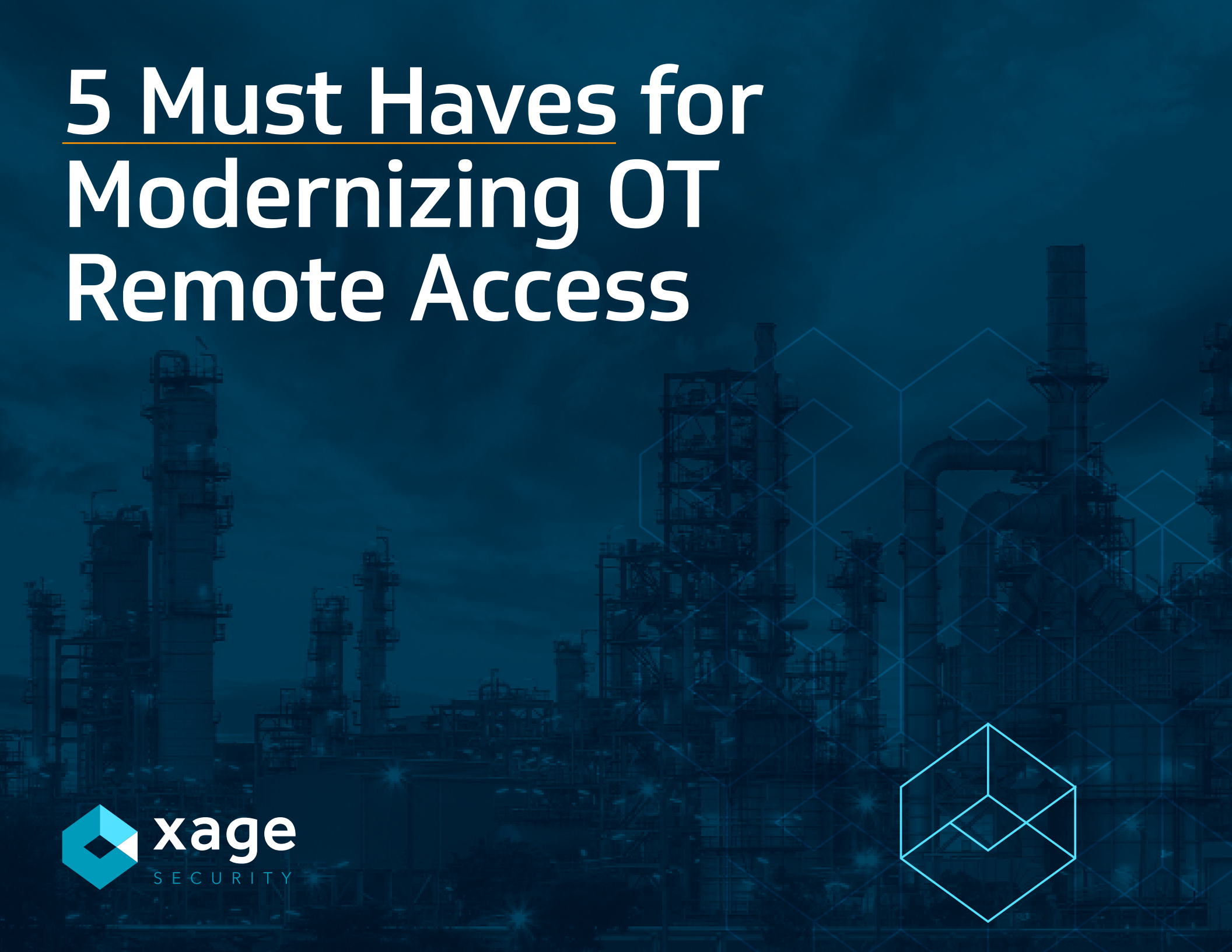
5 Must Haves for Modernizing OT Remote Access



xage
SECURITY

Introduction

Delivering reliable, secure remote access to your Industrial Control Systems (ICS) and Operational Technology (OT) assets is increasingly a top priority for OT leaders like yourself. Whether driven by a rise in remote work, digital transformation initiatives, or improved operational efficiency, the benefits of enabling remote access are far too great to ignore.

