xage GOVERNMENT

Xage Security Fabric: A Zero Trust Foundation for Advanced Cryptographic Threat Readiness

Helping critical infrastructure organizations reduce risk today while preparing for post-quantum cryptography.

Xage provides a decentralized Zero Trust security fabric for IT, OT, and cyber-physical environments. The platform is designed to reduce reliance on implicit trust, centralized access paths, standing privilege, shared credentials, and flat network models. These are the areas that become most important as organizations assess advanced cryptographic risk, post-quantum readiness, and long-term protection of critical systems.

A Standards-Based Security Foundation

Xage provides a decentralized Zero Trust platform designed to protect IT, OT, and cyber-physical environments by moving away from implicit trust, centralized access models, and standing privilege.

- **FIPS 140-3 Validation:** Xage has achieved FIPS 140-3 validation for the Xage Cryptographic Module, Certificate #5229. This provides independent assurance that the platform's cryptographic module has been tested against the current U.S. government standard for secure implementation, approved algorithms, key management, and module integrity.
- **A Relevant Starting Point:** FIPS 140-3 is not the same as post-quantum cryptography, but it is a strong and relevant foundation for customers preparing for future NIST-approved PQC requirements. It demonstrates that Xage is built on validated cryptographic controls today while customers plan their longer-term cryptographic transition.

Post-Quantum Standards Alignment

Xage recognizes that post-quantum readiness will require alignment with NIST-approved PQC standards, including FIPS 203 for key establishment and FIPS 204 and FIPS 205 for digital signatures.

Xage is actively working on alignment with these standards as federal agencies, critical infrastructure operators, browsers, operating systems, and protocol ecosystems transition toward PQC adoption.

For internal Xage Fabric communications, Xage is positioned to support post-quantum secure communication as these capabilities are adopted across the platform. For browser-based access, Xage can support post-quantum secure transport where the browser, client, and protocol stack support PQC negotiation.

This gives customers a practical path forward: validated cryptographic assurance today, active alignment with NIST PQC standards, and a security architecture that can evolve as post-quantum requirements mature.

Decentralized Trust and Secret Protection

A core design principle of the Xage Fabric is to avoid unnecessary concentration of trust, especially around credentials, policies, and critical access paths.

Traditional access architectures often rely on centralized systems such as VPN concentrators, jump servers, shared credential vaults, or static administrator accounts. These systems can become high-value targets because one successful compromise may create broad access across the environment.

Xage takes a different approach. The Xage Fabric distributes trust, policy, identity, and secret protection across multiple Fabric nodes. Sensitive secrets are not stored as complete values in a single central repository. Xage uses Shamir's Secret Sharing to split secrets into cryptographic shares and distribute them across the Fabric.

Shamir's Secret Sharing is based on information-theoretic threshold security. This means that shares below the required threshold provide no usable information about the original secret. In practical terms, a single compromised node, or a sub-threshold set of shares, cannot reveal the protected value.

This reduces the risk associated with centralized credential storage. Access to secrets is governed not only by cryptography, but also by identity, policy, authorization, approval workflows, and session context.

Tamper-Resistant Fabric Integrity

The Xage Fabric uses a distributed ledger and consensus-based model to maintain integrity across policies, identities, access decisions, and audit evidence.

This helps ensure that access activity and policy changes are consistently recorded across the Fabric and protected from unauthorized modification. For regulated IT and OT environments, this provides reliable evidence for compliance reviews, incident investigations, and operational audits.

This capability is particularly valuable for organizations subject to NERC CIP, TSA security directives, and internal cyber governance requirements, where proof of access control, policy enforcement, and session accountability is essential.

Reducing Risk During the PQC Transition

The transition to post-quantum cryptography will take time, especially in OT environments. Many control systems, engineering workstations, PLCs, RTUs, HMIs, relays, vendor appliances, and industrial applications have long operating lifecycles and may not support cryptographic updates in the near term.

Xage helps reduce risk during this transition by enforcing strong access, privilege, segmentation, and audit controls around critical systems, including systems that cannot be quickly modernized.

Key capabilities include:

- Zero Trust access for IT, OT, and third-party users
- Just-in-Time and Just-Enough Access
- Zero Standing Privilege
- Privileged access governance
- Distributed secret protection using Shamir's Secret Sharing and threshold-based reconstruction
- Post-quantum standards alignment for internal Fabric and supported browser-based communication paths
- Session recording and auditability
- Identity-aware segmentation
- Tamper-resistant policy and audit integrity
- Local enforcement for disconnected or low-bandwidth OT sites

These controls reduce the attack surface today while organizations continue planning their broader cryptographic modernization and post-quantum transition strategy.

Supporting Legacy OT Systems

Many OT assets were not designed to support modern authentication, encryption, or rapid cryptographic change. In many cases, replacing or modifying these systems is not practical without creating operational risk.

Xage Extended Protection helps address this challenge by placing identity-aware enforcement around legacy OT assets. Organizations can control who can access specific PLCs, HMIs, engineering workstations, and industrial applications, what communication is allowed, and how sessions are governed, without requiring immediate changes to the protected assets themselves.

This provides a practical path for OT environments: protect critical systems now, reduce exposure, and modernize cryptographic controls over time.

Operational Resilience

Critical infrastructure environments are often distributed and may operate under denied, disconnected, intermittent, or low-bandwidth conditions.

The Xage Fabric is designed to continue enforcing policy locally through distributed Fabric nodes. This means access control and logging can continue even when connectivity to a central environment is degraded or unavailable.

For OT operators, this is important because security controls must support operational continuity without creating new dependencies that interrupt operations.

Summary of Alignment

Xage Capability	Relevance to Advanced Cryptographic and PQC Readiness
FIPS 140-3 validated cryptographic module	Provides a validated cryptographic foundation aligned with current U.S. government standards.
Post-quantum standards alignment	Supports customer readiness for NIST-approved PQC standards, including FIPS 203, 204, and 205.
Internal Fabric and supported browser-based PQC paths	Supports post-quantum secure communication where Xage platform capabilities, clients, browsers, and protocol stacks support PQC negotiation.
Distributed secret protection	Uses Shamir's Secret Sharing and threshold-based reconstruction to reduce centralized vault risk and protect sensitive credentials.
Zero Standing Privilege	Limits long-term credentials and reduces exposure from stolen or misused privileged access.
Identity-aware segmentation	Controls access to critical IT and OT systems and reduces lateral movement risk.
Xage Extended Protection	Helps protect legacy OT assets that cannot be quickly upgraded or cryptographically modernized.
Distributed ledger integrity	Provides tamper-resistant policy, access, and audit evidence.
DDIL resilience	Supports local policy enforcement and logging in disconnected or low-bandwidth environments.