# Xage Security Enables Compliance to the NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has long established guidelines for security critical infrastructure which are published under the NIST Cybersecurity Framework. Compliance with these requirements is often required for the entire system as well as its subcomponents. NIST advocates for a comprehensive approach to securing critical infrastructure with special focus on identification, protection, detection, and prevention of cybersecurity incidents. This document describes a real-world example of the NIST Cybersecurity Framework and demonstrates how Xage enables system wide compliance with NIST requirements.

## IDENTIFY (ID)

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

| Subcategory | Vendor Cybersecurity Compliance Question | Vendor Cybersecurity Reference Controls | Xage Value |
|---|---|---|---|
| ID.AM-1: Physical devices and systems within the organization are inventoried. | Describe in detail how your organization maintains accurate inventories of its information systems and components. | • CCS CSC 1<br>• COBIT 5 BAI09.01, BAI09.02<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>• NIST SP 800-53 Rev. 4 CM-8 | Xage Fabric contains inventories of devices and systems in the OT and IT environment. In addition, Xage provides capabilities to detect the addition of new devices/systems and the removal of these assets. Xage inventory can be integrated with additional visibility and resource management tools, and leveraged to automatically track inventory. |
| ID.AM-2: Software platforms and applications within the organization are inventoried. | Describe in detail how your organization maintains accurate inventories of its approved operating systems and applications. | • CCS CSC 2<br>• COBIT 5 BAI09.01, BAI09.02, BAI09.05<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>• NIST SP 800-53 Rev. 4 CM-8 | Xage controls interactions between devices, software applications, and platforms in the OT and IT environment. Xage deploys Fabric nodes into the environment that identify software versions, configurations, installed applications, and controls interactions based approved policies including versions and configurations of applications. |
| ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third- | Describe in detail how your organization establishes and documents cybersecurity-related roles and responsibilities for the | • COBIT 5 APO01.02, DSS06.03<br>• ISA 62443-2-1:2009 4.3.2.3.3 | Xage integrates with multiple directory services including Active Directory, LDAP, certification authorities to provide comprehensive access control universally across the operation based |

| | | | |
|---|---|---|---|
| party stakeholders (e.g., suppliers, customers, partners) are established | entire workforce, including third-party stakeholders (e.g., suppliers, partners, service providers, etc.). | • ISO/IEC 27001:2013 A.6.1.1<br>• NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 | on specific user and resources roles, location, type, and training. |

## PROTECT (PR)

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

| Subcategory | Vendor Cybersecurity Compliance Question | Vendor Cybersecurity Reference Controls | Xage Value |
|---|---|---|---|
| PR.AC-1: Identities and credentials are managed for authorized devices and users. | Describe in detail how your organization has robust processes for managing user credentials through their lifecycle and managing the authorization of devices to access their networks and information. | • CCS CSC 16<br>• COBIT 5 DSS05.04, DSS06.03<br>• ISA 62443-2-1:2009 4.3.3.5.1<br>• ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9<br>• ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3<br>• NIST SP 800-53 Rev. 4 AC-2, IA Family | Xage enables unified user and resource access management with Single Sign-on (SSO) and Multi-Factor Authentication (MFA) universally across the operation with full visibility for auditability. With Xage, organizations can unify identity and access management for users such as employees , temp employees, contractors from multiple directory services as well as resources such as Windows machines, Linux machines, RTUs, PLCs, SCADA apps into a single platform. Operators are able to monitor all authentication and access attempts, enforce specific authentication schemes, disable accounts and revoke access to assets (as a response to a threat, or contract termination), and force credential rotation. In addition, operators are able to automatically revoke access due to policy violations (i.e. changing password every 3 month). |
| PR.AC-2: Physical access to assets is managed and protected. | Describe in detail how your organization has robust processes for managing access to their physical environments. | • COBIT 5 DSS01.04, DSS05.05<br>• ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8<br>• ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3<br>• NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 | Xage integrates with physical access control systems (e.g. card readers, biometric scanners). All identity management is done via a single platform avoiding risks that can occur due to mis-synchronization (i.e. user removed from AD, but was not removed from the biometric scanner). Xage is designed to be a distributed and autonomous system, as such, it operates without network connectivity and will be able to enforce authentication and authorization at the edge without dependency on connectivity to the center and even in cases of partial system failure. |
| PR.AC-3: Remote access is managed. | Describe in detail how your organization has robust processes for managing | • COBIT 5 APO13.01, DSS01.04, DSS05.03 | Xage enables secure remote access to the OT environment with fine-grained role-based access control to individual assets |

