Case Study

Zero-Trust Remote Access for 94 Vessels Across Global Waters

How a Global Cruise & Hospitality Operator Secured IT/OT Systems Across the World's Largest Fleet.

Executive Summary

INDUSTRY	FLEET	DEPLOYMENT	EMPLOYEES
Maritime / Cruise & Hospitality	94 Vessels, 9 Brands	< 1 Hour / Site	150,000+

The world's largest cruise operator — with 94 vessels, 9 brands, and more than 150,000 employees across roughly 150 countries — faced an urgent cybersecurity challenge. Dozens of third-party vendors required both remote and on-vessel access to critical operational technology systems including bridge navigation, engine automation, HVAC, and safety equipment. Legacy VPN infrastructure provided broad network access rather than asset-specific control, creating unacceptable risk in an industry experiencing a 150% surge in OT cyberattacks.

After four cybersecurity incidents in recent years — including ransomware and phishing breaches resulting in significant regulatory penalties — the operator needed a fundamentally different approach. The organization deployed Xona, a purpose-built zero-trust secure access platform supporting both remote and local access, across all 94 vessels and shoreside sites, achieving 100% elimination of direct endpoint-to-asset connectivity. The result is zero direct network access — users interact with OT systems in real time, but their endpoints are never connected to the OT network. Deployment took under one hour per site, with some installations completed in as little as 20 minutes. Today, the operator's cybersecurity operations centers in two global locations monitor every vendor session in real time, with full video recording and instant termination capabilities.

Industry Context: The Maritime Threat Landscape

The maritime industry has entered a new era of cyber risk. As vessels have become increasingly connected — with IP-networked navigation, propulsion, cargo handling, and passenger systems — they have also become attractive targets for threat actors. The convergence of IT and OT aboard modern ships has created attack surfaces that did not exist a decade ago.

The scale of the threat is significant. Research has documented a **150% surge in maritime OT cyberattacks**, with ransomware as a leading vector (measuring OT-specific attacks on maritime targets).

Separately, industry-wide maritime cyber incidents rose **103% year-over-year (measuring all reported maritime cyber incidents)**. Vessel OT systems — including electronic chart displays, dynamic positioning, engine management, and ballast water systems — are routinely accessed remotely by original equipment manufacturers for maintenance, diagnostics, and firmware updates. Each of these remote sessions represents a potential intrusion point.

The regulatory environment has responded with urgency. In January 2025, the U.S. Coast Guard published its most comprehensive maritime cybersecurity regulation to date, establishing requirements for:

- **MFA for all remotely accessible OT systems**
- **Network segmentation between IT and OT environments**
- **Designated Cybersecurity Officers available 24/7**
- **Comprehensive cybersecurity plans based on risk assessments**
- **Cyber incident reporting effective July 16, 2025**

This regulation joined existing frameworks including IMO MSC.428(98) for maritime cyber risk management in safety management systems, and IACS Unified Requirements E26/E27 for cyber resilience on vessels. For a global fleet operator, the compliance burden is not a future concern — it is an immediate operational reality.

The Challenge

The operator's fleet of 94 vessels and numerous shoreside hospitality facilities depended on dozens of third-party vendors and OEM contractors for critical system support. These vendors required access to some of the most sensitive systems aboard each vessel:

- **Bridge navigation systems and electronic chart displays**
- **Engine automation and propulsion controls**
- **HVAC and environmental management**
- **Safety and fire suppression systems**
- **Hotel management and passenger-facing IT systems**

The existing remote access infrastructure suffered from several fundamental shortcomings:

- **Broad network access via VPN.** Legacy VPN solutions granted vendors access to wide network segments rather than specific assets. Once connected, a vendor — or an attacker using compromised vendor credentials — could potentially reach systems far beyond their authorized scope.
- **No session recording or real-time audit.** When vendors connected to vessel OT systems, there was no capability to record sessions, monitor activity in real time, or provide forensic evidence after the fact. Auditors had no way to verify what actions vendors had taken on critical systems.
- **Shared credentials.** Vendor teams commonly shared login credentials, making it impossible to attribute actions to specific individuals. This practice directly conflicted with zero-trust principles and regulatory requirements for unique user identification.
- **No instant termination capability.** If a security incident occurred during a vendor session, there was no mechanism to immediately disconnect that session or disable all remote access to a vessel.
- **Expensive on-site support requirements.** When remote access was unavailable or too risky, vendors traveled to vessels for on-site support at costs exceeding $2,000 per visit — a significant operational expense for a fleet of 94 vessels.
- **Satellite bandwidth constraints.** Vessels at sea rely on satellite links with limited bandwidth and variable latency. Traditional remote access tools performed poorly in these conditions, creating frustration for vendors and delays in critical maintenance tasks.

The stakes were not theoretical. The operator had experienced four cybersecurity incidents in recent years, including two ransomware attacks and two phishing breaches, resulting in **$6.25 million in regulatory penalties**. With maritime cyber incidents surging industry-wide and new regulations taking effect, the operator recognized that incremental improvements to its existing approach would not be sufficient.

The Solution

After evaluating alternatives, the operator selected Xona — a purpose-built zero-trust secure access platform designed specifically for operational technology environments. Xona's architecture addressed every dimension of the operator's challenge:

Protocol Isolation. Rather than tunneling vendor connections directly into the vessel network, Xona acts as an intermediary. OT protocols — RDP, SSH, VNC — are terminated at the gateway inside the vessel's trusted network. Only encrypted pixel streams are delivered to the vendor's browser over HTTPS port 443. The vendor's endpoint never touches the OT asset. No malware, ransomware, or lateral movement can traverse a pixel stream.

