THE SHADOW AI CRISIS

MILL POND RESEARCH

XILOS

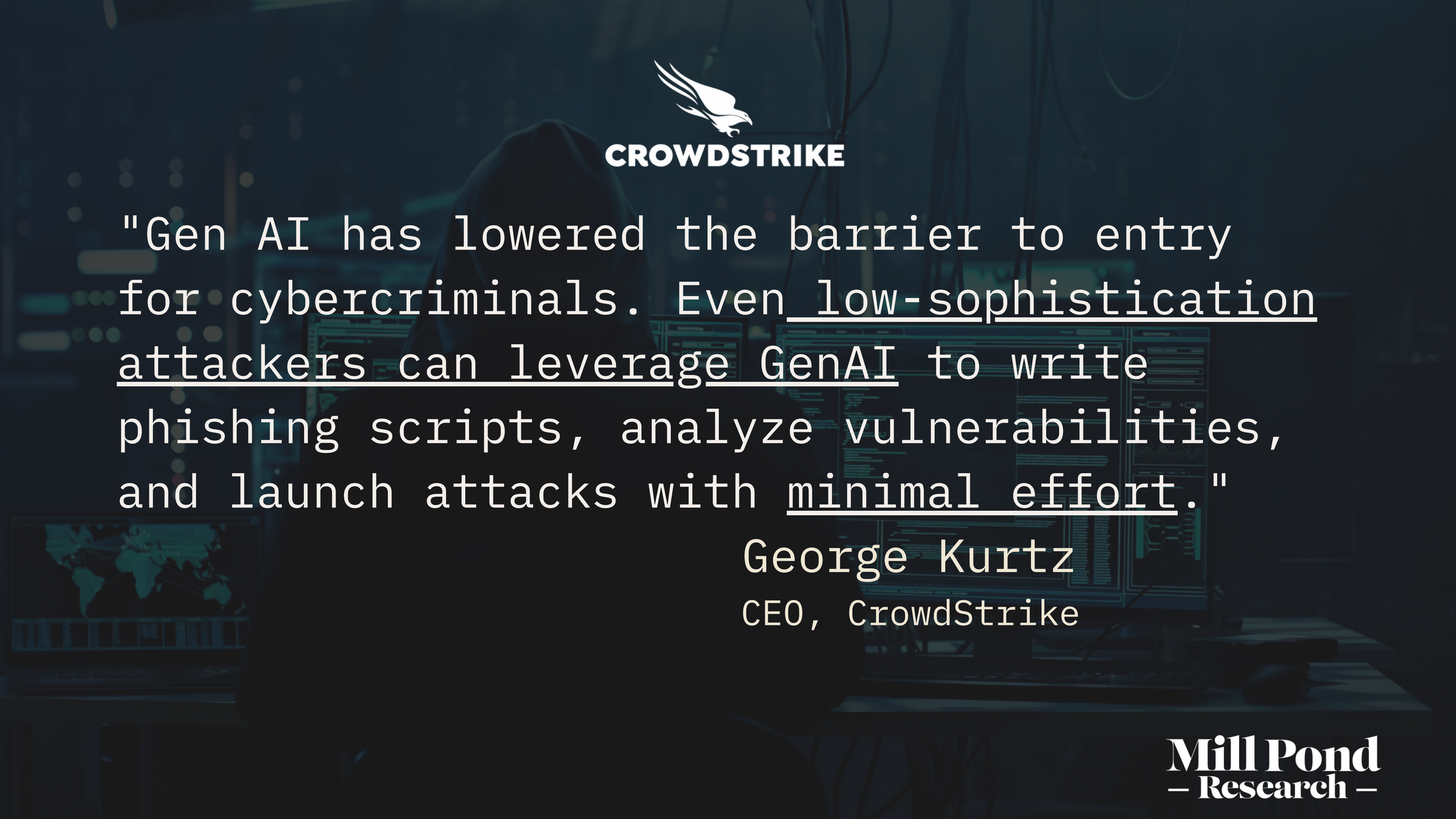
THE ***RAPID ADOPTION*** OF **AI** IN **ENTERPRISES**