As quickly as remote access adoption has grown, so has the risk of disruptive cyberattacks targeting your critical operations infrastructure. Against this backdrop, you face intense pressure to maintain production uptime while complying with new cybersecurity mandates.

Until recently, you've had no choice but to turn to IT-centric tools to address your OT remote access demands. Unfortunately, IT-centric tools—such as traditional VPNs and jump servers—are no longer sufficient to meet the needs of today's operational environment.

Operational leaders can no longer afford to settle for the status quo: a patchwork of point solutions to compensate for the shortcomings of IT-centric tools in OT environments.

The time is now to modernize your OT remote access.

In this eBook, you'll learn:

- Why IT-centric remote access tools fall short
- Five criteria for modernizing OT remote access
- What are the expected benefits of a zero trust approach

You will also read about the experiences of other industrial organizations after each embraced a modern, zero trust remote access strategy.

Let's get started!

The New Realities Facing Industrial Organizations

It was once unthinkable to make physically-isolated Operational Technology (OT) assets and Industrial Control Systems (ICS) remotely accessible. Yet, today practically every industrial organization enables secure remote access.

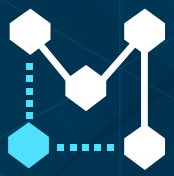
Common Drivers for OT Remote Access

Operational Efficiency

Rapidly troubleshoot and recover from production issues to minimize costly downtime.

Health and Safety

Maintain continuous operations at remote, hard-to-reach sites, even in potentially dangerous places.



Remote Work

Tap into expertise and workforces regardless of location or when faced with global crises like COVID.

Digital Transformation

Accelerate data-driven innovation, build new business models, and enhance customer experience.

Ongoing convergence of OT and IT infrastructure, adoption of cloud computing, and third-party dependencies (i.e., supply chain partners, vendors, and contractors) mean OT remote access is here to stay. The benefits are far too great to ignore.

The Stakes Have Changed

Despite the significant advantages offered by OT remote access, operational leaders face emerging risks and challenges that, left unchecked, jeopardize all that is gained.

#1
Rising Cyber Threats Targeting Operational Environments

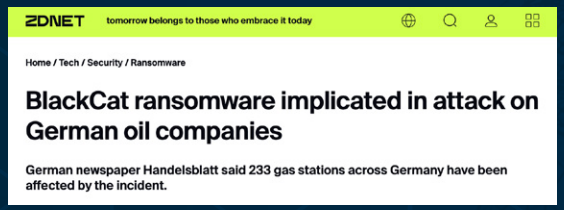
Over the past decade, operators have experienced an alarming rise in cyber threats targeting industrial organizations and critical infrastructure. The escalating risk of disruptive cyberattacks and costly ransomware threaten productivity, safety, and reliability.

#2
Increased Pressures on Operational Productivity

Economic uncertainty and supply chain headwinds intensify already high pressure on operational leaders to maintain productivity levels and output. Achieving high yields and cost efficiencies while protecting the safety of operations personnel put a significant strain on OT infrastructure.

#3
Expanding Regulatory and Industrial Mandates

Government agencies and regulatory bodies stepped up efforts in response to escalating threats by issuing an array of new and expanded cybersecurity mandates. With national security on the line, these mandates aim to fortify vulnerable critical infrastructure and defend essential sectors.


ZDNET tomorrow belongs to those who embrace it today

Home / Tech / Security / Ransomware

BlackCat ransomware implicated in attack on German oil companies

German newspaper Handelsblatt said 233 gas stations across Germany have been affected by the incident.


CYBERSECURITY DIVE Deep Dive Library Topics

DIVE BRIEF

Colonial CEO says ransomware hackers exploited legacy VPN

Published June 9, 2021


MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

The Impact of IT-Centric Tools

Historically, OT teams had little choice but to adopt the tools IT was already using to address remote access demands. As if the stakes weren't high enough already, IT-centric tools rarely come optimized for the unique requirements of OT. This leaves you facing a fourth challenge: the shortcomings of IT-centric remote access tools.

