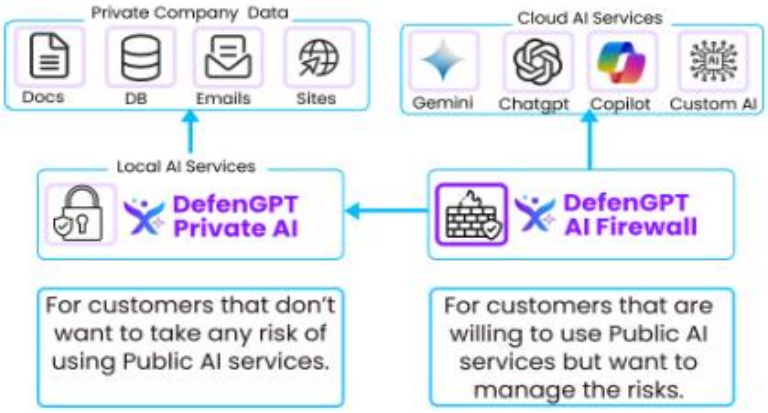
Defenix
Intelligent Defence Unmatched Resilience

Privacy First AI Platform

Data Privacy and Risk Management for AI

Product Overview

DefenGPT provides security and governance for Generative AI usage, featuring a real-time Firewall to control AI risks, including ChatGPT/Copilot and local AI services. It offers a Private/On-prem AI solution for regulated companies, ensuring data confidentiality.



Private AI Solution

On-prem/ Private AI

Generate insights from your company data with zero data exposure using a local Chatbot

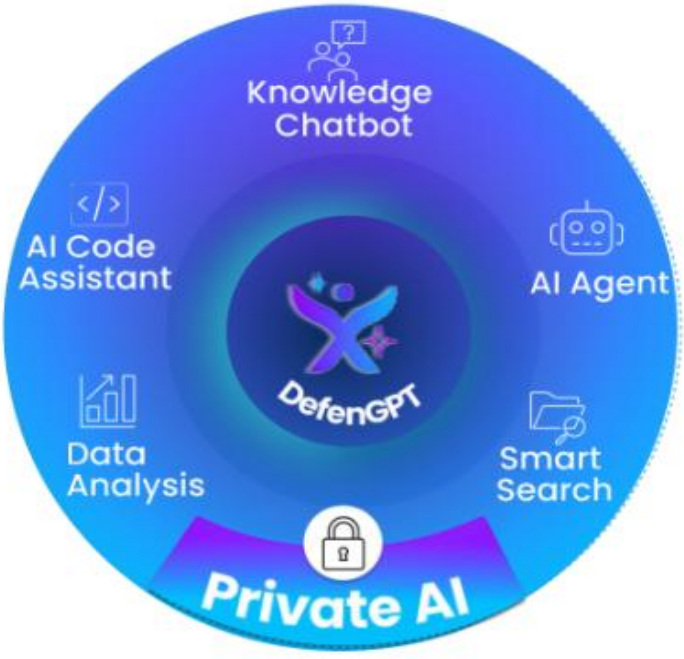
Privacy: Complete Chatbot AI solution with no internet exposure.

Deployment: Available as an on-premises or private cloud solution.

Local AI Modules: Uses the best open-source AI Modules.

Access control: Generate answers based on source data access.

Grounding: Data connectors to most important sources, such as files, sites, emails, and meetings.



Private AI Modules

Knowledge base (RAG) chatbot
Generate answers from all company-connected sources and pre-trained knowledge.

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

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

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

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

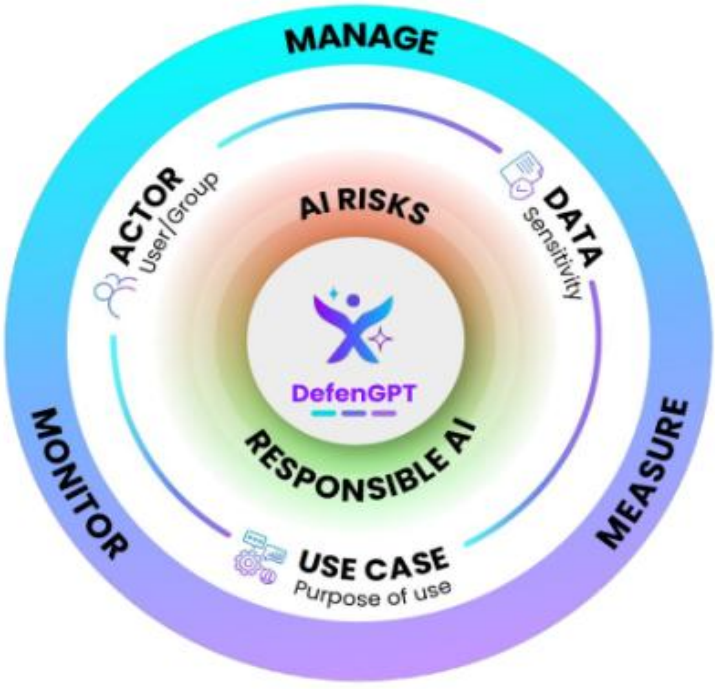
Learn More

AI Firewall Solution

AI Firewall for Governance and Security

Mitigating AI risks with visibility and control of AI usage

Visibility and Usage: View what users are using AI for.
Risk Management: Complete activity auditing for risk management.
Data Protection: Prevent sensitive data from being exposed .
AI Governance Policy: Enforce usage policies per group/ user to ensure responsible AI usage.
Data Sensitivity: Identify and manage sensitive data such as PII and HIPPA.
Identify Objectives: Identify activity objectives (e.g., asking for legal advice or improving code, price inquiry).
Public AI Support: Support for online AI like ChatGPT, Gemini, Copilot or local AI.

