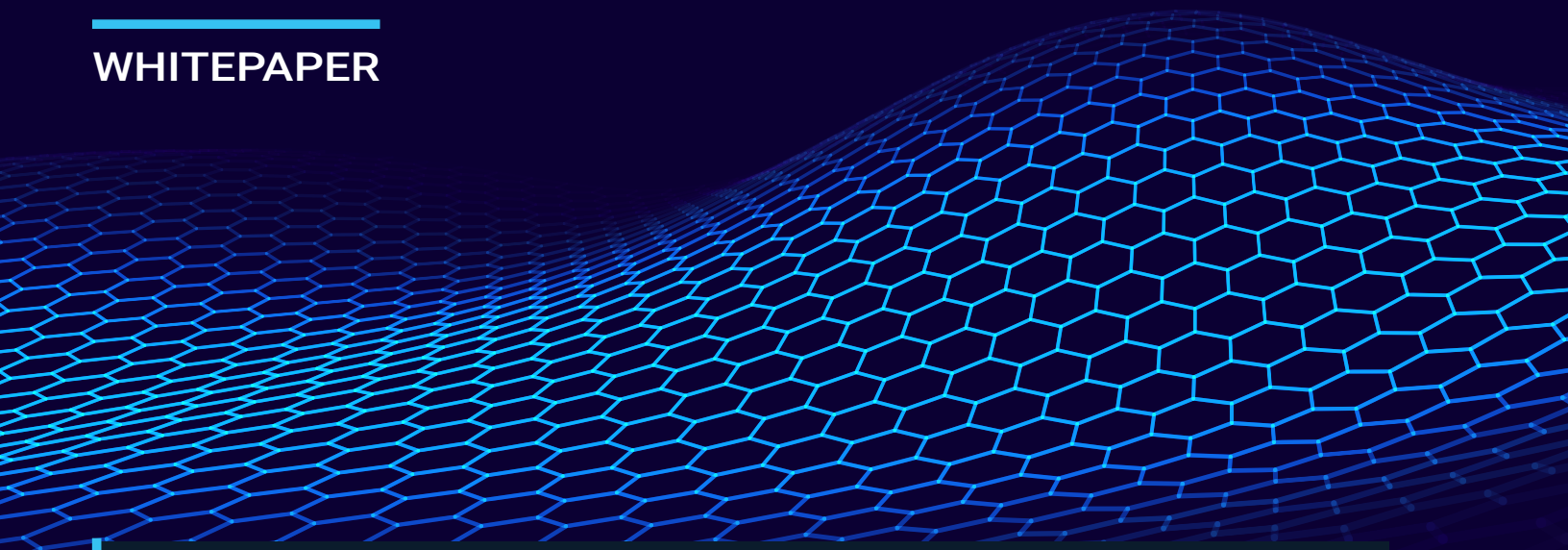
xage SECURITY

Asset Protection

Identity-based access control and asset-level microsegmentation across IT, data centers, AI infrastructure, and operational technology

WHITEPAPER



Asset Protection reduces the exposure of every asset and permits only explicitly authorized interactions,combining identity-based access control, asset-level microsegmentation, and session-scoped enforcement. If hackers gain access to your network, Xage's Asset Protection hides your organization's assets from the attackers' malware, preventing the attack from proceeding even when your organization's assets and resources have vulnerabilities that would otherwise be exploited by the attackers.

xage SECURITY

Protect the critical systems that power business and operations—without forcing a wholesale network redesign or placing agents on every asset.

Executive Summary

Organizations depend on chains of interactions spanning people, workloads, applications, data, management systems, AI agents, and operational technology. One compromised identity or system becomes consequential when it can discover and reach everything around it. Traditional boundaries reduce exposure, but broad trust inside those boundaries can still connect malware to high-value assets. AI increases the speed and scale of cyber-vulnerability discovery and exploitation, while patching cannot keep pace across every legacy, high-availability, and mission-critical system.

Xage addresses that gap with two coordinated layers. The distributed Xage Zero Trust Identity Fabric establishes identity, policy, credential services, authorization context, brokering, and audit evidence. Xage Extended Protection (XEP) enforces these access policies close to individuals, devices, groups, switches, workloads, applications, or controllers. Together, they create only authorized human-to-machine and machine-to-machine interactions just-in-time, then remove that reachability when it is no longer needed—reducing risk and blast radius while supporting uptime, operational resilience, and stronger audit evidence.

EXECUTIVE TAKEAWAY

Reduce reachable attack surface, contain compromise, preserve uptime, and give authorized personnel and machines controlled access to the exact resource they need.

The Problem: Compromise Becomes Consequence

Attackers often enter through ordinary means: a stolen credential, vulnerable application, exposed remote service, compromised supplier, trusted account, or manipulated AI agent. The initial event becomes serious when accumulated trust and weak internal segmentation let the attacker traverse shared services, management planes, data-center workloads, and OT assets.

