

Sponsored by Tempered

SMART BUILDINGS 2.0



Airwall The next-gen air gap

Digital Age Cyber Security for Manufacturing

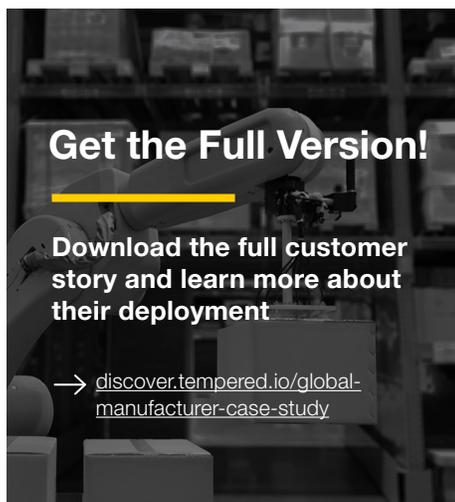
Why a global manufacturer stopped
using interior firewalls to protect
critical systems from lateral attacks

SEGMENT SCADA SYSTEMS FROM THE IT NETWORK

Plant managers are confident their industrial control systems are hidden from view by unauthorized users and devices, allowing them to operate in secure isolation

This global manufacturer of advanced materials and components serves a range of customers from aerospace to government. The company has more than 100 manufacturing plants across 30 countries. These facilities operate in highly confidential environments due to the classified materials produced in them. What's more, some of the plants work with H1 hazardous materials with an explosive element, making 24x7 monitoring a critical function to maintain safety.

An MPLS network connects all 100+ plants worldwide with a flat Layer 2 network. Once on the network in any of the facilities, a bad actor could move laterally to the systems, workstations or servers in any of the other plants anywhere in the world. A lack of adequate segmentation exposed the entire network to lateral attacks by malicious actors.



CHALLENGES AT A GLANCE

- ❑ Easy lateral movement across flat L2 network
- ❑ Disruption of H1 monitoring could be catastrophic for plant and surrounding community
- ❑ Internal security audit failures
- ❑ Persistent malware threat in one division
- ❑ Mandate to comply with NIST segmentation requirement
- ❑ Live data jacks in every building create broad threat surface
- ❑ 24x7 manufacturing means network downtime is untenable

1 PLANT SECURED AND SEGMENTED IN UNDER 2 DAYS

Eliminating network complexity and maximizing security with Airwall

The company had traditional networking and security technology in place, including switches and routers for local networking and firewalls and VPNs for security. Nevertheless, malware was able to breach, traverse and persist in the network despite legacy security controls such as VLANs, firewall rules, ACLs, VPNs, 802.1x authentication and security certificates. The malware threat exposed the company to significant cybersecurity risk.

The small IT team sought alternatives to the existing configurations. Initial estimates for internal firewalls and ACLs for segmentation were about \$1 million per plant. Deployment would take about 2 months for each plant.

Purpose-built for IIoT

A proof of concept with Tempered Networks showed that micro-segmentation could be achieved at a significantly lower cost, with deployment taking less than 2 days per plant. The industrial control systems would be completely cloaked and unreachable by unauthorized

BENEFITS AT A GLANCE

-  **Stronger Security**
Entire plants are now cloaked from the rest of the MPLS and L2 shared network with the HIP-fortified network; no unauthorized communication to ICS devices
-  **Easier to Manage**
Shop floor can administer overlays versus requiring CCNE-caliber staff and provide better consistency, resiliency, and predictability; no net new personnel required
-  **Lower Costs**
Acquisition cost of Tempered Networks Airwall was 20% of traditional firewall approach; deployment in under 2 days versus 2 months for traditional solution

entities. And, the solution could be implemented by the company's current staff.

