ADVANTECH
Enabling an Intelligent Planet

xage

Cybersecurity Modernization for Critical Infrastructure Industries

With a zero trust, mesh overlay approach, modern cybersecurity solutions like Xage Security Fabric allow mission-critical operations to run reliably, securely, and keep pace with shifting compliance requirements.

Numerous organizations and enterprises worldwide are strengthening digital infrastructure in an effort to move from information-based operations to intelligent, data-based operations. This evolution has ushered in a new round of digital transformation covering both IT (Information Technology) and OT (Operational Technology) systems. Through real-time data and information, enterprises can make timely, valuable decisions on production, machine maintenance, supply chain, and workforce to create more innovative business models.

As businesses and operations embrace digital transformation, they spread across enterprise systems, cloud services, and ecosystem partners, which involves interactions between various users, applications, machines, and data streams. For enterprises with various locations or sites, existing infrastructure is unable to provide the security and responsiveness needed for changing business models. The evolution of existing security models is essential to optimize operations and support a connected workforce.

While IT/OT convergence strategies help organizations grow and compete, they also open the door to risk. Integration can expose mission- and business-critical systems to cyber threats through existing vulnerabilities and newer threats in connected networks. According to the U.S. Department of Homeland Security, previous legacy systems were at less risk due to the separation of IT systems and additional physical protection measures. With the convergence of IT and OT systems, cybersecurity approaches should also evolve to protect operations.

Many businesses are not sufficiently prepared to tackle cybersecurity risks when converging systems. While the Industrial Internet of Things (IIoT) has become a vital competitive factor in critical industries, associated equipment, operations, and networks remain a main target of cyberattacks. Recent high-profile intrusions in mission-critical applications, such as oil & gas pipeline systems and municipal water systems, highlight the potential risk.

Protecting Critical Industry Operations

Data is crucial for effective operations and automation, but it is even more vital in critical infrastructure industries that can affect the safety of field and floor personnel, in addition to the public. Data must be objective and trusted in order to make mission-critical decisions in both IT and OT environments. If critical data is manipulated or breached, it can lead to hazardous, costly events, with impacts that reach beyond the bottom line.

Standard security technologies for OT and IT system protection, such as firewalls, VPNs, and access management tools, are not evolving fast enough to meet changing needs in critical infrastructure applications. Today’s security solutions are also usually outdated, overly complex, inflexible, and lack the ability to scale for distributed operations. A scalable, robust cybersecurity architecture is needed that not only protects assets, but also advances the business.

Keeping up with Security Directives and Compliance Requirements

High profile, critical industry operations also must keep up with evolving government cybersecurity mandates and compliance requirements, all without affecting overall productivity. These cybersecurity mandates, along with escalating cyber attacks, are drivers of cybersecurity modernization in many industries, such as energy, utilities, and defense.

For example, the Transportation Security Administration (TSA) issued its Cybersecurity Directive in 2021 for owners and operators of oil and natural gas pipelines in the U.S. The TSA's directive and recent revisions target continued efforts to build cybersecurity resilience in critical pipelines, and businesses must comply. To keep up, organizations need to cyber harden operations by utilizing a zero-trust-led security approach.

Another example includes hardware certifications required for rugged or hazardous locations, commonly found in energy and utility industries. Occupational Safety and Health Administration (OSHA) Publication 3073 defines a hazardous location (HazLoc) as an area where flammable liquids, gasses or vapors, or combustible dusts exist in quantities that can produce an explosion or fire.

In hazardous locations, specially-designed equipment and installation techniques are required to protect against the explosive and flammable potential of substances. With innumerable industry experience, Advantech designs and develops inter-operable devices that meet industry-specific and location certifications to mitigate safety risks. Various Advantech product lines are also industry specific, such as for power and energy or intelligent transportation, to meet a range of certifications and requirements.

Xage Zero Trust Security Approach

With a zero trust approach to protecting OT systems and OT-IT interconnections, Xage security solutions utilize identity-based access control to protect users, machines, apps, and data at the edge and cloud. Xage Fabric enforces Zero Trust Access (ZTA) to secure operations and data, which includes overall system visibility and managed access that adjusts dynamically for convenience and safety. Dynamic ZTA security means flexibility for end-users that have unique access needs.

Xage works with existing systems with no changes required to operational assets or networks. A mesh overlay approach to implementing zero trust capabilities allows for easy deployment without affecting existing equipment. Cybersecurity mesh essentially defines a security perimeter based on the identity of a person, asset, or application. It enables a modular, responsive security approach by centralizing policy orchestration and distributing policy enforcement.

Whether you are in IT, OT, security, network management, process engineering, operations or business transformation, the Xage Fabric is flexible for varying end user needs.