- **71% of businesses** now use generative AI, a **33% increase in 2 years**
- End users across organizations experiment **ahead of formal policies**
- Low barriers to entry and slow institutional adoption drives **rapid unsanctioned adoption**

THE ***IMPENDING*** **AGENTIC AI REVOLUTION**

- In the *near future*, a majority of AI prompts will come from agents rather than people
- **65% of Fortune 500 companies** will deploy autonomous agents across multiple business functions by 2026

Mill Pond Research



"Gen AI has lowered the barrier to entry for cybercriminals. Even low-sophistication attackers can leverage GenAI to write phishing scripts, analyze vulnerabilities, and launch attacks with minimal effort."

George Kurtz

CEO, CrowdStrike

Mill Pond Research

*"Current AI policies **do not fully address** the unique **risks of agentic systems.**"*

McKinsey & Company

*"Enterprise cybersecurity frameworks **do not account for autonomous agents** that can act with discretion."*

---

*"**AI governance often fails** because it's implemented as departmental initiatives **rather than enterprise strategy** with board-level ownership and accountability."*

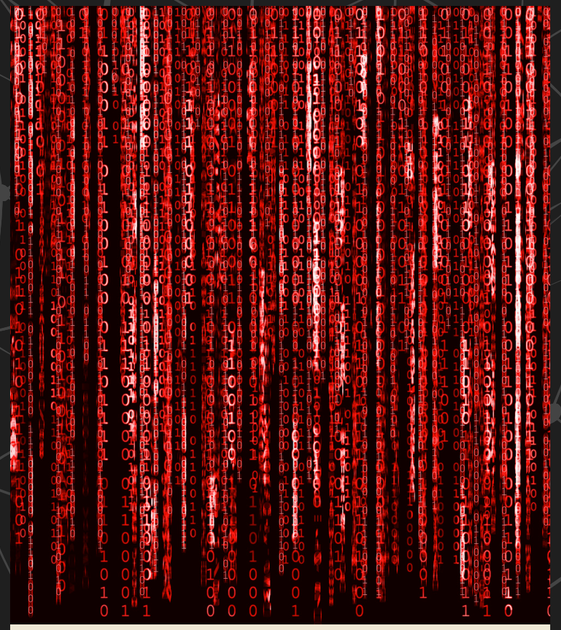
paloalto NETWORKS®

Mill Pond Research

THE SHADOW AI CRISIS CREATES *CRITICAL CHALLENGES*

LACK OF VISIBILITY

INADEQUATE SECURITY



PROLIFERATION OF SHADOW AI

SILOED DATA

Mill Pond Research

97% of organizations lack basic access controls for AI systems

On average, each shadow AI breach costs organizations **$4.63 million** or **$670,000 more** than a non-AI data breach.

65% of shadow AI breaches involved compromised customer PII

IBM's 2025 Cost of a Data Breach Report

Mill Pond Research

THE CONSEQUENCES

CIOs

- **Loss of control**
- **Inefficient** resource allocation
- Innovation **friction**
- Measurement **challenges**

CISOs

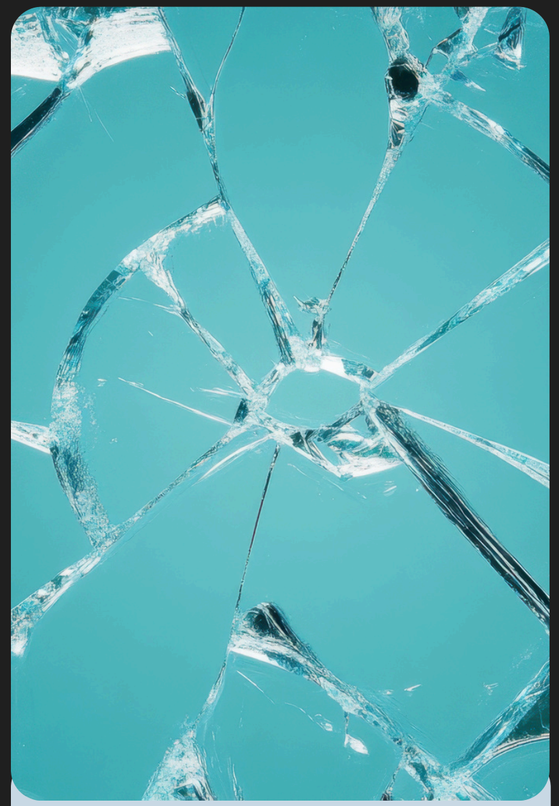
- **Data leakage**
- Compliance **violations**
- Extended **attack surfaces**
- **Lack of traceability**
- **Unclear** responsibility