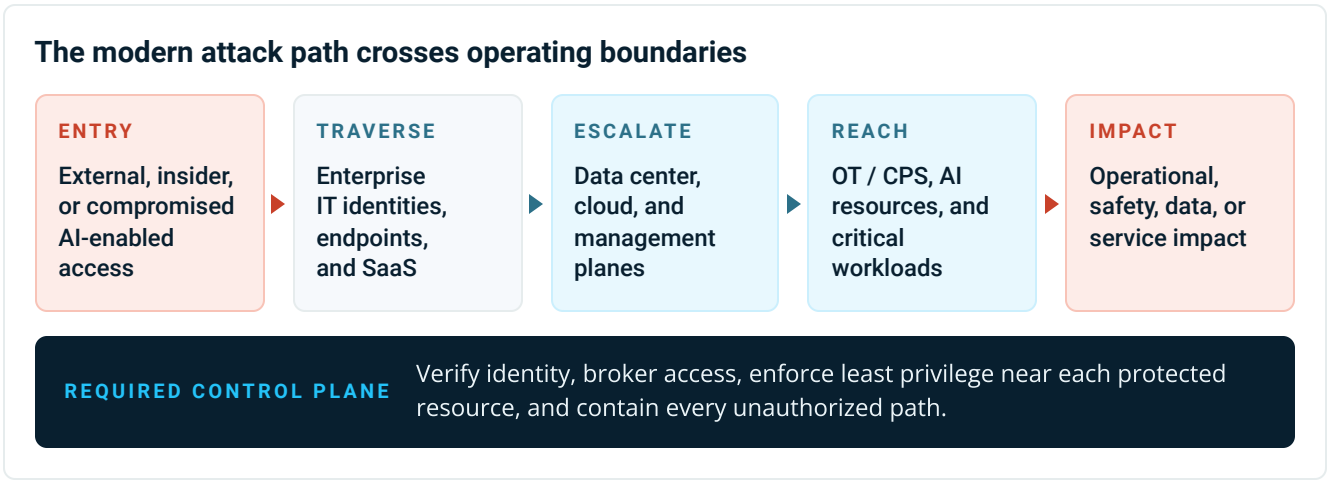


Figure 1. A generic attack path across enterprise, data center/cloud, AI, and OT environments.

AI compresses the time between discovery and exploitation, while many legacy or high-availability assets cannot be patched on demand. The practical objective is to assume prevention may fail—and to keep one compromised component from creating a usable path to everything that matters.

What Effective Protection Requires

Effective critical asset protection must narrow access from a broad network allowance to a specific interaction while supporting layered architectures, mixed-generation assets, operational availability, and maintainability. It must work across both modern and legacy protocols without requiring every protected asset to run an agent or support current authentication methods.

ASSET-LEVEL CONTROL

Make the final controller, workload, application, service, or data resource the policy target.

HUMAN + MACHINE IDENTITY

Treat users, devices, services, workloads, applications, and AI agents as policy subjects. Bind machine access to an approved identity and endpoint fingerprint. When an identity or fingerprint changes, deny or isolate the machine until it is revalidated.

JUST-IN-TIME, TIME-LIMITED ACCESS

Create the least-privilege path only when the approved task begins. Remove the path at logout, timeout, revocation, or policy change.

LEGACY SUPPORT

Protect assets that cannot host agents, support modern authentication, or tolerate frequent patching.

LOCAL ENFORCEMENT

Continue policy decisions at remote, air-gapped, or degraded sites without continuous cloud reachability.

AUDITABILITY

Connect the initiating identity, final target, policy decision, protocol, action, and session.

LATERAL CONTAINMENT

Control east-west interactions inside a zone as well as traffic crossing zone boundaries.

DISTRIBUTED RESILIENCE

Keep approved operations running during central-service, cloud-connectivity, or security-component failures. Use local enforcement, redundancy, and tested recovery procedures so security infrastructure does not become a single point of operational failure.

The architecture test

Can an unauthorized identity discover the asset? Can a valid identity reach more than its approved target? Does access persist longer than the task? Does policy survive loss of central connectivity? Can investigators trace the initiating person or machine to the final asset and action?

SUCCESS CRITERION

The end state is not more segments. It has fewer unauthorized interactions and smaller consequences when one identity, workload, or device is compromised.

This resource-centric approach aligns with zero trust and microsegmentation principles by basing access decisions on verified identities, protected assets, and explicitly authorized communications.

How Xage Identity Fabric and XEP Work

Xage Critical Asset Protection combines a distributed trust layer with policy enforcement close to protected resources. The Fabric establishes identity and policy; Xage Nodes authenticate, authorize, and broker access; and XEP enforces those decisions inline.

XEP hosts a distributed software-defined networking (SDN) controller that controls connectivity across complex distributed environments. By seamlessly orchestrating policies from the Xage Identity Fabric down to the edge, the XEP provides a unified control plane that enables consistent and scalable enforcement across any number of distributed locations.

xage SECURITY

At the heart of its value proposition is the ability to enforce precise, granular security through intelligent flow control. The XEP controller identifies and controls network flows at a granular level, allowing organizations to permit or deny traffic based on device identity, application type, communication protocols, and other policy criteria. By dynamically enforcing these tailored access policies at the network edge, XEP ensures that data is only exchanged between authorized assets, significantly reducing the attack surface while maintaining the operational flexibility required for dynamic ecosystems.