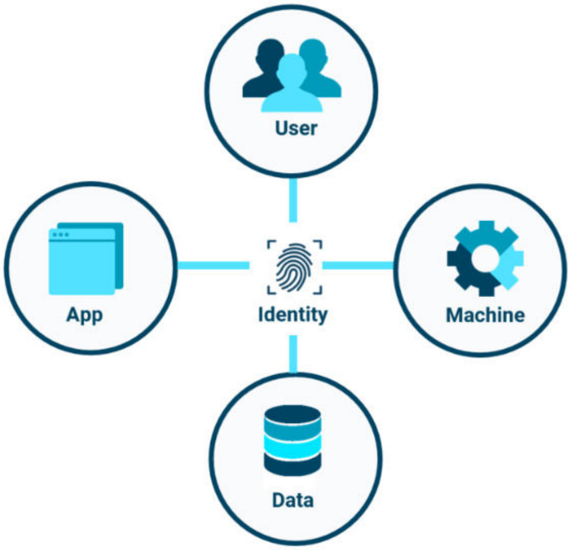
LEARN MORE

CLASS/DIVISION STANDARD 101

Standards categorize HazLoc areas into three classes (Class I, II, and III) and two divisions (Division I and II). The class identifies the properties of the substance and the division identifies the presence of a substance under operation conditions. With advancements in edge-computing and sensing devices unlocking system optimization — something only high-processing power and software can do — major Class 1/Division 2 certification is needed for electronic equipment used in HazLoc areas.

- **Class 1** – Flammable gasses, flammable liquid produced vapors, and combustible liquid produced vapors. Example: Natural Gas, Propane, Hydrogen, Methanol, etc.

- **Division 2** – Ignitable concentrations of flammable gasses, flammable liquid-produced vapors, or combustible liquid produces vapors that are not likely to exist under normal operating conditions.



Interoperability with Advantech Rugged Hardware

Utilized in many mission-critical applications, particularly in remote and/or demanding environments, Advantech designs, manufactures, and supports network devices that are simple to deploy, simple to use, and simple to manage. Two Advantech feature devices compatible and ideal for Xage Security include the UNO-2271G-V2 industrial edge IoT gateway, which runs the latest in Intel CPU technology, and the FWA-1211 industrial cybersecurity appliance with Intel Atom™ processing.

Advantech's UNO edge gateways provide reliable hardware in ruggedized form factors that deliver optimal efficiency and flexibility for supporting edge infrastructure and devices. The FWA-1211 appliance design is explicitly for cost-efficient networking in mainstream security applications.

Features of the FWA-1211 cybersecurity appliance includes the following:

- Intel Atom™ x5-E3940 / x3-E3930 Processor
- 1 x DDR3L 1600/1867MHz SODIMM, up to 4GB
- 1 x GbE Copper Management port
- 4 x 10/100/1000 Mbps Copper ports with 2 segments of LAN bypass
- 2 x 10/100/1000 Mbps SFP ports
- 1 x 2.5" SATA SSD bay; 1 x mSATA slot
- Wide operating temperature with IP40 rating
- Dual power input: 9~36V

LEARN MORE

Features of the UNO-2271G-V2 gateway include the following:

- Intel Celeron® Dual core N6210/ Intel Pentium® Quad core N6415 processor with 4GB/8GB DDR4 onboard memory
- Compact, robust, fan-less, and cable-free system with high stability
- Operating temperature -4°F ~ 140°F in industrial environments
- Modular design offers optimized basic unit with 2 x GbE, 2 x USB 3.2 Gen1, 1 x HDMI 1.4

- Optional second stack for increased functionality including PoE, COM, wireless connectivity (Wi-Fi, Bluetooth, Cellular LTE), or more than 20 additional I/O options via Advantech iDoor expansions
- Built-in TPM2.0 for hardware-based security