Business Leaders

- Deployment **bottlenecks**
- **Inconsistent** performance
- **Lack of knowledge** transfer
- **Ongoing tension** between security and innovation

Mill Pond
— Research —

Current Market Offerings Fall Short



FRAGMENTED APPROACH

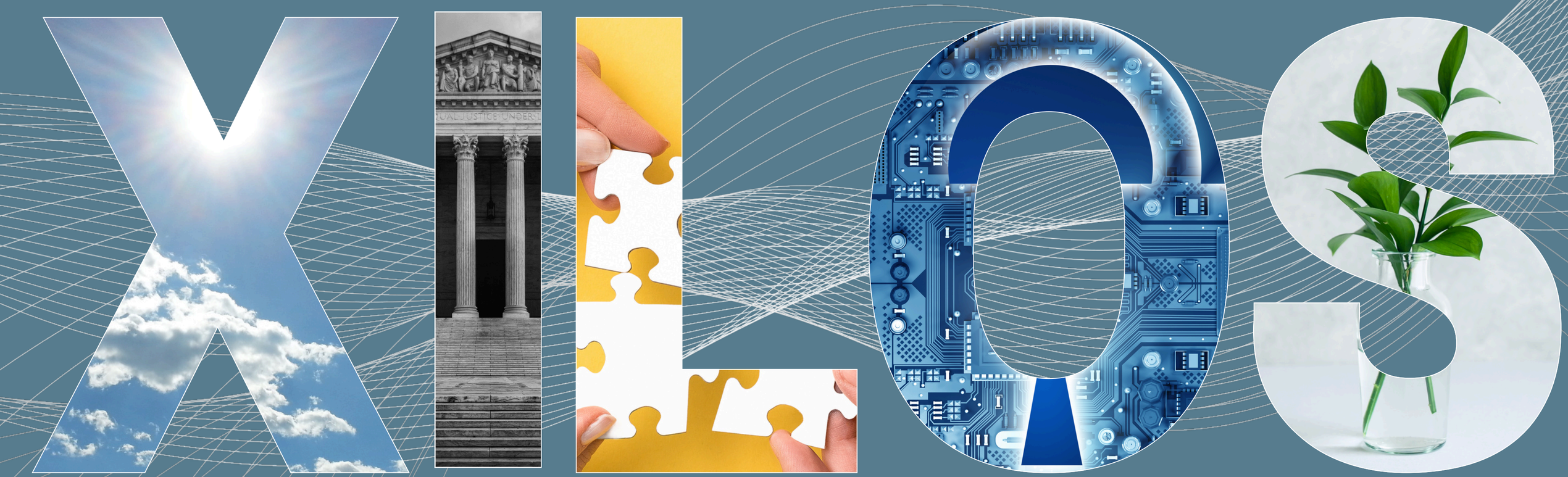
OUTDATED SECURITY FRAMEWORKS

GOVERNANCE GAPS

TECHNICALLY LIMITED

Mill Pond Research

The Ideal Solution



Complete Visibility | Governance Integration | Cross-Agent Orchestration | Robust Security | Easy Implementation

XILOS

Mill Pond Research

XILOS

Mill Pond Research

OBSERVES

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 what and why happen incidents happened 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

SECURES

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 Model
Leverage our natural language model built specifically for enterprise AI security

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

Hybrid Model Support
Simultaneously utilize both public and private LLMs according to security requirements

