Xilos

Mill Pond Research

Transform Risk into Revenue

Intelligent AI Infrastructure for Modern Enterprise Security & Productivity

The AI Security Crisis

Every day, your employees send thousands of queries to AI systems. Each interaction is a potential security breach. Without visibility or control, sensitive data flow freely to external providers while costs spiral out of control.

Observe. Secure. Orchestrate.

Your organization's transformation starts here. Xilos provides the intelligent infrastructure that empowers organizations to reap all of the benefits of AI while reigning in control of their data streams.

Learn how Fortune 500 companies are securing their AI future →

Xilos

Mill Pond Research

XILOS is a prompt-based intelligence platform that observes, secures, and orchestrates agentic AI to maximize the efficiency and utility of all connected AI systems and agents — across every department, team, and use case in your organization.

Observe

Highlights all connected agents and services — empowering CISOs and CIOs to monitor, assess, and manage usage with unmatched clarity, ease of use, and control.

Secure & Route

Restriction and routing rules are applied ensure safe AI usage — applying safeguards to ensure the protection of private company and customer data.

Orchestrate

Incoming queries and responses are cached and enhanced with company context, creating more insightful questions and answers.

Xilos solves the security challenges of agentic AI by intercepting outbound LLM calls and determining which are allowed, while proactively blocking those that are not.

Xilos learns and understands context from every prompt and every agent it has ever seen, then uses that knowledge to append or refine all future prompts.

Xilos includes an orchestration layer to interconnect all prompts, enabling them to learn from one another.

Xilos breaks down silos and sharing the most relevant information with those who need it through prompt caching.

About Mill Pond Research

Mill Pond Research delivers enterprise-grade agentic AI solutions that transform business operations. As active members of the US AI Safety Institute Consortium, we are at the forefront of developing and deploying responsible AI solutions while modernizing legacy systems without costly overhauls. The team combines technical innovation with business strategy, guiding clients through AI implementations that deliver measurable ROI and a competitive advantage in today's evolving technological landscape.