| | | | |
|---|---|---|---|
| | remote access to their network for users and contractors. | • ISA 62443-2-1:2009 4.3.3.6.6<br>• ISA 62443-3-3:2013 SR 1.13, SR 2.6<br>• ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1<br>• NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 | (e.g. devices, apps) in the environment. Xage supports encrypted remote sessions and provides a protocol break when required.<br>With Xage, all access to the OT assets is granted only when asked for and only for the period of time needed for the operation at hand.<br>Access is granted to authorized personnel, after going through proper authentication & authorization (including MFA), and carefully monitored for auditing purposes.<br>Xage facilitates remote access which is encrypted end-to-end, and does not allow direct interaction to the protected assets (i.e. all session traffic is securely terminated at Xage) - which drastically reduces the attack surface. |
| PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. | Describe in detail how your organization has robust processes for managing permissions in their corporate network, applications and other information systems. | • CCS CSC 12, 15<br>• ISA 62443-2-1:2009 4.3.3.7.3<br>• ISA 62443-3-3:2013 SR 2.1<br>• ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4<br>• NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 | Xage enables role-based access control access to every interaction across the operation including support for separation of duties and least privilege. Xage is built with IT/OT in mind, including workflows for emergencies, temp employees, and contractors.<br>Once identities and resources (e.g apps, devices) are identified and defined within Xage, role-based interaction policies can be created and then enforced across the enterprise and the operation. Multi-factor authentication schemes can be defined on a per resource and user basis requiring MFA in certain locations and for certain procedures.<br>Xage automates workflows, such as expiration of user accounts and passwords after a certain time, rotating credentials, enabling temporary access in case of emergencies to name a few. All permissions (policy) changes are logged in a tamperproof manner for auditability. |
| PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate. | Describe in detail how your organization has robust processes for managing network traffic throughout their corporate network, to their applications and other information systems. | • ISA 62443-2-1:2009 4.3.3.4<br>• ISA 62443-3-3:2013 SR 3.1, SR 3.8<br>• ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1<br>• NIST SP 800-53 Rev. 4 AC-4, SC-7 | Xage performs network segmentation based on the identity of individual devices, systems, and users. While typical network segmentation tools create static trust between different zones and operate based on the underlying infrastructure (IP), Xage uses an identity-based approach to control interactions within and across trust zones. |

| Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | | | |
|---|---|---|---|
| **Subcategory** | **Vendor Cybersecurity Compliance Question** | **Vendor Cybersecurity Reference Controls** | **Xage Value** |
| PR.DS-1: Data-at-rest is protected. | Describe in detail how your organization protects sensitive information as it rests on storage. | • CCS CSC 17<br>• COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06<br>• ISA 62443-3-3:2013 SR 3.4, SR 4.1<br>• ISO/IEC 27001:2013 A.8.2.3<br>• NIST SP 800-53 Rev. 4 SC-28 | Xage Fabric allows organizations to establish identity management and granular access control by device, application, user, and data stream, to protect data at unparalleled specificity – such as by topic or time – down to the level of individual data values if desired.<br>The data is replicated through the Fabric nodes, to assure it is highly available and not lost in cases of partial system failure.<br>Data is encrypted on a granular basis while at-rest based on data publisher and individual subscriber using a combination of PKI, AES, and Shamir Secret Sharing technology. Data access is also controlled with the same granularity using identities managed through the Fabric.<br>Xage Fabric also controls the data location, based on individual data value and access policy configuration. |
| PR.DS-2: Data-in-transit is protected. | Describe in detail how your organization protects sensitive information as it is transmitted across networks. | • CCS CSC 17<br>• COBIT 5 APO01.06, DSS06.06<br>• ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2<br>• ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3<br>• NIST SP 800-53 Rev. 4 SC-8 | Xage provides end-to-end data authenticity, integrity, and privacy capabilities with strict granular role-based access control. Data in-transit is protected using IPSec tunnels and TLS sessions for individual interactions. Xage system automatically manages keys, certificates, and related authentication whether data is shared inside the operation, control center, data center, cloud, or the broader ecosystem of the organization's customers and partners. |
| PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. | Describe in detail how your organization has robust processes that manage assets through the lifecycle of removal, transfer and disposition. | • COBIT 5 BAI09.03<br>• ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1<br>• ISA 62443-3-3:2013 SR 4.2<br>• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7<br>• NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 | See ID.AM-1 |
| PR.DS-4: Adequate capacity to ensure | Describe in detail how your organization has robust | • COBIT 5 APO13.01 | Xage Fabric is designed as a distributed system with no single point of failure. |

