DefenGPT

Private AI Suite

DefenGPT Private AI Suite

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

Intelligent Defence. Unmatched Resilience.

Defenix

Intelligent Defence. Unmatched Resilience

The Enterprise AI Deadlock

The Drive for Innovation

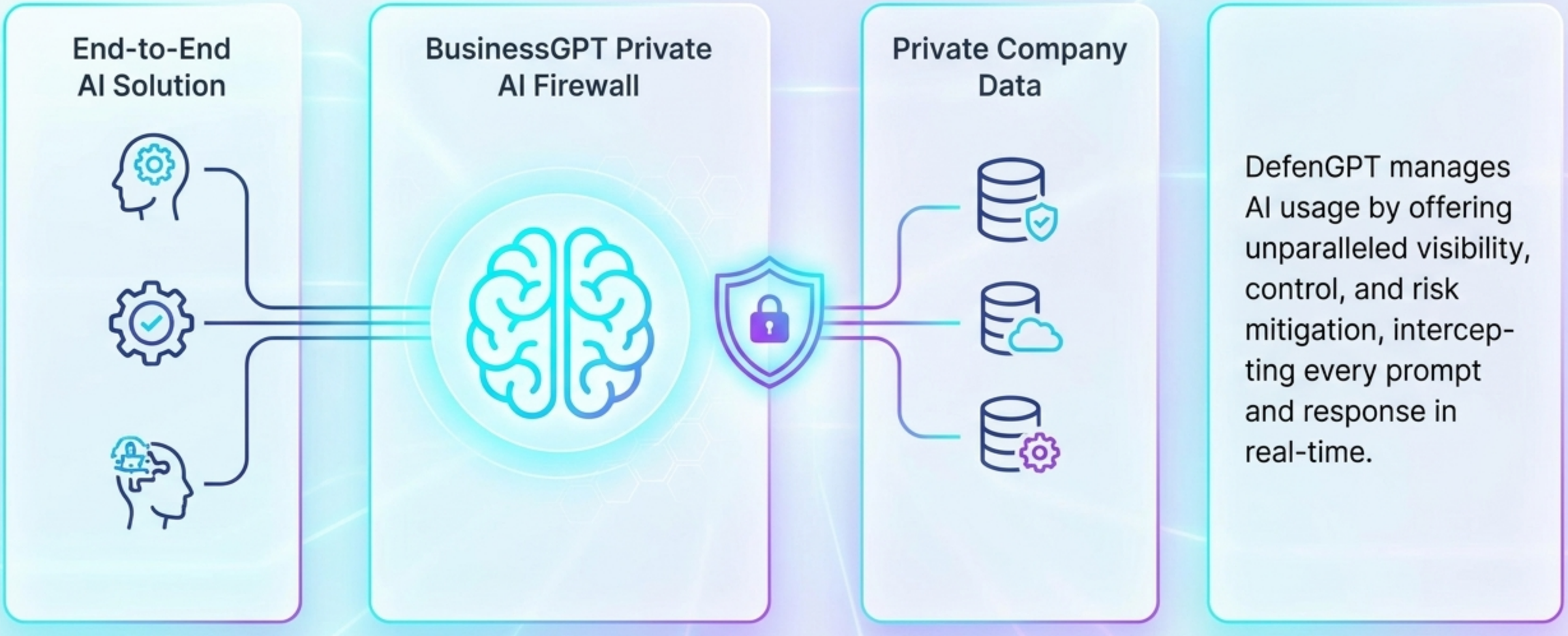
Modern enterprises require the transformative analytical power of large language models like ChatGPT, Copilot, and Gemini to remain competitive.

