Sponsored by Tempered

SMART BUILDINGS 2.0

Airwall
The next-gen air gap

Learn how one of the world's largest cruise lines connected and secured its entire fleet's maritime systems quickly and easily without dry dock downtime and loss of revenue

Tempered Delta Controls (CS)²AI intel IoT Solutions Alliance

SMOOTH SAILING WITH A MORE SECURE NETWORK

The cruise line's IT team transformed an inherently insecure shared network to a protected and isolated segment for the maritime operational systems in just days, without dry docking the ships and re-architecting the network.

As one of the world's largest international cruise lines, this company provides an exceptional holiday experience for the millions of passengers that board each year. Travelers enjoy personal pampering, world-class entertainment and exciting excursions as they cruise to popular destinations on ships the size of small cities.

Behind the scenes, however, it was anything but smooth sailing for the shipboard network that controls the critical maritime systems, including fuel, propulsion, navigation, and more. The complex and poorly architected network put operations at risk when a failed security audit recommended dry dock periods for each ship to allow for an expensive networking overhaul.

"Our audit firm looked at the flat, Layer 2 shipboard network and proclaimed it a security risk for our maritime systems," explains Alex Soukhanov, Director of Moran Cyber. "There was no segmentation of the individual control systems. A vendor for our propulsion systems could also see what was happening with our navigation systems. This was common across the board, where everyone could see everything. Obviously, this is unacceptable risk in today's cyber threat environment." A lack of adequate segmentation exposed the entire network to lateral attacks by bad actors.

CHALLENGES AT A GLANCE

- ❑ Shared network with no segmentation of operational systems
- ❑ Unrestricted access to network by third-party vendors
- ❑ Internal security audit failures
- ❑ Network congestion caused downtime issues
- ❑ Legacy systems had no inherent security
- ❑ Small staff with minimal ability to grow

The audit firm recommended completely re-architecting the network on each ship, which would result in three to four weeks in dry dock and millions of dollars' worth of upgrades per ship. "Dry docking the ships for network upgrades wasn't even a realistic option for us. There is too much revenue at stake even with a small amount of downtime," says Alex. "Plus, the cost of new networking hardware and software was prohibitive, and we didn't have – and couldn't hire – the staff to support hundreds of new firewalls."

FIREWALLS WERE A NON STARTER

We had a chance to ask Captain Alex Soukhanov, Master Mariner/Director at Moran Cyber, about the project.

Captain Alexander N. Soukhanov

Director, Moran Cyber
Moran Shipping Agencies, Inc.

Moran Cyber is a team of maritime and industrial cybersecurity professionals who work to protect commercial ships and port infrastructure from cyber threats, as industry digitalizes and moves to greater technology integration.

Q: What was it that encouraged you to go with Tempered when it came to this maritime security challenge?

A: Tempered Networks provided us with a solution that was tested and vetted by an owner and operator of a large fleet of ships. Tempered's solution filled an immediate need to mirco-segment networks that were flat by design, and control accesses by multiple vendors. This is primarily for safety reasons in order to protect highly sensitive marine systems from cyber threat, and to mitigate unnecessary maritime risk to life, property, and the environment.

Q: What kinds of cyber security challenges do you have to address aboard ship?

A: Cybersecurity challenges in maritime are unique because of the manner of integration and management of technologies, procurement, and security practices. The spectrum of cyber maturity in the maritime industry is vast and inconsistent, most are below average. Companies are short on technical capability to manage, and have little or no cybersecurity budget, let alone the organic human capital.

Cruise ships require persistent connectivity required for recreation, financial transaction processing, healthcare operations, customer data, and ICS control systems for navigation. All compelling targets for cyber attacks.

MORAN CYBER

"Tempered Networks offers the best solution that is relevant to our industry and cost effective."

Captain Alex Soukhanov,
Master Mariner, Moran Cyber

BENEFITS AT A GLANCE

Lower Cyber Risks

Protected maritime systems from unauthorized access and cyberthreats, and decreased attack surface by 90% by segmenting and isolating maritime systems from the general network

Improved Operational Efficiency

Reduced downtime and traffic congestion with a cleaner network and without having to re-IP anything or add new headcount

Reduced Costs

Integrated legacy and modern maritime systems without requiring "fork-lift" upgrades

Vessels are largely dependent on third parties for support, primarily because they're mobile. But these are also the largest moving objects in the world, and with more and more systems connected to the internet for visibility and optimization reasons, the risk of exposure to cyber breaches also increases if security isn't prioritized.

