Xilos

THE GOVERNANCE LAYER FOR AGENTIC AI

- Complete AI Visibility
- Accelerates Business Processes
- Realtime Anomaly Detection
- Prevents Data Leakage
- Ensures Regulatory Compliance
- Cross-Agent Learning
- Breaks Down Data Silos
- Private Dedicated LLM Hosting
- Reduces Token Costs

MILL POND RESEARCH

OBSERVE, SECURE, AND PROTECT YOUR AI INFRASTRUCTURE

The rapid adoption of AI agents has created both **opportunity and risk** for today's enterprises. While these technologies drive innovation, increase revenue, and reduce costs, they've also spawned a **shadow AI crisis** as organizations implement multiple public and private models across departments **without IT oversight** and outside traditional cybersecurity frameworks that were built to track and manage network activities.

As a result, agentic AI systems will freely multiply across your network, operating entirely outside the visibility and control of your CIO and CISO. This unmanaged proliferation has led to **data leakage, compliance violations, and fragmented implementations** that prevent organizations from realizing the full benefits of their AI investments. With a 2025 Komprise survey revealing that **79% of organizations have experienced negative incidents from unmanaged AI use**, coupled with predictions that agent-generated prompts will soon outnumber those from humans, securing and orchestrating your agentic AI has become an urgent priority.

Xilos strikes the perfect balance—enabling the innovation and efficiency of Agentic AI while securing your infrastructure. This novel dual-approach allows your organization to **increase revenue, maximize operational efficiency, and reduce costs without compromising security**.

Xilos provides a comprehensive infrastructure that sits between your AI prompts and models, creating a **secure networking fabric that observes, secures, and orchestrates** all agentic AI activity across your enterprise. The platform gives you complete visibility into every agent interaction, prevents unauthorized data sharing, and breaks down AI silos to **transform isolated implementations into a cohesive intelligence network**.

By intercepting outbound LLM calls, enforcing security policies, and enabling agents to learn from one another, Xilos allows you to **safely deploy agentic AI at scale while maintaining control and maximizing business value**.

MILL POND RESEARCH

Xilos SOLUTION OVERVIEW

Observe

Xilos provides **complete visibility** into every AI agent interaction across your enterprise, **delivering actionable insights** that transform hidden AI activities into transparent, manageable assets you can **monitor, measure, and optimize**.

Complete Agent Visibility

Gain 100% visibility into every query from every agent connected to your network

Behavioral Analytics

Access detailed insights into agent behavior patterns across your entire infrastructure

AI-Driven Reporting

Understand not just what is happening, but why, with intelligent reporting tools

Proactive Anomaly Detection

Identify unusual patterns and potential security issues before they impact your organization

Comprehensive Logging

Maintain records of all incoming queries + responses for auditing

Secure

Xilos secures by **intercepting and filtering AI interactions** in real-time, **preventing data leakage** while enabling secure access to both public and private LLMs through a **proprietary security framework** built specifically for autonomous AI systems.

Query Interception

Block unauthorized LLM calls while allowing approved interactions

Real-Time Query Modification

Mask or remove unsafe components from queries without disrupting operations

Proprietary Security Engine

Leverage our natural language engine built specifically for agentic AI security

Private LLM Hosting

Host private, air-gapped LLMs for your most sensitive data and operations

Hybrid Model Support

Simultaneously utilize public and private LLMs according to security requirements

Orchestrate

Xilos orchestrates isolated AI systems into **unified intelligence** by enabling agents to s**hare contextual knowledge** across your organization — breaking down departmental silos to deliver **more precise, company-specific insights** towards your goals.

