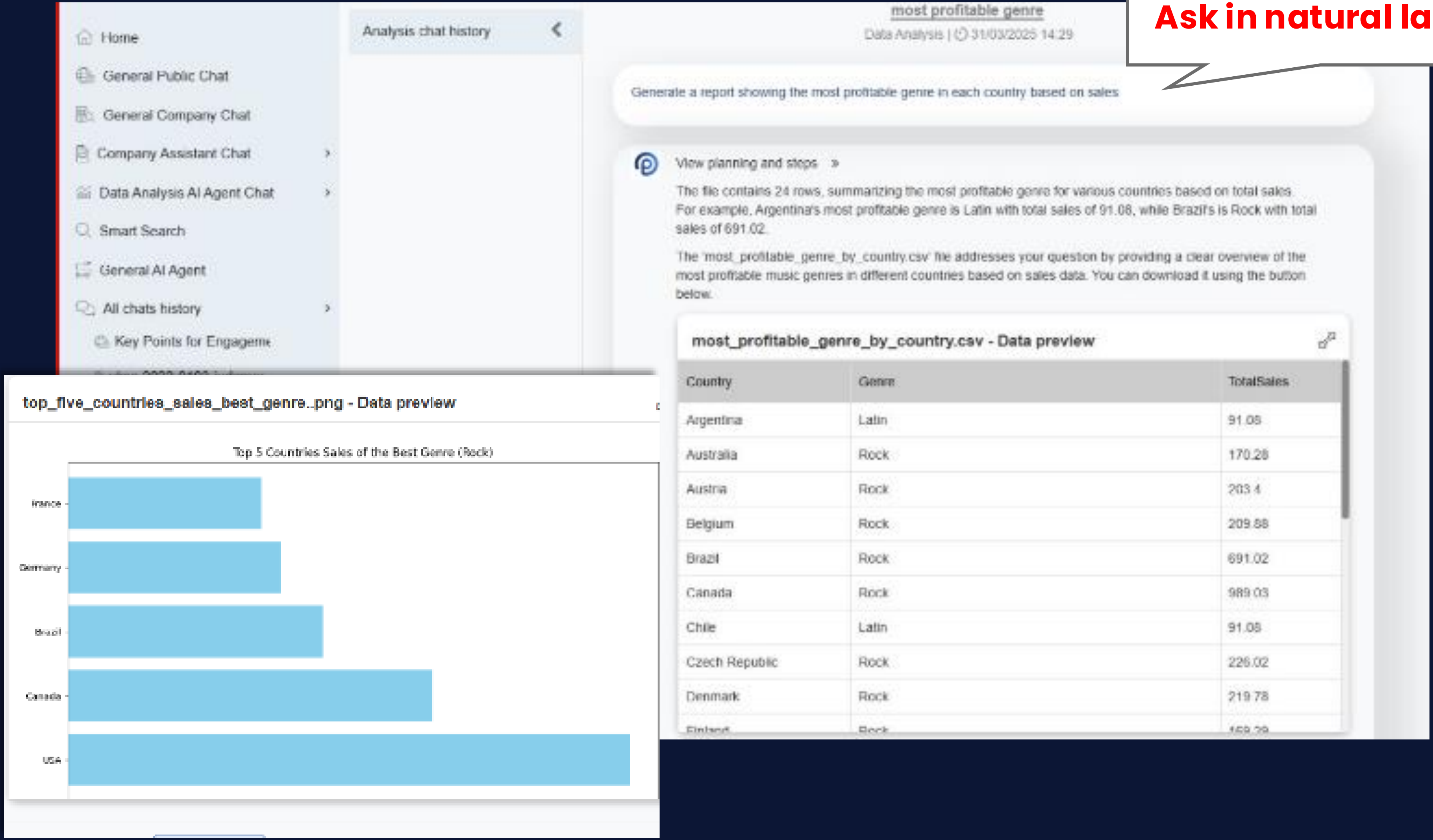
Define pre-built instructions on how to respond

Choose your preferred model

Data Analysis- Powered by AI Agents

Analyse data by asking questions in Natural Language

Ask in natural language



most profitable genre

Data Analysis | 31/03/2025 14:29

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

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 91.08, 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.