FABRIC

Administers identities, assets, credentials, policy, distributed trust, and audit evidence.

XAGE NODES

Authenticates and authorizes locally with SSO and phishing-resistant MFA, broker and proxy approved sessions, and carries policy across multi-hop interactions.

XEP

Enforces human-to-machine and machine-to-machine policies inline near physical or virtual resources.

V2P STUDIO

Discovers assets, observes required interactions, and helps translate them into enforceable policy.

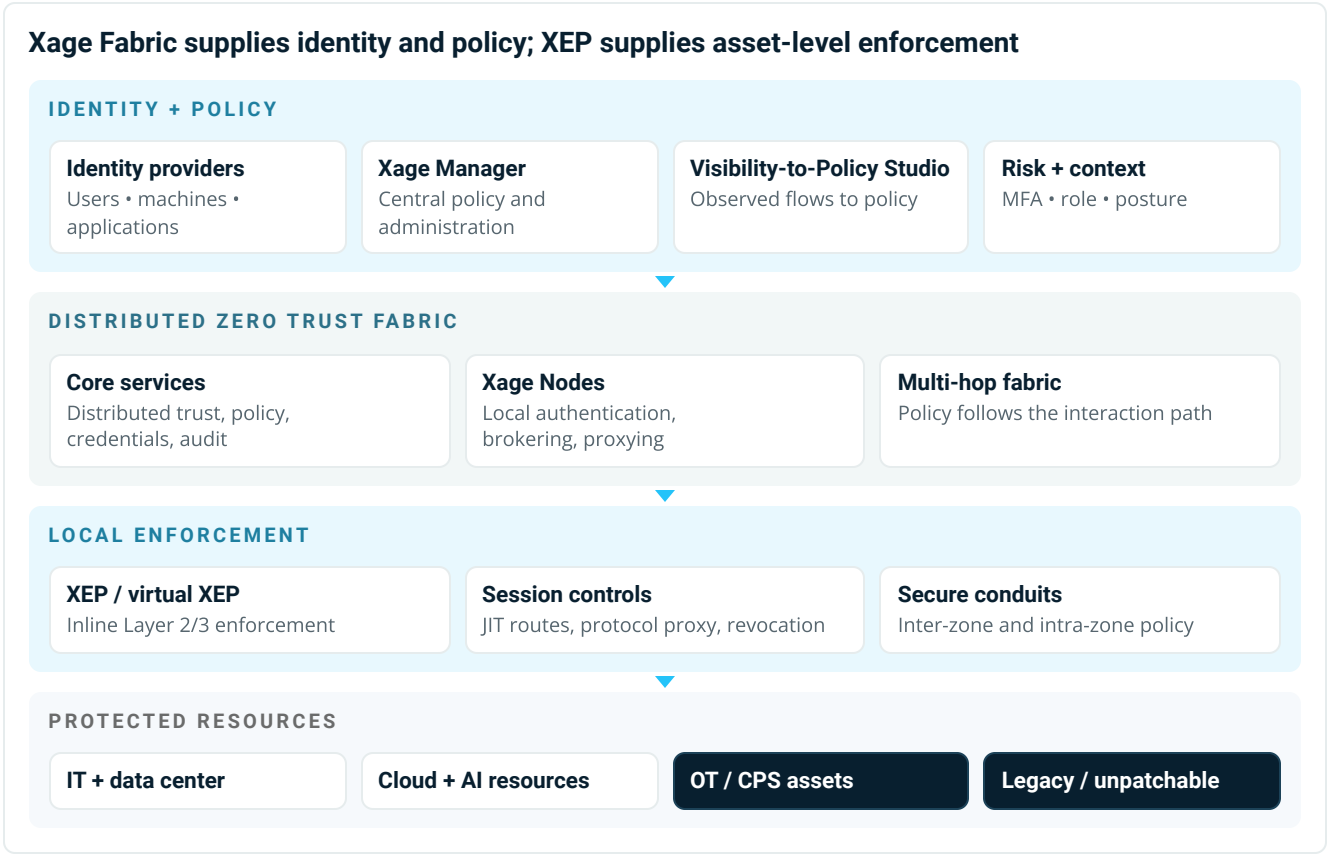


Figure 2. High-level Xage Zero Trust Identity Fabric and XEP architecture.

