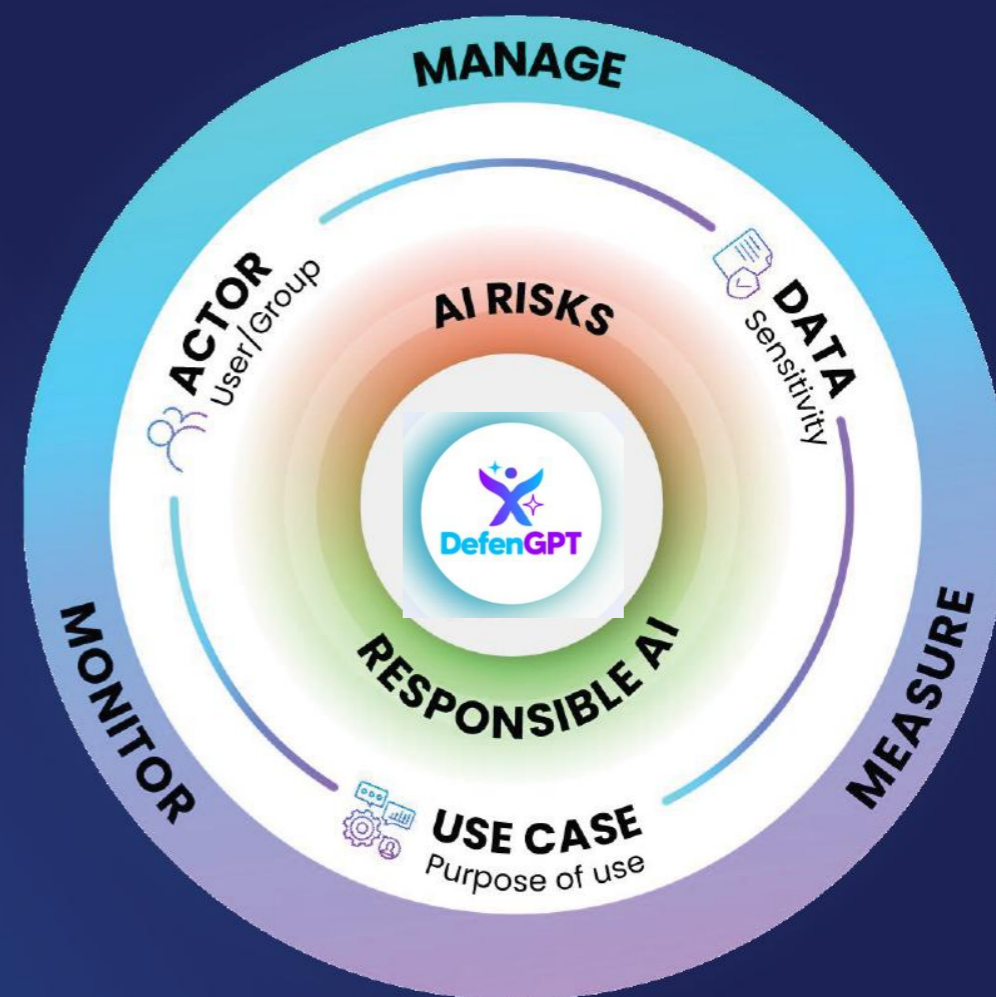


DefenGPT

AI Firewall

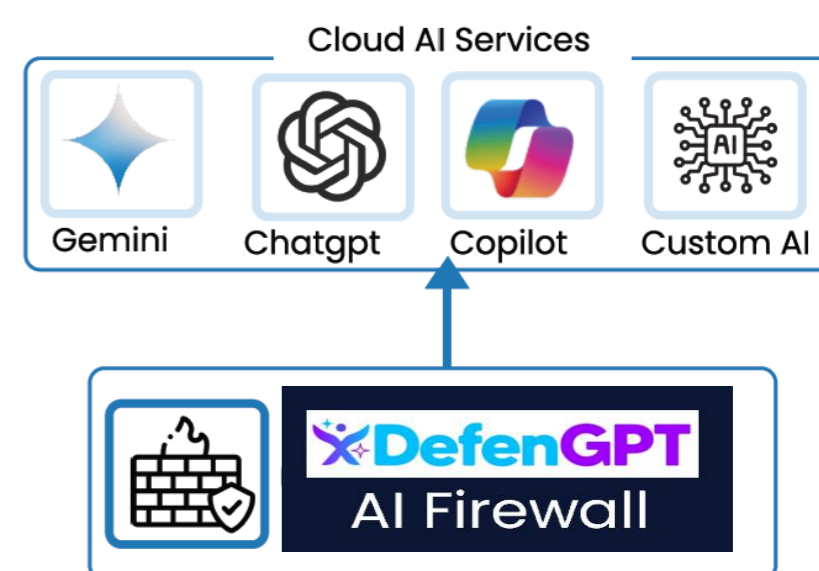
Mitigate AI Risks with Visibility & Control



Product Overview

DefenGPT AI Firewall helps businesses manage AI usage by offering visibility, control, and risk mitigation.

Combining Governance and Security, the AI Firewall empowers companies to control how AI services like ChatGPT, Copilot, and Gemini are utilized while safeguarding sensitive data and enforcing organizational policies. This real-time solution is ideal for businesses that need robust AI Oversight, especially those in regulated industries.



