Defenix
Intelligent Defence Unmatched Resilience

DefenGPT
AI Firewall

Mitigate AI Risks with Visibility & Control

The enterprise bridge to safe, compliant, and highly productive Public AI adoption.

The AI Imperative

Workforces demand access to Generative AI to maintain competitive productivity.

How do organisations leverage Public AI services **without sacrificing data sovereignty?**

The Regulatory Reality

Exposing sensitive corporate data, PII, and trade secrets to public LLMs violates HIPAA, GDPR, and core infosec policies.

Unrestricted Access

Productivity: High

Shadow AI Risk: Critical

Regulatory Compliance: Failed

Outcome: Immediate exposure to data exfiltration and OWASP LLM vulnerabilities.

Complete Block / Ban

Productivity: Zero

Shadow AI Risk: High (Employees bypass controls via personal devices)

Regulatory Compliance: Passed (Technically)

Outcome: Loss of competitive edge, high workforce frustration.

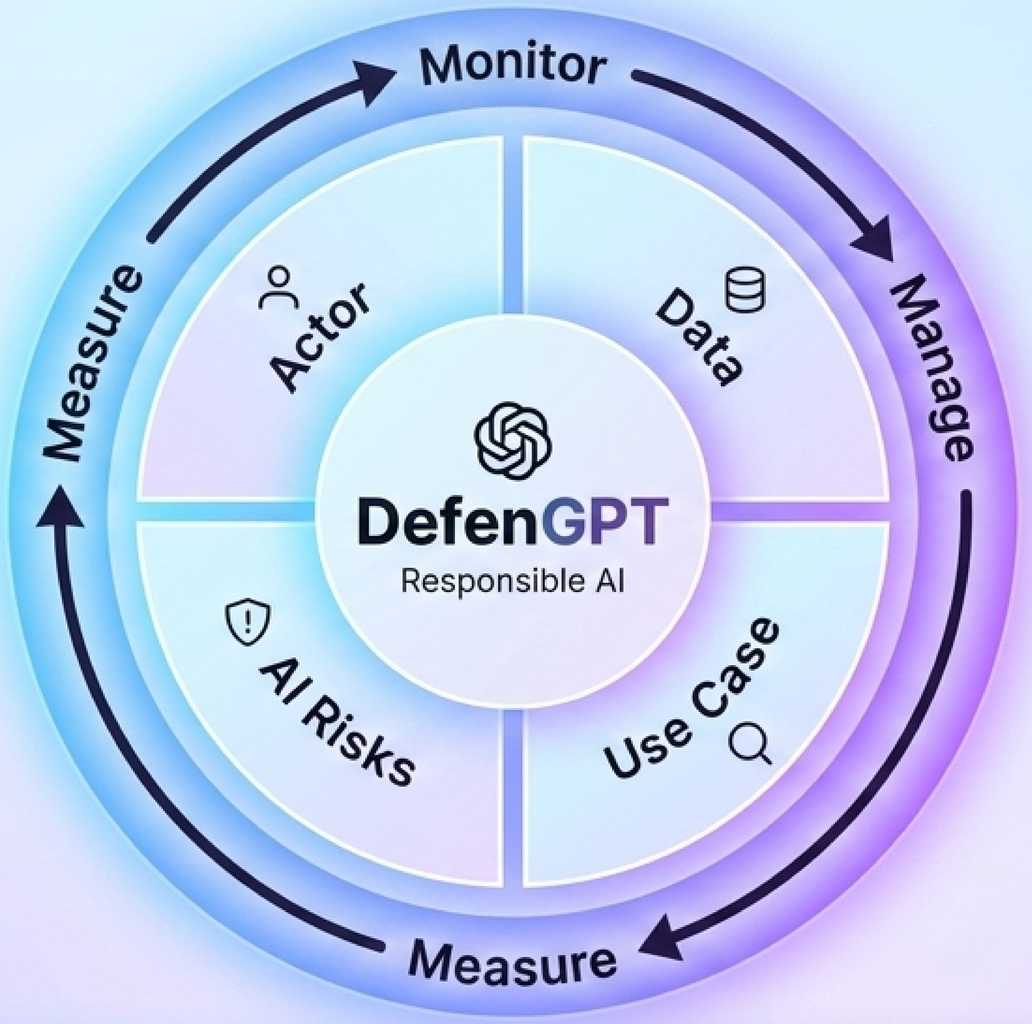
DefenGPT Governed Access

Productivity: High (Frictionless access to ChatGPT, Gemini, Copilot)

