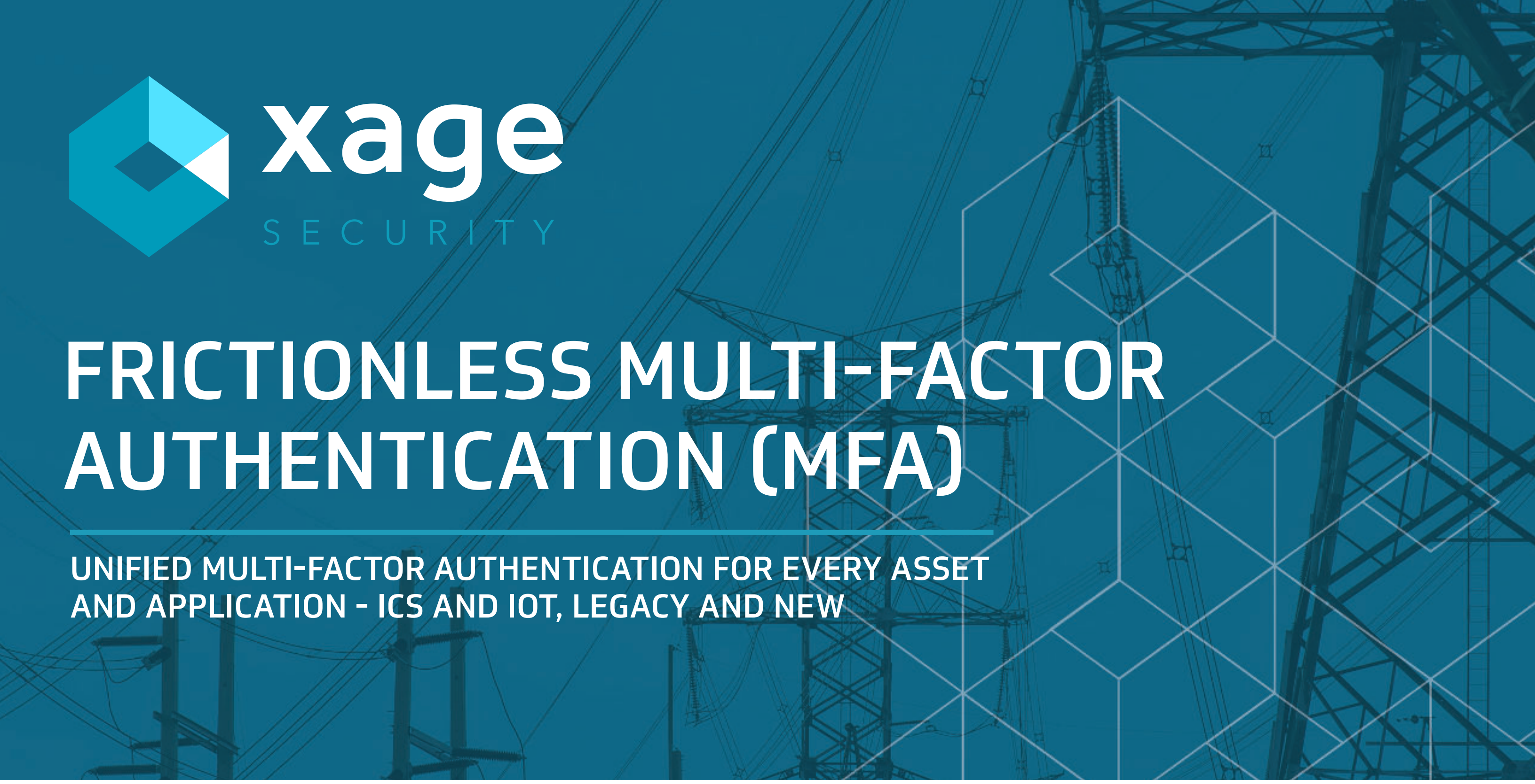


xage SECURITY

FRICTIONLESS MULTI-FACTOR AUTHENTICATION (MFA)

UNIFIED MULTI-FACTOR AUTHENTICATION FOR EVERY ASSET AND APPLICATION - ICS AND IOT, LEGACY AND NEW

Use Case

Industrial operations are transforming with data-driven automation requiring digital interactions within and across OT, IT, cloud environments, and ecosystem participants. This transformation exposes the limitations of traditional security controls and concepts (firewalls, DMZ, VPN), which are based on securing the enterprise network perimeter.