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

Key Capabilities

Governance

Monitor AI usage, manage risks, ensure compliance, and enforce responsible AI with policy-based controls

Security

Prioritize data privacy with data classification, sensitivity control, and secure deployment options for complete protection.

Governance Features

AI Monitoring: Track and analyze AI usage.

Advanced Risk Rules: Set rules for AI usage.

Business Safeguarding: Prevent negative outcomes from AI.

Data Taxonomy: Categorize AI activity by usage and topic.

AI Risk Management: Identify and mitigate AI risks.

AI Governance Policies: Enforce responsible AI usage policies.

Shadow AI: Understand how users are using AI.

Security Features

Data Sensitivity: Manage sensitive data (PII, HIPAA).

Rule-based Enforcement: Enforce rules to mitigate AI risks.

Data Protection: Prevent sensitive data exposure.

Data Classification: Classify user input data for risk analysis.

Input Validation: Handle threats like prompt injection.

OWASP LLM Top 10: Address top LLM threats.

Benefits

☑ Increased Visibility

Offers detailed tracking and reporting on AI adoption and usage, enabling businesses to optimize AI strategies.

☑ Data Privacy

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

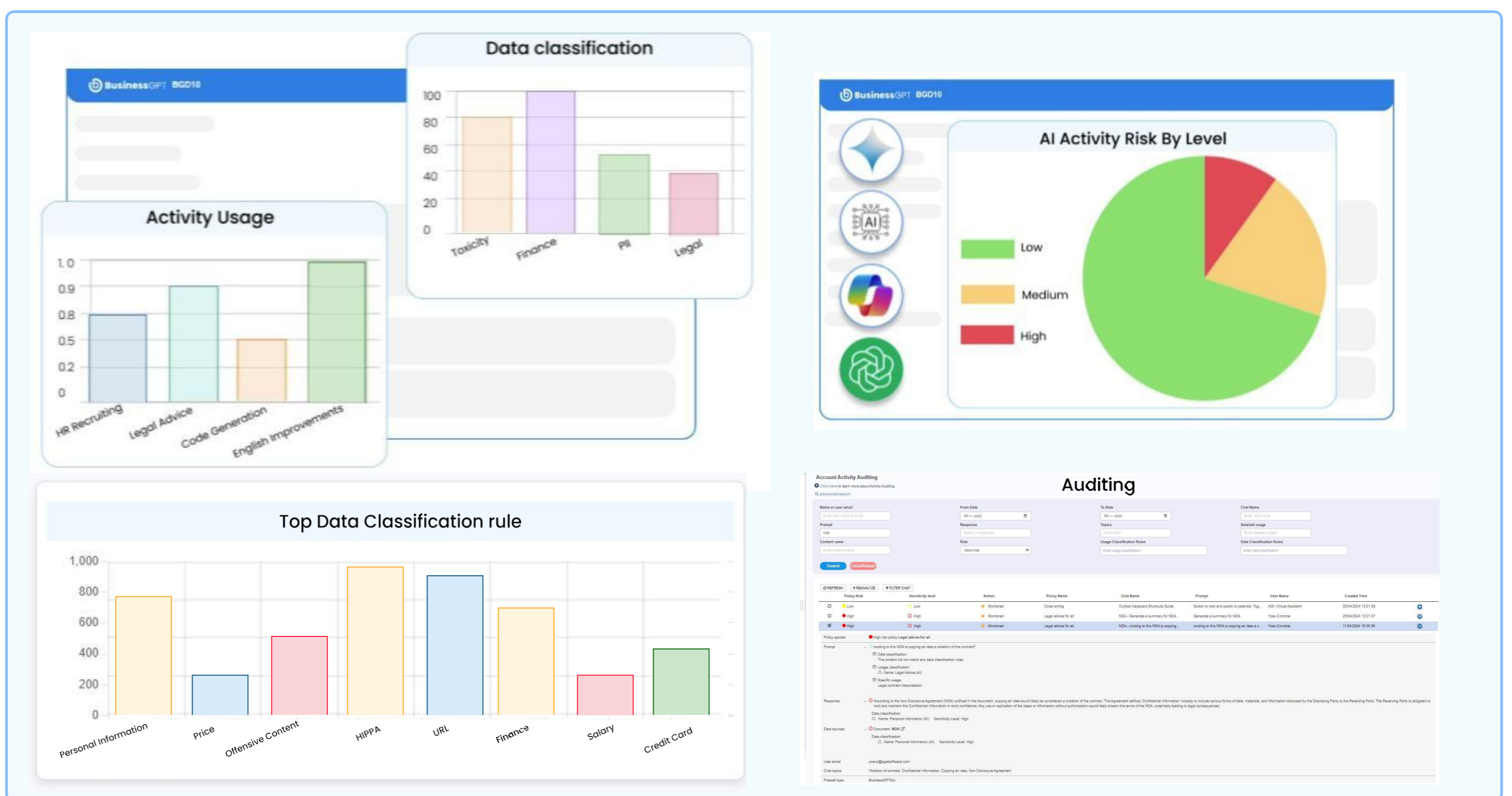
☑ Enhanced Compliance

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.

AI firewall at Work



 Try DefenGPT **AI Firewall** for **FREE** today... [Click Here](#)