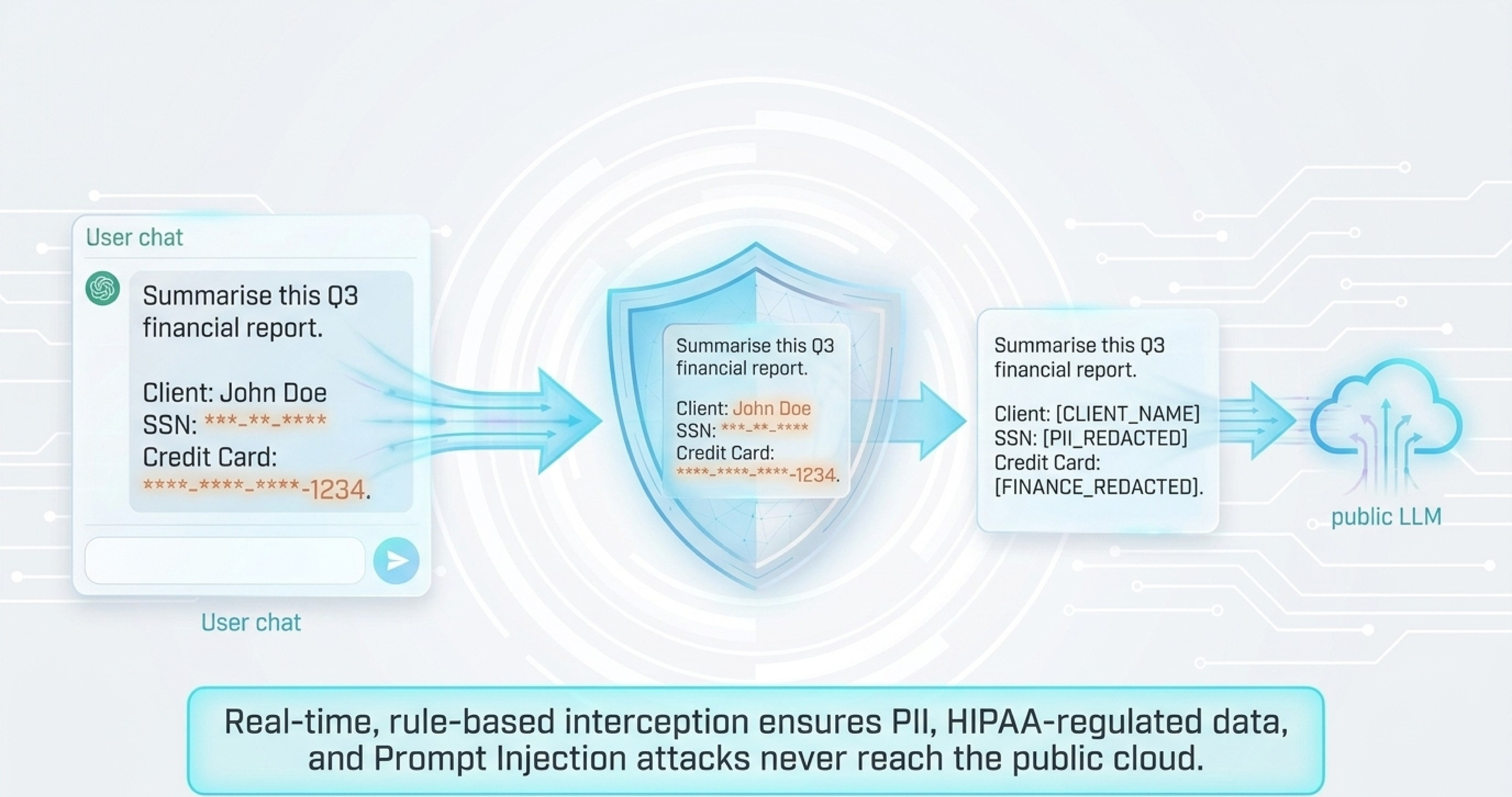
Shadow AI Risk: Neutralised (Full visibility)

Regulatory Compliance: Verified (Real-time PII redaction and policy enforcement)

Outcome: Unmatched resilience and safe innovation.