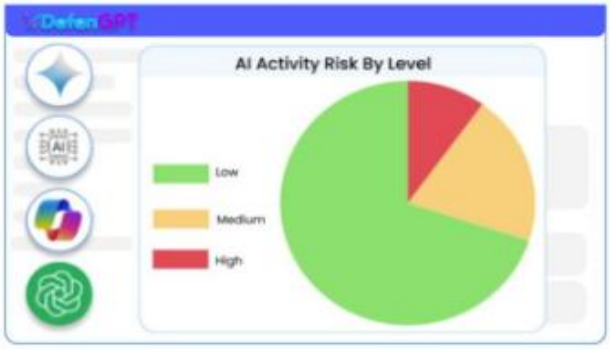


Learn More

DefenGPT Capabilities

AI Governance

- Monitoring AI usage
- Measure risk based on defined company policies
- Manage risks by defining rules controlling AI usage
- Define Responsible AI for your company
- Compliance – Maintain compliance with regulations



Security

- Ensure zero data exposure.
- Privacy first with data classification and sensitivity control
- Solve top OWASP AI risks of external attackers.
- Available as a private end-to-end solution or as a proxy to existing AI service

Benefits Of DefenGPT

Control AI usage across platforms
ChatGPT, Gemini, Copilot, Internal and external AI systems.

Secure sensitive data by regulations
PII, HIPPA, Finance.

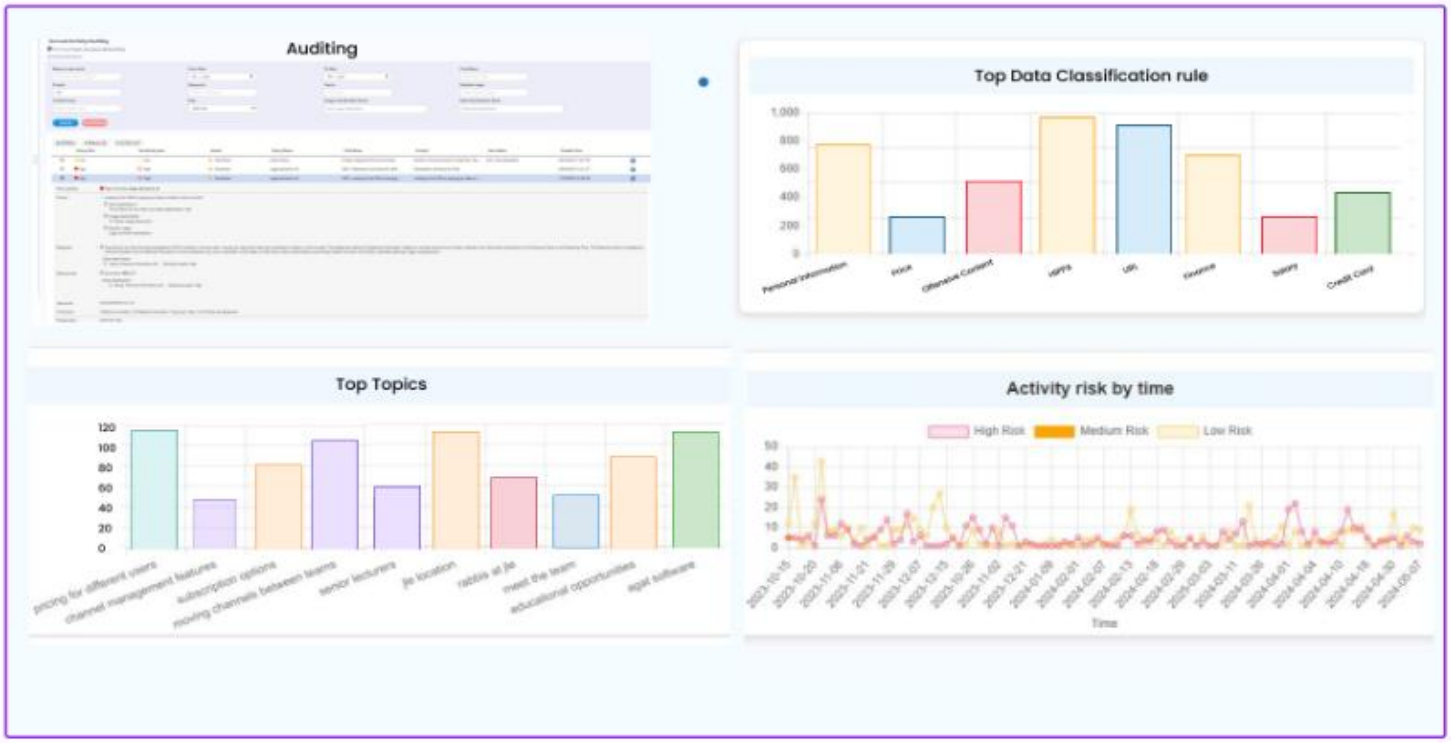
Mitigate OWASP risks
Prompt injection, Prompt leak, Jailbreak, DDoS.

Manage AI Usage
Users, Content, Activity.

Handle risks
Reputational damage, IP lost, Financial Business Loss.

Implement AI Governance
Internal Policies.

Management Dashboard



Get a **free trial** today to experience the power of the **DefenGPT** Assistant and take your operations to new heights. Click Here

DEFENIX Sales@defenix.co.uk Frien Barnet Road, London N11 3BU, United Kingdom