Kinder Morgan Transforms Data Center Access Security and Control with Xage

Strengthening Security, Accelerating Productivity, and Unifying Zero Trust Access Across the Stack

Overview

Kinder Morgan, Inc. (NYSE: KMI) is one of the largest energy infrastructure companies in North America. With approximately 82,000 miles of pipelines, the company transports around 40% of the natural gas consumed in the United States, along with other key resources such as gasoline, crude oil, and carbon dioxide.

Having already deployed Xage to secure its Operational Technology (OT) systems, Kinder Morgan identified a new opportunity to improve the security of its IT infrastructure—specifically, **modernizing access to its extensive data center environment.** For this initiative, they turned once again to Xage Security.

Challenge

Kinder Morgan's extensive data center environment consists of thousands of servers and hundreds of systems and users. Historically, remote connections for server administrators provided access without including granular just-in-time controls. Administrators needed enhanced safeguards to defend against today's advanced cyber threats.

What's more, the way data centers are used is evolving—with more users, such as data scientists, requiring access, and a greater number of applications of different kinds, including HPC, ML and AI, running and interacting within the environment, further amplifying the potential cybersecurity dangers. Aware of the growing risk, Kinder Morgan sought a more robust solution to strengthen access control for their data center environment, shrink the attack surface, and eliminate the risk of overprivileged access.

.

KINDER MORGAN INC.

"After seeing the impact of Xage in our OT environment, expanding into the data center was a no-brainer. The platform had already proven itself—resilient, adaptable, and aligned with our Zero Trust strategy. We trusted Xage to deliver, and they did. We appreciate finding a partner that delivers equal expertise in both IT and OT environments."

- Mark Huse, CIO, Kinder Morgan

Solution

Building on the success of Xage in securing its OT systems, Kinder Morgan expanded its deployment of the Xage Fabric into its data center environment. Thanks to its modular, extensible architecture, the Xage Fabric seamlessly adapted to the company's diverse digital infrastructure, making the transition both straightforward and highly efficient.

Strengthen Identity Verification with Multi-Factor Authentication

A core pillar of the Xage deployment was the integration of comprehensive **Multi-Factor Authentication (MFA)** into Kinder Morgan's IT access controls. As credential-based attacks continue to rise—driven by phishing, malware, and social engineering—relying solely on passwords poses a clear risk, especially for privileged accounts accessing sensitive infrastructure.

Xage introduced MFA as a foundational security control, requiring users to verify their identity through multiple factors such as secure email prompts or hardware tokens. This added layer of verification ensured that even if a password were stolen or guessed, access could not be granted without successful secondary authentication.

Importantly, MFA didn't just block unauthorized access—it helped enable a **Zero Trust model** by making all privileged sessions contingent on real-time identity validation. With Xage, every login attempt is verified, logged, and gated by policy—ensuring that only verified users could initiate privileged sessions.

This shift strengthened security, helping Kinder Morgan enforce its security policies with minimal disruption.

Enable Zero Trust with Just-in-Time and Just-Enough Access

Deploying the Xage Fabric served as a foundational step in establishing a **Zero Trust architecture,** shifting away from implicit trust models to continuous verification of admins and devices. Rather than granting always-on access based on static roles, Xage enabled just-in-time (JIT) and just-enough access—core Zero Trust principles that further reduced exposure.

Just-in-time access ensures that elevated privileges are granted only at the exact moment they are needed and for the minimum duration required. This, along with MFA, greatly reduces the risk of attackers' ability to exploit stale or compromised credentials.

Just-enough access enforces strict privilege boundaries by limiting users to only the specific managed systems, commands, and actions necessary for their role or task—eliminating broad, unnecessary access that could be weaponized by insiders or in the event of a breach.

By enforcing these controls through Xage's automated, policy-driven access framework, Kinder Morgan improved its security posture while simultaneously reducing administrative complexity.