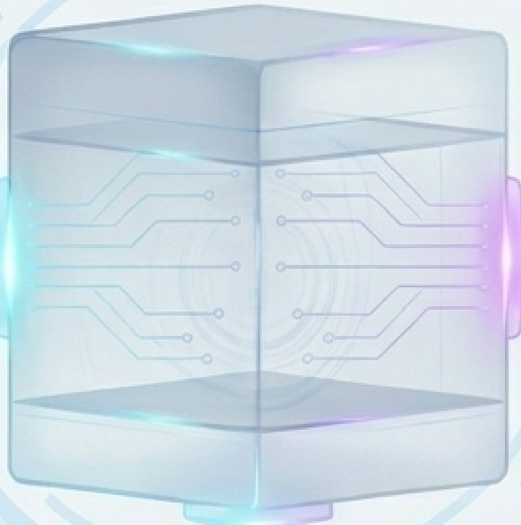
DefenGPT acts as an **intelligent perimeter**—sitting **seamlessly between your workforce** and Cloud AI Services. It ensures every prompt and response is **measured against your unique organisational policies** before leaving your network.



Real-time, rule-based interception ensures PII, HIPAA-regulated data, and Prompt Injection attacks never reach the public cloud.

Enterprise Governance

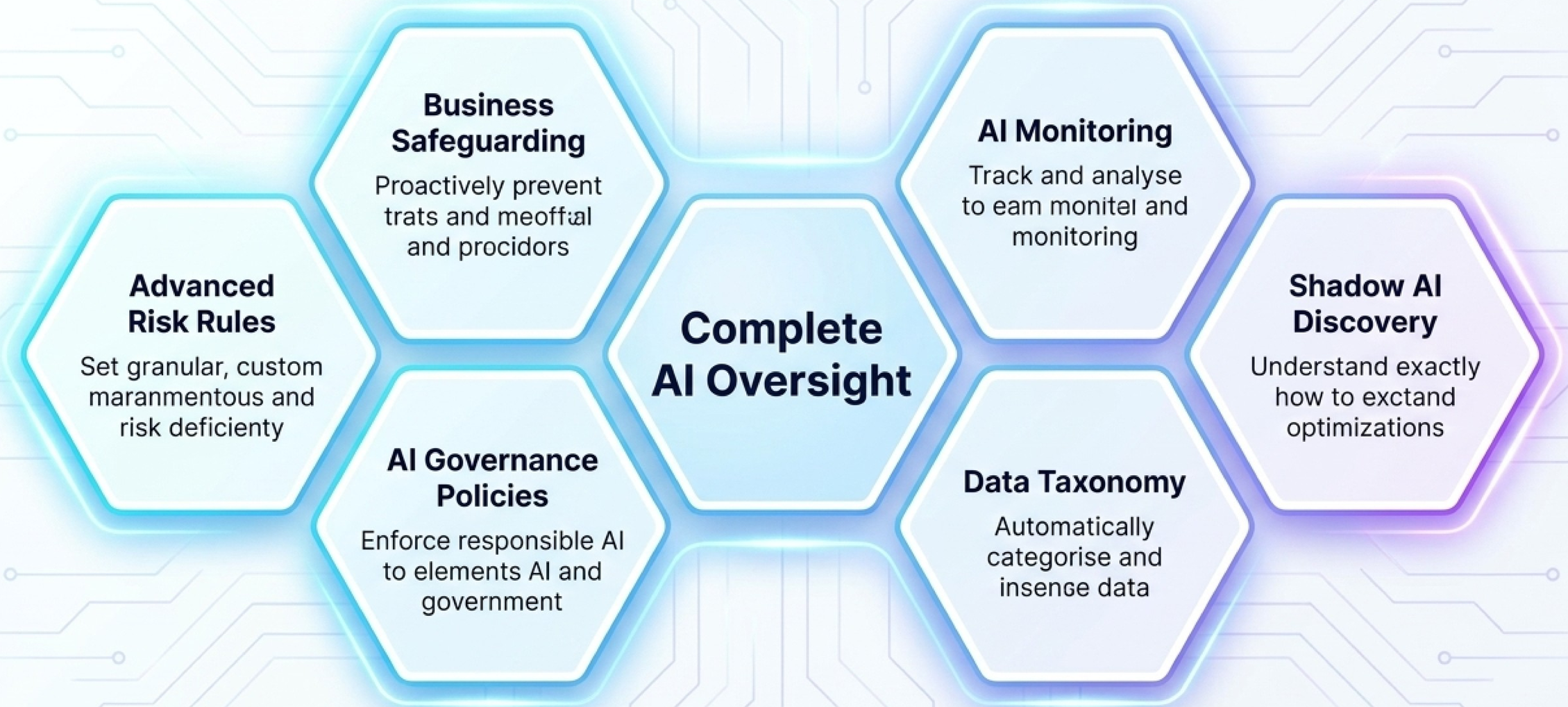
Monitor usage, enforce responsible AI, and maintain absolute compliance.