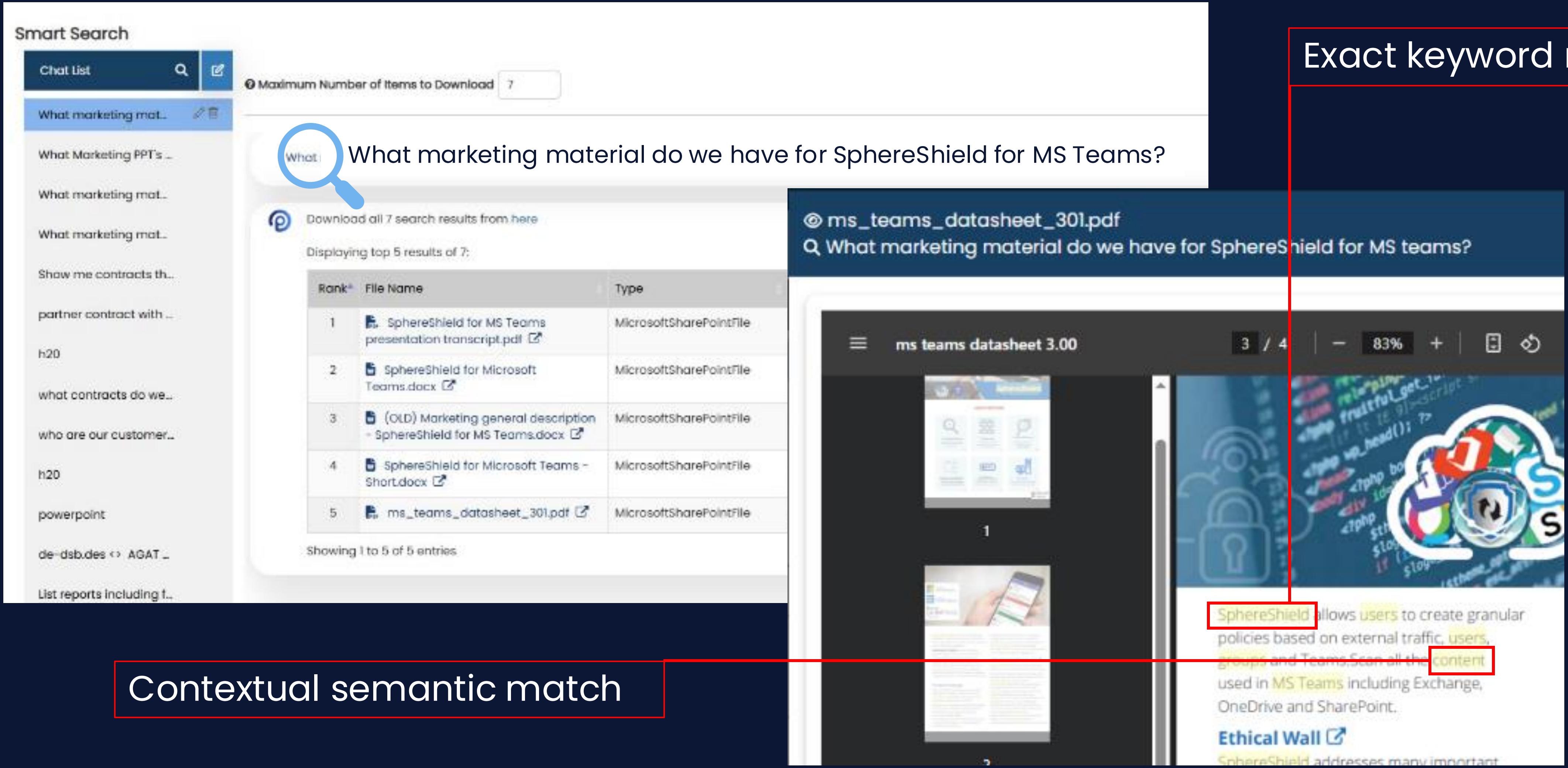
most_profitable_genre_by_country.csv - Data preview

Country	Genre	TotalSales
Argentina	Latin	91.08
Australia	Rock	170.28
Austria	Rock	203.4
Belgium	Rock	209.88
Brazil	Rock	691.02
Canada	Rock	989.03
Chile	Latin	91.08
Czech Republic	Rock	226.02
Denmark	Rock	219.78
Finland	Rock	169.29

top_five_countries_sales_best_genre..png - Data preview

Company Data Smart Search

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



Smart Search

Maximum Number of Items to Download 7

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

ms_teams_datasheet_301.pdf
What marketing material do we have for SphereShield for MS teams?

