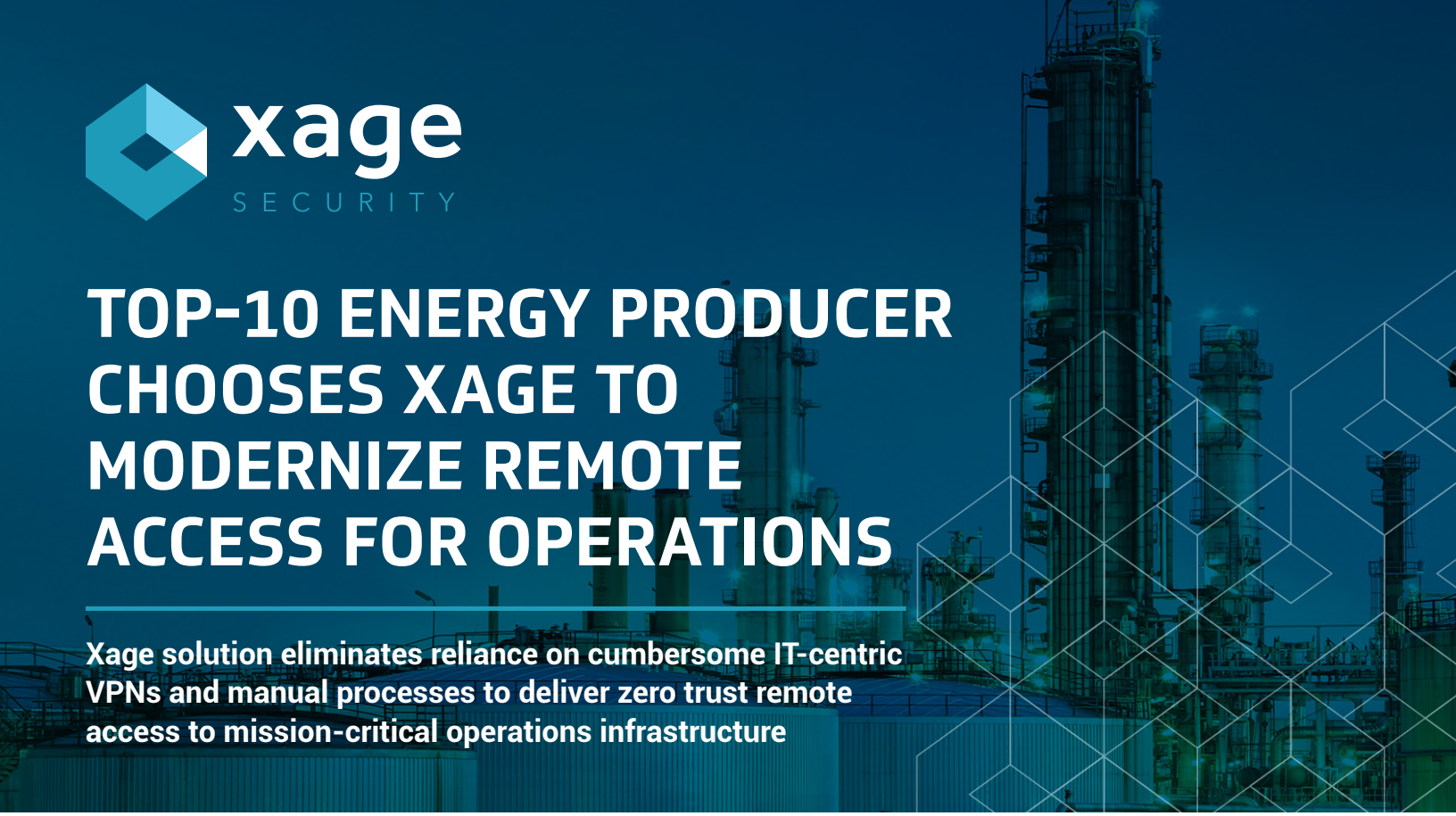

TOP-10 ENERGY PRODUCER CHOOSES XAGE TO MODERNIZE REMOTE ACCESS FOR OPERATIONS

Xage solution eliminates reliance on cumbersome IT-centric VPNs and manual processes to deliver zero trust remote access to mission-critical operations infrastructure

Overview

A global oil and gas leader selected Xage Security to modernize secure remote access to their critical operations infrastructure.

As a major player in the energy industry, the company operates petroleum and natural gas exploration sites and delivery systems worldwide. To avoid costly production interruptions, the company depends on continuous defenses to protect its Operational Technology (OT) systems and converged OT-IT environments from cyber threats. It must also provide timely remote access to over 50 sites and numerous offshore platforms to maintain continuous operations.

The company increasingly suffered from the shortcomings of the traditional, IT-centric VPN solution they had previously used for remote access. This caused hours of lost productivity and operational downtime, costing up to a million dollars per hour. To streamline operations and adopt a modern, resilient zero trust security approach, the oil and gas firm turned to Xage Zero Trust Remote Access.

