Tempered

Learn how a global manufacturer protected their facilities with invisibility and micro-segmentation.

Global manufacturer makes its industrial control systems invisible

Airwall Solution eliminates network complexity and enables micro-segmentation for a global manufacturer of advanced materials and components.

Challenges

The manufacturer's 100-plus plants across 30 countries were on a flat, Layer 2 MPLS network that wasn't adequately segmented, exposing systems to lateral attacks by malicious actors. The company had failed internal security audits and now needed to adhere to NIST segmentation requirements.

Solution

The team deployed Airwall Solution without rearchitecting their existing network infrastructure, enabling micro-segmentation for their industrial control systems. This solution rendered their systems invisible to attacks and unreachable by bad actors.

Wins

The company's manufacturing plants are now protected and segmented, with no unauthorized communication to industrial control system devices. As a result, the company was able to meet NIST compliance requirements cost-effectively and with no additional headcount.

"We have hundreds of applications that are hard-coded with IP addresses on the factory floor. We were able to leave our network flat but carve it up with no downtime. No other technology could do that."

VP of SCADA Security

The challenge

Outdated network security can pose risks for any operation, but it is especially concerning if that operation deals with life-threatening materials. That was the case for this global manufacturer, which serves industries ranging from government to aerospace and produces advanced H1 hazardous materials with an explosive element. 24/7 monitoring was crucial — any disruption could be catastrophic to both the plant and the surrounding community.

Despite these high stakes, the manufacturer was still on a flat, Layer 2 MPLS network, employing traditional technologies such as switches and routers for local networking, and firewalls and VPNs for security. The network attack surface was significant, as malware was able to breach, traverse, and persist despite security controls such as VLANs, firewall rules, ACLs, VPNs, 802.1x authentication, and security certificates.

To make things worse, every building had thousands of live data jacks, all of which were opportunities for malicious actors to enter the network and attack critical industrial controls and sensitive resources.

One particularly vulnerable division was unable to remove a persistent malware threat on its own, requiring the Department of Homeland Security (DHS) to lead the months-long removal process. The malware threat exposed the company and its customers to theft of intellectual property, including customer designs and specifications of proprietary components and parts.

Unsurprisingly, the company failed internal security audits. As a result, the Chief Information Security Officer (CISO) issued a mandate to implement network segmentation for all business units in compliance with NIST network security standards.

A small IT team explored alternatives to existing configurations, but their findings presented additional challenges: initial estimates for segmenting via internal firewalls and ACLs were about $1 million and two months' deployment time per plant, plus additional headcount.

"Rearchitecting our network with any of these traditional tools would have been prohibitively expensive, time-consuming to deploy, and difficult to manage," explained the manufacturer's Director of SCADA security. "Having to re-IP our hard-coded applications and devices was a total showstopper. We needed a better way to segment and secure our network."

The solution

A proof of concept from Tempered revealed that they could achieve network security at a significantly lower cost, with deployment taking less than two days on average per plant. With Tempered, the manufacturer was able to deploy an overlay network on their existing network infrastructure.

Tempered's Airwall Solution combined a Software-Defined Networks (SDN), Zero Trust Network Access (ZTNA), and a Software-Defined Perimeter (SDP) to control communication between key devices on the network. The team implemented the solution quickly, covering the first building with over 700 connected systems across 10 manufacturing lines in just half a day.

Customer success

Cloaked devices: The Airwall Solution made the company's industrial control systems completely invisible and unreachable by unauthorized entities. Effectively segmenting visibility and access meant that HMI controllers could only listen to the HMI/SCADA master server. Now, nothing else on the network can see or communicate with any of these devices.

Micro-segmentation: The company was able to micro-segment various operational systems according to functionality. All communications for these systems leveraged encrypted peer-to-peer secure tunnels with Tempered's Airwall Solution.

Security compliance: This global manufacturer now meets NIST compliance requirements cost-effectively and with no additional headcount.

> *"We were trained on this technology while doing our first deployment. Our staff was able to do another 20 facilities without additional training or paying for professional services. Once we understood the mechanics of the technology, we could deploy the solution ourselves — it's that easy. In 48 hours or less, we can take a 50,000-square-foot manufacturing facility and make it invisible with zero downtime."*
>
> **Director of SCADA Security**

Deployed Airwall Solution components

Airwall Edge Services coupled with Airwall Conductor created a solution that made their industrial control systems invisible and segmented their access.

Airwall Conductor: The team deployed the orchestration engine for provisioning, segmentation, allocation, and revocation of the network. This allowed for visualization of the network segmentation and granular whitelisting.

Airwall Gateways: Physical Gateway 500s enabled the team to limit access across their flat network, protecting industrial control and operational systems.

Tempered delivered defense-in-depth

1 Zero-Trust Network Access (ZTNA)

2 Software-Defined Network (SDN)

3 Software-Defined Perimeter (SDP)

4 Multi-Factor Authentication (MFA)

5 Micro-segmentation for every endpoint

6 Lateral movement eliminated

without expense-in-depth

20% of the cost of traditional IT solutions

Deployed in 30 FTE days instead of 310 FTE days

Did not require additional network admins

Want to see what Airwall can do for you?
Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500