xage GOVERNMENT

Xage Cyber Hardens Critical Assets on the Ground and In Space

Achieving Zero Trust for Space Assets Across Federal and Commercial Cooperation

The Challenge

One of the core challenges in securing space-based infrastructure is the highly distributed nature of the assets. Once a satellite is in orbit, it is difficult or impossible to install new cybersecurity capabilities. This places additional pressure on the cybersecurity measures taken at the ground stations that function as communication hubs and data centers for controlling satellites and capturing the valuable data they generate. Assuring the confidentiality, integrity, and availability of this data as it traverses multi-party organizations and networks of varying security levels is of mission-critical importance.

Featured Customer: U.S. Space Force

The USSF Space Systems Command awarded Xage Security Government a $17 million contract to deliver zero trust cybersecurity for existing terrestrial-based infrastructure, distributed assets, and hybrid satellite architectures.

Read The Announcement

Critical Infrastructure Cybersecurity Challenges - Ground and Space

Security Challenge	Xage Solution
Access Management and Control across highly distributed assets, from ground stations to satellites.	Xage delivers Identity-based Access Management via an overlay cybersecurity mesh that supports modern and legacy devices across OT, IT, DMZ and the Cloud, enabling Multi-layer MFA and Access Management.
Secure Remote Access to critical assets.	Xage delivers Zero Trust Remote Access with multiparty collaboration, full session recording, and multi-hop architecture.
Sharing Data Securely, and Ensuring Data Integrity, across Multi-party Public-Private Partnerships.	Xage delivers Zero Trust Data Exchange with access control and malware scanning to assure the confidentiality, integrity, and authenticity of data from source to network edge to data consumer.
End-to-End security, from manufacture to launch of critical space-based assets.	Xage enables inter-party collaboration, from defense industrial base (DIB) manufacturers to DoD agencies and other partners, to assure CMMC requirements are fulfilled.

xage GOVERNMENT

To secure space and other critical infrastructure, the Department of Defense (DoD) is moving to adopt zero trust principles across the seven pillars established in the DoD Zero Trust Roadmap. The pillars are User, Device, Application & Workload, Data, Network & Environment, Automation & Orchestration, and Visibility & Analytics. Across all of these pillars, the DoD has established more specific goals pertaining to asset inventory, access control, authentication and authorization, monitoring, segmentation, and more.

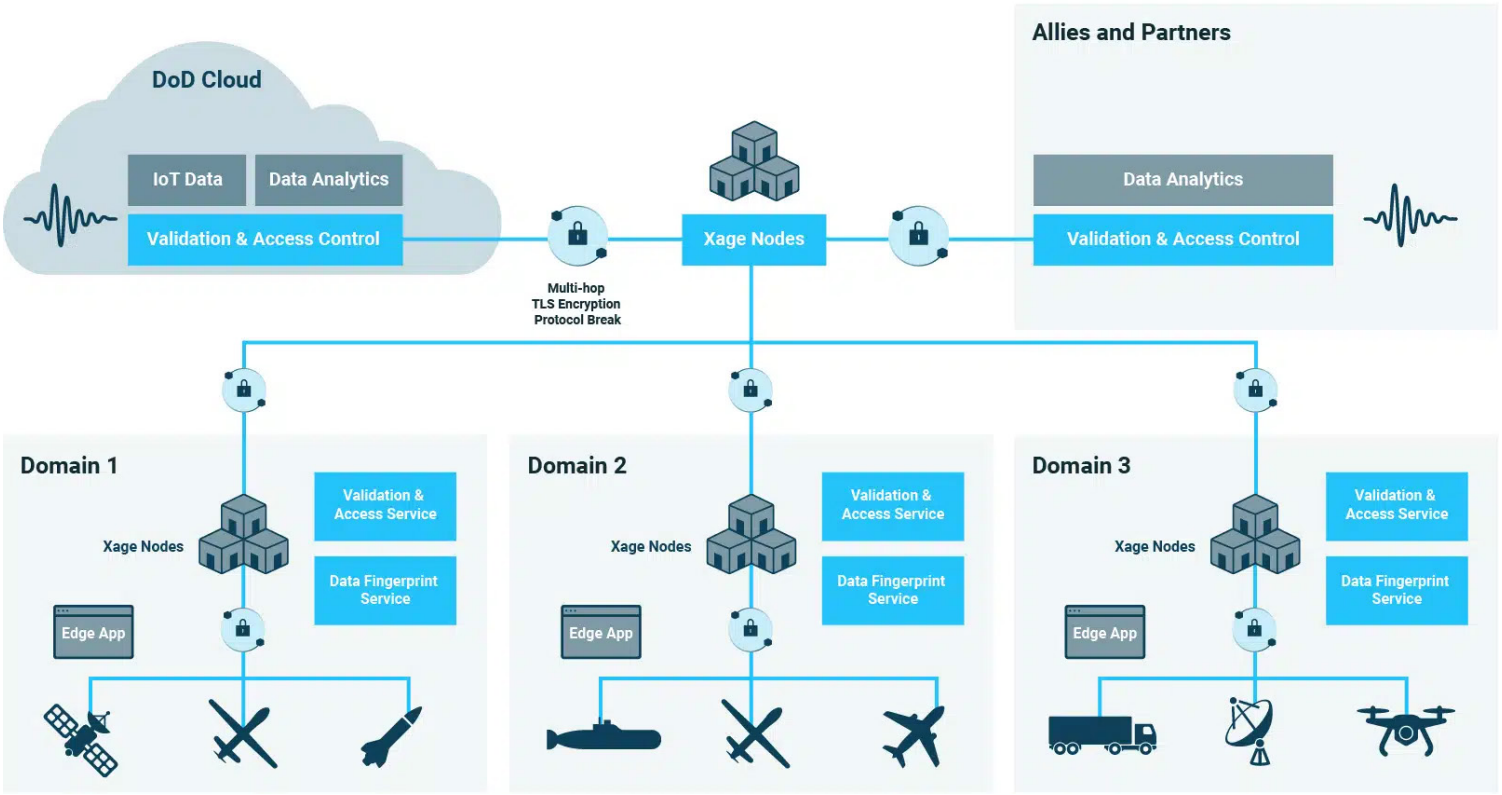
Additionally, there are increasing demands on federal agencies to adopt new cybersecurity technology to secure our nation's most critical assets and systems.

Achieving DoD Zero Trust Goals with Xage

Xage will support USSF in reaching the goals outlined in the Zero Trust roadmap by delivering:

- Identity-based Access Control with granular, centrally managed policy and distributed enforcement that keeps working in DDIL environments.
- Zero Trust Remote Access across legacy and modern assets via a single platform.
- Protection and prevention against the increasing wave of cyberattacks targeting critical infrastructure assets.

Learn more about how Xage delivers Zero Trust for DoD Agencies and Partners



xage GOVERNMENT