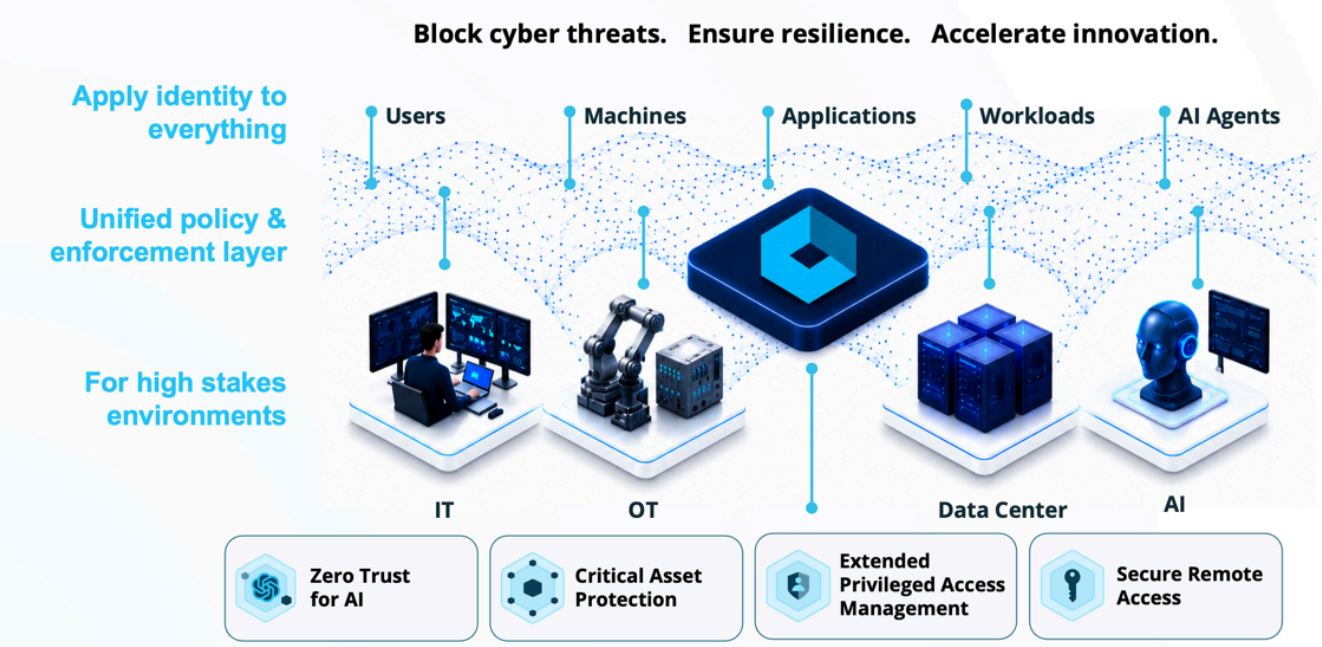


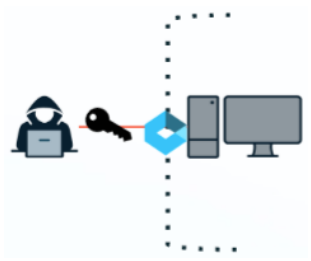
Figure 3. Xage Zero Trust Identity Fabric applies identity and unified policy across human and non-human identities.

ARCHITECTURE PRINCIPLE

Centralized administration does not require continuous connectivity to Fabric Nodes or XEPs. Distributed policy services and local enforcement support disconnected and degraded operations. Deployments should also validate redundancy, component-failure behavior, and recovery so protection does not interrupt approved operations.

Four Ways Xage Identity Fabric and XEP Protect Critical Assets

Together, the Xage Identity Fabric and XEP apply four preemptive controls that do not depend on detecting malicious behavior first: reduce exposure, broker approved access, authenticate and authorize every interaction, and contain the reach of a compromised identity or resource—even across networks and systems.

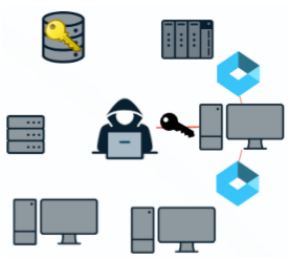


STEP 1

Initial Access (Compromised identity or rogue device)

Xage prevents initial intrusion

- Authenticates users and machines
- Auto-rotated credentials and MFA prevent stolen credentials from being weaponized
- Least privilege by default
- Unauthorized devices cannot automatically communicate with other assets



STEPS 2, 3, 4

Discovery, Lateral Movement, & Privilege Escalation

Xage blocks lateral movement and privilege escalation

- Least privilege access policies by default
- Identity-based machine-to-machine control prevents lateral movement

STEP 5

Data Exfiltration For Dual Extortion

Xage prevents theft of credentials

- Distributed password vault
- Encryption
- Fingerprinting and integrity checks
- Zero trust control for all data access and movement

STEP 6

Propagate & Trigger Malware

Xage prevents ransomware propagation

- Malware detection through ICAP integration
- File integrity checks to assure no tampering
- Limit blast radius

Figure 4. Existing Xage controls applied across the attack chain. The four protections below organize those controls around the asset interaction.

1. Hides Assets

The Xage Fabric overlays existing networks from cloud to edge and granularly controls network paths, sessions, and credentials using identity, policy, and context. Whether users, agents, or systems are local or remote, they cannot see anything on the network before authentication and authorization. Once authenticated, they see only the assets they are authorized to access.

