UNIVERSAL ACCESS CONTROL FOR INDUSTRIAL OPERATIONS

XAGE ENFORCEMENT POINT (XEP)

Use Case

Historically, industrial operators restricted access by isolating their control devices and systems. Today, operators are modernizing by connecting previously isolated assets, despite the well-documented security threats. With the 23 billion IoT devices installed in 2018 – a number forecast to grow to more than 75 billion by 2025 – the risk of a catastrophic cybersecurity failure is constantly increasing. In the face of IoT growth and increased machine autonomy, we need to expand and rethink cybersecurity to comprehensively protect our networks of intelligent (and legacy) devices.

To do so, we have created a way to protect every device and every interaction between devices, providing the most modern and powerful access control and in-field identity management, while eliminating the prospect of disrupting (or worse yet, ripping out) vulnerable existing infrastructure.

Xage Enforcement Point

The XEP acts as a filter controlling access into and out of individual devices and controllers, providing enforcement of the access policies and authentication requirements held in Xage's tamperproof security fabric. Since the XEP is not dependent on the security features, if any, of the devices and controllers themselves, it delivers a unified and comprehensive security solution for industrial operations, enabling organizations to protect all their systems – whether password-protected or not, modern or legacy. XEP works across all equipment to improve efficiency, enable any-to-any machine-to-machine cooperation and automation, secure production data from the source machine to the cloud, deliver single-sign-on convenience, and match technician access rights with job functions to reduce on-site errors.

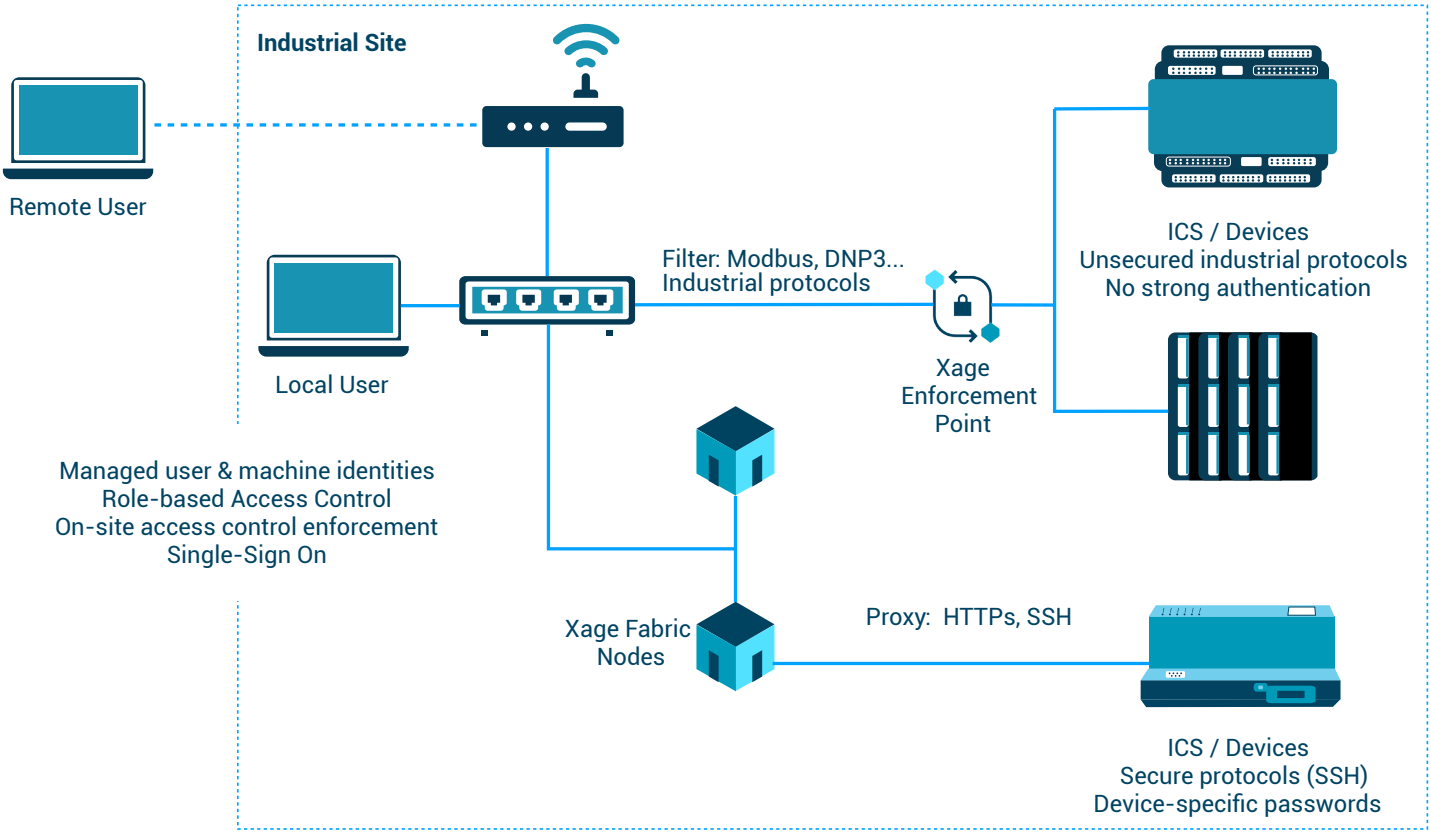
Administrators have full visibility with edge-to-cloud monitoring and an auditable record of all access attempts, successful or not. Attempts to bypass the XEP generates an alert in the system, so organizations know immediately if an attacker has attempted to compromise an industrial asset or data.

XEP also improves efficiency through off-site access and individual safety, enabling employees to access oil pads, windmills, mines, and other harsh environments remotely. This limits travel, saving significant time and money, and improves employee health and safety– before an attempted hack has even been prevented.

XEP is non-intrusive and applicable to virtually all device types such as machines, controllers, meters, and sensors regardless of the vendor, generation, type, make, model, or means of connectivity.

www.xage.com | hello@xage.com

How it Works



Xage Security Suite

Xage delivers industrial-grade security to the edges of highly decentralized industrial and commercial operations, empowering operators to manage user and device identities, credentials, and access control policies with ease. The Xage Security Fabric enables users and systems to interface with field devices across the entire operation, using centrally managed credentials with authentication and enforcement at the edge. The Xage Security Fabric is deployed across Xage Brokers in the data center and Xage Nodes at the edge. Xage delivers role-based access control services using a decentralized architecture, enabling uninterrupted service delivery over intermittent network connections without a central point of failure. The Xage Security Fabric uses consensus-based security techniques to ensure data confidentiality, enforce access restrictions and self-heal even if part of the network is compromised – so the larger the deployment, the more secure the system becomes.

The Xage Broker integrates with existing identity and services, making specific identities, credentials, and access control policies available and enforceable at the edge. Xage thus integrates industrial IoT devices and control systems (PLCs, RTUs, meters) with enterprise identity management systems such as LDAP, Active Directory, and RADIUS. With Xage, users and systems interface with IoT devices using managed identities and permissions instead of device specific credentials. The solution integrates with existing devices and protocols. Xage Nodes also integrate with HMIs, providing RBAC for users and industrial processes running in the SCADA environment. Additionally, Xage ensures regulatory compliance by rotating credentials and providing a log of every credential use and operation, making audits quicker, easier, and cheaper for the operator.

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