Q: With the recent Coast Guard Cyber Threat Advisory and global cyber tensions heating up what advice would you give to maritime shipping executives?

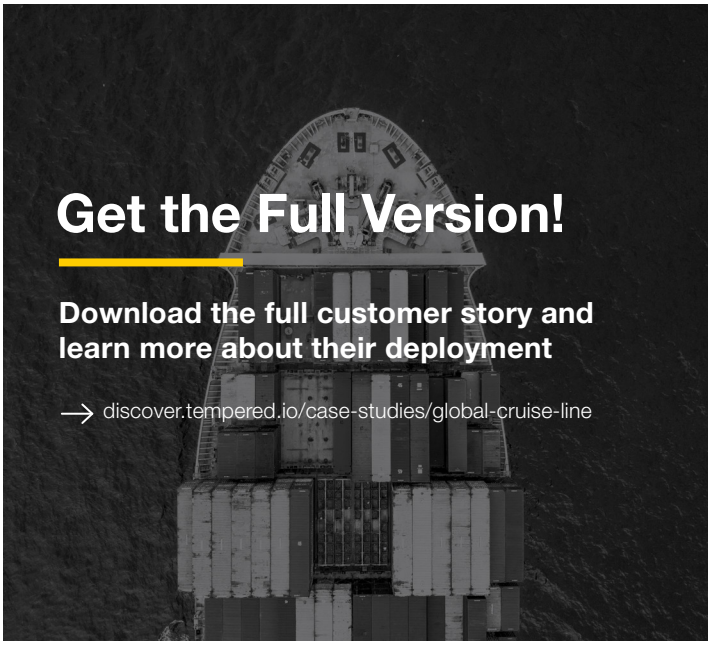
A: First, establish a baseline to understand ("identify") your assets and networks, and the people and processes as they relate to cybersecurity. The assessment is the basis of all strategies. Tempered is a superior technology solution if you deem it necessary to implement new or a higher level of network segmentation, particularly if your previous design leaves critical systems exposed and unprotected. This is really important if you operate vessels, because the source of the cyber-attack doesn't matter – no one belongs in these systems unless they're controlled and authorized. This is a safety matter with far-worse consequences than simple data loss. Tempered Networks offers the best solutions that is relevant to our industry and cost effective.

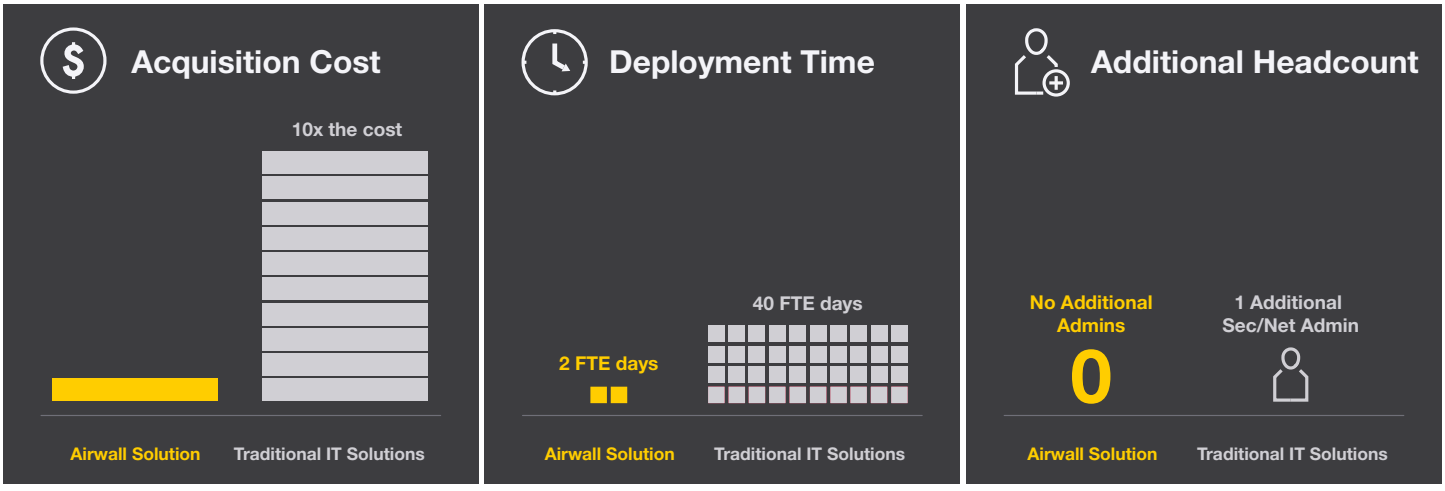
"Cybersecurity challenges in maritime are unique because of the manner of integration and management of technologies, procurement, and security practices."