By hiding assets from unauthorized users and systems, Xage reduces reconnaissance and vulnerability-scanning opportunities. Attackers cannot target what they cannot see.

OT EXAMPLE

An engineering laptop may reach the approved HMI yet remain unable to enumerate or directly connect to other controllers.

IT / AI EXAMPLE

A workload or AI agent may reach an approved API call, MCP tool, or data service without receiving standing reachability to adjacent calls, tools, or systems.

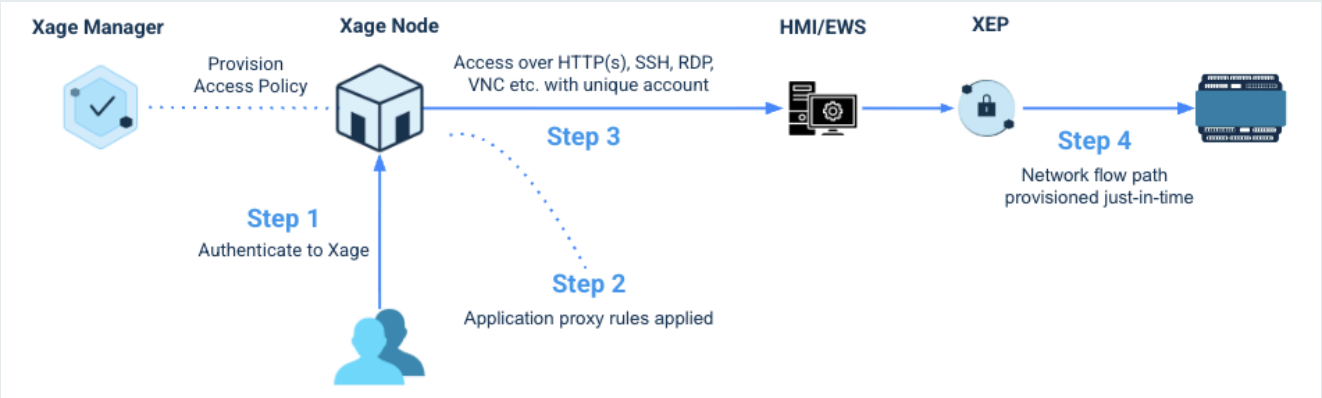


Figure 5. Identity follows the authorized interaction; a second downstream asset remains hidden and unreachable because policy does not authorize it.

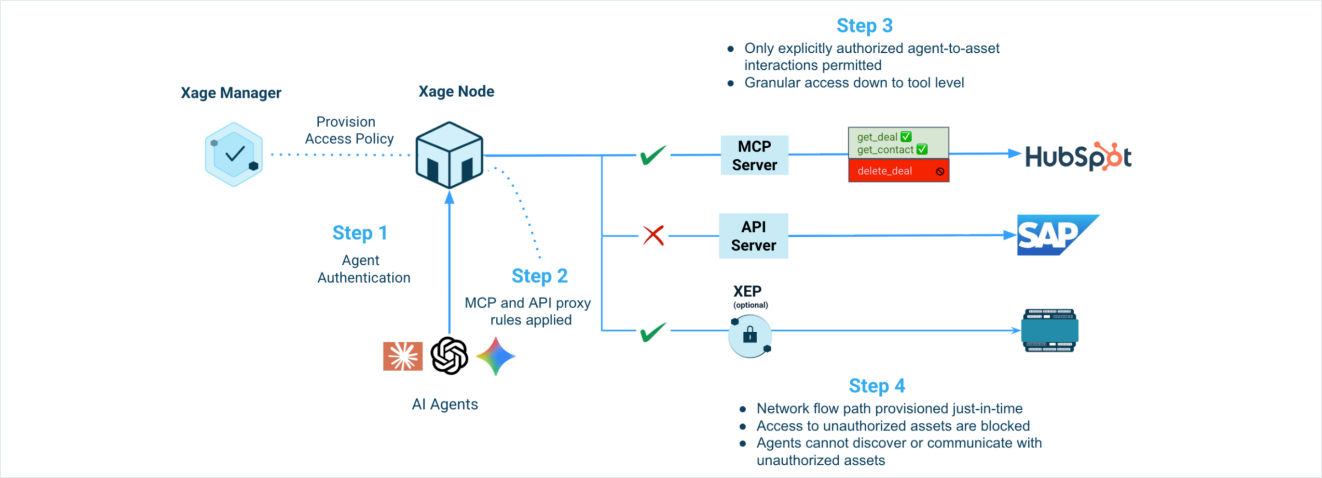


Figure 6: AI Agents can interact only with authorized data sources via MCP or API; authorization granted down to individual tool level

2. Enforces Secure, Brokered Access

The Fabric evaluates the requester, target, protocol, context, and time. Every requester—including a user, device, workload, service, or AI agent—must be authenticated and authorized. There is no direct network connectivity between users and protected assets. All traffic is proxied through the Xage Fabric. Protocol breaks and inspection points prevent exploits and malicious payloads from reaching protected resources.

