Securing Remote Access for a Steel Manufacturer with Xage Security

Overview

A leading global steel manufacturer deployed Xage to provide Secure Remote Access (SRA) across multiple of its major production facilities. The manufacturer is a global industrial operation employing thousands across numerous sites and serving industries such as automotive, construction, HVAC, and large-scale manufacturing.

Challenges and Requirements

As part of an initiative to strengthen operational technology (OT) security, the organization sought to replace its existing Cisco ASA–based remote access solution. The legacy VPN enabled broad, unrestricted access to the network for employees and third-party vendors, creating unnecessary risk in an environment where uptime and safety are paramount.

The reliance on VPNs required laptops to be configured manually with agents before allowing users—internal or third party—onto the network. This process was slow, operationally burdensome, and expensive. Once connected, users had access to the entire network, rather than being limited to the specific assets required for their role.

The team also wanted to reduce its reliance on complex firewall configurations in the OT environment. Managing and updating firewall rules introduced operational overhead and potential gaps that could be exploited through ransomware, spoofing, or other cyber threats.

The manufacturer needed a more granular, identity-based approach to access control that would reduce complexity while improving security.

Headquarters

USA & Europe

Industry

Steel Manufacturing

Key Takeaways

- Replaced VPN with Zero Trust remote access built for OT environments
- Delivered granular, identity-based access that reduced attack surface
- Improved uptime, productivity, and cost efficiency through fast deployment and simplified workflows

Outcomes

The manufacturer selected Xage Security as its SRA provider to meet OT-specific access and protection requirements, replace the VPN, and reduce dependence on firewalls.

Xage SRA enables granular, identity-driven access policies for both remote users and applications. This ensures users receive only the just enough and just-in-time access, thereby reducing the attack surface and preventing lateral movement inside the environment.

Why IT-Centric Tools Fail in OT Environments

Traditional IT remote access tools often fall short in industrial OT settings. VPN-based access typically provides all-or-nothing connectivity, increasing exposure if user credentials are compromised. Such vulnerabilities allow lateral movement across critical OT systems, introducing risk to operations, safety, and the environment.

Reduced Risk

By replacing the legacy VPN with Xage Secure Remote Access, the organization implemented Zero Trust controls across all users, devices, applications, and workloads.

With Xage, security administrators gained the ability to enforce fine-grained, identity-based access down to individual OT assets. These dynamic access policies significantly reduced the attack surface, limiting potential lateral movement within the operational environment.

Xage also eliminated shared accounts and introduced centralized, auditable logging for all sessions, helping the organization improve accountability and meet NIST-aligned security baselines, including MFA, access controls, and proper logging practices.

External penetration testers were unable to breach the deployment, reinforcing the solution's effectiveness.

Improved Uptime

For high-output manufacturing facilities, maximizing uptime is critical. Xage's deployment required no disruptive changes to operations, and the installation was completed in just two days at each facility.

Because Xage safeguards assets regardless of software version, the team reduced its need for planned maintenance windows and minimized risks associated with unpatched systems.

Unlike VPNs, Xage's identity-based segmentation prevents lateral movement, reducing the likelihood of cyber incidents that cause costly unplanned downtime.

xage SECURITY

Enhanced Productivity

Users quickly adopted Xage's browser-based workflows, noting that access was easier than previous methods, especially when collaborating with third-party OEMs.

Administrators benefitted from simplified provisioning and deprovisioning, which takes only seconds for both employees and external users. Session recording added accountability for third-party access.

Given the manufacturer's global footprint, Xage provided seamless remote access to the facilities from anywhere, enabling distributed teams to collaborate securely and efficiently.

Cost Savings

The shift to Xage SRA delivered measurable savings by eliminating the need to configure and ship laptops to external vendors and employees. Identity management became significantly faster, reducing dependency on multiple third-party systems. Remote visibility and control also decreased reliance on OEM site visits, lowering maintenance and travel costs.

Conclusion

The deployment of Xage Security's Secure Remote Access solution marks a major advancement in securing the steel manufacturer's IT and OT environments. By replacing outdated VPN methods with Xage's Zero Trust-based approach, the organization improved its security posture, increased uptime, simplified operations, and achieved meaningful cost savings.

The successful rollout has already prompted expansion of Xage SRA to additional facilities, reinforcing the value of modern, OT-aware access solutions in large-scale industrial environments.

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.