

## Defenix DefenGPT AI Security Platform vs Traditional SASE / ZTNA Vendors

### Microsoft/ Paloalto/ Zscaler/Netskope

#### Executive Comparison for CISOs, CIOs, Boards & Government Decision Makers

The majority of SASE and ZTNA vendors were designed to solve **network security, user access, cloud security, and application access challenges**.

Defenix was built specifically to solve **AI Security, AI Governance, AI Compliance, AI Risk Management, and Private AI adoption challenges**.

As organizations increasingly adopt ChatGPT, Microsoft Copilot, Gemini, Claude, AI Agents, MCP Servers, Autonomous Workflows, RAG Platforms, and Private LLMs, traditional SASE vendors provide only partial visibility into AI activity.

DefenGPT AI Security Platform addresses the entire AI lifecycle—from discovery and governance to runtime security, compliance, auditability, and sovereign AI deployment.

#### Executive Summary

Capability	DefenGPT AI Security Platform	Microsoft	Palo Alto Prisma SASE	Zscaler	Netskope
SASE	Limited	✓	✓	✓	✓
ZTNA	Limited	✓	✓	✓	✓
CASB	Limited	✓	✓	✓	✓
SWG	Limited	✓	✓	✓	✓
AI Governance	✓✓✓	Partial	Partial	Partial	Partial
AI Firewall	✓✓✓	Limited	Limited	Limited	Limited
AI Agent Security	✓✓✓	Emerging	Emerging	Emerging	Emerging

Capability	DefenGPT AI Security Platform	Microsoft	Palo Alto Prisma SASE	Zscaler	Netskope
Prompt Inspection	✓✓✓	Limited	Partial	Partial	Partial
Prompt Injection Protection	✓✓✓	Limited	Partial	Partial	Partial
Model Governance	✓✓✓	No	No	No	No
AI Gateway	✓✓✓	No	No	No	No
AI Risk Management	✓✓✓	Partial	Partial	Partial	Partial
ISO 42001 Support	✓✓✓	No	No	No	No
AI Compliance Automation	✓✓✓	Limited	No	No	No
Private AI Platform	✓✓✓	Limited	No	No	No
Fully Air-Gapped AI	✓✓✓	No	No	No	No
Sovereign AI Deployment	✓✓✓	Limited	No	No	No
On-Premise Deployment	✓✓✓	Partial	Limited	Limited	Limited
AI Security Operations	✓✓✓	Partial	Partial	Partial	Partial

## The Core Difference

### Traditional SASE Vendors Focus On:

#### User Access Security

- Secure Web Gateway
- VPN Replacement

- ZTNA
- CASB
- Remote User Access
- SaaS Visibility
- Network Segmentation

Primary question they solve:

**"Can the user securely access the application?"**

**DefenGPT Focuses On:**

**AI Governance & Security**

- AI Usage Discovery
- Shadow AI Detection
- AI Risk Monitoring
- Prompt Security
- AI Agent Governance
- LLM Security
- AI Compliance
- AI Data Leakage Prevention
- AI Runtime Protection
- AI Auditability

Primary question DefenGPT solves:

**"Can the organization securely adopt AI without introducing governance, compliance, privacy, operational, or reputational risk?"**

**AI Visibility**

**Microsoft / Palo Alto / Netskope / Zscaler**

Can identify:

- User visited ChatGPT

- User visited Gemini
- User visited Claude

Limited visibility into:

- Prompt content
- AI conversation risk
- AI governance posture
- AI model behavior

### **DefenGPT**

Provides:

### **Shadow AI Discovery**

Discovers:

- ChatGPT
- Copilot
- Gemini
- Claude
- Perplexity
- Grok
- DeepSeek
- Custom AI Applications
- Embedded AI Services
- Browser-based AI
- AI Agents

Provides:

- User-level visibility
- Department-level visibility
- Risk categorization

- Business impact analysis

## **AI Security**

### **Traditional Vendors**

Mostly focus on:

- URL filtering
- CASB controls
- Application access

Cannot deeply inspect:

- Prompts
- Responses
- LLM interactions
- Agent workflows

### **DefenGPT AI Security Platform**

#### **Prompt Guardian**

Provides:

- Prompt Inspection
- Prompt Classification
- Prompt Injection Protection
- Sensitive Data Detection
- Policy Enforcement

#### **Model Guardian**

Provides:

- Model Governance
- Model Risk Monitoring
- Model Performance Monitoring
- Hallucination Detection

- Model Usage Analytics

### **AI Gateway**

Provides:

- AI Traffic Mediation
- Centralized Governance
- Policy Routing
- Model Selection
- AI Request Control

### **Anomaly Detection**

Provides:

- AI Abuse Detection
- Data Exfiltration Detection
- Agent Misuse Detection
- Insider Threat Identification
- Behavioral Monitoring

### **AI Agent Security**

#### **Traditional Vendors**

Current limitations:

Most SASE vendors were never designed to govern:

- AI Agents
- MCP Servers
- Agentic Workflows
- Autonomous Decision Making

### **DefenGPT**

Provides:

#### **Guardian Agent**

Purpose-built for:

- Agent Governance
- Agent Monitoring
- Agent Auditing
- Agent Risk Management
- Agent Authorization

Controls:

- What agents can access
- Which tools they can invoke
- What actions they can perform
- What data they can consume

### **Compliance & Governance**

#### **Microsoft / Palo Alto / Zscaler / Netskope**

Offer:

- Security controls
- Compliance reporting

However they do not provide dedicated AI Governance frameworks.

### **DefenGPT**

Purpose-built for:

#### **AI Governance**

Supports:

- ISO 42001
- NIST AI RMF
- EU AI Act
- GDPR
- PDPL

- Industry AI Regulations

Capabilities:

- AI Risk Registers
- AI Asset Inventory
- Governance Workflows
- Policy Management
- AI Audit Trails
- Compliance Reporting

### **Sovereign AI & Private AI**

#### **Traditional Vendors**

Depend heavily on:

- Public cloud infrastructure
- SaaS services
- Internet connectivity

Not suitable for:

- Defense
- Intelligence
- National Security
- Air-Gapped Environments

#### **DefenGPT Private AI**

Supports:

#### **Fully Air-Gapped Deployment**

No internet required.

#### **Fully On-Premise Deployment**

Customer controls:

- Infrastructure

- Models
- Data
- Security

### **Sovereign AI**

Ideal for:

- Ministries
- Defense
- National Security
- Critical Infrastructure
- Oil & Gas
- Utilities

### **AI Security Operations**

#### **Traditional Vendors**

Provide:

- SOC monitoring
- Network analytics
- Threat monitoring

Limited AI-specific capabilities.

### **DefenGPT AI SOC**

Purpose-built for:

- AI Threat Monitoring
- AI Incident Response
- AI Risk Analytics
- AI Governance Monitoring
- AI Compliance Monitoring

Capabilities:

- AI Attack Detection
- Prompt Attack Detection
- Agent Abuse Detection
- AI Data Leakage Monitoring
- AI Runtime Security

### **Board-Level Benefits of DefenGPT**

#### **Reduce AI Risk**

Prevent data leakage, model abuse, and unauthorized AI usage.

#### **Accelerate AI Adoption**

Enable business units to use AI securely and confidently.

#### **Ensure Regulatory Compliance**

Support AI governance and compliance initiatives.

#### **Protect Corporate Reputation**

Reduce risks associated with AI misuse and sensitive data exposure.

#### **Enable Sovereign AI**

Deploy AI entirely within customer-controlled environments.

#### **Future-Proof the Organization**

Secure emerging technologies such as:

- AI Agents
- Autonomous Workflows
- MCP Servers
- Private LLMs
- Generative AI Platforms

## **C-Level Conclusion**

Microsoft, Palo Alto Networks, Zscaler, and Netskope were built to secure users, applications, networks, and cloud services.