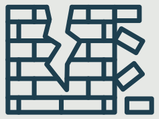
ORCHESTRATES

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

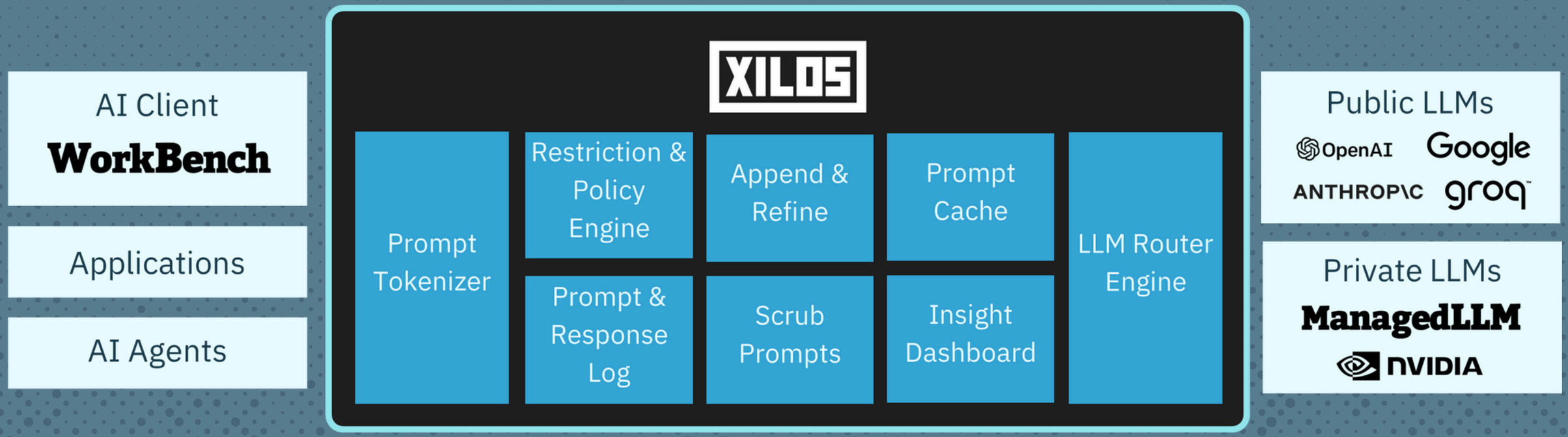
Cross-Functional Information Sharing
Deliver contextually relevant information across all departments



Data Silo Elimination
Break down AI barriers to create a unified intelligence framework

Mill Pond
– Research –

A Complete AI Governance Ecosystem



Our Partners aws Azure IBM infoblox NIST ORACLE SailPoint Secure AI ZEALSTRAT

XILOS

READY FOR HIGH-SECURITY DEPLOYMENTS

Deploy private, air-gapped LLMs for highly-sensitive workloads

Automatically route sensitive traffic to secure environments

Maintain security and privacy while leveraging AI capabilities

The **only AI Governance Ecosystem** to deliver secure LLM integrations — **right out of the box**

U.S. Department of War

NIST CENTER FOR AI STANDARDS AND INNOVATION (CAISI)

NIST U.S. ARTIFICIAL INTELLIGENCE SAFETY INSTITUTE

NIST CYBERSECURITY FRAMEWORK

XILOS

OUR RESULTS

CIOs

- **Precise metrics** demonstrating **AI ROI**
- A **clear path to AI adoption** across the enterprise
- **Elimination** of redundant AI **investments**

CISOs

- **100% visibility** into AI activity
- Significant **reduction of data leakage** through Shadow AI channels
- Completely **comprehensive audit trails** for **compliance**

Business Leaders

- **Faster** development and deployment cycles
- More **accurate** and **consistent** AI outputs
- Enhanced **cross-functional collaboration**

Mill Pond Research

MILL POND RESEARCH

XILOS

WorkBench

THANK YOU

MillPondResearch.com
Xilos.AI
contact@millpondresaerch.com