GUARDING YOUR PUBLIC AI USAGE

DefenGPT vs. Microsoft Purview

A Strategic Competitive Analysis for Enterprise AI Security

DefenGPT

Strategic Overview and Core Purpose

Two Distinct Security Domains Working Together

Microsoft Purview

Data Governance & Compliance

Key focus areas:

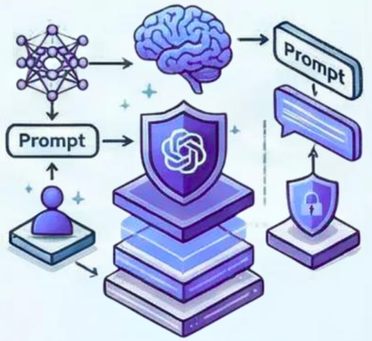
- Data classification and sensitivity labeling
- Data Loss Prevention (DLP) policies
- Insider risk management
- Regulatory compliance reporting
- Microsoft ecosystem protection

DefenGPT AI Firewall

AI Security
AI Security & Governance

Key focus areas:

- AI prompt and response security
- Generative AI interaction control
- AI threat detection and prevention
- Cross-platform AI governance
- Enterprise AI usage visibility



Strategic Insight: Purview protects your data assets. DefenGPT protects how you interact with AI.

Protection Layer and Scope

Understanding What Each Solution Protects

Microsoft Purview

- Protects Data at Rest
- Protects Data in Motion
- Microsoft Ecosystem Focus
- Traditional Data Governance

DefenGPT AI Firewall

- Real-Time AI Prompt Inspection
- AI Response Filtering
- Cross-Platform AI Interactions
- Next-Generation AI Protection

Defending Against AI-Specific Threats

DefenGPT's Unique AI Security Capabilities

Prompt Injection Detection

Prompt Injection Protection

Detects and blocks malicious instructions embedded within user prompts

DefenGPT: ✔ Native Support

Microsoft Purview: ✗ Not Available

Adversarial Instructions

Adversarial Prompt Defense

Identifies attempts to manipulate AI model behavior through crafted instructions

DefenGPT: ✔ Real-time Detection

Microsoft Purview: ✗ Limited Coverage

Model Manipulation

Model Behavior Protection

Prevents unauthorized attempts to alter AI model responses and outputs

DefenGPT: ✔ Advanced Protection

Microsoft Purview: ✗ Not Supported

Traditional data governance tools protect your data.
DefenGPT protects your AI interactions.

Shadow AI Discovery and Usage Visibility

Comprehensive AI Platform Discovery vs. Limited Ecosystem Monitoring

Microsoft Purview
Limited AI Visibility

- Ecosystem-specific monitoring only
- Basic telemetry from Microsoft Copilot
- No discovery of external AI tools
- Limited usage analytics

DefenGPT AI Firewall
Complete AI Discovery

- Full discovery of all public GenAI platforms
- Automatic detection of ChatGPT, Gemini, Claude usage
- Department-level AI usage insights
- Detailed analytics on who, how, and why

Shadow AI poses significant governance risks when organizations lack visibility into actual AI tool usage

AI Interaction Auditing and Session Control

Comprehensive Governance Through Complete AI Visibility

Microsoft Purview

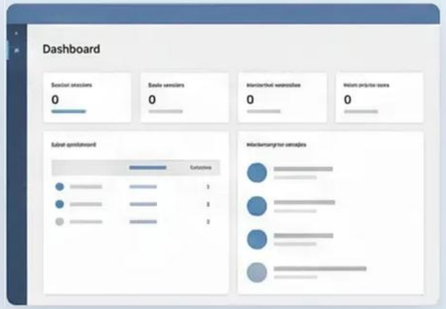
Limited AI session visibility

Basic activity monitoring within Microsoft apps only

No dedicated AI interaction logging

Indirect governance through DLP policies

No session-level AI audit trails



DefenGPT AI Firewall

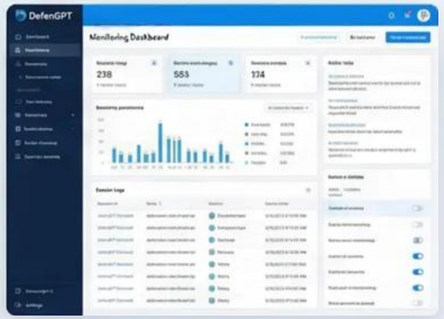
Complete audit trail of all AI sessions and interactions