Captain Alex Soukhanov,
Master Mariner, Moran Cyber

Tempered succeeded when traditional network security approaches failed because it offered a purpose-built approach to the unique demands of IIoT cybersecurity, including: increased availability/resiliency; unprecedented scalability; easy management and fast connection and isolation.

Tempered's advance devices, including internal firewalls and network access controls, reducing complexity, costs and operating requirements, on land or sea.

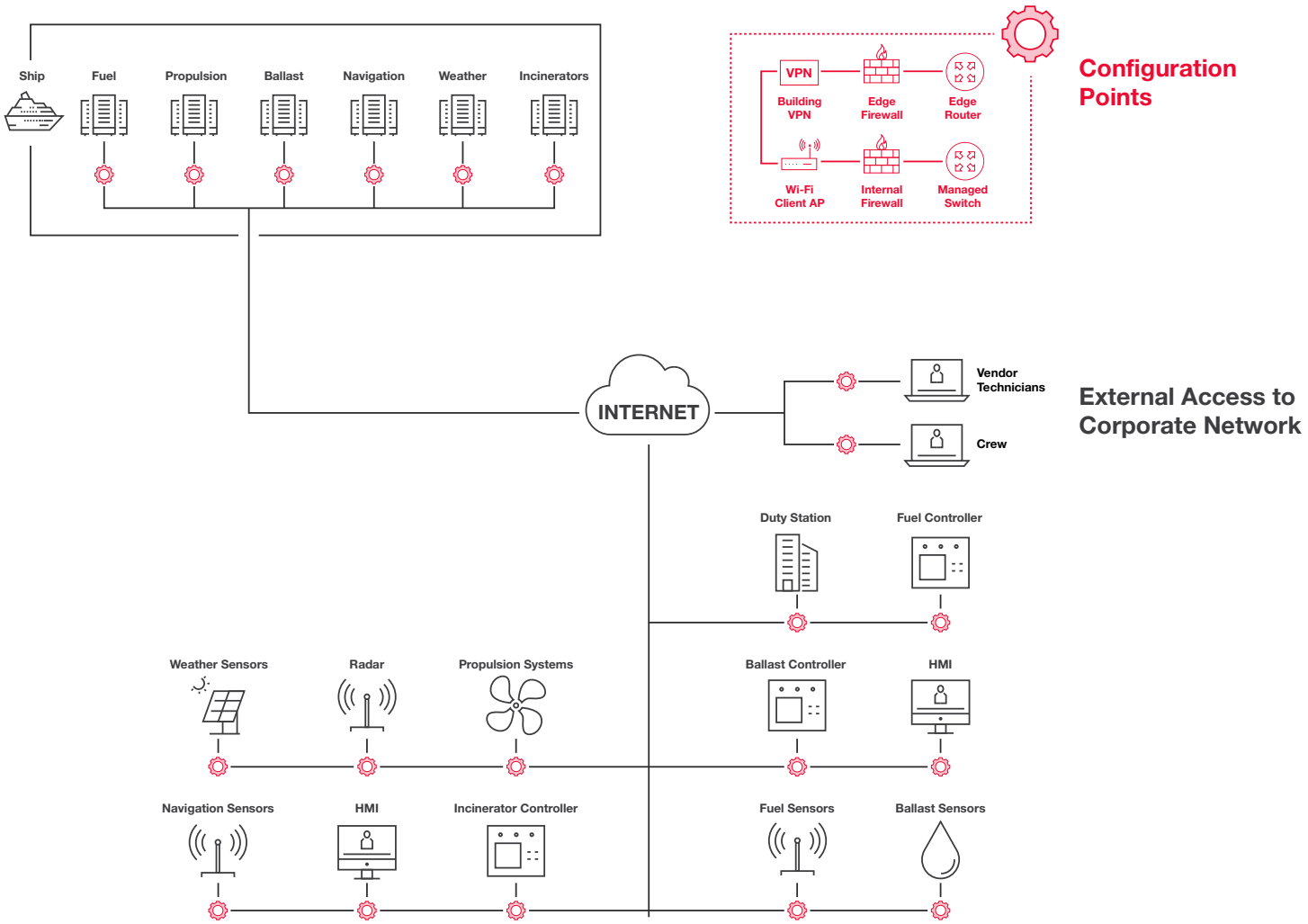




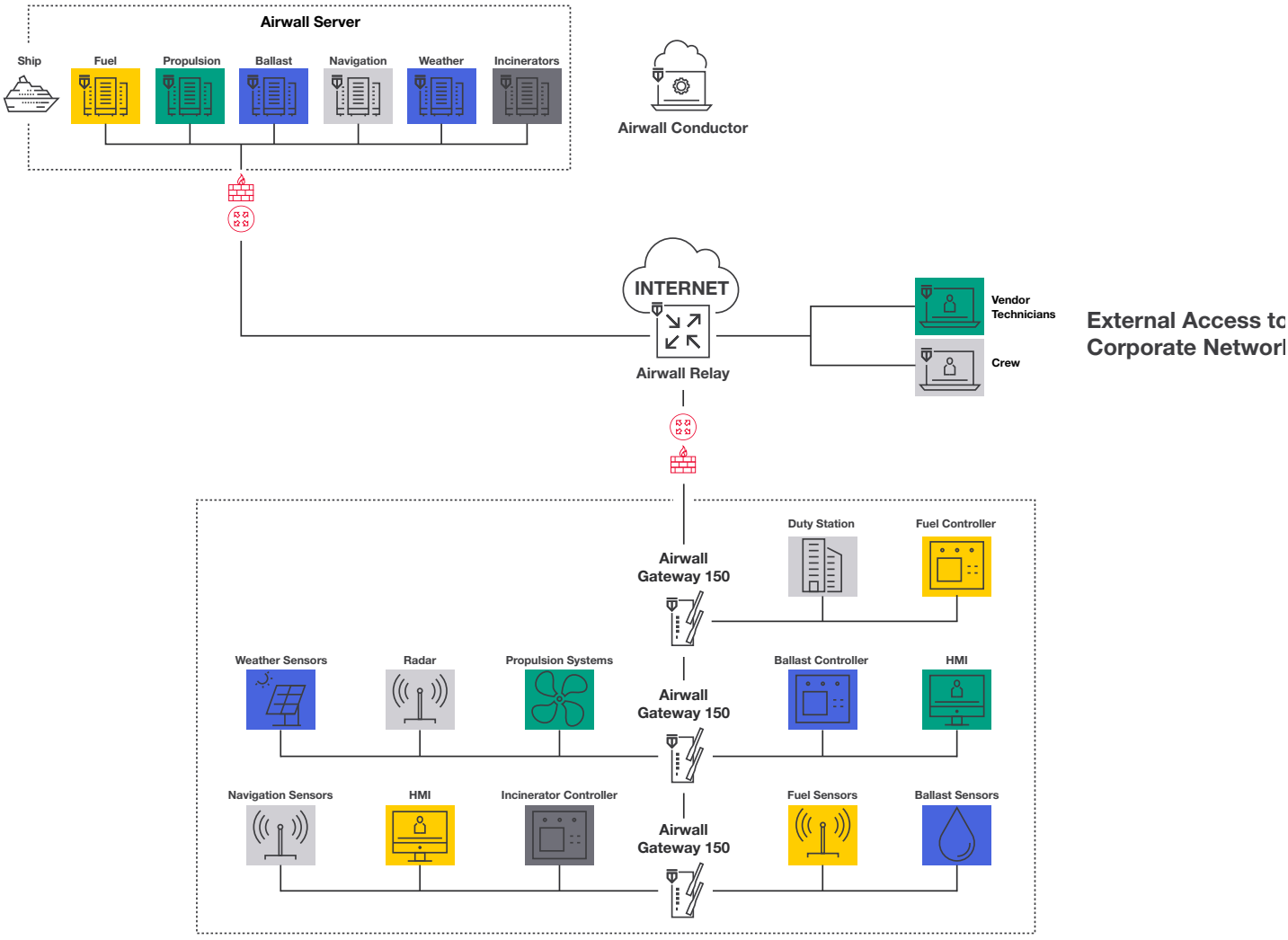
AN ISOLATED, PROTECTED AND COST-EFFECTIVE NETWORK

The first consideration, submitted by a leading networking and security vendor, would have required substantial downtime, a massive capital outlay and needed the support of an expanded security team. When the client pushed back at the costs, the audit firm searched for a new approach. With Tempered, the capital outlay was a fraction of the cost; the deployments could be done on ships while at sea; and no additional security staff needed to be hired to support the enhanced security.

Before



After



Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500