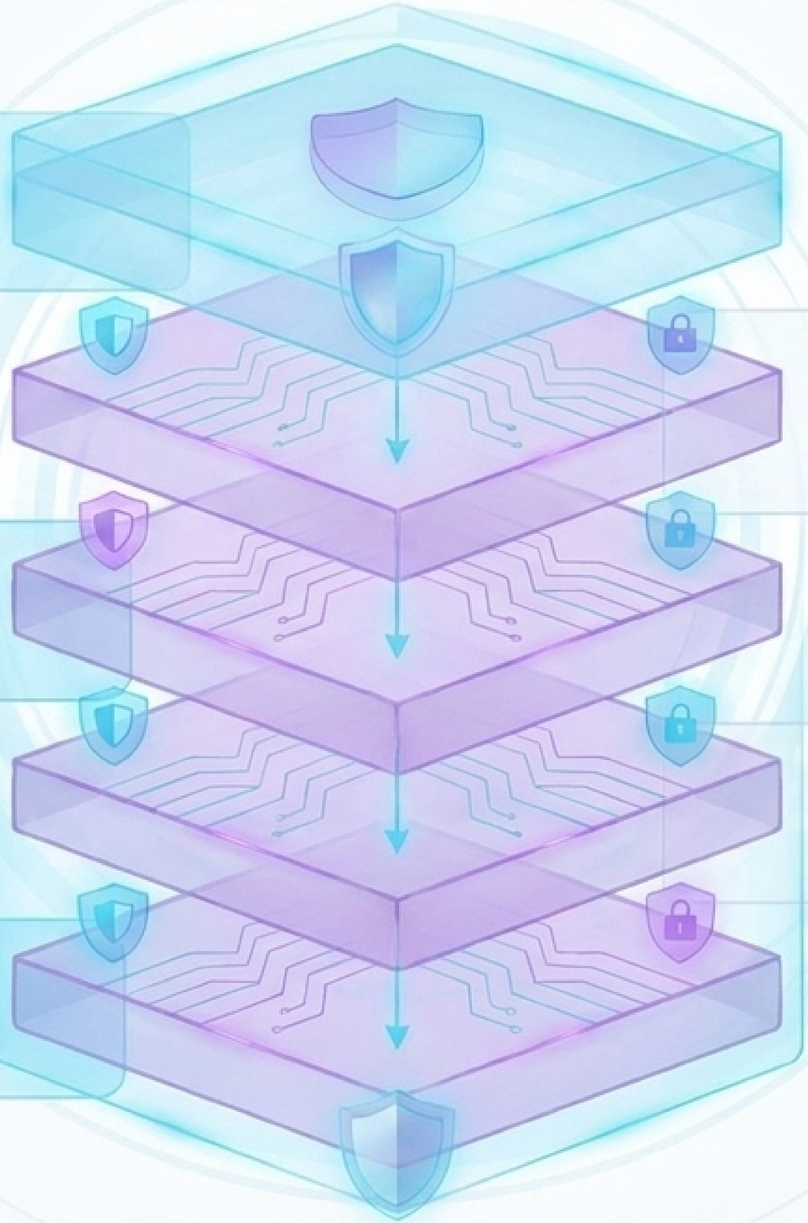
Fortified Security

Prioritise data privacy with classification, sensitivity control, and threat mitigation.

A unified platform empowering regulated industries to control how Public AI is utilised, without inhibiting productivity.


