xage SECURITY

DYNAMIC DATA SECURITY

Use Case

Digital transformation enables industries to optimize their operations, engage with their customers, and create new product and service offerings. Data-driven operation is the key factor in successful digital transformation efforts. Working with data brings important challenges, from data capture, transportation, and storage while maintaining authenticity and integrity to controlling data access and sharing amongst multiple parties.

Sharing data between different systems, locations and parties enables organizations to pursue new business opportunities that were not feasible in the past - examples range from secure business-partner collaboration to transactive energy - and opens the door for new revenue streams. Data can also reduce operating costs, by enabling better end-to-end process optimization to reduce downtime and maintain excellence in quality and reliability. Data sharing enables applications such as supply chain optimization, effective custody transfer in industries such as oil & gas, and integration of distributed energy resources in the electrical grid. Unlocking the promise of data-driven digital transformation introduces new opportunities for revenue, sustainability, operational efficiency, ecosystem cooperation, and technical innovation.

Success in data-driven business transformation requires overcoming several data-handling challenges, notably: Distribution, security, and availability.

Distribution: To get the data moving from edge-to-edge, edge-to-center and cloud, across locations and organizations, is a challenging undertaking. Operational networks are distributed and complex in nature, often containing isolated segments with intermittent connectivity and a mix of new and legacy devices.

Security: The data transfer mechanism must assure that data is not read or tampered with (in-transit or at-rest) by an unauthorized actor, and provide a mechanism to validate the authenticity of the data's origin. In addition, it must enable compliance with enterprise policy and regulations - enforcing granular role-based access control for the data, and controlling where each piece of data is to be stored. Securing the data is critical, since, for data to be actionable, it must be trusted, both within the organization and for multiparty interactions.

Availability: Data must be available even in cases of malfunction, whether a physical hard drive fails or network connectivity is down, to ensure the continuous operation of OT and IT systems.

The adoption of data-driven business models and operations requires an architecture that enables reliable data sharing edge-to-edge as well as edge-to-center/cloud. The solution must address methods for identity-based access control and data integrity & privacy in both a single organization and a multi-party environment.

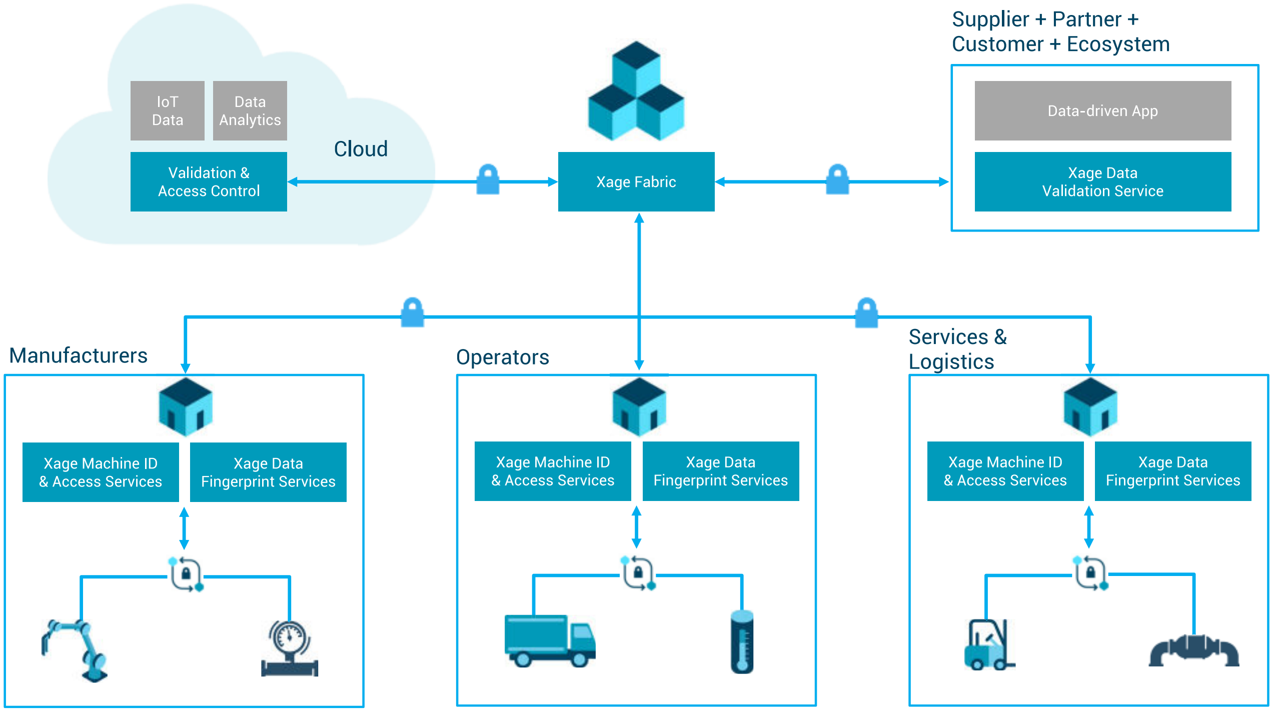
Xage's Dynamic Data Security

Xage's Dynamic Data Security enables organizations to cooperate across entire data platforms, while ensuring authenticity, integrity and privacy between different applications, machines, organizations, and locations, allowing multiple participants to securely access data in any location. Xage's operational data-hardening solution tamperproofs and seamlessly replicates the data and the data's identity information (i.e. the data's security fingerprint or metadata) via the Xage Fabric to wherever the data is consumed. As part of this process, the Xage Fabric provides reliable, dynamic and secure "point-to-point" data transmission via the distributed fabric, overcoming the challenges of intermittent connectivity and complex network architectures. Now, organizations can safely share data from the edge to the datacenter and to the cloud, creating new operational insights and innovations — and enabling data-driven applications with customers and suppliers.

How it Works

The Xage Security Fabric ensures data authenticity (guaranteeing the data's originating source), integrity (ensuring data has not been changed) and privacy (ensuring authorized access only), 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 regulations.
- Access control—limiting data access to authorized users only, delivering granular data sharing and access management enforcement under the control of policies set globally or by each data producer.
- Enabling every authorized data consumer (user or application) to verify the data's authenticity and integrity.
- Central policy definition with distributed enforcement at edge, center, and cloud.
- Public cloud and 3rd party data stores support.
- Optional API for data ingestion and consumption for deep integration with other 3rd party applications/ devices and industrial protocols.


IoT Data
Data Analytics
Validation & Access Control
Cloud
Xage Fabric
Supplier + Partner + Customer + Ecosystem
Data-driven App
Xage Data Validation Service
Manufacturers
Operators
Services & Logistics
Xage Machine ID & Access Services
Xage Data Fingerprint Services
Xage Machine ID & Access Services
Xage Data Fingerprint Services
Xage Machine ID & Access Services
Xage Data Fingerprint Services