EPIC Midstream Secures Modern Energy Infrastructure, Enhancing Usability for Greater Security and Productivity

How the midstream operator achieved complete ROI in three months while improving productivity, meeting regulatory mandates, and strengthening security with Xage

Formed in 2017, EPIC owns and operates midstream infrastructure, including 800 miles of pipeline, across Texas and New Mexico. EPIC transports oil for four of the top five producers in Texas.

In 2022, EPIC launched an initiative to overhaul its cybersecurity framework. The initiative was led by the security team, with participation from IT, operations, measurement, automation, instrumentation, and ultimately board-level oversight. The ultimate goal of the initiative was to reduce risk to the enterprise and increase resilience against attacks. Aligning with regulatory requirements was also a consideration for the initiative, although EPIC was not directly subject to any regulation at the time of the initiative. This was both a proactive decision (it is only a matter of time before EPIC will be required to be compliant), as well as a business decision to demonstrably reduce the risk to its enterprise and to the enterprises that they serve.

Since its inception, EPIC has taken an innovative approach. While most organizations in the oil and gas industry have a mix of modern and legacy assets, EPIC was built from the ground up, allowing it to implement a modern, cloud-first infrastructure.

EPIC Midstream relies on the Xage Fabric Platform to secure its 800 miles of midstream pipeline. Through an innovative security initiative that put usability first, EPIC improved security and met regulatory requirements ahead of schedule – all while reducing costs and improving its employees' productivity.

- **3 months to recoup investment**
- **400% annual ROI**
- **100% cloud-native**
- **POC deployment in 1 hour**
- **Met TSA compliance requirements**

When it came to building its security practice the same remained true. Not only did the EPIC team want to take a converged approach to securing EPIC's modern energy infrastructure, but the team also wanted to do it with usability as a central driving force behind the initiative.

The focus on usability and user experience was borne out of years of working on similar initiatives across multiple organizations. From first-hand observation, the programs that did not holistically consider the impact to the end user always saw a surge in policy violations – creative ways that people found to work around controls in the name of getting their job done. The leaders at EPIC knew that the best way to ensure the success of a security initiative was through adoption. And adoption would only happen if the solution was easy to use.

EPIC selected Xage Security for the unique approach to zero trust access and protection. The distributed architecture and simple user interface made it easy for employees to access the systems that they needed from anywhere. Whether on site, at HQ, or from the comfort of their home, users experience the same interface and access, cutting down on the need to learn multiple systems or circumvent security. Furthermore, Xage allowed EPIC to consolidate policy management across the entire enterprise – from Information Technology (IT), Operational Technology (OT), and cloud – into a central engine.

Xage fulfilled all of the security and regulatory requirements outlined in the new security framework. The broad applicability of the Xage platform allowed EPIC to avoid procurement of point solutions. Additionally, the ease of administration of Xage allowed EPIC to reduce management overhead – both of in-house employees and with third-party vendors.

Requirement: Decrease Enterprise Risk

Since EPIC was building its security architecture from the ground up, it had a lot of flexibility regarding where to start. EPIC began proof of concepts with several technology providers with solutions ranging from detection and response to visibility tools. Whatever solution EPIC selected would need to decrease risk to the enterprise in three core areas: operational environment, cloud, and third-party risk.

Operational Environment

Protecting its midstream assets is EPIC's top priority. While traditionally OT is isolated from the rest of the environment; increasingly, the boundaries between domains have been evaporating as enterprises recognize the benefits of greater connectivity of these systems. For EPIC, these benefits included greater monitoring, faster troubleshooting, and the ability to access OT systems remotely.

EPIC recognized that with greater connectivity comes greater risk. Its business has a strong culture of security-first.

"My advice to anyone using or thinking about using Xage: be creative. Don't let your imagination limit you on what this solution can actually do. There are not a lot of limits on what Xage can protect. Don't be afraid to think outside of the box. Don't be afraid to think too big."

- Mark Forsythe, Senior Infrastructure Architect with EPIC

xage SECURITY

From the CEO down, the message is clear – do not do anything if you cannot do it securely. Greater connectivity had to be balanced by demonstrable improvements in security.

The Operations team at EPIC had some specific requirements. Like many organizations in the oil and gas industry, EPIC's environment is made up of a diverse set of assets, which requires a modernized cybersecurity architecture to secure the entire environment. EPIC had attempted to bring in an outsourced SOC, which ended up costing a lot without delivering sufficient protection for its diverse environment.

Implementing Xage Fabric Platform, EPIC was able to secure its entire environment from a single interface. Xage enabled remote access and granular access controls to legacy devices as well as applications. The platform was so easy to use, there was no need to support an external SOC.

Cloud
EPIC's network is 100% cloud-hosted in Azure, and EPIC is beginning a migration of its SCADA devices into the Azure environment. This process was quoted to cost upwards of $7 million with other point solutions. EPIC was able to avoid this cost and completely protect its Azure SCADA instances with Xage.

> ***"I started securing my architecture at the edge and quickly realized that anything I could use Xage for in OT, I could extend to my IT use cases too. Xage is far from just an OT tool. It's a highly converged IT-OT solution."***
> **- Mark Forsythe**

Third-Party Risk
Like many enterprises in oil and gas, EPIC had to balance the challenge of locking down its systems and granting access to a diverse set of third parties. EPIC sought a solution that would provide more granular access controls than a traditional VPN, which would grant unfettered access to its entire environment.

