

The logo for DefenGPT, featuring a stylized 'X' icon with three stars above it, followed by the text 'DefenGPT' in a blue and purple font.

**Private AI Suite**

# DefenGPT Private AI Suite

The Secure, Private, On-Premise AI Solution for Regulated Industries

Intelligent Defence. Unmatched Resilience.

The logo for Defenix, featuring a stylized 'X' icon with three stars above it, followed by the text 'Defenix' in a blue and purple font, with the tagline 'Intelligent Defence. Unmatched Resilience' below it.

# The Enterprise AI Deadlock

## The Drive for Innovation



Modern enterprises require the transformative analytical power of large language models like ChatGPT, Copilot, and Gemini to remain competitive.



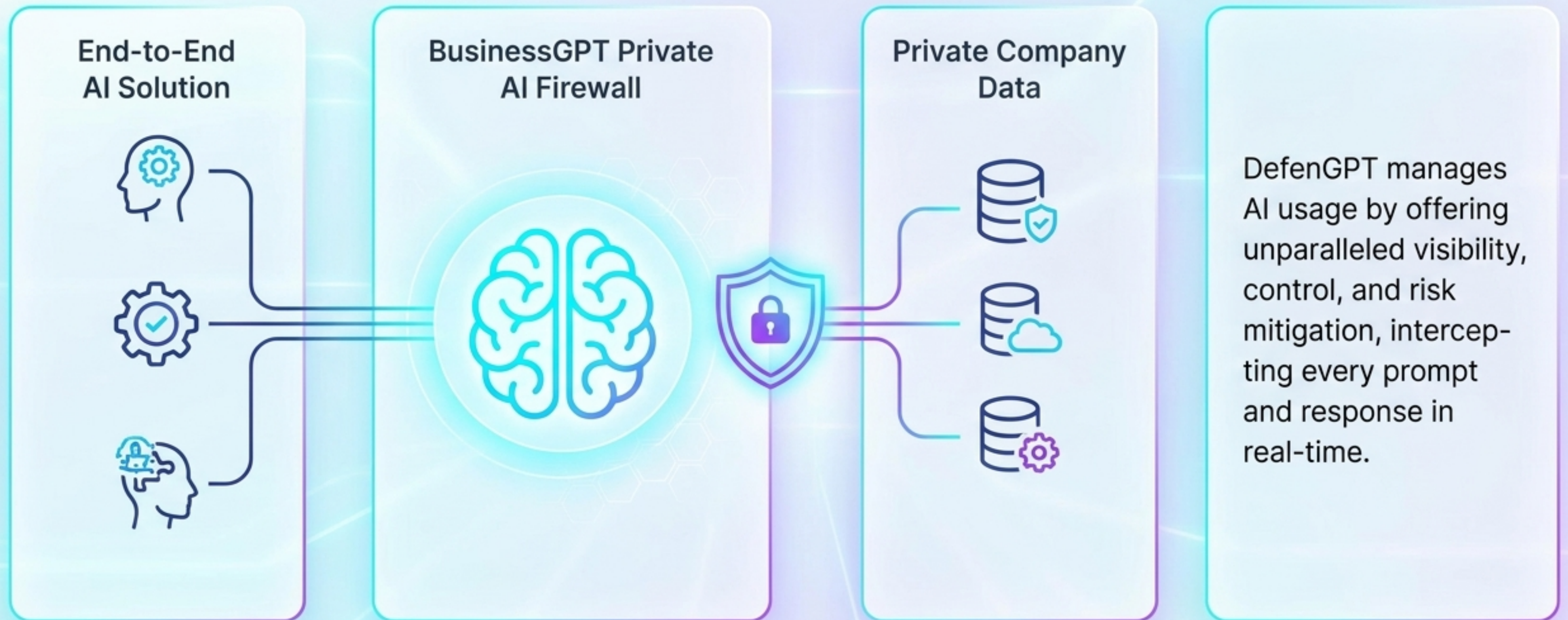
## The Wall of Regulation



Customers in regulated industries cannot take any risk of using Public AI services due to severe data leakage, compliance violations, and IP exposure.

**The DefenGPT AI Firewall.** A real-time solution combining Governance and Security that empowers companies to control how AI services are utilised while safeguarding sensitive data and enforcing organisational policies.

