xage SECURITY

Zero Trust for Real World Operations

Xage Security provides Zero Trust Solutions to ensure operational resiliency within and across operational technology (OT), IT, and IoT systems. Our cybersecurity mesh solution, the Xage Fabric, has three distinct capabilities that leverage the Zero Trust principles: Identity & Access Control, Remote Access, and Data Security. Our patented approach enables security policies to be centrally managed while the enforcement is distributed across the Fabric from cloud to the operational edge resulting in no single point of failure or compromise while ensuring DOD mission assurance, defensive operations, and resiliency. ***Xage is providing Zero Trust for Real World Operations Today.***

www.xage.com | hello@xage.com

How does the Xage Fabric apply to the DOD mission?

"Protecting the warfighter's capability to sense, make sense, and act at all phases and levels of war, across domains, and with partners to deliver information advantage at the speed of relevance." JADC2 Imperative

The DOD's Operational Edge and the ability to share real time information across various units is a high priority to ensure operational dominance. However, In the last two years, digital attacks targeting industrial control systems (ICS), critical infrastructure, and operational assets have become more targeted and sophisticated. Attackers are targeting both applications and the underlying infrastructure (e.g., windows server applications, network equipment, industrial control systems). Malware is armed with state-of-the-art worm-like capabilities that can easily bypass traditional security controls such as firewalls, VPNs, and Jump Boxes, and spread across IT, OT, and cloud environments.

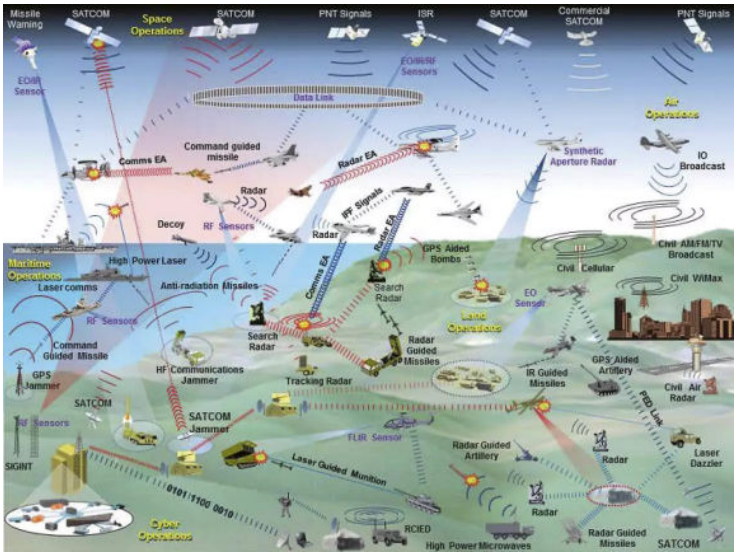
Ensuring secure access and visibility to protect systems and networks supporting mission operations is imperative. For the operator, access should be seamless, automated, with least privileged access to the device level, while site and domain administrators have full visibility, control, and auditability of every interaction. Approaches based on implicit trust and network access as the only protection measures for the warfighter networks should be replaced with identity-based controls for all assets – human, device, mission sensor, workstation, etc.

Today the DOD Zero Trust Architecture is comprehensive from an IT systems perspective, however, it does not expand into best practices for operational technology assets and their networks. The Xage Fabric was purpose built for operational systems using zero trust principles for access control and data security. With the Xage Fabric leveraging a cyber mesh architecture, operational assets (including Mission Sensors/OT, IIOT and Cloud environments) can be protected to ensure data integrity and authenticity to support the mission. The Fabric is agentless, deploys with minimal network changes, while supporting assets and sensors already in the field.

What challenge are we solving?

As we look to the future, we see several challenges to secure the tactical edge of the modern Internet of Battlefield Things (IoBT). Figure 1 depicts the complexity of the highly connected and distributed modern battlefield. Each weapon system has multiple sensors producing high value data, and whose integrity and tamper-prevention must be always assured across the system(s).The DOD has rightly acknowledged that secure cross domain C2 (command and control) is an imperative.

Figure 1: Internet of Battlefield Things



Source: https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/

Until recently, each service has designed and implemented its own C2 tactical network, which brings with it inherent interoperability and security challenges in the modern battlespace where the time to react and coordinate across systems is critical in realizing battlefield outcomes.

