Customer Case Study

Global Manufacturer Controls Critical Infrastructure on 3rd Party Networks

A company's journey to achieve simple micro-segmented access to its systems running on-premises at customer facilities to meet stringent Service Level Agreements.

Customer Requirements

- Securely connect and collect remote ICS monitoring data from customer sites
- Deploy and operate across customer and other networks they don't control
- Enable deployment by local technicians with no IT or security training
- Deploy and manage without requiring new headcount or expertise to operate
- Ensure high availablily and resiliency

Solution

- A private overlay network that can be deployed on any transport or network without having to change infrastructure
- Micro-segmented secure connectivity to remote ICS and SCADA systems
- Simple centralized management of devices on untrusted, 3rd party networks
- On-demand access control and provisioning with overlay networks

Benefits

- 97% faster secure provisioning of ICS and SCADA systems
- 90% reduction in attack surface
- 50% lower capex and opex
- Reliable and hardened connectivity—even in remote, hard-to-reach locations
- Total flexibility by leveraging 3rd party networks (e.g. cellular, customer, ISP networks)

Overview

A leading industrial gas company manufactures, sells and distributes atmospheric, process and specialty gases to customers in the aerospace, chemicals, food and beverage, electronics, energy, healthcare, and manufacturing industries in over 50 countries. The global manufacturer installs and maintains production plants on its customers' facilities, running highly automated chemical processes managed by industrial control systems (ICS). To deliver on its service level agreements (SLAs), the manufacterer must continuously monitor the safety and availability of its customers' production environments.

Challenges

The manufacturer has a full-time monitoring center at its operations headquarters to remotely monitor on-premises customer equipment, as well as a secondary operations center in a different geographic location. Some plants had no remote monitoring capability, leaving them without a reliable way to ensure the safety and security of these critical pieces of infrastructure.

The manufacturer's customers have process control technicians perform general oversight and maintenance of the physical plant, but these local technicians often have no IT, network, or cyber-security training. Furthermore they are not allowed to access the manufacturer's network.

The company needed a connectivity solution that could be deployed across a variety of production environments, networks they didn't own or control, and could also integrate with existing monitoring infrastructure. They also wanted a solution that would not require wholesale changes to the underlying network and would support both legacy and new ICS and SCADA systems, regardless of operating system.

Attempting to solve the problem, the company evaluated other networking options including:

- General-purpose and industrial cellular modems
- Enterprise and industrial VPNs with IPSec tunneling
- Private network services through large telecom providers

 |

TEMPERED NETWORKS

Ultimately, it found those solutions to be too complex, unmanageable at scale, unsecured, and far too expensive. Deployment could take up to 6 months and ongoing maintenance for solutions like VPNs and IPSec would require about two dedicated full time employees at headquarters. Also, given the geographic distribution of customer locations, they would have needed a team of IT experts who could travel to customer sites to support the alternate solutions.

The Solution

By implementing Tempered Networks' Identity Defined Networking (IDN) solution with identity-based segmentation, the manufacturer quickly and cost-effectively deployed hardened overlays over existing third party networks. The company has strengthened the security of its remote connections to protect critical infrastructure and ensure reliable remote monitoring of its distributed production facilities.

Stronger Security and Operational Integrity

The manufacturer has secure communications between remote facilities and its monitoring centers using hardened micro-segmentation that isolates ICS systems. Instant and secure connectivity is established over cellular, customer, or ISP networks. The solution enables centralized control over all aspects of support and maintenance, including the revocation of components that become lost, stolen, broken, or otherwise compromised. In addition, the manufacturer's primary and secondary monitoring centers now have graceful failover between sites.

Easy Deployment and Management

The manufacturer was able to deploy IDN without requiring skilled IT resources at the remote customer locations. The manufacturer's OT staff centrally configures security, connectivity, and monitoring aspects of the remote connections, and can expand, modify, or revoke connections in minutes. The intuitive management console makes it easy for the administrator to restrict connectivity to specific devices in each production plant that require remote monitoring, minimizing exposure of critical infrastructure.

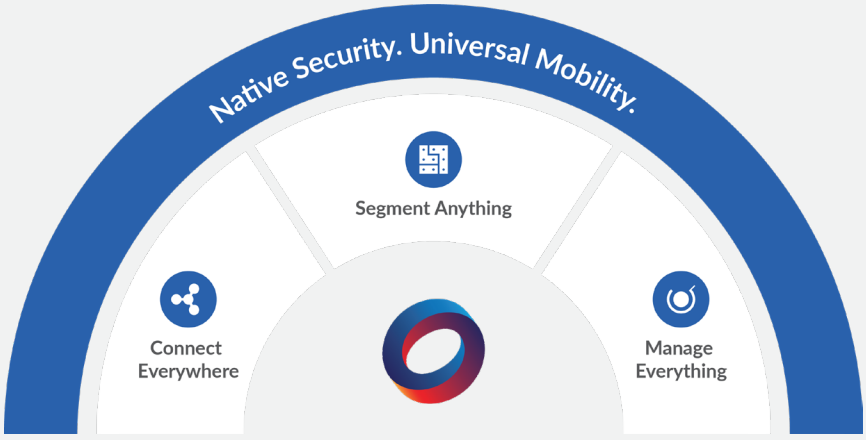
Achieve Customer SLAs with Low TCO

IDN enabled the manufacturer to modernize and expand remote monitoring of customers' critical production assets without changes to its existing security and network infrastructure. The scalable solution allows staff to quickly and easily bring new production facilities online while maintaining the high level of remote monitoring and management the manufacturer requires to deliver on SLAs. The 'drop-in' solution does not require on-site technicians at customer sites for installation, maintenance, or troubleshooting, keeping OpEx low.

"The central console allows us to instantly add devices and makes it easier and faster to provision, regardless of where our equipment is located."

Summary

Today, the manufacturer can easily monitor its production facilities around the world and ensure their security and availability. The Tempered Networks' solution delivers segmented and secure remote connectivity, increased operational efficiency and system availability, and significantly reduced costs. The organization has peace-of-mind by serving its customers on a hardened, zero trust network that's highly resilient.



Experience the same simplicity, security, and cost-savings that our customers achieved.

To learn more or schedule a no obligation demo, email info@temperednetworks.com or visit www.temperednetworks.com