| | | | |
|---|---|---|---|
| availability is maintained. | processes to ensure sensitive information is available for its users. | • ISA 62443-3-3:2013 SR 7.1, SR 7.2<br>• ISO/IEC 27001:2013 A.12.3.1<br>• NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 | Fabric utilizes blockchain technology in nodes enabling peer-to-peer synchronization and consensus mechanisms to ensure tamperproofing. As such, Fabric is designed to be deployed across thousands of locations to ensure that data is available where needed with high scalability and availability even at times of intermittent network connectivity. |
| PR.DS-5: Protections against data leaks are implemented. | Describe in detail how your organization has implemented protection mechanisms against data leaks. | • CCS CSC 17<br>• COBIT 5 APO01.06<br>• ISA 62443-3-3:2013 SR 5.2<br>• ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3<br>• NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 | Data stored in Xage Fabric is encrypted on a per publisher and subscriber basis end-to-end. Data stored in the Xage Fabric is encrypted using a threshold based encryption technique called Shamir Secret Sharing.<br>Shamir's Secret Sharing divides a secret into parts. Each participant is given a unique part. To reconstruct the original secret, a minimum number of parts, or threshold, is required. The threshold is less than the total number of parts and is configurable. A subset of participants can reconstruct the original secret.<br>Compromises on Fabric will require simultaneous access to multiple (threshold) Xage Fabric nodes to provide their shares making data leaks substantially more difficult compared to central databases and not exploitable. |
| PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. | Describe in detail how your organization has robust processes to ensure software, firmware and information maintain their integrity. | • ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8<br>• ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3<br>• NIST SP 800-53 Rev. 4 SI-7 | See ID.AM-2 |

## Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

| Subcategory | Vendor Cybersecurity Compliance Question | Vendor Cybersecurity Reference Controls | Xage Value |
|---|---|---|---|
| PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | Describe in detail how your organization creates and maintains logs of maintenance and has processes to approve and control maintenance tools. | • COBIT 5 BAI09.03<br>• ISA 62443-2-1:2009 4.3.3.3.7<br>• ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5<br>• NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5 | Xage provides a platform to manage identities and access policies which includes ability to enable and limit access to assets based on location, time, and operation by technicians and their roles, organizations, and training levels.<br>This capability enables automation of maintenance schedules as well as provides an immutable audit trail of interactions including who, when, where |

| | | | |
|---|---|---|---|
| | | | and what was performed. This is true for both remote and on-site maintenance. |
| PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | Describe in detail how your organization creates and maintains logs of remote maintenance and has processes that approve remote maintenance. | • COBIT 5 DSS05.04<br>• ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8<br>• ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1<br>• NIST SP 800-53 Rev. 4 MA-4 | See PR.MA-1 |
| **Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.** | | | |
| **Subcategory** | **Vendor Cybersecurity Compliance Question** | **Vendor Cybersecurity Reference Controls** | **Xage Value** |
| PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | Describe in detail how your organization creates audit logs on information systems and reviews them in accordance with security policies. | • CCS CSC 14<br>• COBIT 5 APO11.04<br>• ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4<br>• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12<br>• ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1<br>• NIST SP 800-53 Rev. 4 AU Family | Xage provides tamperproof audit logs for all user authentication and access activities. Xage enables operational and control event correlation to specific users, location and time. Xage fabric enables interaction vistionlity across the operation while providing audit records in a central location with support for integration with SIEM systems.<br><br>In addition to access, authentication and interaction logs, Xage also records all device, users, and policy changes as well as alerts on potential suspicious activity such as frequent access attempts, policy violations, and lateral movement to name a few. |
| PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. | Describe in detail how your organization restricts access to information systems and incorporates the security principle of least privilege. | • COBIT 5 DSS05.02<br>• ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4<br>• ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, | Xage allows access to devices based on identity, role, locations, and operation to each protected asset..<br>As mentioned, Xage will deny ALL network access to a resource (even a legacy device which might not have authentication in place) unless the user, device or application has authenticated (via the Xage enforced authentication policy). Once authenticated, only the specific functions based on the user authorization level will be opened (i.e. ports, or specific functions such as Modbus read, etc...). This assures that authenticated and authorized personnel have access only to functions allowed per their individual profile policy. |