Why IT-centric Remote Access Tools Fall Short

In light of the challenges mentioned earlier, industrial organizations that rely on IT-centric remote access tools often end up with a patchwork of point solutions to compensate for the lack of native OT support.

Shortcomings of IT-centric Tools

Traditional VPNs

Commonly deployed but provide all-or-nothing access when relied on for remote connectivity to critical infrastructure environments. Brute forcing credentials, or buying stolen ones, makes this easy for threat actors to capitalize upon. When that fails, attackers simply exploit vulnerabilities in remote access protocols such as RDP, or other common VPN shortcomings.

Firewalls and Access Control Lists (ACLs)

Cumbersome and complex to manage which increases the risk of ransomware, spoofing, and other cyberattacks.

While it is common to move remote OT traffic to a DMZ, this often requires hundreds if not thousands of complicated firewall rulesets. Complexity leads to operational friction and increased risk.

Jump Servers and Privileged Access Management (PAM)

Jump servers are a common tactic to avoid direct internet connectivity to OT assets.

However, every remote user requires an account. Over time, these workstations accumulate hundreds of user accounts, many of which go stale and are rarely deprovisioned, making them fertile ground for cyberattackers. This drives operators to purchase costly Privileged Access Management (PAM) tools, perpetuating the cycle of tool bloat without improving security.

IT-Centric ZTNA Solutions

Zero Trust Network Access (ZTNA) solutions are an improvement over traditional VPNs for IT network access, but lack the capability to maintain defense-in-depth across OT security layers. ZTNA often requires endpoint agents that simply cannot be installed on OT assets.

READ OUR GUIDE to Why IT-Centric Access Solutions such as VPNS and Jump Servers Fall Short for OT

What Lies Below the Waterline

The familiar iceberg metaphor, where more lies below the waterline than meets the eye, couldn't be more apt. Industrial organizations often must add security controls or make infrastructure changes to close gaps in the highlighted shortcomings of IT-centric tools.

The complexity builds fast and creates new risks for your OT teams. There are new tools to maintain in concert with operational systems and complicated change control challenges to navigate. A lack of comprehensive visibility of remote access session activity further impedes your team's ability to quickly uncover and respond to security incidents or production outages.

Instead of fluid access, remote users suffer through a disjointed and suboptimal experience which not only risks operational productivity, but creates the ideal conditions for cyberattacks and failed regulatory compliance.

Cyber-Hardening Gaps

Reactive and disjointed remote access leads to protection gaps, limiting the effectiveness of defenses against escalating and sophisticated threats.

Productivity and Safety Risks

Poor remote access experience adds friction that slows operator productivity and endangers operational safety.

Compliance Shortfalls

Added complexity and limited visibility across a patchwork of tools run afoul of regulatory requirements or make it difficult to demonstrate compliance

Modernizing Your OT Remote Access

By now it should be abundantly clear that your existing, IT-centric approach to OT remote access is no longer sufficient to meet the challenges facing today's industrial organizations.

As you evaluate alternatives to your existing remote access tools, keeping the following five considerations in mind is essential. Each is a crucial success criterion for modernizing your secure remote access without compromising user experience, operational efficiencies, or the cybersecurity posture of your OT infrastructure.

5 Essentials of a Modern Remote Access Solution

#1

Enforces Least-Privilege Access Control

Cyberattackers often compromise privileged accounts to expand their access in a target environment. Enforcing the principle of least privilege is a crucial cybersecurity control for your remote access strategy.

Look for a remote access solution that shifts from a traditional network-centric to an identity-centric security model while accounting for OT's unique access control challenges.

To achieve this, your secure remote access solution should create an individual identity for every asset regardless of native device controls. Only when each OT asset identity forms its own perimeter can you consistently enact and enforce granular access policies across your OT, IT, and cloud networks.

Look for a remote access solution that shifts from a traditional network-centric to an identity-centric security model.

