xage SECURITY

Unified Zero Trust for Data Centers and IT

New applications and requirements are reshaping data centers and IT environments, but also expanding the enterprise attack surface—from new apps, LLMs and AI agents to backend digital infrastructure and critical cyber-physical systems like cooling, power, and building management. Point products fall short against today's threats like data leakage, rogue AI and insider misuse to attacks on the digital and physical systems that keep the enterprise running. As threats become more dynamic, with AI itself being weaponized for attack purposes, organizations need certainty and resilience in their security posture.

Xage's Unified Zero Trust platform delivers identity-first protection across every layer of the stack—spanning digital workloads (apps, LLMs, AI agents, and data) and cyber-physical systems (DCIM, HVAC, BMS, power, and cooling). By enforcing **identity-first, least-privilege access across every interaction—human, machine, agent, and system**—Xage prevents lateral movement, blocks unauthorized data exposure, and ensures compliance. Whether it's securing an LLM-to-database query, a vendor session into DCIM, or access to a GPU cluster, Xage applies the same rigorous, tamperproof, identity-based control.

Unleash Data Center Potential—Without Compromising Security

Harden the Attack Surface

Enforce least-privilege, just-in-time access, and network segmentation policies, and eliminate unmanaged VPNs and traditional PAM solutions.

Simplify Compliance and Operations

Centralize security, visibility, and control across IT, OT, cloud, and AI workloads.

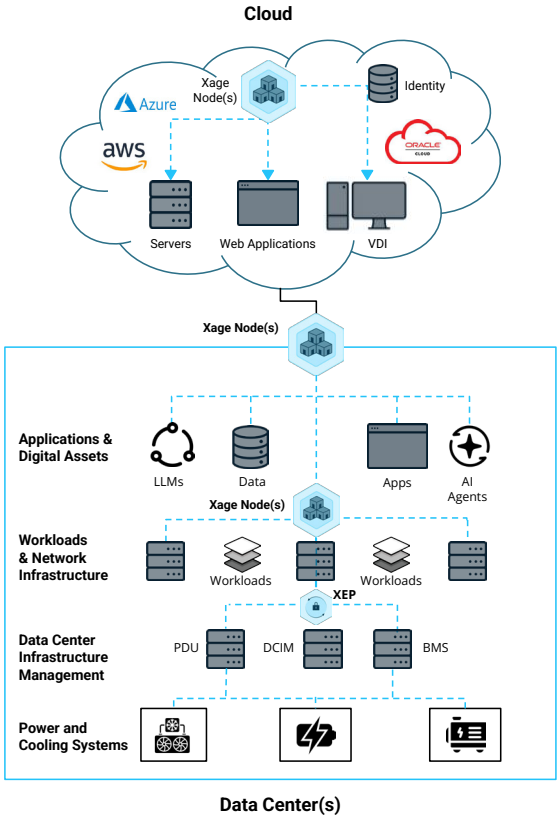
Designed for Scale

Distributed, resilient architecture ensures protection even during outages or air-gapped deployments.

Xage Secures the Full Data Center Stack

The Xage Fabric enforces identity-based Zero Trust across workloads, infrastructure, and non-IT systems (e.g. OT systems) as demonstrated below in the architecture diagram. By overlaying fine-grained policy enforcement, credential management and vaulting, segmentation, and identity-driven access across distributed and hybrid environments, Xage eliminates unmanaged access and blocks lateral movement.

The result: unified, resilient protection across compute, storage, applications, AI, and the critical infrastructure that powers an enterprise's business.



Zero Trust, Identity-Based Access Management for Workloads

Granular Just-in-Time and Just-Enough Access: Xage enforces identity-based access control (IBAC) at the asset level—spanning servers, storage, VMs, databases, and applications—to apply least-privilege permissions and block lateral movement. Just-in-time and just-enough access provides only the minimal, temporary permissions required, eliminating standing privileges and insider risk. By replacing flat networks and unmanaged VPNs with identity-verified connections, only authorized users, applications, or agents can interact with systems. Context-aware authorization further narrows activity to specific endpoints and actions—for example, read-only access to a single database—reducing misuse while preserving operational agility.