LEARN MORE

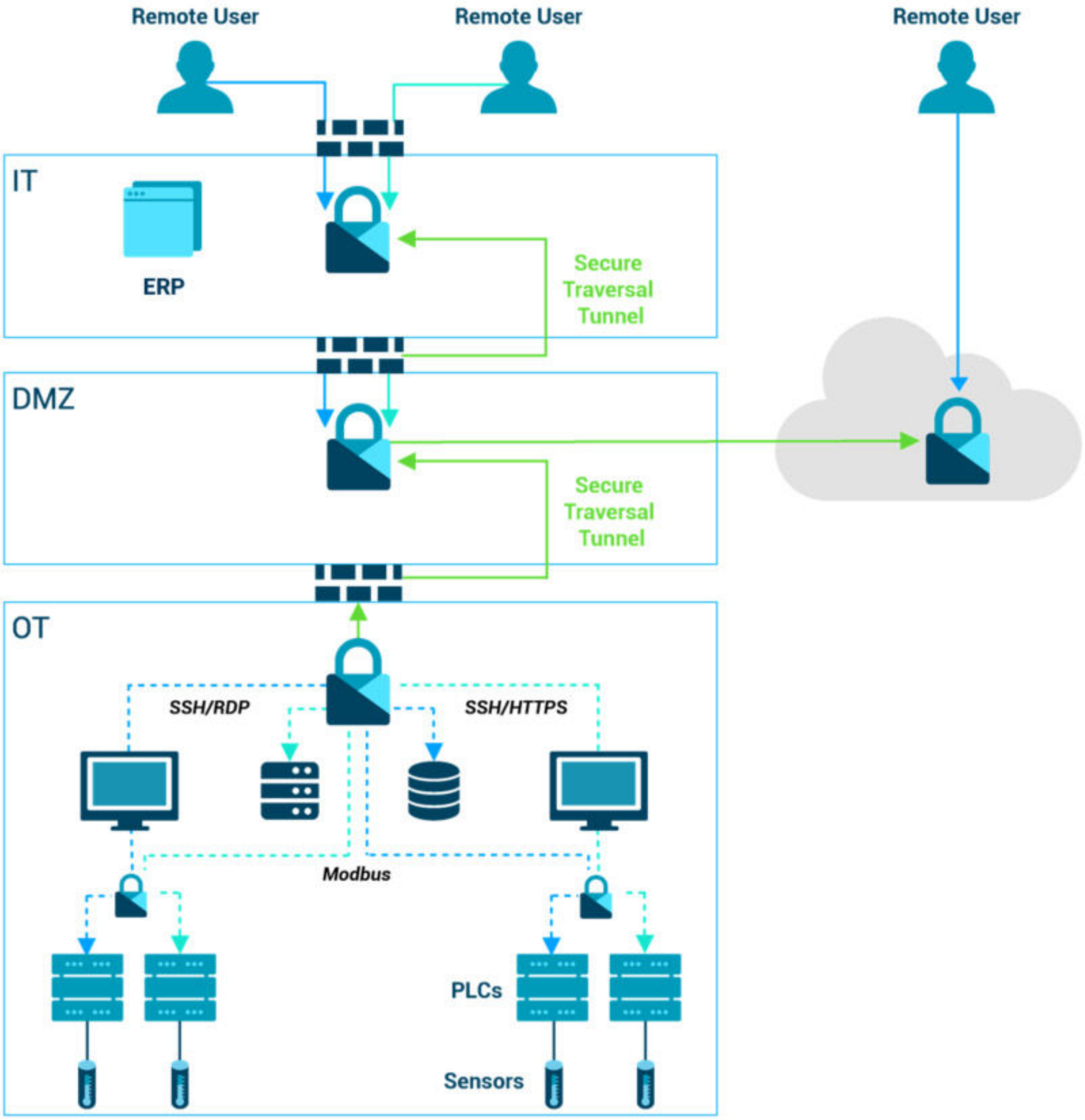
As cybersecurity evolves from static, network-based perimeters, organizations must also evolve with a zero trust protection methodology based on user, asset, and data stream identities. Critical data protection is vital for maintaining security and compliance as data travels across networks outside of traditional OT siloes.

The integration of IT and OT is inevitable, but there are cybersecurity approaches that help prevent exposing IT or OT infrastructure to breaches. Partnerships like Xage Security and Advantech help deliver comprehensive security solutions for customers who need to implement risk-free digital transformation in complex industries.

KEY XAGE FABRIC BENEFITS

- **Remote and local access management** for users, apps, machines, devices, and data with support for multi-layer environments, isolated networks, and OT assets such as PLCs and RTUs.
- **Identities for users, assets, and even data and policies** to control interactions with each other.
- Reliance on implicit trust, network segments, static accounts, or firewalls rules. Xage Fabric **eliminates the need for complex and fragmented technologies** such as VPNs, jump boxes, credential vaults, and firewalls management tools.
- **Zero-trust segmentation**, an identity-based approach that simplifies zones and conduits while providing granular control over interactions within and across zones OT sites, control centers, data centers, and cloud environments.
- **Multi-layer, Multi-factor authentication** (MFA) deployed as an overlay with no changes to assets.
- **Universal IAM** supports both legacy and new devices and apps with Single Sign-On and federation across multiple providers.
- **Dynamic data security** for dynamic and controlled data sharing and file transfer with tamper proofing authenticity, integrity, and privacy and overlay malware scanning.
- **Centralized management with distributed enforcement** utilizing a highly available mesh architecture with no single point of failure or compromise delivering resilient security control even over intermittent networks.
- **Compliance with government cybersecurity mandates** for critical infrastructure.
- **Reduced costs and complexities** (to improve productivity and accelerate digital transformation).

Xage Fabric Solution Deployment



Contact Us to Learn More or Schedule A Demo

Reach out to the Advantech team at ANA.SmartSpaces@advantech.com or request a demo directly from Xage at: Xage.com/request-a-demo.

Advantech Corporation
Industrial IoT Group

Cincinnati, OH Office
4445 Lake Forest Drive, Ste. 200
Cincinnati, OH 45242 USA
Toll Free Tel: 1-800-800-6889
Tel: 1-513-742-8895
Fax: 1-513-742-8892

Milpitas, CA Office
380 Fairview Way
Milpitas, CA 95035-3062 USA
Toll Free Tel: 1-800-800-6889
Tel: 1-408-519-3891
Fax: 1-408-519-3888

Call Center: 1-888-576-9668
Tech Support/RMA: 1-877-451-6868
Web: www.Advantech.com

Ottawa, IL Office
707 East Dayton Road
Ottawa, IL 61350 USA
Tel: 1-815-433-5100
Fax: 1-815-433-5109

ADVANTECH
Enabling an Intelligent Planet