# The DefenGPT Solution Architecture



# Activating Enterprise Intelligence



## Knowledge Chatbot (RAG)

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



## Data Analysis

Analyse large datasets, generate reports, and visualise trends through simple, natural language inputs.



## Smart Search

Retrieve exact company content search results using a highly accurate Private Hybrid search of Semantics and Keywords.

# Secure Deployment & Contextual Grounding

## Secure & Private Deployment



### Local / On-Premise

Local on-premise security system, and driver & stock a secure.



### Strictly Private Cloud

Strictly Private and Cloud storage across a trusted private management.

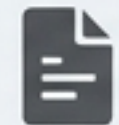
## Factual Data Grounding



CRM



Knowledge Bases



Meeting Transcripts



Chats



Emails



**Secure Digestion Engine**

Factual data grounding ensures secure ingestion and output products and strong leading.

# Granular Governance and Zero-Trust Control



## Contextual Access Control

The AI only generates answers based on the specific source data the individual user has verified permission to access.



## Data Sensitivity Management

Automatically identifies, tags, and manages highly sensitive data classes, including PII, HIPAA-regulated health data, and Finance records.



## Monitor AI Usage

Comprehensive, unalterable auditing. Measure, manage, and review all AI interactions across the enterprise.

# Command Centre: Actionable Auditing

### Account Activity Auditing

Click here to learn more about Activity Auditing

Advanced search

Non-er user email: Enter user name or email

From Date: 05-11-2024

To Date: 05-11-2024

Chat Name: Enter chat name

Prompt: nbs

Response: Search in response

Topics: Enter topic

Deleted usage: Enter deleted usage

Context name: Enter context name

Risk: Selected

Usage Classification Rules: Enter usage classification

Data Classification Rules: Enter data classification

Search Clear/Reset

REFRESH 1 SEARCH 1 FILTER ON

Policy Risk	Sensitivity level	Action	Policy Name	Chat Name	Prompt	User Name	Created Time
Low	Low	Mentioned	Code review	Default Keyword Shortcuts Guide	Send to me and watch to calendar. Top...	ADN Visual Assistant	30040524 17:01:55
High	High	Monitored	Legal advice for all	NDA - Generate a summary for NDA...	Generate a summary for NDA	Yan Genize	250E0023 13:22:57
High	High	Monitored	Legal advice for all	NDA - reading the NDA a copying...	reading in this NDA a copying an clas a...	Yan Genize	1706E024 15:00:26

Policy applied: High risk policy: Legal advice for all

Prompt: 

- binding on the NDA a copying is also a violation of the contract?
- Disallowed: The content did not follow any data classification rules
- Usage Classification:
  - Name: Legal advice (A) - Sensitivity Level: High
- Response usage: Legal advice interpretation

Response: 

- According to the Non-Disclosure Agreement (NDA) entered into between the Client and the Provider, the Client has granted the Provider access to the data and information contained in the NDA for the purpose of providing the services requested by the Client. The Provider is prohibited from disclosing, copying, distributing, or otherwise using the data and information contained in the NDA for any purpose other than the provision of the services requested by the Client.

Data sources: 

- Document: NDA.C7
- Data classification:
  - Name: Personal Information (A) - Sensitivity Level: High

User email: yanin@agobcfuans.com

Chat policy: Violation of contract, Confidential Information, Copying in, Non-Disclosure Agreement

Firewall type: BusinessGPT API

## Granular Search

Filter enterprise-wide usage by User, specific Prompts, Risk Level, or Data Classification Rules.