Modernizing Your OT Remote Access

Five Essentials of a Modern Remote Access Solution

#2

Takes an Asset-Centric Approach

At the heart of every industrial organization are the mission-critical OT assets that comprise your operations. These assets must be the central focus of your secure remote access strategy. Any remote access solution should be able to provide the appropriate level of access, for the required amount of time, to individual OT assets.

Consider secure remote access solutions that are purpose-built for OT. You'll benefit from a solution that overlays and augments the different native security capabilities of your operational systems.

Your remote access solution needs a deep understanding of the unique relationships and behaviors of different OT assets to effectively safeguard all digital interactions and data transfers between devices, applications, and users. Absent this awareness, your OT security teams will struggle to create and enforce granular remote access policies.

Consider secure remote access solutions that are purpose-built for OT.

Modernizing Your OT Remote Access

Five Essentials of a Modern Remote Access Solution

#3

Preserves Security Layers Across OT, IT, and Cloud

Be wary of any remote access solution that exposes vulnerable protocols and at-risk OT devices directly to the internet. For years, operations security relied on physical separation between OT systems and IT environments. The “airgap” provided a sense of security that is rapidly dissipating as digital transformation projects drive the need for interconnectivity between OT, IT, and Cloud assets.

Your remote access solution should preserve logical segmentation while enabling secure traversal of multiple network layers. This includes utilizing a multi-hop architecture that provides session and protocol termination at each layer without added complexity or friction for the remote user.

You’ll also want to look for a secure remote access solution that eliminates the need to open multiple firewall ports to provide remote connectivity via common protocols (e.g., SSH, VNC, PROFINET).

Finally, your remote access solution should achieve these outcomes without disrupting your existing operations infrastructure. Instead, aim to implement an approach that overlays your environment, OT-IT DMZ, and the cloud. Avoid any solution that requires you to rip and replace any part of your architecture.

Your remote access solution should preserve logical segmentation while enabling secure traversal of multiple network layers.

Modernizing Your OT Remote Access

Five Essentials of a Modern Remote Access Solution

#4

Delivers Complete Visibility of Remote Access Activity

A lot can happen during a remote session into your OT infrastructure that affects operational productivity and your cyber-physical systems security posture. Be sure to adopt a secure remote access solution that provides full visibility into all remote session activity.

Your solution should take an identity-aware approach to activity logging, auditing, and session tracing, even if the participating devices lack unique user accounts. Anything less leaves operations teams with more questions than answers when every minute a production process is impacted can lead to thousands (if not millions) in lost revenue.

Identity-enriched visibility into OT remote access speeds forensics for incident response, even offering proactive protection against anomalous behaviors. This level of comprehensive visibility also makes it easier to demonstrate regulatory compliance.

Your solution should take an identity-aware approach to activity logging.

Modernizing Your OT Remote Access

Five Essentials of a Modern Remote Access Solution

#5

Modernizes User Experience Without Limiting Cyber-Hardening

The flexibility offered by remote access must not come at the expense of cyber-hardening your OT environment. It's vital that your remote access solution gives you a way to set a high bar cyber-protection across all of your OT assets.

Make sure your solution can seamlessly add new layers of security controls, regardless of the maturity of native device capabilities. This includes enabling multi-factor authentication (MFA), single sign-on (SSO), advanced secrets management, and other cybersecurity best practices.

Most importantly, it's crucial these added defense-in-depth controls don't lead to a kludgy user experience.

Take a Zero Trust Approach to Remote Access

The importance of adopting a zero trust-based approach is a common thread that runs consistently through each of these considerations. Industrial organizations must shift to a unified approach that delivers granular and just-in-time access controlled down to the asset level.

Embracing a zero trust-driven strategy eliminates remote access friction while adding protection that prevents most attacks before they can begin.

Make sure your solution can seamlessly add new layers of security controls, regardless of the maturity of native device capabilities.

Reduce Complexity. Accelerate Cyber-Hardening.

Successfully meeting demands for secure remote access into your converged OT, IT, and cloud environment starts with adopting a unified approach. A modern solution based on zero trust principles makes it easy to deliver granular, just-in-time access down to individual assets.