Business Safeguarding
Proactively prevent trats and meoffial and procidors
Advanced Risk Rules
Set granular, custom maranmentous and risk deficienty
AI Governance Policies
Enforce responsible AI to elements AI and government
Complete AI Oversight
AI Monitoring
Track and analyse to eam monitel and monitoring
Shadow AI Discovery
Understand exactly how to exctand optimizations
Data Taxonomy
Automatically categorise and insence data

INTELLIGENT PERIMETER: STRATIFIED SECURITY LAYERS



Layer 1: Data Classification

Automatically classify user input data for immediate risk analysis before processing.

Layer 2: Data Sensitivity & Protection

Actively manage and prevent the exposure of sensitive corporate data, including strict PII and HIPAA compliance.

Layer 3: Rule-based Enforcement

Execute rigid, automated rules to mitigate identified AI risks on the fly.

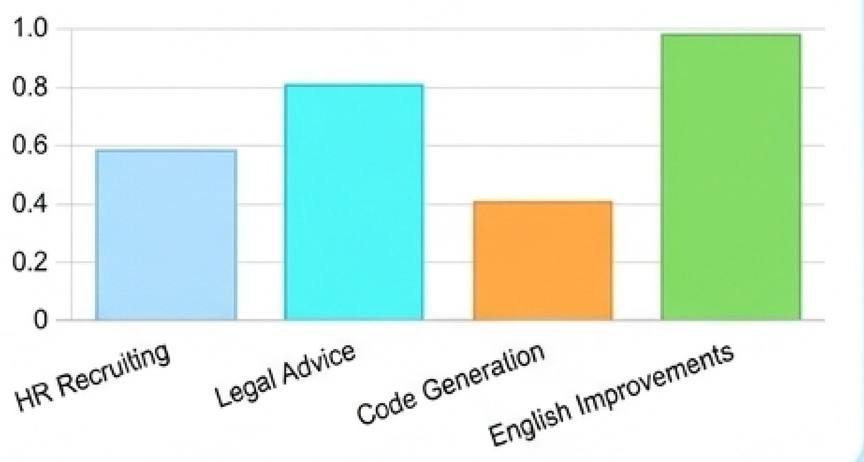
Layer 4: Input Validation

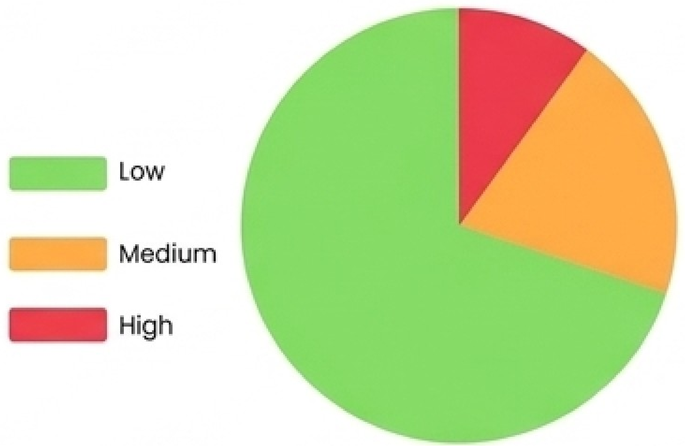
Intercept and neutralise hostile threats, including sophisticated prompt injection attacks.