A local or remote user or AI agent authenticates with the Xage Fabric, optionally using phishing-resistant MFA. Only after successful authentication is access granted to authorized assets and resources. Credentials can be injected just in time into target assets so users and agents never see them, while the Xage Fabric proxies the session to the asset. Xage Fabric Nodes proxy and relay interactions across multiple hops, ensuring that systems remain isolated—sometimes behind several layers—and thereby eliminating direct connections.

That identity is carried through the network as the user interacts with other assets. Xage automatically programs network flows into XEPs to grant access only to specific assets, according to the policy associated with the identity. When a user or agent ends the session, those network paths are removed, proxies are closed, and accounts are removed.

ONE APPROVED TARGET

Permit only the approved identity and endpoint flow rather than opening an entire zone. XEP validates the expected source, destination, protocol, direction, and endpoint fingerprint. Traffic that does not match the approved interaction is denied, helping block unauthorized or malware-driven communications.

CONTROL THROUGH INTERMEDIARIES

Reaching an HMI or workstation does not automatically authorize every asset behind it.

SESSION-SCOPED REACHABILITY

Remove the downstream path at logout, timeout, revocation, or policy change.

LOWER CHANGE BURDEN

Overlay granular control without redesigning every route or installing agents on every endpoint.

PRE-EMPTIVE EFFECT

The first two protections remove unnecessary visibility and replace broad connectivity with one controlled path to one approved resource.

3. Authenticates and Authorizes Every Interaction

Strong authentication and identity verification at multiple layers, including phishing-resistant MFA, validate both the requester and the target resource. Only authorized users, devices, applications, and agents may interact with critical assets.

Xage verifies the identities of both human users and AI agents before granting access to assets. For human users, Xage integrates with enterprise IdPs and supports established enterprise authentication mechanisms, including phishing-resistant MFA. The authenticated identity then informs Xage policy enforcement, determining which assets the user is authorized to access.

Xage authenticates each AI agent through an approved machine identity, such as an OAuth token or API key, and applies least-privilege policy to the tools, APIs, and resources the agent may use. Xage separately authenticates to the downstream enterprise resource using a brokered or just-in-time credential, so the agent does not receive standing privilege or reusable resource credentials. If an agent is compromised or attempts an action outside policy, Xage can deny the action, revoke its access path, isolate it from protected resources, and preserve an action-level audit record.

Xage integrates with multiple enterprise IdPs, allowing organizations to use their existing identity infrastructure while centralizing access and policy enforcement for users, agents, and machine identities. The added benefit is Xage Fabric's ability to authenticate with multiple IdPs in separate layers while applying consistent authorization policies.

For environments where connectivity to a centralized IdP is intermittent or unavailable, Xage's distributed architecture supports offline authentication. Authentication and policy information is securely distributed across the Xage Fabric, enabling authorized users to continue accessing permitted assets.

HUMAN IDENTITIES

Apply MFA, role, approval, least privilege, and time limits to employees, administrators, contractors, and vendors.

MACHINE + AI IDENTITIES

Control device, service, workload, application, and AI-agent interactions with explicit resource policy.

LEGACY DESTINATIONS

Extend modern identity and authorization to assets that cannot natively enforce those controls.

AUDIT CONTINUITY

Correlate the initiating identity, intermediary, final target, decision, and activity.

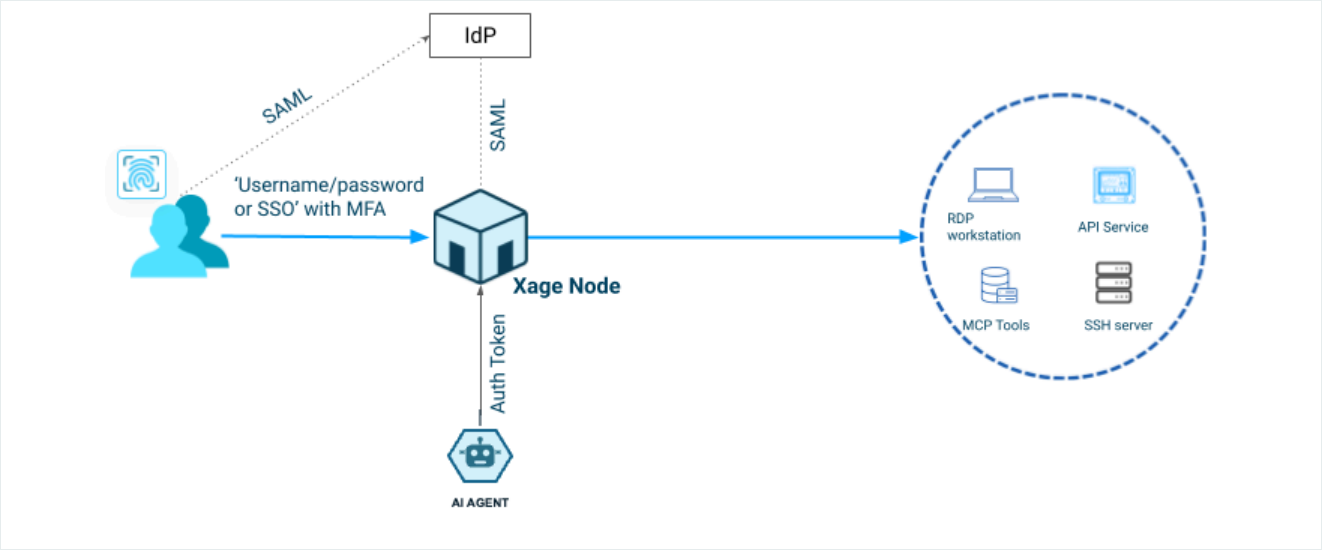


Figure 7. Xage independently authenticates users, AI agents, and machine identities, then enforces policy-based access to downstream assets.