Xage is partnering with the energy producer to implement zero trust remote access to all of its sites – with eighteen locations already up and running – supporting over 600 operational assets and more than 2,000 personnel.

With Xage, the customer secures:

18+
energy production sites

600+
operational assets

2,000+
personnel

© Xage Security 2023 | All Rights Reserved

Challenge

With tens of billions of U.S. dollars in annual revenue at stake, escalating OT threats made it difficult for the energy behemoth to meet its operational efficiency objectives and comply with regulatory mandates with its current remote access approach. The firm's operational and security needs surpassed what was possible using its traditional IT-centric VPN solution.

Securing Third Party and Contractor Access

Because the company must provide remote access to third parties, rigorous access control is required. Mandates further made it necessary to enact granular policies to isolate which assets remote contractors and vendors could access for a limited time.

To meet these conditions, the company would run through a time-consuming process of manual checks and approval workflows involving at least four people. This process often led to hours of lost productivity or, worse, operational downtime risking losses of up to US$1 million per hour.

Safeguarding Remote Access to Aging Hardware and Software Assets

Additionally, internal staff would connect to operational systems via the same traditional VPN. These operators frequently remotely accessed Microsoft Windows operations workstations running aged software as old as Windows XP.

As VPNs generally provide all-or-nothing access, any unauthorized connectivity gained via a weak or compromised VPN credential could result in unfettered network access, wreaking havoc on exposed, vulnerable OT systems.

Maintaining Security When Sites Lose Network Connectivity

Lastly, since offshore rigs can be disconnected from operational control centers due to environmental factors, the energy producer requires an access control approach that could weather any severe climate conditions that risk network connectivity. They need a highly available solution for on-site users to continue to access operational assets securely with as little downtime as possible should a site lose connectivity.

The energy company set out to find a better secure remote access approach to replace the headaches of its existing rigid and manual processes while enabling granular, just-in-time remote access to OT assets.

Solution

After an extensive vendor evaluation, the energy giant chose Xage Security. The Xage Zero Trust Remote Access solution met and exceeded the firm's stringent secure remote access requirements.

Xage enabled the energy company's OT security team to easily create and enforce identity-centric, zero trust remote access control policies spanning the firm's OT and OT-IT infrastructure. What once took hours of manual steps could now be handled in a fraction of the time using the browser-based Xage Policy Manager.

Unlike the company's IT-centric VPN solution, the Xage Fabric augmented defense-in-depth protections by removing the need to expose vulnerable remote connectivity protocols or assets directly to the internet. Furthermore, the multi-hop mesh architecture with session and protocol termination at each layer prevents direct interaction with protected OT assets.

© Xage Security 2023 | All Rights Reserved

The Xage Fabric architecture also met the firm's high availability and redundancy requirements. The tamperproof distributed access enforcement provided by Xage Fabric nodes – which can be utilized across OT and IT environments – allowed the company to strategically deploy several remote sites. If one site goes down, the Xage Fabric automatically redirects the remote user to another location without disrupting workflows.

Thanks to Xage's agentless approach, the oil and gas producer could overlay the Zero Trust Remote Access solution on its current operations environment. And Xage Fabric software was deployed on ruggedized hardware to handle the harsh elements that oil and gas infrastructure can face regularly.

Since deploying Xage did not require them to alter or rip and replace any existing OT or OT-IT infrastructure, the company was up and running at each new site quickly and without costly operational disruption.

Results

Xage Zero Trust Remote Access solution is implemented in eighteen of the oil and gas company's sites supporting over 2,000 operational personnel. Dozens more sites will come online in the coming months, with the ultimate goal of enabling access for up to 85,000 personnel.

The Xage solution overcame the limitations and risks of the energy producer's prior IT-centric VPN solution. In addition to enabling the firm to adopt a zero trust security approach without added complexity, Xage Zero Trust Remote Access has provided full visibility and control of all remote access activities. Xage capabilities like multi-user session collaboration speed up troubleshooting while maintaining separation of duties, regardless of the remote connectivity protocol.

Xage gives the oil and gas company further peace of mind with comprehensive remote session audit trails and logging. The company's OT security team controls and tracks who is accessing which assets without requiring additional software or agents, even if the assets themselves lack built-in access management or individual user accounts.

Similarly, the ability of Xage to seamlessly add and elevate security controls for virtually any OT or OT-IT asset in the energy producer's critical infrastructure greatly improves its overall cybersecurity posture. For example, Xage adds Multi-Factor Authentication (MFA) and Single Sign-On (SSO) to assets without native device support for identity-driven security controls.

Together these benefits ensure the company can achieve the operational excellence needed to keep oil and gas production moving smoothly and comply with a range of regulatory mandates.

Learn More

To learn more about how Xage Zero Trust Remote Access protects industrial operations and boosts productivity, even in the harshest of environments, contact us for a free demo.

© Xage Security 2023 | All Rights Reserved