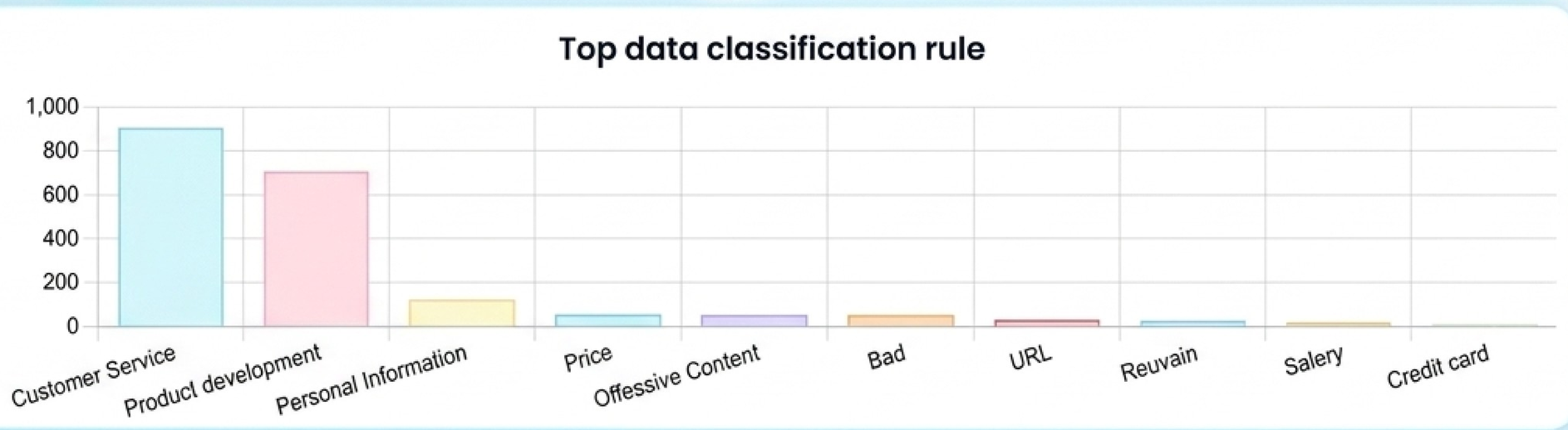
Layer 5: OWASP LLM Top 10

Address and resolve the most critical vulnerabilities standard to Large Language Models.

AI Firewall at Work







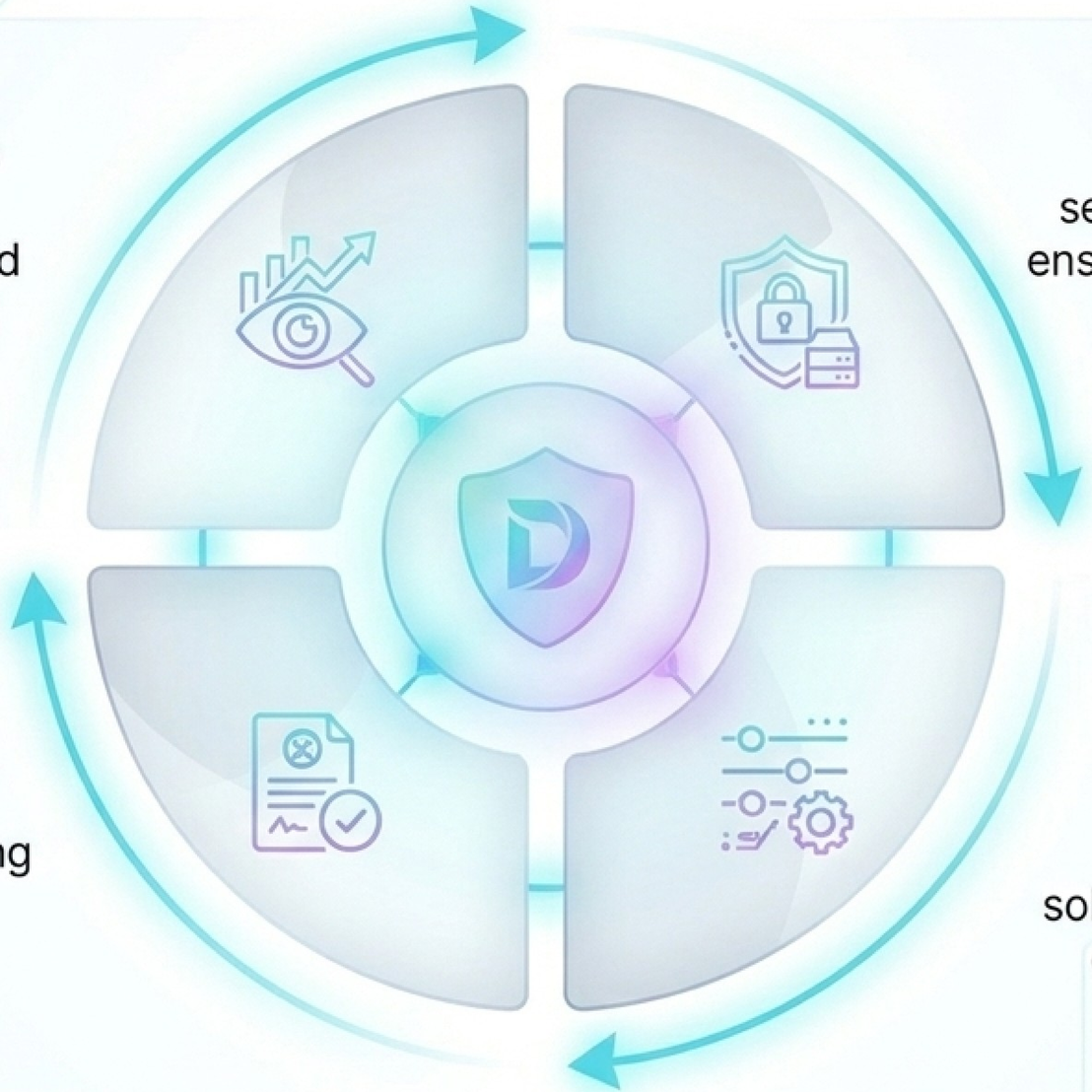
Abstract control translated into actionable oversight. Your entire AI landscape visualised in real-time.