Industrial operations are therefore embracing concepts such as zero-trust and identity-based access control. In short, these approaches grant access to specific resources only based on identity, regardless of the physical and digital whereabouts of the user or application.

It is clear that identity is key, and attackers are indeed focusing their efforts on identity compromise. In Q2 2019 alone, there were 129M phishing attacks. While a few security controls emerged to address this issue (e.g. phishing email protection, phishing training, etc...), attackers have adapted accordingly, and found new attack vectors via social media and ads, and created more targeted and sophisticated phishing campaigns circumventing these security controls.

The trend of using additional measures to complement the traditional username and password with a credential that is tied to human identity (mobile phone, retina scan, fingerprint, SmartCard, RSA ID, etc.) is crucial to preventing security breaches.

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.

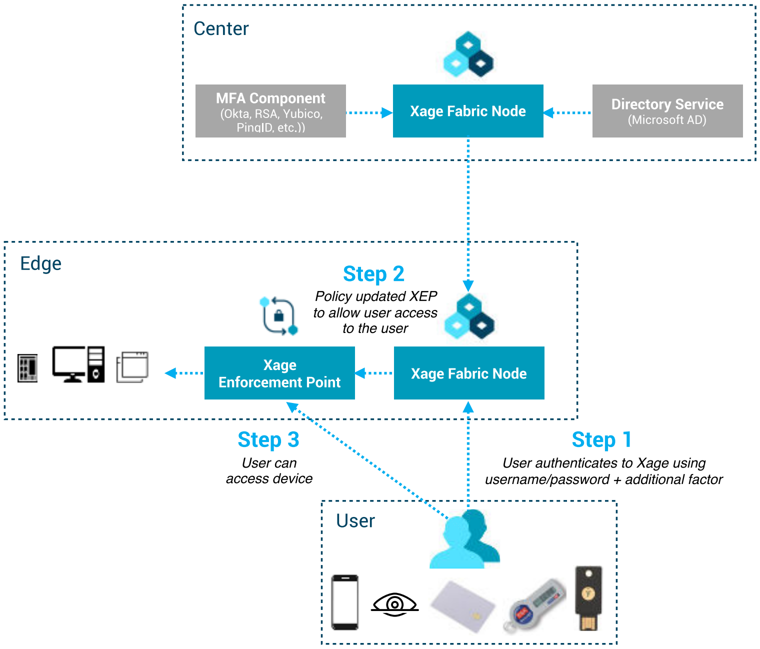
xage

Xage Security for MFA

Xage eliminates the friction of MFA integration into existing environments. By enabling MFA integration with any device and application, Xage allows organizations to add MFA to all of their assets, simplifying management and operation of identity-based MFA protection. Xage provides a unified solution to manage identities of users, devices, and applications as well as the access policies associated with them. Built specifically to support OT/IoT use cases, Xage's highly resilient authentication and enforcement are delivered at the edge and continue to operate even if connectivity to the center is lost. Xage enforces multi-factor identity-based low latency access even over intermittent networks and to isolated assets.

Unified multi-factor authentication (MFA) on currently deployed assets and applications - ICS and IoT, legacy and new

- Allows device-by-device identity-based comprehensive access control
- Xage Enforcement Point (XEP) adds MFA to any legacy one-factor or zero-factor system
- Enables Utilities to standardize on multi-factor authentication methods and extend them across their deployment base of applications, workstations, control devices, etc.
- Enables flexibility in choosing and switching between MFA methods - pins, keys, SmartCards, authentication apps, etc.
- Enables compliance with NERC-CIP 005-6 Part 2.3 which requires MFA for BES Cyber Systems without the need to replace existing assets
- Provides a tamperproof audit trail for all machine-to-machine and user-to-machine interactions


Center
MFA Component
(Okta, RSA, Yubico, PingID, etc.))
Xage Fabric Node
Directory Service
(Microsoft AD)
Edge
Step 2
Policy updated XEP to allow user access to the user
Xage Enforcement Point
Xage Fabric Node
Step 3
User can access device
Step 1
User authenticates to Xage using username/password + additional factor
User

About Xage Security

Xage Security is the universal security solution for industrial operations, creating the essential trusted foundation for every interaction, whether human-to-machine, machine-to-machine, or edge-to-cloud. Xage protects all equipment, delivering identity management, single sign-on, and access control with in-field enforcement across the operation. Xage is the first and only blockchain-protected security solution providing tamperproof, non-intrusive protection and enabling efficient operations and innovation across multiple industries.

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