## Policy Enforcement

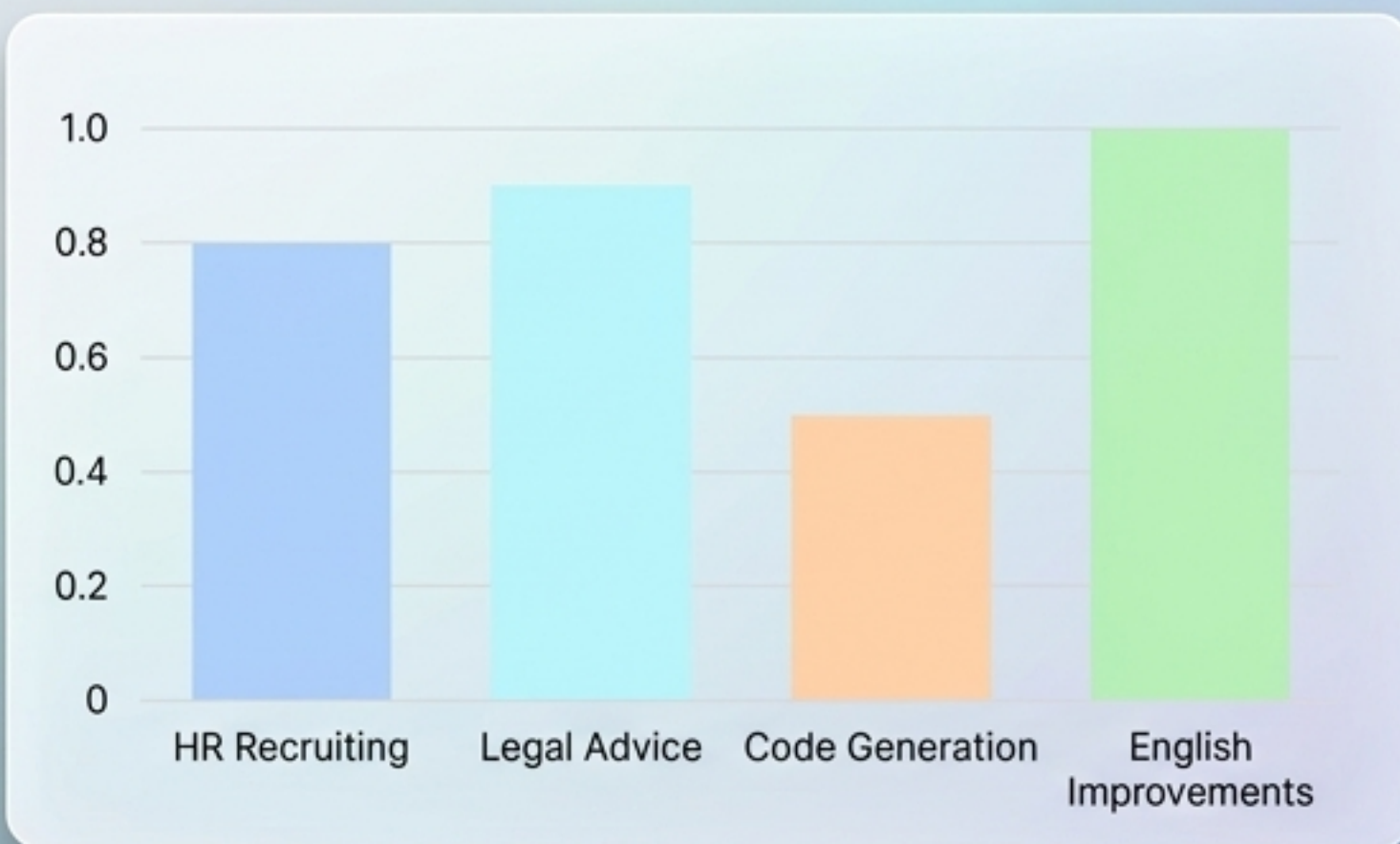
Tracks exactly which policies were triggered (e.g., 'High-risk policy: Legal advice for all') based on user behaviour.

## Firewall Action

Demonstrates how the BusinessGPT API firewall intercepts and handles sensitive inputs before they reach the model.