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

Exact keyword match

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

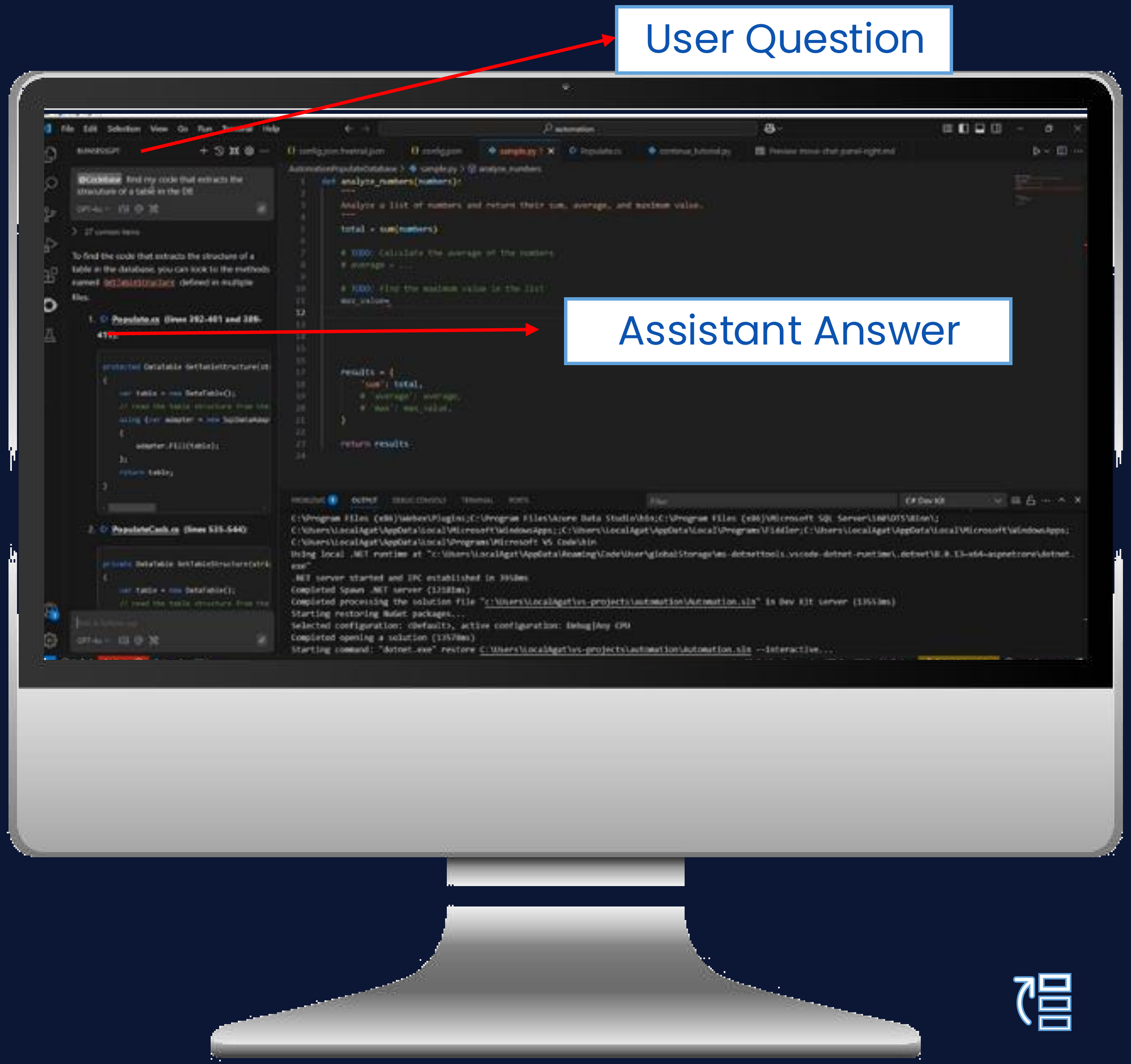
Convert spoken words into text or text into spoken words

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

@Codebase find my code that extracts the structure of a table in the DB

To find the code that extracts the structure of a table in the database, you can look to the methods named GetTableStructure defined in multiple files.

1. Populate.cs (lines 392-401 and 389-419):

```
protected DataTable GetTableStructure(st
{
    var table = new DataTable();
    // read the table structure from the
    using (var adapter = new SqlDataAdap
    {
        adapter.Fill(table);
    };
    return table;
}
```

2. PopulateCash.cs (lines 535-544)

```
private DataTable GetTableStructure(stri
{
    var table = new DataTable();
    // read the table structure from the
```

```
def analyze_numbers(numbers):
    """
    Analyze a list of numbers and return their sum, average, and maximum value.
    """
    total = sum(numbers)

    # TODO: Calculate the average of the numbers
    # average = ...

    # TODO: Find the maximum value in the list
    max_value=




    results = {
        'sum': total,
        # 'average': average,
        # 'max': max_value,
    }

    return results
```

```
C:\Program Files (x86)\Webex\Plugins;C:\Program Files\Azure Data Studio\bin;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;
C:\Users\LocalAgat\AppData\Local\Microsoft\WindowsApps;;C:\Users\LocalAgat\AppData\Local\Programs\Fiddler;C:\Users\LocalAgat\AppData\Local\Microsoft\WindowsApps;
C:\Users\LocalAgat\AppData\Local\Programs\Microsoft VS Code\bin
Using local .NET runtime at "c:\Users\LocalAgat\AppData\Roaming\Code\User\globalStorage\ms-dotnettools.vscode-dotnet-runtime\.dotnet\8.0.13-x64-aspnetcore\dotnet.
exe"
.NET server started and IPC established in 3958ms
Completed Spawn .NET server (12181ms)
Completed processing the solution file "c:\Users\LocalAgat\vs-projects\automation\Automation.sln" in Dev Kit server (13553ms)
Starting restoring NuGet packages...
Selected configuration: <Default>, active configuration: Debug|Any CPU
Completed opening a solution (13570ms)
Starting command: "dotnet.exe" restore C:\Users\LocalAgat\vs-projects\automation\Automation.sln --interactive...
```

Thank You

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

Visit Us at AGATSoftware.com