The benefits of a zero trust approach include:

- **Reduced attack surface area**
  An identity-based, zero-trust security model proactively protects critical operational infrastructure by dramatically reducing the vulnerable attack surface.
- **Unified identity-driven access policy management**
  Avoid the need for separate tools and create unified, granular identity-driven remote access policies across all of your operational assets and remote users.
- **Secure traversal across zones**
  Provide friction-free remote access to all of our users without needing to expose vulnerable OT protocols and at-risk operational assets directly to the internet.
- **Full visibility of all remote access activity**
  Gain peace of mind with comprehensive, identity-based logging of all remote session activity for unmatched visibility for incident response and demonstrating compliance.
- **Streamlined compliance with regulations and mandates**
  Speed up meeting and exceeding regulatory requirements and industry standards with just-in-time remote access.

Accelerate Zero Trust Remote Access Adoption with Xage

With **Xage Zero Trust Remote Access**, security and operational teams can accelerate the adoption of a zero trust remote access approach to defend industrial operations from escalating threats and boost productivity.

The tamperproof, resilient, and highly available Xage Fabric can be deployed as an overlay across your existing OT, IT, and Cloud infrastructure.

This unique mesh architecture removes the need to rip and replace your current investments or suffer disruptive operational changes to protect all digital interactions between users and assets.

Success Story: Top-10 Global Energy Producer

As a major player in the energy industry, the company operates petroleum and natural gas exploration sites and delivery systems worldwide. It must provide timely remote access to over 50 sites and numerous offshore platforms to maintain continuous operations.

The energy producer 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 selected Xage Zero Trust Remote Access.

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. 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 multihop mesh architecture with session and protocol termination at each layer prevents direct interaction with protected OT assets.

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.

READ MORE

Success Story:
One of the World's Largest Steel Manufacturers

With dozens of plants in the United States and operations in Mexico, Brazil, and throughout Central and South America, the steel producer has a vast footprint that requires in-depth coordination and planning to maintain security.

With the onset of the pandemic, the company's personnel needed to log in remotely to manufacturing sites to maintain production. The company began to trial TeamViewer as a solution for access to their OT environments but quickly ran into limitations. They turned to Xage Security and its Zero Trust Remote Access solution.

Xage's zero trust approach manages access via identity and specific authorizations, rather than trusting users simply due to their presence on the operational network. Once an identity is verified, the system provides granular authorization for access to specific OT assets for a specific duration. Additionally, the steel manufacturer assessed audit capabilities and found Xage provided the most reliable, identity-enriched forensics due to its ability to log and record sessions and actions. The company placed a high value on the solution's single sign-on remote access platform with MFA as an added safeguard when accessing OT assets.

The Xage Fabric allowed the company to implement remote access securely without disrupting its existing OT architecture or operations. The steel manufacturer

MITIGATED FINANCIAL LOSSES

for any disruptions while also reducing cybersecurity insurance premiums by demonstrating high maturity and cyber-hardening.

READ MORE

Modernize Without Compromise

As demand for reliable remote access continues to increase, operational leaders must embrace a different approach from the status quo.

Utilize these five “must-haves” as vital success criteria for modernizing your secure remote access without compromising user experience, operational efficiencies, or the cybersecurity posture:

1. **Enforces least-privilege access control**
2. **Takes an asset-centric approach**
3. **Preserves security layers across OT, IT, and cloud**
4. **Delivers complete visibility of remote access activity**
5. **Modernizes user experience without limiting cyber-hardening**

Most importantly, don’t wait to get started. Your current IT-centric tools are no longer sufficient nor an effective strategy for OT remote access and urgently need to change.

Modernize OT Remote Access with Xage Security

Fortunately, Xage makes it easy to shift. Unlike other remote access solutions, Xage’s Zero Trust Remote Access solution bolsters defense-in-depth and supports Purdue Model best practices with secure traversal of zones.

To learn more about how Xage Zero Trust Remote Access protects industrial operations and boosts productivity, **contact us for a free demo.**

xage SECURITY

www.xage.com | hello@xage.com