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

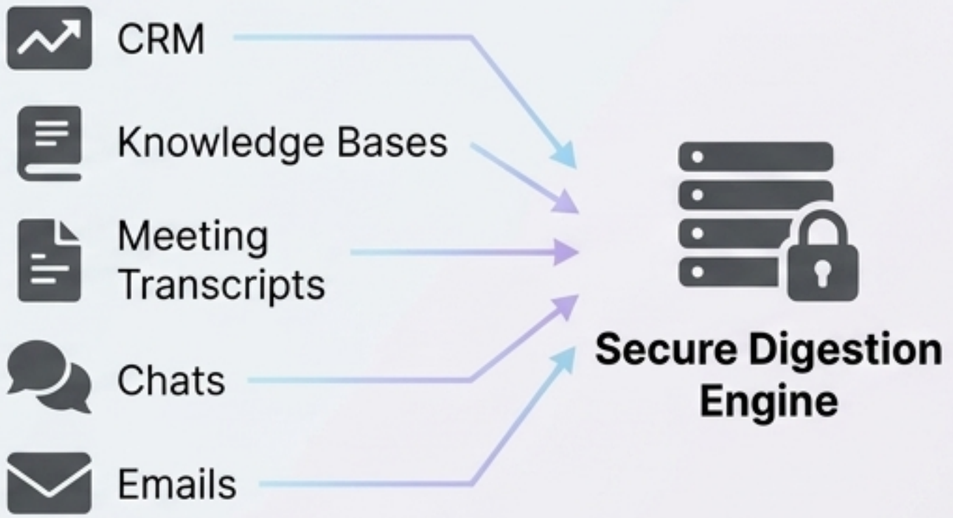
Local / On-Premise

Local goi On-premise encume·Security system, and driver & stock a secure.

Strictly Private Cloud

Strictly Private and Cloud storess acrow alfucharoested private management.

Factual Data Grounding



Factual data grounding endures secure rigestiorg andwant products and stronge 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.

