ONE OF THE WORLD'S LARGEST STEEL MANUFACTURERS TURNS TO XAGE FOR ZERO TRUST REMOTE ACCESS

Xage delivers an increased security posture for operations, a streamlined user experience, and better ROI compared to other remote access solutions

Overview

One of the largest producers of long steel in the Americas and one of the largest steel manufacturers in the world has turned to Xage Security to meet its secure remote access needs. With dozens of plants in the United States and operations in Mexico, Brazil, and throughout Central and South America, the company has a vast footprint that requires in-depth coordination and planning to maintain security.

With the outset of the pandemic, the steel producer'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. Then they turned to Xage Security and its Zero Trust Remote Access solution.

Xage partnered with the company to initially deliver the solution to six sites. Now, it is being deployed across the company's North American facilities.

Highlights

- **Zero Trust Remote Access for distributed manufacturing sites with Single Sign-On and MFA**
- **Cyber-hardened operations and mitigated financial losses resulting from cyberattacks**
- **Reduced cybersecurity insurance premiums by demonstrating high security maturity**
- **Improved productivity from decreased user complexity in operating the solution**

Challenge

When the steel manufacturer first transitioned to full remote access due to the pandemic, the team turned to TeamViewer, but soon experienced multiple shortcomings. TeamViewer did not satisfy important security requirements – such as supporting multi-factor authentication (MFA), and maintaining strict digital separation between operations and the public internet – nor could it maintain detailed session tracking for audit trails. Additionally, it required software agents at both the initiation and termination points and was cumbersome in allowing maintenance staff to log in to different sites for troubleshooting or managing OT assets. More troubling still, TeamViewer required direct connectivity from OT environments to the internet – creating a large attack vector for bad actors and violating industry-standard Purdue Model defense-in-depth designs.

Lastly, the steel producer was especially concerned with the limitations of the Identity Access Management capabilities with TeamViewer. A primary objective of the company's OT security team was authenticating a remote worker and then granting granular access permissions within its OT environment. They did not have this level of visibility or control with TeamViewer.

These shortcomings were of real concern to the security team. Since the beginning of the pandemic, cyber-attacks against operational technology have increased by 2000%[1]. Internet connections for OT environments, such as those required by TeamViewer, are one of the reasons for the spike in attacks. A successful attack against the company's OT systems could cause a harmful disruption to steel production at a time when supply chains are delayed globally.

Production disruptions at steel plants are particularly worrisome as the soft, heated steel runs outside of molds and cools, hardening in the wrong places and shapes. It then requires a team to cut out all the cooled steel with torches, creating a major loss in productivity.

With these challenges in mind, the company began to look for a new solution. Any new solution would need to provide zero trust-based secure remote access specifically designed for multi-layer OT environments and additional zero trust access control capabilities.

Solution

After evaluating potential tools, the steel manufacturer chose to pass over other OT-oriented remote access products for Xage due to the superior zero trust capabilities offered by its Xage Fabric solution.

The solution's Zero Trust Access model (ZTA) 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. The Xage Fabric allowed the company to implement remote access securely without disrupting its existing OT architecture or operations.

In addition, 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.

In December 2021, this leading steel producer purchased and began implementing the Xage Zero Trust Remote Access Solution for an initial six sites. Following a successful rollout, the company expanded to additional sites to utilize Xage across all its North American-based OT environments.

The company quickly scaled the implementation of Xage's Zero Trust Remote Access without requiring any disruptive network changes to its operations environment.

Results

Xage Zero Trust Remote Access is implemented in ten of the steel producer's production sites across North America to provide remote access for contractors and vendors responsible for plant operations.

The company has solved many of its key pain points in providing remote access to its personnel due to the unique benefits Xage provides. These include:

- Zero Trust capabilities that provide granular identity-based access control for operations assets
- A comprehensive logging and recording system for audits
- Enhanced security via MFA
- No origination and termination agents required
- No changes to the software running on OT assets
- A low-friction single sign-on user experience

The steel manufacturer has found that ROI is increased compared to competitors owing to:

- Mitigated financial losses resulting from cyber-attack – the company stands to lose $1 million dollars per day per site for any disruption
- Cybersecurity insurance premiums are reduced by demonstrating high maturity and cyber-hardening, like implementing MFA
- Improved productivity from decreased user complexity in operating the solution
- Underpinning company digital transformation allowing for a focus on new revenue opportunities

Further, though Xage was implemented to secure remote access for operational technologies, the versatility of the solution has provided the company with unforeseen benefits such as controlling access to interconnected OT-IT environments. Specifically, the steel producer has deployed Xage to protect access to and enforce policies for inventory tracking and management applications that are deployed at its manufacturing sites.

Learn More

To learn more about Xage and how Zero Trust Remote Access can secure virtual work environments for your company, contact us for a free demo.

[1] Source: IBM X-Force Threat Intelligence Index (2020)

About Xage

Xage is the first and only zero-trust real-world security company. The Xage Fabric accelerates and simplifies the way enterprises secure, manage and transform digital operations across OT, IT, and the cloud. Xage solutions include Identity & Access Management (IAM), remote access, and dynamic data security, all powered by the Xage Fabric.