Granular Search: Filter by user, date range, risk level, or specific data classification rules.
Complete Prompt & Response Logging: Retain a full history of exact user prompts and LLM outputs for compliance addits.
Violation Tracking: Instantly see exactly which governance policy was triggered, the sensitivity level, and the automated action taken.
Account Activity Auditing
Click here to learn more about Astivity Auditing
Advanced search
Name or user email
Enter user name or hoali
Frem Date
To Date
Chat Name
Enter chaf name
Prompt
nda
Response
Search in response
Topics
Enter topic
Detailed usage
Enter detailed usage
Content name
Enter content name
Risk
Select ruk
Usage Classification Rules
Usee sage classification
Data Classification Rules
Data data classification
Search
ClearReloed
REFRESH
+ REANALYZE
FILTER RTAT
Policy Rick
Sensitivity level
Action
Policy Name
Chat Name
Prompt
User Name
Created Time
Low
Low
Moniiored
Code writing
Outlock Keyboard Shortcuts Guide
Swith to mall and ewilch to celender. Teg...
AOV-Virtual Assistant
30/04/2024 13:01:58
Ugh
High
Meniiored
Legal advice for all
NDA - Generate a summary for NDA...
Generala a summary for NDA
Your Combie
20/04/2024 12:21:17
Mgh
High
Menfored
Legal advice for all
NDA - codling to this NDA is copping ...
coding to this NDA is copying an idea a s...
Your Combie
11/04/2024 15:38:38
Policy appled
High rick coily Legal advice for all
Prompt
croding in the NDA is copying an idea a vielation of the contacl!?
Data classification:
The sentant did not match any data classification rules
Usage classification:
Name. Legal Advice (AI)
Specific usage:
Legal contiact interpretation
Response
According ta the Non-Diaclouse Agreement (NDA), andited in the document, copying an idea easisl llaly is inaud I ksad a vicieller of the centent. The sentriment definss "Confidentisl Information" bmady is include verious forms of data, materials, and discloses disclosed by the Receiving Party to the Receiving Party. The Receiving Party is triggered to helll and menkina the Confideotiel Informstien in data confidence. For ooe or regination of the dleas of Information eothon euthamation would ltary madch the dsein in the RIOA, podtantly, leseling tn legel requieremeres.
Data classification:
Name. Personal Information (AI)
Sensitivity Level: NGA
Data sources
Document. NDA
Data classification:
Name. Personal Information (AI)
Sensitivity Level: NGA
User email
yazeik@gettachware.com
Chat topics
Vielation of contract, Confidential Information, Copying on Ides, Non-Disclosure Agreement
Firewall type
BusinessCPTAy:

Unmatched Resilience: The Defenix Advantage

Increased Visibility: Offers detailed tracking and reporting on AI adoption and usage, enabling businesses to optimise AI strategies.

Data Privacy: Protects sensitive data from exposure, ensuring that AI usage adheres to company policies and security protocols.



Enhanced Compliance: Mitigates risks of non-compliance by providing AI governance tailored to regulatory standards.

Risk Management: Allows for granular policy enforcement, making the solution adaptable to different departments or user needs.

Try DefenGPT AI Firewall for free today.

Don’t choose between AI innovation and enterprise security. Deploy the intelligent perimeter.

Defenix
Intelligent Defence Unmatched Resilience

Sales@Defenix.AI

Website: www.defenix.ai