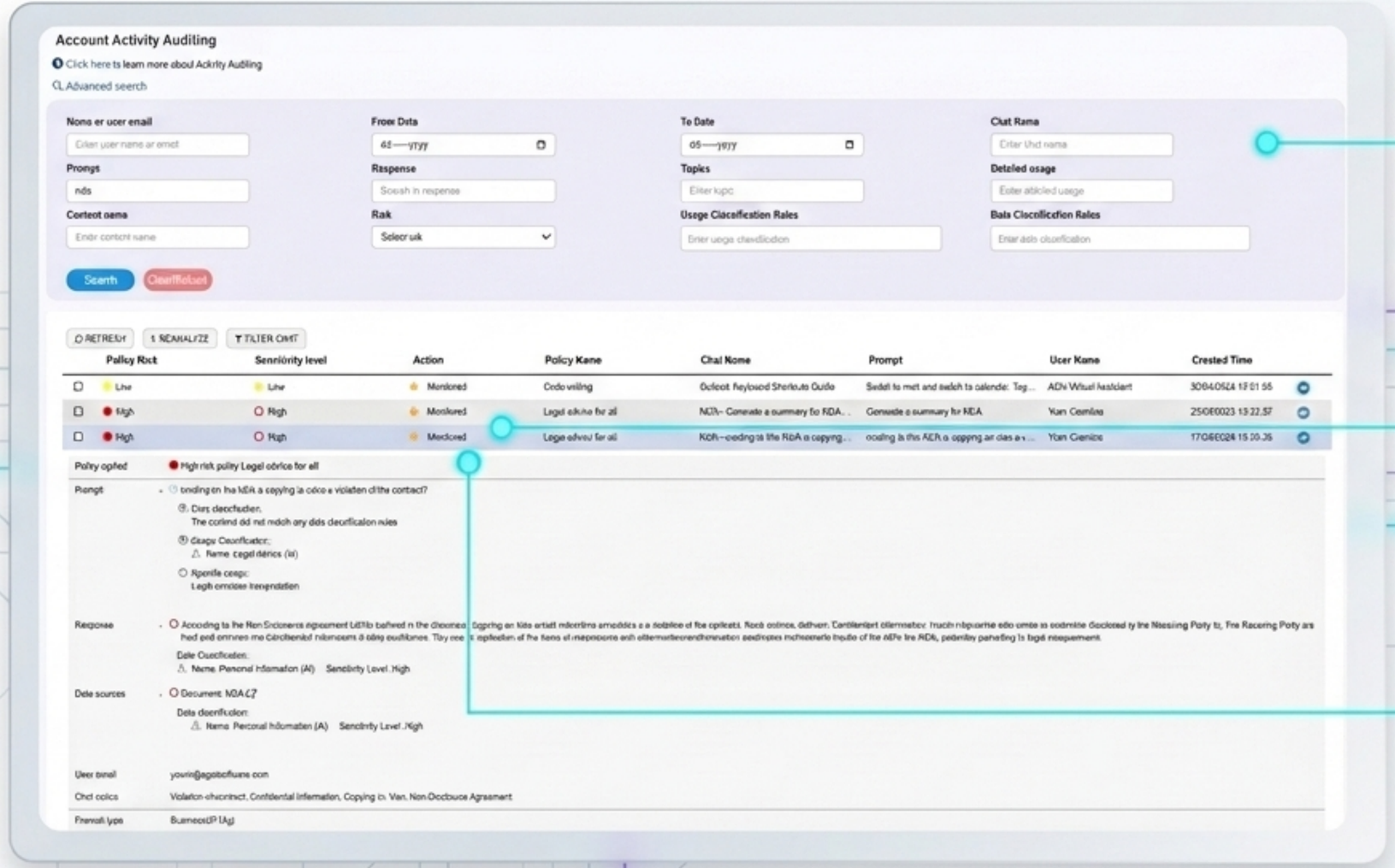
Data Sensitivity Management

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



Granular Search

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

Policy Enforcement

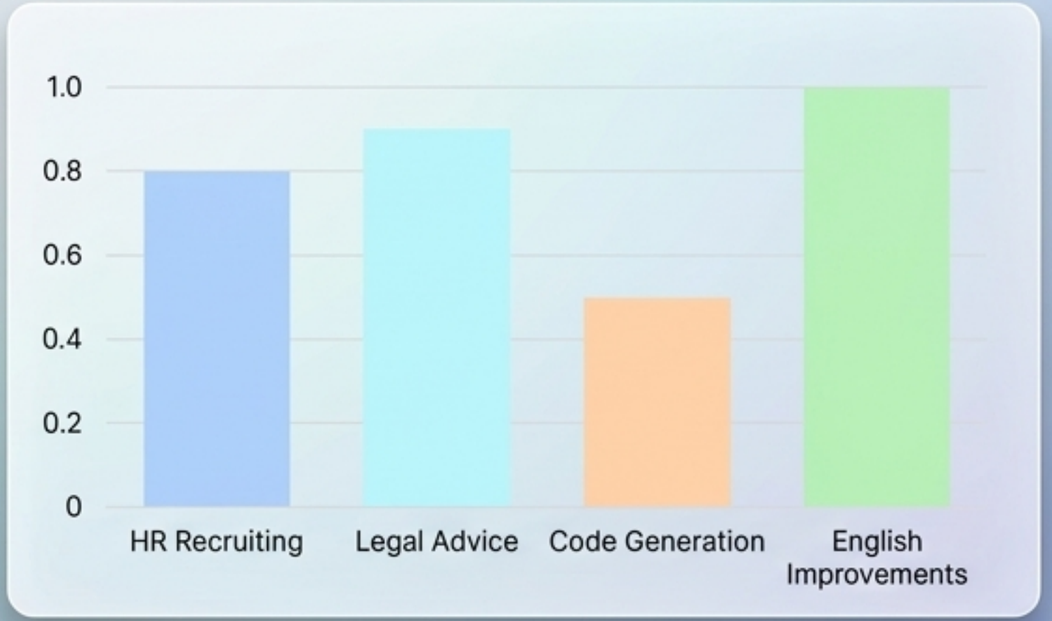
Tracks exactly which policies were triggered (e.g., 'High-risk policy: Legal advice for all') based on user behaviour.