Privileged Access Management (PAM): Xage eliminates static credentials and reduces the attack surface with session-based credential issuance, automatic credential rotation, and secure storage in a tamperproof, quantum-resistant vault. Just-in-time access ensures both internal users and third-party contractors receive permissions only when needed, minimizing insider risk. Smart session recording with visual playback and searchable transcripts streamlines audits, compliance, and incident response. Delivered from day one without complex account discovery, and unified across IT, OT, and cloud environments, Xage Extended Privileged Access Management (XPAM) enables consistent policy enforcement and rapid time-to-value while maintaining long-term resilience against evolving cryptographic threats.

xage SECURITY

Phishing-Resistant Multi-Factor Authentication (MFA) and SSO: Xage strengthens authentication with seamless SSO integration across distributed identity providers such as Microsoft Azure AD and on-prem AD, spanning multiple data centers, security zones, and IT/OT/Cloud environments. Device-level MFA overlay extends strong authentication even to legacy systems that lack native support. By enforcing phishing-resistant MFA (FIDO2), Xage ensures robust authentication everywhere—including on-premises environments without cloud connectivity—closing gaps that attackers often exploit.

AI Workloads and Application Security: Xage extends Zero Trust protection to AI components such as LLMs and AI agents, unifying control across the full AI and data center stack within a single Fabric. This includes secure, fine-grained access to private data sources; seamless LLM-to-data integration across layered and zoned networks; and just-in-time, least-privilege access for AI workflows. Xage also enforces agent-to-agent (A2A) and MCP (Model Context Protocol) security, applies AI guardrails to prevent data leakage or misuse, and delivers governance and compliance through comprehensive auditing of all AI interactions.

Secure Remote Access For Any Assets

Agentless, Browser-Based Access: Xage enables secure remote access without the need for VPNs or endpoint agents. All interactions occur seamlessly through a hardened browser connection, ensuring strong separation between user devices and data center assets. This approach reduces the risk of malware propagation while simplifying access for both desktop and mobile users, delivering security with zero client-side complexity.

Zero Trust Network Access (ZTNA) with Multi-Hop Architecture: Xage enforces Zero Trust Network Access by terminating and re-validating sessions as they traverse zones—including cloud, IT, DMZ, and internal data center segments. This multi-hop design ensures that only authorized access and data transfers are allowed, while blocking day-zero attacks and maintaining strict separation between environments. By removing the need for complex firewall rule changes, Xage simplifies administration while strengthening security boundaries.

Distributed Mesh Architecture: Xage's distributed mesh enforces policy locally at each node while maintaining central orchestration, ensuring continuous protection even during connectivity loss or network interruptions. With no single point of failure, the architecture provides resilient enforcement across all workloads—including those in isolated or air-gapped segments—while extending Zero Trust coverage seamlessly across IT, OT, and cloud environments.

Modern and Secure Authentication: Xage modernizes authentication across diverse environments by requiring users to authenticate with the latest standards while proxying sessions to legacy assets that lack native support. This approach ensures strong, consistent security without disrupting operations or requiring invasive system upgrades, allowing even outdated systems to be protected under a unified Zero Trust framework.

Remote Access with Native Apps: Xage extends Zero Trust protection to users who require access through native desktop tools such as PuTTY, database clients, or engineering applications. The Xage Access Connector (XAC) delivers secure connectivity with granular policy control, ensuring that even traditional client sessions are mediated through Zero Trust containment points. This approach provides users with the flexibility of their preferred tools while maintaining strict enforcement of access policies and endpoint posture checks.

Power and Cooling System Protection

Asset-Level Zero Trust for OT Infrastructure: Xage applies the same identity-based Zero Trust controls to power, cooling, and BMS devices and applications as it does to digital workloads. This ensures only verified personnel can access or modify critical environmental controls, reducing the risk of tampering with the systems that safeguard DCIM, PDU, BMS and hardware operations.

System Shielding with Microsegmentation & Virtual Patching: Xage protects vital OT infrastructure with policy-driven microsegmentation and virtual patching, shielding systems from threats without requiring disruptive updates or downtime. This layered defense prevents exploitation while maintaining system availability and operational continuity.

