xage SECURITY

PROTECTING DEPLOYED ASSETS WHILE MEETING NERC CIP REGULATIONS

The Xage solution secured distributed assets paving the way for grid modernization.

ABOUT THE COMPANY

This large power generation and distribution utility serves 7.6 million retail customers across six states in the southeastern United States. With an electric generation capacity of 49,500 megawatts, the company owns and operates diverse power generation assets, including a portfolio of renewable energy assets.

INDUSTRY

Power Generation and Distribution

HEADQUARTERS

Southeastern United States

HIGHLIGHTS

- **Single dashboard to manage all interactions across the grid**
- **Grid digital infrastructure protection without modification**
- **Scalable solution to policy enforcement and compliance**
- **Future-ready for distributed intelligence innovation and grid modernization efforts**

www.xage.com | hello@xage.com

xage SECURITY

CHALLENGE: MANAGING REMOTE AND LOCAL ACCESS TO CRITICAL INFRASTRUCTURE

Serving 7.6 million retail customers across six states in the southeastern United States, this large utility is challenged to remotely and locally control access to its critical infrastructure, including the relays, switches, and controllers that it uses in its substations. Per NERC CIP regulations, the company must ensure control and auditability of IEDs, EMS systems, and workstations in control systems and transmission stations.

An IT security executive at the company says, "We have to protect the transient devices in the field that our workforce uses to access substation equipment. There are penalties for failing NERC CIP compliance. Our challenge is that our network of distributed assets is growing. But centralized IT security solutions aren't designed to solve our problem. Xage offers the solution we need to protect our decentralized assets in the field."

"We did an initial assessment that revealed that every interaction across our network was authorized against our current policies."

To ensure compliance with NERC CIP, the company has created a security policy that specifies:

1. Password and key rotation across distributed IEDs within 30 days after employee leaves and at least once a year otherwise
2. Logs of all failed and successful access and login attempts
3. Detection and prevention against malicious code

SOLUTION: SECURING DISTRIBUTED DEVICES WITH DECENTRALIZED PROTECTION

To secure the company's distributed operations, the team deployed Xage Nodes across its digital assets in the field. With Xage Policy Manager, the team automatically discovered and cataloged its networked devices. The next step was to control access to the devices using unique identities for its maintenance operators. All interactive remote access sessions now require Multiple Factor Authentication--operators need to provide a password and a token.

Xage Policy Manager seamlessly:

- integrated with existing Active Directory systems utilized by the utility,
- created multiple user and devices groups and policies,
- distributed those policies across multiple substations and generation facilities automatically and without the need for additional hardware.

"We did an initial assessment that revealed that every interaction across our network was authorized against our current policies. We reviewed the audit logs recorded in Policy Manager--these showed that the company would meet strict NERC CIP regulations ahead of schedule. To say we were pleased would be an understatement," says the IT security executive.

With Xage, the company is able to deploy to and integrate with existing assets without modifying them. Their security team can now detect new or transient devices and control accessibility based on the device, user role, training and location.

Through Xage's decentralized architecture, the team can access IEDs with managed credentials and multiple factors even with broken or intermittent

xage SECURITY

connections to the company's directory service. This access extends to IEDs such as relays, switches, and controllers from multiple vendors and architectures being designed into the utility's transmission, distribution, generation and microgrid operations.

The security executive says, "To give us the flexibility and protection we need, we've created a converged model for managing security that works across multiple vendors regardless of any vendor-specific capabilities, essentially creating single sign-on for all our industrial assets."

With Xage, the company has an automated and decentralized security solution to protect its distributed critical infrastructure while ensuring compliance with evolving regulations and standards like NERC CIP.

FUTURE READY FOR GRID MODERNIZATION

One of the many benefits associated with Xage Security platform is its ability to protect today's distributed assets, while preparing the utility for grid modernization initiatives that include significant digitalization, networking and even distributed intelligence capabilities at the grid edge.

With the Xage Security fabric, the utility gained a foundation for grid modernization projects such as distributed energy resources and transactive energy, which require machine-to-machine data exchange with high integrity and access control across multiple protocols. Advancing beyond traditional security models, Xage distributes authentication and private data across the network of devices, providing tamper-proof communication, authentication and trust that ensures security at scale.

Advancements in networking, including peer-to-peer transactions and distributed computing on devices in the field including running multiple applications on single devices. These new capabilities can create significant cost savings by reducing the complexity of distribution grid management for new technologies including microgrids.

With Xage, the utility grid modernization team was able to design and test applications running in an architecture to support distributed and autonomous operations before deploying them. These operations can include distribution automation, distributed energy resource management, and identity and access management for fog computing 'apps'.

One such operation demonstrated and tested was managing microgrid operations with distributed applications and a publish and subscribe message bus for sharing operational data between devices.

The Xage Security fabric enabled the utility to create identities for deployed applications including setting access policies for these apps at the edge. It also supported multiple network types, a variety of protocols, and data integrity and access control by topic in the distributed edge architecture.

"Xage's any-to-any approach addressed a major challenge for our security and operational teams."

"Xage's any-to-any approach addressed a major challenge for our security and operational teams. By creating identities and automating the security policies at the edge, we could introduce these new capabilities more cost effectively without compromising security. By creating a platform that's multi-vendor and interoperable with various networks, dependency on a single vendor or standard doesn't impact our time to market."

xage SECURITY

SUMMARY

"We've got a strict security policy that specifies password and rotation across our IED. We need to log all access attempts--those that worked and those that failed. And if an unauthorized user accessed our operations, we need detection and protection against potentially malicious code. Xage is helping us implement our policy, protect our operation and meet NERC CIP compliance."

IT security executive, Large U.S. utility

HIGHLIGHTS

- **Single dashboard to manage all interactions across the grid**
- **Grid digital infrastructure protection without modification**
- **Scalable solution to policy enforcement and compliance**
- **Future-ready for distributed intelligence innovation and grid modernization efforts**

ABOUT XAGE

The Xage Security Suite is the first and only blockchain-protected security platform for the Industrial Internet of Things (IIOT). Xage creates the essential trusted foundation for secure interactions between machines, people, and data. Advancing beyond traditional security models, Xage distributes authentication and private data across the network of devices, creating a tamper-proof "fabric" for communication, authentication and trust that ensures security at scale. Xage supports any-to-any communication, secures access to existing industrial systems, underpins continuous edge-computing operations even in the face of irregular connectivity, and gets stronger and stronger with every device added to the network. Xage customers include leaders in the largest industries, spanning energy, utilities, transportation and manufacturing.

www.xage.com | hello@xage.com

xage SECURITY