4. Contains Compromise and Lateral Movement

Microsegmentation restricts communications to explicitly authorized paths, preventing attackers from moving between systems. Xage simplifies and extends traditional zones-and-conduits architectures through dynamic zero-trust segmentation and automated, policy-controlled secure tunnels that connect only approved users, agents, machines, and assets. This limits the blast radius and contains breaches before they spread.

XEP provides dynamic **machine-to-machine segmentation** by dividing traditionally flat networks into distinct groups of users, agents, and assets and controlling the communication paths between them. Xage discovers and inventories assets, creates identities for them, and provides a registration workflow. IPsec tunnels between XEPs form optionally, serving as secure conduits for inter-zone communication and optionally encrypting data in transit. Xage supports both just-in-time and persistent segmentation policies.

XEP tunnels provide more than secure connectivity; they enable fine-grained policies between assets. Rather than allowing unrestricted interaction between entire network zones, organizations can define explicit policies that specify which assets may interact within and across zones. XEP enforces these policies at the asset level, limits communication to required interactions, and continuously monitors for violations and behavior changes. Policies can be unidirectional or bidirectional. By restricting communication pathways according to explicit policy and continuously monitoring behavior, XEP helps isolate systems and contain the impact of a compromise.

Xage Visibility-to-Policy (V2P) Studio accelerates the transition from asset discovery to enforceable microsegmentation. It shows the assets and communications observed by XEP so teams can identify required interactions and translate them into least-privilege policies. Administrators can create recognizable device identities, organize assets into logical groups, and build policies from actual behavior instead of packet captures, spreadsheets, or assumptions.

Organizations can begin with XEPs in monitoring mode, review and refine proposed policies, and move to enforcement when ready. This evidence-based approach reduces manual effort, overpermissive policies, and the risk of operational disruption while accelerating deployment across new, expanding, or acquired environments.

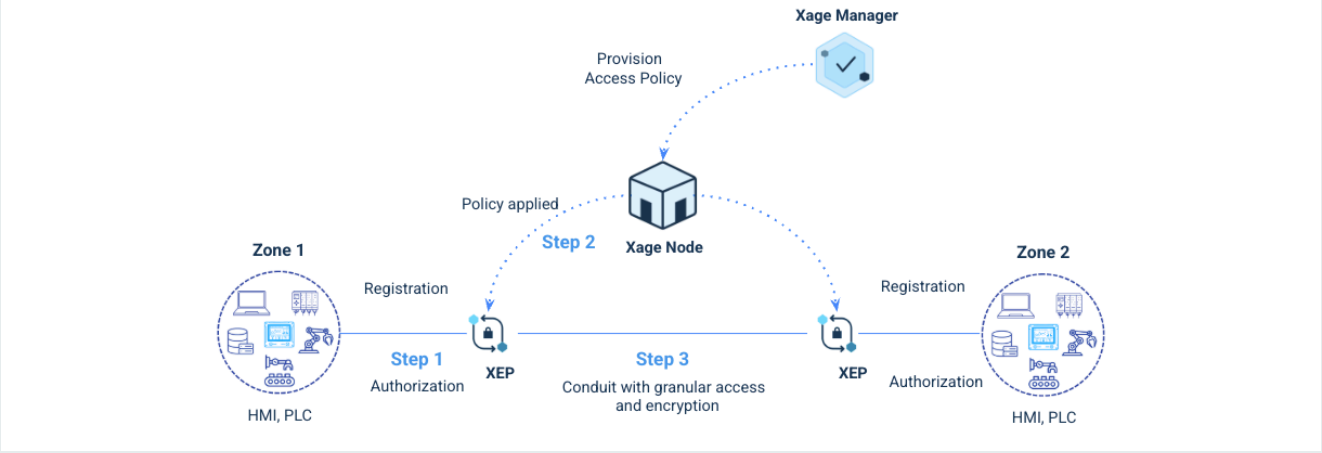


Figure 8. XEP supports policy-controlled conduits between zones and granular controls between assets inside a zone.

Asset Protection vs. Firewalls

Modern NGFWs remain essential for external boundaries. The Xage Fabric, combined with XEP, adds a different control plane: identity-aware, session-scoped enforcement close to critical assets. The strongest architecture uses each where it is most effective.

