xage SECURITY

UNIVERSAL MULTI-FACTOR AUTHENTICATION FOR INDUSTRIAL OPERATIONS

Use Case

Many industrial operations include machines with no password protection, or basic lock/unlock features that lack secure access control. In the last two years alone, digital attacks targeting industrial control systems (ICS) and operational technology increased by over 2000%.

Many of these attacks involved a combination of exploiting known vulnerabilities in supervisory control and data acquisition (SCADA) and ICS hardware components, along with default-password and password-spraying attacks leveraging brute force login techniques.

Furthermore, recent estimates project the number of IoT connections to rise to 83 billion by 2024, with the industrial sector accounting for around 70% of those connections.

The layering of new and legacy systems and technologies, combined with an increase in remote work for the foreseeable future, gives operators less visibility and control over logins happening from various locations at all times – and puts them at massive cyber risk if they leave assets unprotected.

Multi-factor Authentication Scheme

- **Something you know: username/password, pin**
- **Something you have: phone, app, SmartCard, RSA ID**
- **Something you are: fingerprint, retina scan**

Adopting MFA

Organizations are adopting MFA measures to protect identities and access to devices and applications. Compliance standards and guidelines such from NIST, NERC-CIP and IEC-62443 are now requiring MFA to be integrated into enterprise and operational environments.

Most organizations face difficulties integrating existing MFA solutions into their environments. OT/IoT environments are heterogeneous and include legacy devices without any security functionality built into them, managing and operating existing MFA solutions across the different vendors poses an additional challenge. Hence, most organizations are finding it extremely difficult to adopt MFA solutions and integrate them across the entire fleet.

While the partial implementation of MFA solution in the network may provide some value, it leaves the rest of the environment exposed, making non-MFA enabled assets a potential entry point for an attack.

www.xage.com | hello@xage.com

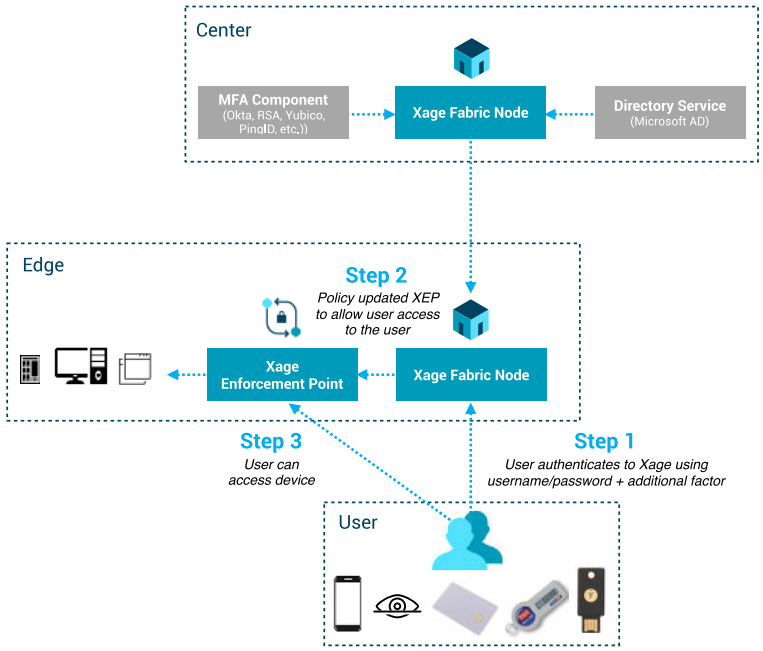
xage

Xage Security for MFA

Xage's enables MFA for any device and application, so industrial organizations can enforce authentication with multiple-factors (passwords, one time token, biometric, etc.) across their entire system. For the very first time, operators can add MFA to all of their assets (new and legacy), and enforce universal multi-factor, identity-based, low latency access on remote assets, even over intermittent networks. Xage's highly resilient authentication and enforcement are delivered at the edge and continue to operate even if connectivity to the center is lost—ensuring universal tamperproofing without additional dependencies. As a result, Xage's MFA solution mitigates a vast array of common cyberattacks, including password spraying attacks, password theft, identity theft attacks, and phishing attacks to plant malware on target devices.

Xage's unified MFA capabilities include:

- Identity-based comprehensive access control per device and application, with integration of additional factors as needed
- MFA enforced via the Xage Enforcement Point (XEP) to any legacy one-factor or zero-factor system
- Distributed MFA-protected access control, even for assets disconnected from the center
- Standardization of multi-factor authentication methods and extends them across their deployment base of applications, workstations, control devices, etc.
- Flexibility in choosing and switching between MFA methods (pins, keys, SmartCards, authentication apps, etc.)
- Compliance with multiple standards across verticals, without the need to replace existing assets
- Tamperproof audit trail for all machine-to-machine and user-to-machine interactions



About Xage Security

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.

Xage Security
445 Sherman Avenue, Suite 200
Palo Alto, CA 94306