Firewall Action

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

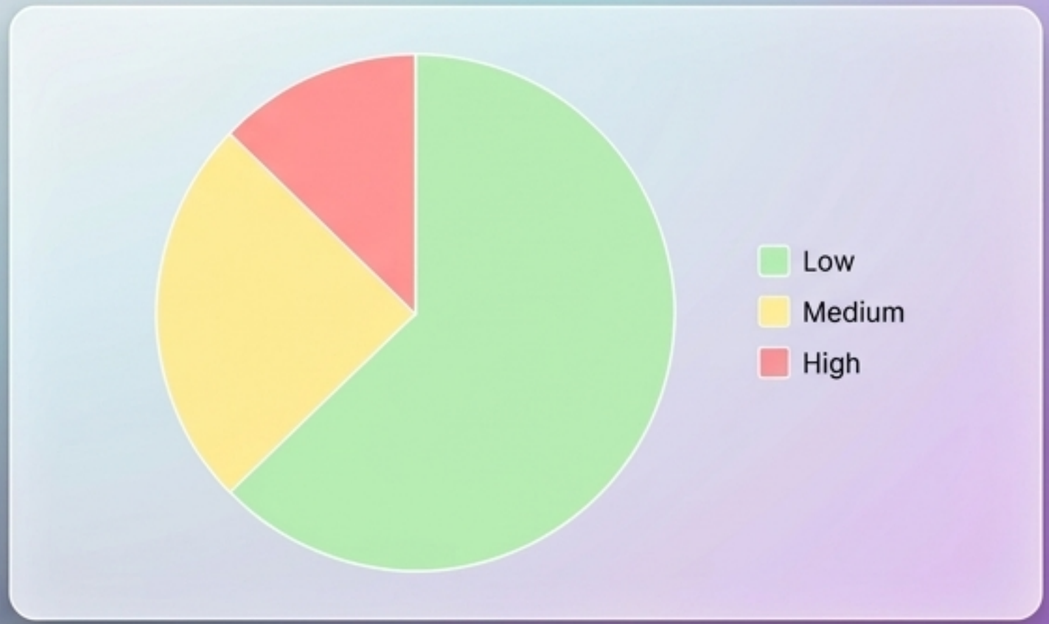
Command Centre: AI Activity & Risk Analysis

Activity Usage



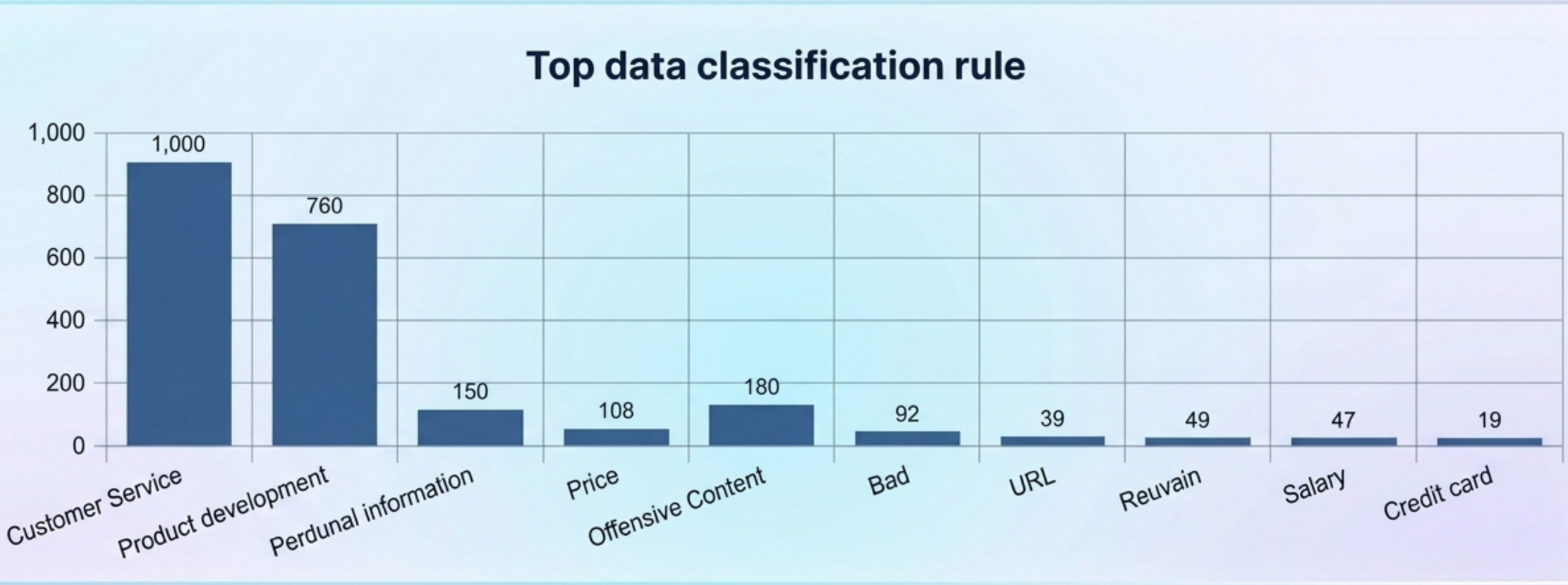
Pinpoint exactly where and how your organisation is leveraging AI to drive productivity.

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



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...

Defenix

Sales@Defenix.AI

Website: www.defenix.ai