DECISION CRITERION	NEXT-GENERATION FIREWALL (NGFW)	XAGE FABRIC + XEP
Natural enforcement point	Perimeter, aggregation point, or routed traffic path	Near individual assets, groups, switches, workloads, or controllers
Deployment requirements	Requires network architecture changes	Inline XEP hardware operates transparently in the network as a bump-in-the-wire enforcement point near a protected device, group, or switch. Virtual XEP provides equivalent policy enforcement in virtualized environments. Neither model requires software on the protected endpoint.
Access duration	Allowed network paths are often persistent	Approved interaction is created for the session and removed at logout, timeout, or revocation
Identity context across multiple hops	No identity context as interaction traverse within zones and across networks	Associates the final asset access decision with the initiating human, machine, or AI identity within zones and across networks
Protection for legacy assets and vulnerable protocols	No protocol break or session termination; relies on error-prone inspection of vulnerable protocols	Adds proxy and inline control with session termination and protocol conversion, without requiring an endpoint agent on the protected asset
Scanning exposure	Controls scanning only at the perimeter	Suppresses unauthorized discovery and reachability through the XEP
Credential handling	No application, device, or resource credential handling	Brokers approved sessions, injects credentials, and shields managed credentials and vulnerable protocols from the requester
Disconnected operations	Limited. Relies on centralized authentication services.	Distributed policy and local enforcement are designed for DDIL (denied, degraded, intermittent, and limited-bandwidth) connectivity
Core strength	External (internet) boundary control, traffic inspection, and broad segmentation	Asset-level access, identity continuity, session-scoped reachability, and lateral containment

Table 1. Architecture-level comparison. Actual capabilities depend on vendor, product, licensing, integrations, topology, and configuration.

PRACTICAL ANSWER

Keep NGFWs where external boundary control matters. Add Xage where the decisive requirement is asset protection and lateral containment.

Business Outcomes

The value of critical asset protection is not measured by the number of policies deployed. It is measured by the business risk, downtime, and operational burden removed from the systems and processes that generate revenue, protect data, support customers, and enable growth.

Xage limits the resources a compromised identity, workload, AI agent, or device can reach, reducing the blast radius of an attack. By containing incidents at the individual interaction or asset level, organizations can keep authorized operations and unaffected systems running. Just-in-time, time-bounded access replaces broad standing privileges and manual credential handling, while modern compensating controls extend the useful life of legacy systems that cannot be frequently patched or upgraded.

Xage also reduces the cost and complexity of implementing granular protection. Its agentless overlay adds identity-based access and segmentation without redesigning every network path or installing software on every endpoint. Consistent policies can be applied across OT, enterprise IT, data centers, cloud, edge, and AI environments. Centralized evidence connects each identity, access decision, target asset, and activity record to simplify investigations, audits, and control validation.

Where Critical Asset Protection Matters

In OT and cyber-physical environments, Xage allows engineers, operators, and HMIs to communicate only with approved controllers and devices, helping maintain production while reducing unnecessary intra-zone exposure. In data centers, it restricts administrator, application, and service access to management systems and other critical infrastructure. In cloud and AI environments, it controls how workloads and AI agents interact with data, APIs, models, and services. At distributed or remote sites, local policy enforcement continues to protect critical assets when central or cloud connectivity is degraded or unavailable.

Measuring Business Value

Organizations can establish a credible business case by tracking a small set of operational measures: the number of critical resources each identity or workload can reach, the number of persistent privileged and machine-to-machine paths, the time required to grant or revoke access, and the completeness of identity and activity evidence. Successful deployments should reduce reachable attack surface and standing privilege while improving containment speed, control availability, and audit completeness.

Design for Operational Reality

Before scaling, organizations should validate authorization and enforcement during connectivity loss and test revocation, latency, logging, recovery, and other failure conditions. Deployment boundaries should align with business requirements, operational test plans, and applicable security frameworks. Firewalls and detection technologies should remain in place where they provide valuable boundary inspection and threat visibility.

Conclusion: Close the Path, Not Just the Perimeter

Defending assets means moving beyond traditional perimeter security. Organizations must secure every interaction—whether it occurs within internal zones, through third-party intermediaries, among cloud workloads, or across disconnected environments. Xage Zero Trust Identity Fabric and XEP carry identity and policy to the protected resource, create only the authorized path, and contain everything else.

To see how Xage can protect one high-consequence interaction in your environment, request a demo or speak with Xage at xage.com.

START YOUR PLAN

Bring together the asset owner, operations, security, and access teams for a focused Asset Protection working session. Select one priority interaction, map its current exposure, agree on the approved end state, and define the operational and security measures that will determine success.

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 policy and enforcement layer across users, machines, applications, workloads, and AI agents. The platform combines secure remote access, privileged access management, microsegmentation, and AI security in a single architecture that continuously authenticates, authorizes, and governs every interaction. By helping organizations block cyber threats, ensure resilience, and streamline operations, Xage enables them to accelerate innovation with confidence. Learn why organizations like the U.S. Air Force, Kinder Morgan, and ScottsMiracle-Gro choose Xage at xage.com.

xage SECURITY