| | | | |
|---|---|---|---|
| | | SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7<br>• ISO/IEC 27001:2013 A.9.1.2<br>• NIST SP 800-53 Rev. 4 AC-3, CM-7 | |
| PR.PT-4: Communications and control networks are protected. | Describe in detail how your organization leverages mechanisms to protect network communications. | • CCS CSC 7<br>• COBIT 5 DSS05.02, APO13.01<br>• ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6<br>• ISO/IEC 27001:2013 A.13.1.1, A.13.2.1<br>• NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 | See all Access requirements (PR.AC). |

## DETECT (DE)

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.

| Subcategory | Vendor Cybersecurity Compliance Question | Vendor Cybersecurity Reference Controls | Xage Value |
|---|---|---|---|
| DE.AE-2: Detected events are analyzed to understand attack targets and methods. | Describe in detail how your organization analyzes security events to understand attack targets and methods. | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2<br>• ISO/IEC 27001:2013 A.16.1.1, A.16.1.4<br>• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 | See PR.PT-1 |

| | | | |
|---|---|---|---|
| DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. | Describe in detail how your organization aggregates data sources to better understand the total impact of a security event. | • ISA 62443-3-3:2013 SR 6.1<br>• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 | Xage event logs (device access, authentication attempts, actions) can be sent via syslog to any SIEM for correlation and enrichment. |
| **Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.** | | | |
| **Subcategory** | **Vendor Cybersecurity Compliance Question** | **Vendor Cybersecurity Reference Controls** | **Xage Value** |
| DE.CM-1: The network is monitored to detect potential cybersecurity events. | Describe in detail how your organization network is monitored to detect potential cybersecurity events. | • CCS CSC 14, 16<br>• COBIT 5 DSS05.07<br>• ISA 62443-3-3:2013 SR 6.2<br>• NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 | Xage audit logs can be used to find patterns and detect malicious activity.<br>Xage automatically detects anomalous activity such as frequent access attempts, simultaneous access attempts, policy violation, lateral movement, to name a few. |
| DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed. | Describe in detail how your organization monitors for unauthorized personnel, connections, devices and software to detect potential cybersecurity events. | • NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 | See PR.PT-1 |

## RESPOND (RS)

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

| **Subcategory** | **Vendor Cybersecurity Compliance Question** | **Vendor Cybersecurity Reference Controls** | **Xage Value** |
|---|---|---|---|
| RS.MI-1: Incidents are contained. | Describe in detail how your organization has processes in place to contain a security incident. | • ISA 62443-2-1:2009 4.3.4.5.6<br>• ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4<br>• ISO/IEC 27001:2013 A.16.1.5<br>• NIST SP 800-53 Rev. 4 IR-4 | Another advantage of managing the entities and the access control in a single place is the ability to respond quickly, and possibly automatically once an attack is identified. For example, if a user account credentials were stolen and the organization is able to detect that (based on anomalies in the access patterns and the actions for example), the |

| | | | |
|---|---|---|---|
| | | | organization can quickly respond by revoking that user access from systems across the operation (which will revoke physical access, network access, PLC access etc.) to contain the incident and limit the impact.<br>Integrating Xage with an IDS/IPS or other detection solutions to fully automate this process - thus stopping and attack quickly and limiting its impact |

## About Xage

The Xage Security Fabric is the universal security solution for modern industrial operations, creating the essential trusted foundation for every interaction, whether human-to-machine, machine-to-machine, or edge-to-cloud. The fabric protects all equipment, from new IoT devices to vulnerable legacy systems, delivering identity management, single sign-on, and access control with in-field enforcement across the industrial operation. Xage is the first and only blockchain-protected security solution providing tamperproof, non-intrusive protection and enabling efficient operations and innovation across all industries. Xage customers include leaders in manufacturing, energy, utilities, and transportation.