DefenGPT AI Security Platform was built to secure, govern, monitor, audit, and operationalize Artificial Intelligence itself.










As AI becomes a strategic business platform rather than just another application, organizations require a dedicated AI Security and Governance layer that sits above traditional SASE and ZTNA architectures.

DefenGPT complements existing SASE investments while providing the AI-specific visibility, governance, security, compliance, and sovereign deployment capabilities that traditional security platforms were never originally designed to deliver.

# DEFENIX

## Defenix: The Complete AI Security Ecosystem

Three powerful solutions. One unified mission: **Secure AI. Protect What Matters.**

	 <b>DEFENIX AI FIREWALL</b> Protect AI Interactions. Stop Threats in Real-Time.	 <b>DEFENIX PRIVATE AI</b> Run AI Privately. Keep Data Yours.	 <b>DEFENIX AI SECURITY PLATFORM</b> Secure Everything. Manage Risk. Prove Trust.	 <b>Stronger Together.</b> <b>End-to-End AI Protection.</b> Defenix AI Firewall, Private AI, and AI Security Platform work together to secure every layer of your AI journey.
 Purpose	Secure AI interactions and prevent threats at the gateway.	Enable private, on-premise or VPC-hosted AI for data sovereignty.	Unify visibility, control, and governance across the AI lifecycle.	
 What It Does	Monitors and filters AI prompts and responses in real-time.	Delivers enterprise-grade AI models in your secure environment.	Discovers, assesses, monitors, and governs AI systems end-to-end.	
 Key Capabilities	<ul style="list-style-type: none"> <li>Prompt &amp; Response Filtering</li> <li>Threat Detection (Jailbreaks, PII, Toxicity, Data Leakage)</li> <li>Real-time Policy Enforcement</li> <li>Custom Guardrails</li> </ul>	<ul style="list-style-type: none"> <li>On-Premise / VPC Deployment</li> <li>Data Never Leaves Your Environment</li> <li>Support for LLMs &amp; GenAI Workloads</li> <li>BYO Model &amp; Infrastructure Flexibility</li> </ul>	<ul style="list-style-type: none"> <li>AI Discovery &amp; Inventory</li> <li>Risk &amp; Compliance Assessment</li> <li>Continuous Monitoring &amp; Alerts</li> <li>Policy Management &amp; Governance</li> <li>Audit Trails &amp; Reporting</li> </ul>	
 Key Benefits	<ul style="list-style-type: none"> <li>Block threats before they reach the model</li> <li>Prevent data leakage &amp; misuse</li> <li>Ensure safe, responsible AI usage</li> </ul>	<ul style="list-style-type: none"> <li>Maximize data privacy &amp; sovereignty</li> <li>Meet regulatory &amp; compliance needs</li> <li>Maintain full control over AI operations</li> </ul>	<ul style="list-style-type: none"> <li>Reduce AI risk across the enterprise</li> <li>Ensure compliance &amp; accountability</li> <li>Build trust in AI with visibility &amp; control</li> </ul>	 <b>AI FIREWALL</b> Protects every interaction.
 Ideal For	Enterprises using public or third-party AI models (e.g., ChatGPT, Claude, Gemini, etc.)	Enterprises with highly sensitive data or strict compliance requirements needing private AI.	Enterprises building, deploying, or scaling AI across functions and teams.	 <b>PRIVATE AI</b> Secures your data and infrastructure.
 Works With	Works with any LLM or AI application 	Deploy with your infrastructure (On-Prem, VPC, Hybrid, Air-Gapped) 	Integrates with your AI stack, tools, and security ecosystem 	 <b>AI SECURITY PLATFORM</b> Governs your AI ecosystem with confidence.

 Defenix is your trusted partner for building, securing, and scaling AI—safely, privately, and responsibly.