Remote Maintenance Access for Vendors: Xage enables temporary, tightly controlled access for maintenance vendors with session recording, live monitoring, and automatic revocation when work is complete. Supporting multiple protocols such as RDP, VNC, SSH, HTTP/S, and OT protocols such as Modbus, DNP3 and BACnet, all external exposure is contained through Zero Trust fabric and protocol proxying to ensure secure, auditable vendor interactions.

Resilient & Offline Enforcement: With distributed enforcement nodes, Xage maintains policy control even in isolated networks or during connectivity loss. This resilience is critical for edge deployments and air-gapped data center segments, ensuring continuous Zero Trust protection under all conditions.

Access Management for DCIM Solutions: Xage extends governance to Data Center Infrastructure Management (DCIM) platforms by securing privileged accounts and enforcing authentication for all DCIM-driven actions. It also controls how DCIM interacts with downstream cyber-physical assets—such as PDUs, cooling, and BMS systems—ensuring that every change is both authenticated and authorized.

Secure Machine-to-Machine Communication

M2M Policy Enforcement: Xage secures machine-to-machine (M2M) interactions by controlling and monitoring protocol-level communications between applications, LLMs, AI agents, orchestration tools, and infrastructure services. By enforcing identity-based access policies, Xage ensures that telemetry, model data, and configurations are transferred only between authenticated and authorized entities, preventing unauthorized connections or data leakage while maintaining operational integrity.

Protocol Support: Xage supports a broad range of protocols—including RDP, SSH, HTTP/S, and Modbus, DNP3, BACnet — across IT, OT, cloud-native, and legacy environments to deliver Zero Trust Network Access (ZTNA) without disruption. For AI-specific use cases, Xage extends this protection to Agent-to-Agent (A2A) interactions and the Model Context Protocol (MCP), ensuring secure coordination, policy enforcement, and guardrails for LLMs and AI agents.

Monitoring, Analytics, and Integrations

Immutable Audit Trails & Session Recording: Xage provides full visibility into user activity across workloads, infrastructure, and OT systems with tamperproof audit trails and complete session recording. Visual playback and searchable logs helps to comply with standards such as NIST, IEC 62443, NIS2, and NERC-CIP, while ensuring accountability and rapid forensic investigations.

Xage Insights, Risk Management & Adaptive Access: With real-time analytics across users, devices, and applications, Xage delivers continuous visibility into risk and behavior patterns. AI-powered insights enable adaptive access—automatically recommending or enforcing policy changes based on detected anomalies—to reduce threats while optimizing operational efficiency.

Integration with Threat Detection Platforms: Xage integrates with leading security platforms such as Darktrace and Forescout to extend continuous monitoring across IT and OT environments. By correlating Zero Trust access events with anomaly detection systems, Xage enables faster incident response and stronger protection against evolving threats.

Key Benefits of Xage Unified Zero Trust for Data Centers and IT

Xage delivers future-ready Zero Trust for modern data centers and AI environments. By unifying access control, PAM, ZTNA, zero trust segmentation and OT protection within a single distributed platform, Xage ensures secure access, continuous enforcement, and full-stack resilience. From compute and storage to AI applications, cooling, and power, Xage enables organizations to scale securely, comply confidently, and operate without compromise.

Advantage	Value Delivered to Data Centers
End-to-End Coverage for Distributed Environments	Secure digital workloads, AI applications, and OT systems alike with zero trust policy enforcement
Asset-Level Zero Trust	Fine-grained control across compute, storage, apps etc. and HVAC/ power/BMS assets
Distributed, Resilient Architecture	Maintains protection during outages, isolation, or failover
Agentless Operation	Simplifies third-party and vendor access, does not require any system-level changes
Adaptive Access	Accelerates incident response and policy optimization and automatically adapts access using risk and threat analysis
Virtual Airgaps and Microsegmentation	Reduces attack surface without disrupting network topology
Jailbreak-Proof AI Data Protection	Enforce policy at protocol level for LLMs, AI agents, and applications

About Xage Security

Xage Security is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.

xage SECURITY