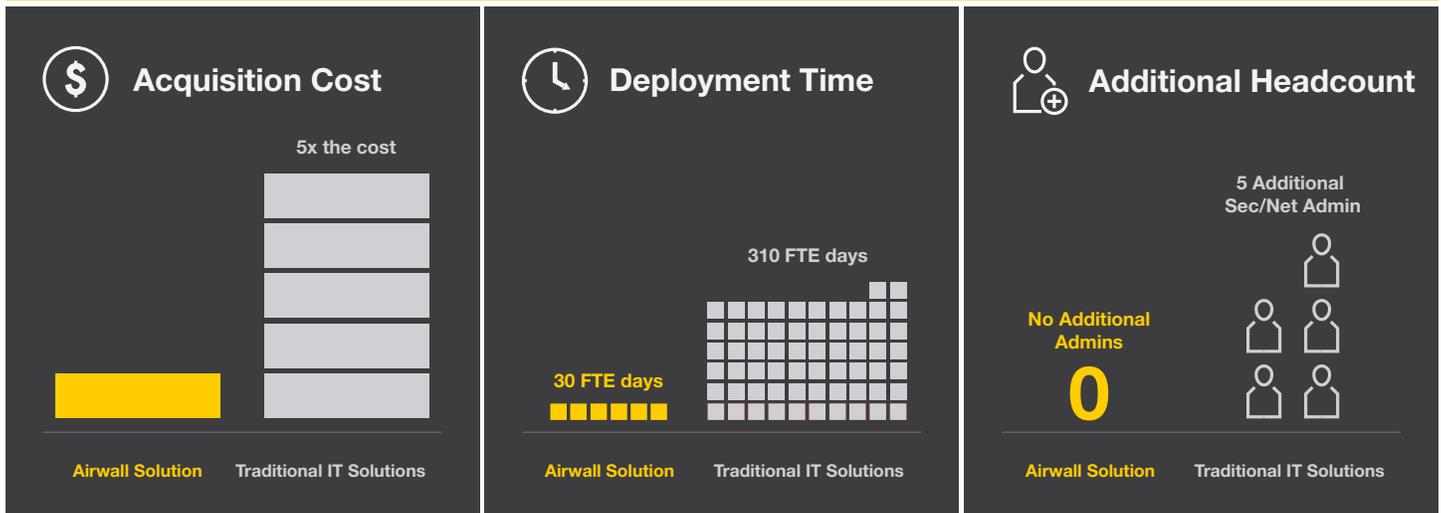
What sealed the deal was the ability to meet NIST requirements and provide network segmentation without having

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



Why a global manufacturer stopped using interior firewalls to protect critical systems from lateral attacks.

The team covered the first building with over 700 connected systems across 10 different manufacturing lines in half a day without disruption



ISOLATE, SECURE, PROTECT AND SIMPLIFY

Cloaking industrial workstations renders them undiscoverable by unauthorized users and systems

This manufacturing company has grown quite large through mergers and acquisitions. The business units operate independently but are overseen by a centralized IT/OT strategy. The network threat surface across the company was significant. There were thousands of live data jacks in every building—any of which could be used by someone with malicious intent to get on the network and then move laterally to critical industrial controls and other sensitive resources.

One division experienced a persistent malware threat that it was unable to

remove on its own. The Department of Homeland Security (DHS) was brought in to help with 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.

More worrisome, however, is that bad actors could disrupt the continuous monitoring of hazardous materials used in some of the plants. This poses a catastrophic danger for the company and surrounding communities if undetected conditions were to lead to an explosion.

Subsequently, the CIO/CISO issued a mandate to implement network segmentation for all business units and to comply with NIST standards for network security.

Improving network security

Network segmentation was essential to protect systems from each other and to eliminate unauthorized access to industrial controls. The company looked at traditional options: internal firewalls, VPNs, VLANs and cumbersome access control lists (ACLs). “Re-architecting our network with any of the traditional methods would have been prohibitively expensive, costing about a million dollars per plant plus new

staff members to support it,” according to the Manager of Networking Systems. “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 Tempered Networks Airwall allowed the manufacturer to deploy an overlay network on top of the existing network infrastructure. Airwall combines automated orchestration with the industry-standard host identity protocol (HIP) to lock down communications between key devices on the network. For example, the HMI controllers can only talk to the HMI/SCADA master server, and nothing else on the network can even see – let alone

communicate with – any of these devices. They also are blocked from the Internet. They are micro-segmented, cloaked and hidden from view. The company has similarly micro-segmented its various operational systems according to functionality. All communications for these systems utilize encrypted peer-to-peer secure tunnels.

Fast and simpler networking

Cost-effective Airwall devices were deployed to connect specific devices through Tempered Networks’ AirConnector, an identity-based routing system that easily establishes secure tunnels. “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,” says the Director of SCADA Security. “In 48 hours or less, we can take a 50,000 square foot manufacturing facility and cloak it with zero downtime.”

This solution allows OT systems to live alongside IT systems without the danger of forbidden communications among the systems. Moreover, the network now meets all requirements for NIST-specified segmentation. Plant operators are confident their systems are secure.

“We have hundreds of applications that are hard coded with IP addresses for our devices 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 Security

Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500

