KINDER MORGAN SELECTS XAGE TO CYBER-HARDEN CRITICAL INFRASTRUCTURE

One of the Largest Pipeline Energy Infrastructure Companies in North America Protects Against Escalating Cyber Attacks and Improves Employee Productivity with Xage

Overview

Kinder Morgan, Inc. (NYSE:KMI) is one of the largest energy infrastructure companies in North America. They have approximately 82,000 miles of pipelines that transport 40% of the natural gas in the U.S., as well as gasoline, crude oil, carbon dioxide, and more. They also have hundreds of terminals that store and handle renewable fuels, petroleum products, vegetable oils, and other materials.

Kinder Morgan faced and addressed several challenges in its digital transformation journey to protect its Operational Technology (OT) environment against escalating cyberattacks and to comply with government regulations. Like many large pipeline operators, Kinder Morgan was required to meet the security requirements set forth in the Transportation Security Administration's (TSA) Security Directives 2A, 2B, and 2C.

Kinder Morgan selected Xage Security to implement a scalable Zero Trust solution as one part of its continual effort to enhance protection of its OT and IT assets to ensure critical infrastructure resilience.

"We rely on experts like Xage Security to protect and secure our critical infrastructure. Xage provided us with an innovative approach to cyber harden OT and IT infrastructure as well as help us meet regulatory requirements."

Mark Huse, Chief Information Officer, Kinder Morgan

Cybersecurity Challenges

Kinder Morgan has deployed OT systems composed of Programmable Logic Controllers and other typical OT devices and software applications interacting with each other and human users in real-time. These systems include new devices with robust security controls and older devices with varying security capabilities. It is challenging to successfully implement security controls that address both new and old technology.

These factors resulted in steep challenges around access control and privileged access management, as well as limited logs and audit trails for tracking changes to OT systems. Kinder Morgan considered all factors when deciding to include Xage Security as part of their overall security posture designed to meet current cybersecurity requirements across systems and assets.

Kinder Morgan needed the ability to implement additional granular policies within their OT architecture for different groups or individual personnel. Rather than the traditional zone-based access control policies, Kinder Morgan desired the ability to provide individual users with time-limited access to OT devices, and the ability to restrict access to individual assets based on identity and the enforcement of appropriate levels of privilege. In addition to controlling user access, Kinder Morgan was also interested in developing a method to allow appropriately authorized users to transfer data files between IT and OT securely.

Existing access control methods, although effective, were not as nimble as what Xage had to offer. To secure their business and assure continued delivery of services to their customers, Kinder Morgan sought technology to enhance their existing access management and remote access capabilities to protect critical infrastructure.

Cyber Hardening Solution

Kinder Morgan evaluated several security solutions, and found traditional IT-centric Zero Trust solutions could not be implemented effectively in an OT environment. Traditional solutions failed to fully address network architectures and Purdue model requirements for layers of internal security separation. The solution for Kinder Morgan needed to improve its access management policies and privilege enforcement while taking a Zero Trust-based approach.

Ultimately, the Information Security and OT teams selected the Xage Fabric after an extensive evaluation to verify security, scalability, and operational criteria were met for Kinder Morgan's environment. Kinder Morgan is moving to deploy Xage Fabric across its OT environment.

Xage assisted Kinder Morgan on its path of taking a Zero Trust approach to identity and access management, privileged access management, machine-to-machine communication policy enforcement, and secure remote access. Xage's overlay approach to implementing Zero Trust capabilities without impacting existing equipment or the network was critical to easing implementation.

Outcomes

Kinder Morgan met its objectives with the Xage Fabric rollout of improving the security posture and reducing risks due to cyberattacks by implementing identity-based granular policy enforcement.

The Xage Fabric provided the following technology capabilities to help cyber-harden Kinder Morgan's critical infrastructure:

- Implement a scalable and consistent access control approach across multi-vendor OT systems and synchronize with Active Directory for single sign-on.
- Deliver Zero Trust identity verification and access policy enforcement across the OT environment, as well as moving toward IT infrastructure access control for servers across multiple data centers.
- Protect all OT systems with Multi- Factor Authentication (MFA) to meet TSA requirements.
- Mitigate risks due to possible compromised file uploads into the OT environments via scanning and blocking malicious files.

- Verify and control all connections and interactions between users, devices, and apps, whether they come from inside or outside the network perimeter.
- Improve access visibility by logging interactions between users and devices, thus helping establish reliable audit trails for investigating security incidents.
- Enable a distributed architecture with decentralized policy enforcement that provides access management even when remote sites do not have connectivity to the central site, ensuring continuous independent operation at all locations.
- Ensure no single point of security failure exists via multi-node architecture, so security services continue uninterrupted, even if a site loses network connectivity or an attacker succeeds in a partial compromise.

Xage provided the following business benefits to Kinder Morgan:

- Increased personnel productivity through a consistent approach to access management with single sign-on for OT assets.
- Reduced application maintenance costs by integrating their applications and processes with the Xage Fabric, enabling single sign-on for all applications and staff.
- Delivered the required cyber hardening without disruption to Operations.

Learn More

Learn more about Xage Solutions and Capabilities and Contact Us for a free demo.

About Xage Security

Xage is the first and only zero trust real-world security company. Xage's solutions and services accelerate and simplify the way enterprises secure, manage and transform digital operations across OT, IT, and cloud. Xage products include identity-based access management, remote access, and dynamic data security, powered by the Xage Fabric. Xage also offers Cybersecurity Services, which deliver expert design, implementation, and support services to accelerate the adoption of proactive cyber-defense and underpin secure digital transformation. Xage is currently offering a free trial for secure remote access to qualified critical infrastructure operators.