xage SECURITY + Microsoft

SOLUTION BRIEF

Xage + Microsoft: Securing Enterprise Agentic AI from Identity to Action

Enable AI autonomy without expanding trust

AI agents retrieve sensitive data, invoke tools, delegate tasks, and execute actions across enterprise systems. Securing them requires controls over both the agent and the resources it can reach, especially as workflows span SaaS, cloud, data centers, operational technology (OT), and edge environments.

Xage extends Microsoft's foundation with deterministic authorization and enforcement outside the model, at both the agent and the resource. Every tool call, API request, and delegated action is checked against what the agent is approved to do, whether the agent runs in Copilot Studio, Foundry, or a custom runtime, and whether it reaches SaaS, cloud, OT, or edge systems.

Complementary capabilities, layered protection

Microsoft: Agentic AI security foundation

Microsoft provides Agent 365 for agent visibility and administration, Entra for agent identity and access, Purview for data protection and compliance, Foundry for agent, model, and tool management, and Defender and Sentinel for threat protection and security operations.

Xage: Agent-side and Resource-side Zero Trust Enforcement

Xage Zero Trust for AI adds:

Agent Sentry

Runtime visibility and control around supported agent runtimes, including prompts, tool usage, API calls, network access, and local system interactions. Each agent gets a unique identity and a tamperproof, action-level record.

Resource Gateway

Authentication and authorization of access to protected resources and LLMs through supported MCP and API paths across SaaS, databases, cloud services, OT, and edge systems.

Distributed least privilege

Identity-based policies, just-in-time access, time-bound delegation, and multihop privilege enforcement across heterogeneous workflows.

Action-level accountability

Records of initiating users, executing agents, resource interactions, and policy decisions, with telemetry exportable to SIEM and SOC tools.

Shadow AI discovery

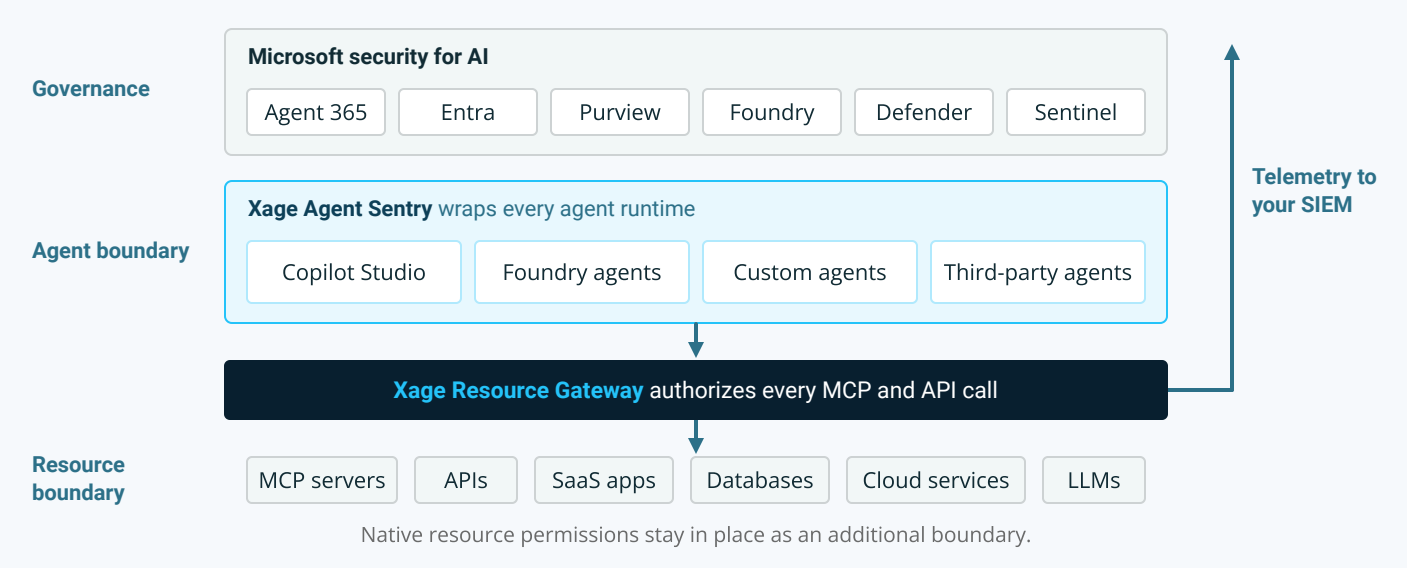
Finds unmanaged agents and AI applications and brings them under policy or isolates them.

Credential Management

Securely stores and rotates API keys and tokens agents use with applications and data sources, so a compromised agent cannot expose them.

 © Xage Security | All Rights Reserved

Deployment Architecture



Design principle **Authorization is enforced outside the model, and protected resources are reachable only through controlled paths.**

Operational coordination: Define identity mappings, policy ownership, escalation paths, and telemetry correlation across Xage and Microsoft controls. Policies do not sync automatically between platforms.

What Xage adds to your Microsoft security stack

Extend existing investments.

Keep Agent 365, Entra, Purview, Defender, and Sentinel as your system of record. Xage adds enforcement at the agent and resource boundaries and sends action-level telemetry to your SIEM.

Cover agents beyond Microsoft runtimes.

Xage Agent Sentry and Resource Gateway apply unified policy to custom runtimes, third-party agents, MCP servers, and systems in data centers, private and third-party clouds, OT, and edge environments.

Protect data on every path.

For Agent 365, Purview DLP enforcement covers human-to-agent and agent-to-human interactions in Teams, SharePoint, OneDrive, and email. Xage redacts PII and confidential data on agent-to-tool and agent-to-agent paths, and agents inherit existing user and application permissions without data retagging.

Keep delegation and revocation enforceable downstream.

Xage traces identity and delegated privilege across multi-agent chains. A low-privileged user cannot escalate through a privileged agent, delegated rights are task-specific and time-bound, and zero standing privileges limit what lingering sessions can reach after an agent is disabled.

About Xage Security

Xage Security is the leader in Zero Trust for high stakes environments. The Xage Fabric Platform applies identity to everything, creating a unified enforcement layer across users, machines, and AI agents. By helping organizations block cyber threats, ensure resilience, and accelerate innovation, Xage enables them to operate with confidence. Learn more at xage.com.

www.xage.com | info@xage.com | © Xage Security | All Rights Reserved

xage SECURITY