Full prompt and response logging for governance

Detailed session-level AI activity audit trails

Granular AI prompt policies and enforcement

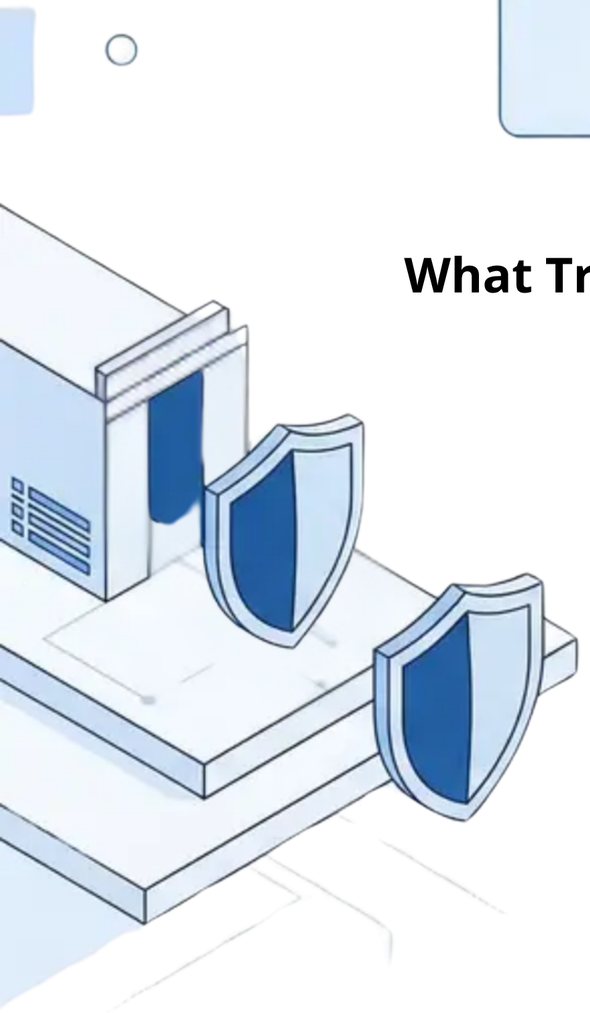
Real-time monitoring across all AI platforms



DefenGPT provides the audit trail and governance controls that traditional data governance platforms cannot deliver for AI interactions

Addressing the Enterprise AI Security Gap

Traditional security tools protect data, networks, and applications – but they do not protect AI interactions



What Traditional Security Protects:

Data Assets
Network Infrastructure
Endpoint Devices
Applications

The New Attack Surface:

AI Interactions
Prompt Exchanges
Model Communications

DefenGPT Introduces:

AI FIREWALL

A security layer between Users → Applications → AI Models

A Complementary Security Architecture

End-to-End Protection Through Strategic Partnership

Microsoft Purview
Data Governance Foundation

- Data classification & sensitivity labeling
- Data Loss Prevention (DLP) policies
- Insider risk management
- Compliance & regulatory governance
- Microsoft ecosystem protection

DefenGPT AI Firewall
AI Interaction Security

- Real-time AI prompt inspection
- AI threat detection & prevention
- Shadow AI discovery
- AI usage monitoring & auditing
- Cross-platform AI governance

The Complete Enterprise AI Security Stack

Organizations can confidently enable AI innovation while maintaining comprehensive security, governance, and compliance across all data and AI interactions.

Evolution to AI Governance

The Strategic Transformation

From Data-Driven to AI-Driven Organizations

From Data Protection to AI Interaction Security

From Compliance Monitoring to AI Governance

The New Security Imperative

As enterprises embrace public AI tools like ChatGPT, Copilot, and Gemini, traditional security must evolve to govern AI interactions, not just data assets.

DefenGPT AI Firewall: Enabling Safe Enterprise AI Adoption Through Comprehensive AI Governance