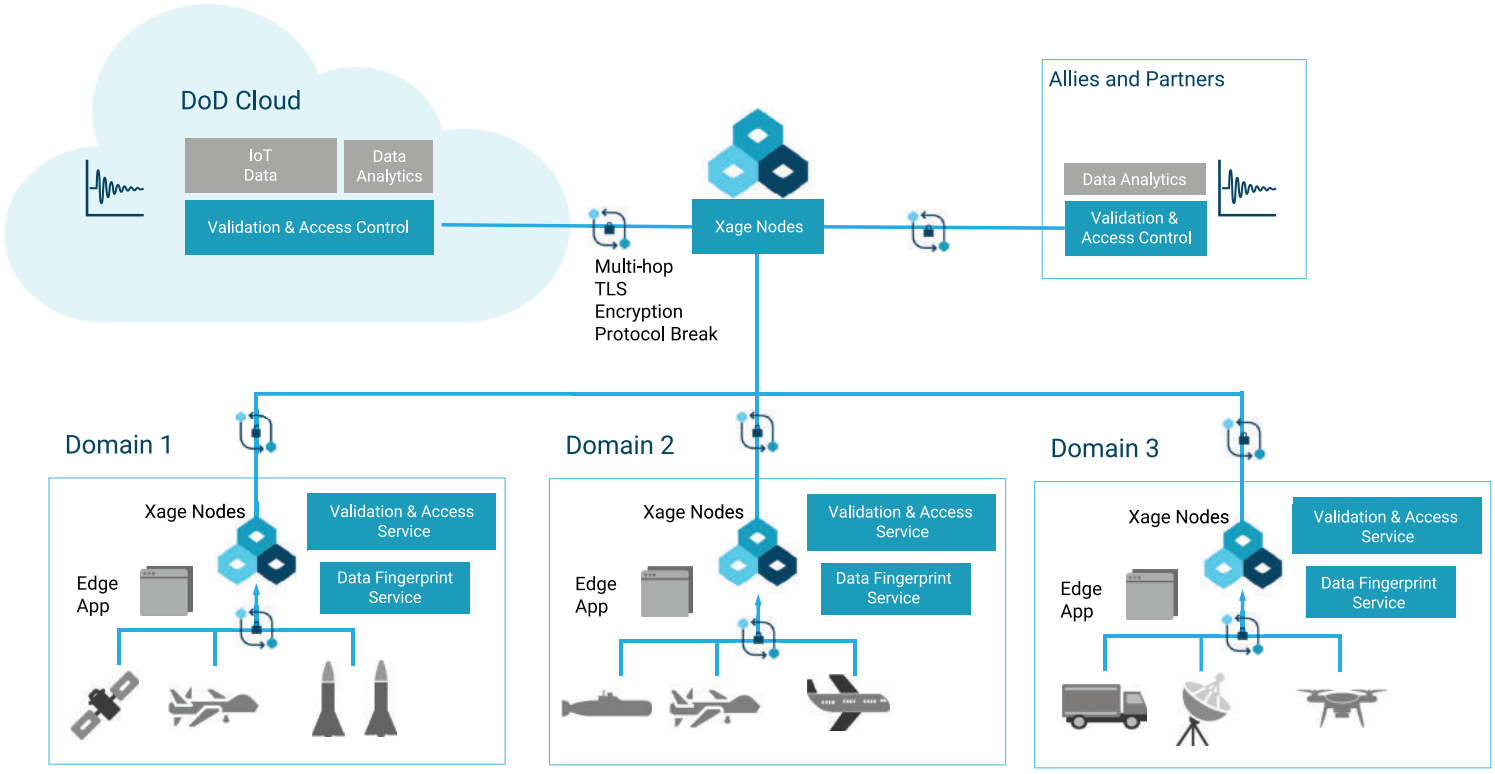
Today we are forced to defend across a spectrum of legacy and modern systems. We need solutions that are resilient, flexible, and provide systems of systems security and secure data sharing regardless of network type, cloud provider, operational applications, or devices. The Xage Fabric is protocol aware and can protect devices that haven't traditionally had security protection in the past, allowing us to bridge the gap between legacy and modern systems making a more secure warfighter environment.

How does The Xage Fabric Work?

The Xage Fabric's approach uses zero trust principles to protect identity-based interactions, decoupled from a specific network, device, or system; this makes it the ideal cyber platform to deliver universal access control and data protection for the system of systems architectures.

The Fabric can secure the data plane from the edge to core to cloud which is addressing the strategic challenge associated with the Resilient Information Sharing, specifically the move away from platform-centric data link to more distributed data sharing, multi-service network architectures as shown in Figure 2.

Figure 2: Cyber Hardened, Dynamic Data Sharing, & Distributed Enforcement



Xage Fabric Features	Description
Cyber-hardening with distributed enforcement	• Distributed enforcement allows security services to be delivered (authentication, authorization, etc.) locally and autonomously without connection to the policy engine or a central location. • Creates a more resilient security architecture to protect complex distributed systems providing autonomous edge operations to ensure resilient machine-to-machine communications.
Zero Trust Secure Remote Access	• Zero Trust-based ¬Remote access control to both assets and information to be shared by multi-party (such as ecosystems, allies, etc.) • Secure access through OT DMZ using Xage Fabric proxy capabilities for various operational protocols (e.g., SSH, HTTP/S, RDP, Modbus, etc.) • Granular identity and role-based remote access to specific assets (not just trust zones) per security policy automatically orchestrated end-to-end, and with no account, asset, or firewall changes required • Protocol, session, and encryption termination at the Xage Fabric Node, such that direct communication with protected assets is never allowed • Tamper-proofed audit logs and session recordings for all actions and interactions for compliance reporting
Zero Trust Data Protection & Sharing Ecosystem	• Data authenticity (guaranteeing the data's originating source), integrity (ensuring data has not been tampered), and privacy (ensuring authorized access only) all while enabling dynamic data sharing via: • Creating the "data identity" by digitally hashing, signing, and optionally encrypting the data at source (any application/device/protocol) • Storing the resulting data identity, and optionally the data itself, in the Fabric • Replicating across the Fabric to all the places where the data may be consumed, with granular control on where data resides to meet compliance and governance needs. • Access control–limiting data access to authorized application/tools only, delivering granular data sharing by topic/classification and access enforcement under the control of policies set globally or by each data producer. • Enabling every authorized data consumer (user or visual application) to verify the data's authenticity and integrity. • Central policy definition with distributed enforcement at edge, core, and cloud. • Public cloud and 3rd party data stores support. • Optional outbound facing API for data ingestion and consumption for deep integration with other applications, devices, or protocols

For immediate requests, please reach out to our US Federal Team:

Mr. Travis Hawker
Director DoD & IC
(M) 850-217-7151
travis@xage.com

Mr. Matthew Heideman
VP of Federal
(M) 914-523-1231
matthew@xage.com

Where can I find more information about Xage?

Please visit us at www.xage.com
Follow us on LinkedIn:
https://www.linkedin.com/company/xage-security
Follow us on Twitter: https://twitter.com/xageinc