"Xage Security has strengthened our cybersecurity posture and reduced risk across our data center and OT infrastructure. The Xage Fabric combines strong product capabilities with measurable outcomes. They didn't just help us achieve our Zero Trust goals—they accelerated them and provided immediate value."

- Craig Barrett, CISO, Kinder Morgan

Outcomes

With the implementation of Xage's MFA and just-in-time, just-enough access controls, Kinder Morgan successfully modernized access to its data center environment. The transition to a Zero Trust security model brought immediate and measurable improvements across security, operations, and user experience.

Operational Efficiency & Unified Access

The deployment of Xage delivered improvements across Kinder Morgan's IT and security operations, **driving measurable gains in both productivity and cyber resilience.**

Kinder Morgan's Security Operations Center (SOC) reported significant operational gains following the deployment of Xage alongside process improvements. Notably, Kinder Morgan reported a reduction in cybersecurity tickets compared to historical averages. This translated into fewer security events, faster resolution times, and higher alert fidelity. The SOC team now spends less time managing noise and more time on proactive threat mitigation—contributing to a stronger and more compliant security posture.

Kinder Morgan saw a reduction in cybersecurity tickets after deploying Xage

- **Fewer events and incidents**
- **Faster resolution times**
- **Improved alert fidelity**

For server administrators, AI/ML operators, and data scientists daily workflows were transformed. The adoption of Xage's secure RDP with a "click-to-login" experience replaced the previously manual, credential-based login process, saving time and reducing friction across hundreds of access sessions. **Users described the access experience as intuitive, secure, and streamlined**—empowering teams to accelerate their workflows while maintaining strong security standards.

Critically, Xage's unified access control also enabled seamless navigation across both IT and OT domains—an essential improvement for users who operate in both environments. Rather than toggling between different systems or security models, users now benefit from consistent, policy-driven access regardless of domain. This not only simplifies the user experience but also reinforces operational continuity and cross-domain collaboration.

xage SECURITY

Strengthened Protection Against Credential-Based Attacks

By enforcing MFA across all privileged sessions, Xage significantly reduced exposure to compromised or stale credentials. Even if credentials were compromised, access could not proceed without successful re-authentication and policy validation. In parallel, replacing standing privileges with dynamic, time-bound just-in-time access minimized the potential impact of any breach. With Xage, access became time-bound and tightly scoped, drastically reducing the potential impact of credential compromise.

Zero Trust Enforcement for Remote Access

Xage addressed remote access risk directly by enabling **Zero Trust enforcement for RDP-based access, applying continuous identity and policy validation at every access point.** Xage's approach to secure RDP access eliminated the use of native RDP clients and reduced the risks due to any compromised endpoint (ransomware, malware) used for remote access into the data center environment. Xage's approach also ensured administrators no longer bypass segmentation policies, resulting in a more resilient and identity-centric enforcement layer.

Automated, Auditable Access Provisioning

Access provisioning is no longer static or manually managed. Xage introduced automated, policy-based controls that dynamically adjust access based on role, context, and need. This provides full traceability and auditability, which is essential for both compliance and rapid incident response.

Conclusion

Kinder Morgan's deployment of Xage has meaningfully enhanced its **cybersecurity posture, resilience, and efficiency.** By implementing a Zero Trust model across both IT and OT environments, the company achieved unified access control that strengthens protection without compromising productivity.

Xage's distributed architecture eliminated single points of failure, replaced legacy VPN infrastructure, and introduced granular, policy-based access controls that enforce just-in-time and just-enough access. These changes have empowered teams to operate securely and efficiently, even in complex, cross-domain environments.

The seamless integration between IT and OT access controls has further elevated outcomes—reducing risk, simplifying workflows, and creating a consistent security foundation across the organization. These improvements have not only addressed today's threats but have positioned Kinder Morgan to scale securely into the future.

Their experience highlights how **modern, distributed security architectures can redefine access control, mitigate risk, and position cybersecurity as a strategic driver of business performance.**