



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 or revenue loss.

Smooth sailing with secure networking for one of the world's largest cruise lines

Airwall Solution protects critical maritime systems and secures remote vendor access.



Challenges

The cruise line's shipboard network was inherently insecure, with no segmentation of operational systems and unrestricted network access for vendors. Critical maritime systems — including fuel, propulsion, navigation, and more — were exposed and unprotected.



Solution

The team deployed the Airwall Solution on the ships while at sea, without the need for dry docking or any additional staff. They micro-segmented the network across all vessels and implemented secure controls for vendor access.



Wins

Segmenting and isolating their critical marine systems allowed the team to decrease their attack surface by 90% and created a cleaner network, reducing downtime and traffic congestion and improving operational efficiency.

“Tempered offers the best solution that is relevant to our industry and cost-effective.”

Captain Alex Soukhanov
Master Mariner, Moran Cyber

The challenge

While cybersecurity is getting more complicated across the board, the challenges that the maritime industry faces are especially unique. Cruise ships require persistent connectivity for recreation, financial transaction processing, health care operations, customer data, and ICS control systems for navigation — all compelling targets for cyber-attacks. Vessels' reliance on third parties for support only increases the risk of breaches.

Nevertheless, most cruise lines are short on technical capability, and have little or no cybersecurity budget, let alone the organic human capital.

This was certainly the case for the cruise line that Moran Cyber was called in to support. The shipboard network, which controls critical maritime systems such as fuel, propulsion, and navigation, was complex and poorly architected.

“Our audit firm looked at the flat, Layer 2 shipboard network and proclaimed it a security risk for our maritime systems,” explained 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. Obviously, this is an unacceptable risk in today's cyber threat environment.”

In addition to the lack of segmentation and unrestricted access for third-party vendors, network congestion was causing downtime issues and legacy systems had no inherent security. It was no wonder that the vessels failed an internal security audit.

But the audit's recommendation that they dry dock all of the ships for three to four weeks for a

complete networking overhaul, including millions of dollars' worth of upgrades per ship, wasn't a realistic option. “There is too much revenue at stake even with a small amount of downtime,” said 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.”

The solution

When the client pushed back against these costs, the audit firm searched for a new approach. They found it in Tempered's Airwall Solution.

“Tempered provided us with a solution that was tested and vetted by an owner and operator of a large fleet of ships,” explained Alex. “It filled an immediate need to micro-segment networks that were flat by design, and control access by multiple vendors.”

What's more, Tempered's advanced Host Identity Protocol-based architecture eliminates the need for layers of devices, including internal firewalls and network access controls, drastically reducing complexity and operating requirements. As a result, the capital outlay was a fraction of the cost of alternative solutions, the deployments could be done on ships while at sea, and no additional security staff needed to be hired to support the enhanced security.

Customer success

Lower Cyber Risks: Moran Cyber protected maritime systems from unauthorized access and cyber threats, and also decreased the attack surface by 90% by segmenting and isolating maritime systems from the general network.

Improved Operational Efficiency: The Airwall Solution created a cleaner network, reducing downtime and traffic congestion, without the need to restructure anything or add new headcount.

Reduced Costs: The team integrated legacy and modern maritime systems — no forklift upgrades required.

Taking It Further

As recent Coast Guard Cyber Threat Advisory and global cyber tensions continue to heat up, the Moran Cyber team has peace of mind knowing that they've left their clients in good hands. "This is a safety matter with far worse consequences than simple data loss," explained Alex. "Tempered offers the best solution 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

Deployed Airwall Solution components

A comprehensive solution including Airwall Conductor, Airwall Relays, Airwall Servers, Airwall Gateways, and Airwall Agents enabled the Moran Cyber team to connect and secure maritime systems across the cruise line's entire fleet.



Airwall Conductor: Moran Cyber's team deployed the orchestration engine to provision, segment, allocate, and revoke network access in the cloud. The Conductor allowed them to visualize their segmentation and do granular whitelisting of the network.



Airwall Server: Airwall Servers allowed the team to enable software-defined segmentation for critical maritime systems, encrypt at the individual server level, and enforce a perimeter around each server. Only authenticated and authorized endpoints can discover and communicate with the servers, as each one is completely cloaked.



Airwall Gateways: The Moran Cyber team deployed physical Airwall Gateways to cloak and segment the critical maritime systems.



Airwall Relay: Relays (identity-based routing devices) deployed in front of the overlay network in the cloud allowed the team to securely connect and route traffic across the enterprise WAN via encrypted tunnels. Thanks to these routing devices, no expensive firewalls or complicated VPNs were necessary.




Airwall Agents: Secure remote access was enabled so that the crew and vendor technicians could access critical maritime systems with Airwall Agent software on their devices.





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

 10% of the cost of traditional IT solutions

 Deployed in two FTE days instead of 40 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