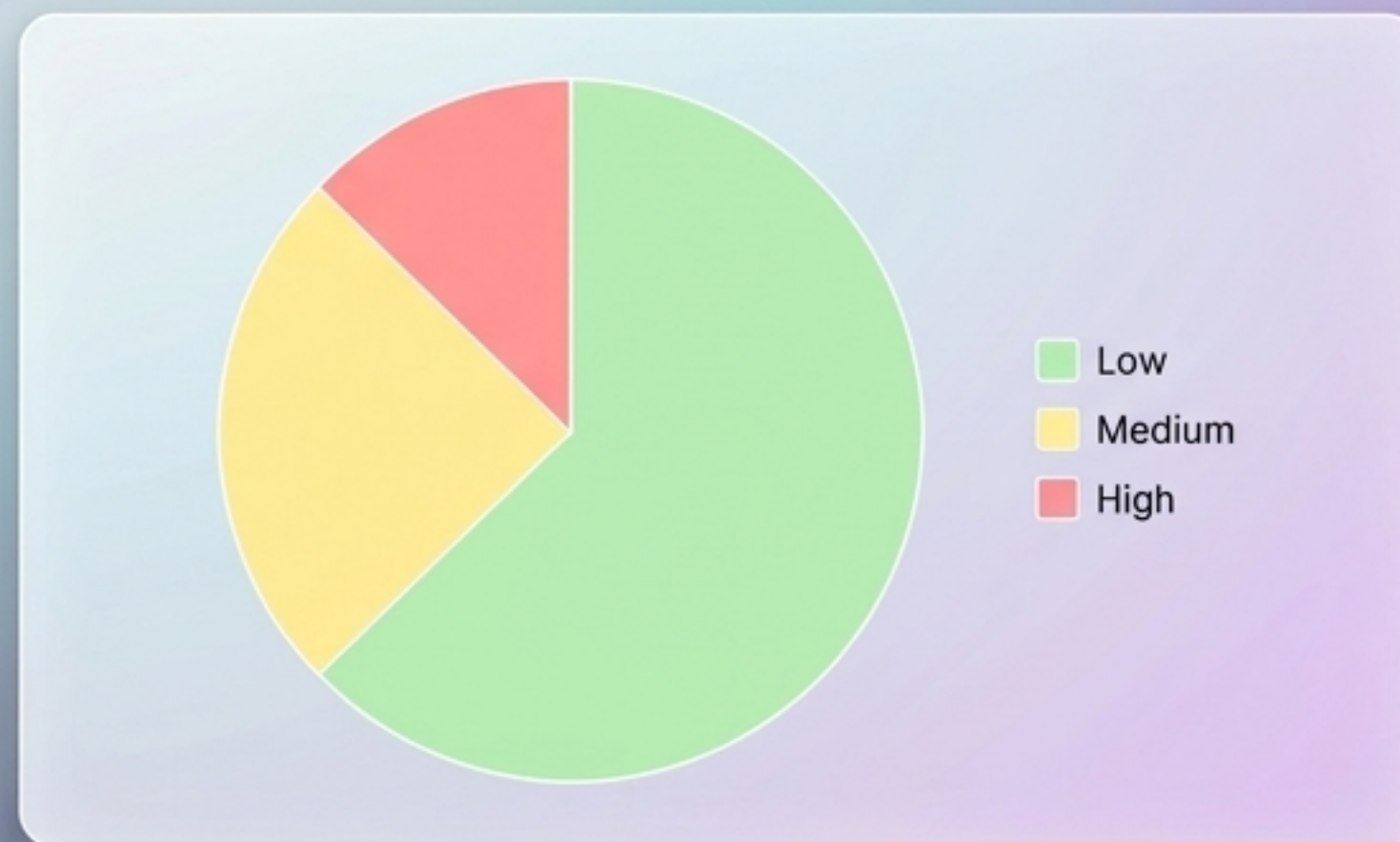
# Command Centre: AI Activity & Risk Analysis

## Activity Usage



Pinpoint exactly where and how your organisation is leveraging AI to drive productivity.

## AI Activity Risk By Level



Gain instant, high-level visibility into enterprise-wide AI query risk, allowing leadership to focus on critical threat clusters.

# Command Centre: Proactive Data Classification

## Top data classification rule



The AI firewall proactively categorises all data payloads in real-time. It actively detects when users attempt to input "Personal Information" or "Credit Card" details into prompts, automatically protecting sensitive data from some external exposure and allowing for granular, automated policy enforcement.

# The DefenGPT Value Matrix



## Data Privacy

Protects sensitive data from exposure.



## Risk Management

Allows for granular policy enforcement.



## Increased Visibility

Offers detailed tracking and reporting on AI adoption and usage.



## Compliance Assurance & Enhanced Access

Private deployment maintains data within company control, while enabling quick retrieval of contextual answers.

# Equip Your Enterprise With Secure Innovation.

The AI your employees deserve, secured by the firewall your compliance demands.

**Try DefenGPT Private AI  
for free today...**