Cross-Agent Learning

Enable your AI agents to learn from one another and continuously improve

Intelligent Caching

Reduce token consumption by up to 20% through our advanced query caching system

Contextual Intelligence

Our system learns your organization's structure and information requirements

Cross-Functional Information Sharing

Deliver contextually relevant information across all departments

Data Silo Elimination

Break down AI barriers to create a unified intelligence framework

MILL POND RESEARCH

Xilos ENTERPRISE-WIDE IMPACTS

CIOs

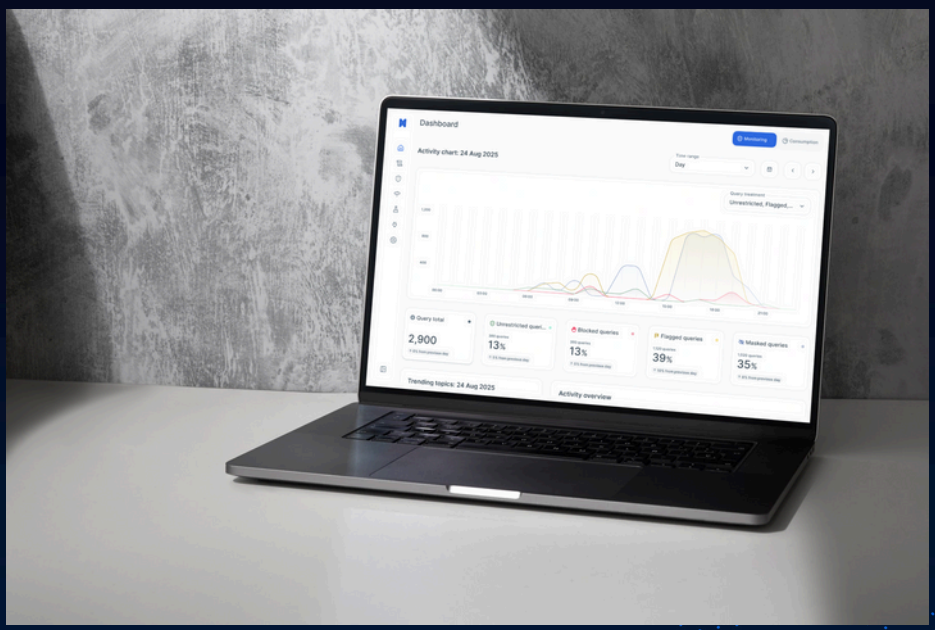
Gain **complete visibility** into all AI tools operating on your network while streamlining organizational efficiency. Xilos helps you break down departmental AI silos, reduce token costs through **intelligent caching**, and enables cross-functional knowledge sharing required for realizing AI's full potential across your entire organization.

CISOs

Secure your AI systems with purpose-built protection that proactively prevents data leakage and policy violations. Maintain compliance with industry regulations with ease all while supporting your organization's AI adoption with confidence.

Business Leaders

Measure and report the business impact of AI with comprehensive dashboards. Reduce risk while driving **competitive differentiation** through **secure, cross-departmental AI** collaboration that accelerates decision-making and augments human capabilities.



MILL POND RESEARCH

FAST INNOVATION WITHOUT SACRIFICING SECURITY

Xilos enables organizations to **accelerate agentic AI innovation** while maintaining robust security by **observing, securing, and orchestrating** all prompt-based interactions. Xilos **eliminates the traditional trade-off between innovation, speed, and security** controls by providing **complete visibility** into your networks AI activity and **preventing data leakage** through real-time query modification. Our patented approach empowers your organization to confidently **deploy AI systems without compromising sensitive data** and within your compliance requirements. Xilos effectively transforms the problems of AI from security liability into an **unstoppable strategic business asset**.

Security & Compliance

Xilos provides a **cutting-edge comprehensive security framework** specifically **designed for agentic AI**. Our platform ensures sensitive company and customer **data remains protected** while maintaining **compliance with industry regulations**.

Operational Efficiency

By orchestrating AI agents across your organization, Xilos enables **automative collaboration between departments**, eliminates redundant work, and provides **contextually relevant information** where it's needed most.

Cost Optimization

Xilos's intelligent caching system **reduces token charges** by automatically serving known answers to common queries, while our orchestration layer ensures you're getting **maximum value from your AI investment**.

Risk Mitigation

With the majority of organizations reporting negative incidents from unmanaged AI use, Xilos provides the **visibility and control needed to prevent costly data breaches** and compliance violations.

New Competitive Advantage

As AI becomes critical to business operations, Xilos enables your organization to **privately and securely deploy agentic AI** to drive innovation and differentiation in your market **without compromising your data to external "data-hungry" services**.

MILL POND RESEARCH

AI GOVERNANCE ECOSYSTEM

Xilos works seamlessly with Mill Pond Research's **WorkBench** platform, creating a **complete end-to-end solution for agentic AI**. **WorkBench** enables you to **create, test, and deploy** sophisticated AI agents. Xilos ensures operate securely within your enterprise environment. This novel integrated approach gives CIOs and CISOs a single source of truth to lower AI risk and increase operational efficiency.

The **Xilos** Rules Engine was built from the ground up as a modular system, supported by a deep **ecosystem of third-party partners**. This architecture enables the creation of vertical-specific rule sets that prevent agentic AI breaches of external policies, while the integrated partner ecosystem strengthens your AI governance by **combining specialized expertise** with **comprehensive solutions to enhance security, compliance, and business outcomes**.

MILL POND RESEARCH

Ready to try it out?
Sign up for a demo to experience first-hand how Xilos can transform your organization's approach to AI
www.millpondresearch.com