EPIC had previously attempted to address this challenge by implementing microsegmentation with complex firewall rules. While this provided some visibility and granularity of access policies, it quickly became cumbersome to manage. EPIC wanted more flexibility and started looking for a solution that could adapt to its environment, not the other way around.

Before Xage, EPIC used traditional mechanisms to provide remote access, including firewalls and VPNs. It did not have a central management system, so all changes were made on an ad-hoc basis. Unlike managing firewalls, EPIC found updating identity-based policy changes much easier with Xage. Changing a policy now takes EPIC approximately five minutes. Using Xage, it is easy for EPIC's security team to know exactly what assets people are accessing and when.

Requirement: Proactive Compliance

Compliance has become a more prominent topic in the oil and gas industry in recent years. While EPIC itself was not subject to any regulation at the beginning of the initiative, the EPIC team wanted to take a proactive approach to compliance – both to be prepared for the future and as an assurance to the customers that they serve.

Transportation Security Administration (TSA) Security Directive
The TSA security directive for pipelines mandates that critical pipeline operators implement measures to enhance cybersecurity resilience of critical OT and IT systems within the oil and gas supply chain.

This includes appointing a cybersecurity coordinator, reporting cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), conducting vulnerability assessments, and implementing specific security measures to protect against ransomware attacks and other threats.

The security measures include regular patching of systems, network segmentation to isolate critical systems, MFA for access control, and ensuring backups are secure and regularly tested. These requirements aim to secure critical infrastructure and prevent disruptions in essential services.

Xage has a number of key capabilities that meet or exceed TSA cybersecurity requirements. Xage is implemented via a cybersecurity mesh approach to ensure high availability for operations. Further, it does not require "ripping and replacing" of existing OT to comply with TSA directives. For example, Xage provides compensating controls to comply with TSA's access control measures when OT assets do not have the native capabilities to implement MFA, password resets, or enforcement of access rights based on the principles of least privilege.

Outcome: Boosted Productivity

By overhauling its security framework, EPIC expected that it would improve its security and meet regulatory standards. However, the ultimate success of the initiative would be judged on whether it impacted productivity.

For EPIC, it was crucial that the chosen solution not disrupt the end-user. If it did, it was a deal-breaker.

When EPIC tested Xage during the proof of concept (POC) phase, it was immediately clear how easy Xage was to use. Xage was up and running in just one hour, compared to other solutions which took three to five days to deploy.

Users reported that the Xage solution made accessing systems easier than in the prior state. In deployment, EPIC found that most users did not notice they were using a security tool. As soon as users access the environment, Xage is working behind the scenes. There is no hassle for valid users, but the system is methodically verifying the access of every user, device, application, and workload, ensuring that they are who they say they are.

From an administrative perspective, Xage made life a lot simpler too. Making identity-based policy changes was straightforward, meaning EPIC did not need to hire extra staff to manage the system. All policy changes were centralized in a single solution for all domains across IT, OT, and cloud. Moreover, microsegmentation capabilities from Xage allowed EPIC to reduce firewall complexity and the time spent managing complicated policies.

Xage's ease of use was also critical for the third parties that need access to EPIC's environment. EPIC works with a diverse set of third parties, including OEM providers and external monitoring services. With Xage, EPIC started managing its OT environment more independently, reducing reliance on expensive OEM contracts.

In short, Xage helped EPIC reduce risk and boost productivity by balancing top-notch security with a user-friendly approach.

xage SECURITY

Outcome: Cost Reduction

100% ROI in Three Months

Xage paid for itself in the first three months of deployment in the EPIC environment. The chief reason for the rapid return on investment was the broad applicability of Xage across the EPIC environment. Initially, EPIC deployed Xage only at the edge – protecting from the outside in. Very quickly, the EPIC team began to wonder how else it could use Xage. Soon, the team was deploying Xage to build layers in the tool by users and devices.

> ***"The only thing about Xage that has slowed me down was my ignorance of how useful it is. Once I began working with it, I soon realized how broadly applicable it could be across EPIC's entire environment. I have not found something that I cannot protect with Xage. And believe me, I've tried."***
>
> **- Mark Forsythe**

There was a broader ROI for the OT side of the business as well. With Xage, EPIC was able to complete a SCADA migration into Azure, while ensuring it met its new security requirements. And while operations teams are often resistant to any changes to their environments, the operations team at EPIC were able to see the value in Xage as well. The migration of SCADA to the cloud is a sizable project. Without Xage, it would have required too many additional tools and an estimated cost of $7 million. With Xage, this cost and complexity were avoided.

> ***"Xage has paid for itself in the first three months of deployment. Now that I'm saving money with it, my only concern is wondering how I can get more of it in my environment."***
>
> **- Mark Forsythe**

Conclusion

EPIC's proactive approach to enhancing its cybersecurity framework with Xage has set a new standard within the oil and gas industry. The transition not only prepared the company for upcoming regulations but also optimized its operational efficiency and security without disrupting user experience. This case study exemplifies how innovative solutions like Xage can significantly bolster security and compliance while supporting business productivity and cost reduction. The success at EPIC serves as a compelling example of how advanced security technologies can be effectively integrated into critical infrastructure sectors.

About Xage Security

Xage Security is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.

xage SECURITY