Zero-Footprint Access. Vendors access Xona through a standard web browser — no VPN clients, agents, plugins, or software installations are required. This eliminated the logistical burden of managing software across dozens of vendor organizations and hundreds of individual technicians.

Both Remote and Local Access. Uniquely, the Xona platform supports secure access for vendors physically aboard a vessel as well as those connecting remotely. On-vessel technicians connect through the same gateway, ensuring that every session — whether local or remote — is authenticated, authorized, recorded, and auditable.

Centralized Management. A centralized management console enables the operator's security team to define access policies, provision and revoke credentials, and monitor sessions across the entire 94-vessel fleet from cybersecurity operations centers located in two global locations.

Session Recording and Oversight. Every vendor session is recorded with full video fidelity, including keystroke and mouse activity logging. Authorized personnel can shadow live sessions in real time and terminate any session instantly using a single-click kill button.

Satellite-Optimized Performance. Xona's PNG-based pixel streaming is optimized for low-bandwidth, high-latency links — precisely the conditions encountered on vessels using satellite connectivity. Vendors report responsive, usable sessions even over constrained links.

Solution Highlights: Xona Key Features
✓ Protocol Isolation — OT protocols never leave the trusted vessel network
✓ Zero Footprint Browser Access — No VPN clients or agents required
✓ Remote + Local Access — Unified security for on-vessel and remote vendors
✓ Centralized Fleet Management — Policy and monitoring across 94 vessels
✓ Full Session Recording — Video-fidelity audit trail for every session
✓ Live Session Shadowing — Real-time oversight with instant kill capability
✓ Credential Injection — Vendor never sees or handles OT passwords
✓ Satellite-Optimized — PNG pixel streaming for low-bandwidth links
✓ Lockbox Emergency Control — Instantly disable all access per vessel
✓ MFA + SSO Integration — SAML 2.0 with enterprise identity providers

Implementation

The deployment was designed for speed and zero disruption — critical requirements for an operator that could not afford to take vessel systems offline during installation.

- **Deployment Time.** Each site was operational in under one hour, with some vessel installations completed in as little as 20 minutes. Xona's overlay architecture requires no network reconfiguration, no firewall changes, and no modifications to existing OT assets.
- **Fleet Scale.** Gateways were deployed across all 94 vessels and shoreside sites. The centralized management platform was installed at the operator's cybersecurity operations centers, providing a single pane of glass for fleet-wide access governance.
- **Vendor Onboarding.** Third-party vendors were provisioned through Xona's federated identity integration, with SAML 2.0 SSO and mandatory multi-factor authentication. Each vendor technician receives a unique identity — no more shared credentials. Access is scoped to specific assets and time windows, with just-in-time provisioning and moderated approval workflows for sensitive systems.
- **Dual Operations Centers.** Cybersecurity teams in two locations now monitor vendor sessions around the clock, leveraging Xona's live shadowing capability to observe sessions in real time and intervene when necessary.

> *"The ability to support both secure remote and local access has been transformative. We can now confidently grant vendors and our team access to the systems they need without introducing unnecessary risk."*
>
> **— Program Manager, Maritime Cyber Security**

Results

The deployment delivered measurable, immediate improvements across security, operations, and compliance.

Results at a Glance
100% Elimination of direct endpoint-to-asset connectivity across all 94 vessels
< 1 Hour Deployment time per site (as fast as 20 minutes)
94 Vessels Fully deployed across the world's largest cruise fleet
2 Global Ops Centers Centralized real-time monitoring from dual cybersecurity operations centers
100% Session recording coverage — every vendor session captured with video fidelity
$2,000+ Saved per eliminated on-site vendor visit
Zero VPN clients, agents, or plugins required on vendor endpoints

- **Eliminated lateral movement risk.** Protocol isolation ensures that vendor endpoints cannot access the vessel network. Ransomware, malware, and unauthorized lateral movement are architecturally impossible — the attack surface that enabled previous incidents no longer exists.
- **Complete session auditability.** Every vendor interaction with vessel OT systems is now recorded, time-stamped, and attributable to a named individual. The operator can produce forensic evidence for any session within seconds, satisfying both regulatory requirements and internal governance standards.
- **Reduced vendor support costs.** With reliable, secure remote access now available even over satellite links, vendors resolve many issues remotely that previously required expensive on-site visits. The operator estimates savings of $2,000 or more per eliminated site visit across a fleet of 94 vessels.
- **Faster vendor response times.** Vendors can now connect to vessel systems within minutes rather than scheduling travel. For time-critical equipment issues — an engine fault, a navigation system alert — this reduction in response time directly improves operational safety and continuity.
- **Simplified vendor governance.** The operator replaced a fragmented approach of VPNs, jump servers, and shared credentials with a single platform governing all vendor access. Onboarding is faster, provisioning is centralized, and deprovisioning is immediate.

Regulatory Alignment

Regulatory Requirement	How Xona Addresses It
USCG Cybersecurity Rule (2025)	**MFA enforced at the gateway layer for all remote and local access. Network segmentation achieved through protocol isolation — IT and OT traffic are architecturally separated. Cyber incident evidence available through comprehensive session recording.**
IMO MSC.428(98)	**Cybersecurity risk management integrated into safety management systems. Controlled vendor access with real-time monitoring and instant termination demonstrates active risk mitigation across the fleet.**
IACS UR E26/E27	**Cyber resilience requirements for vessel systems addressed through protocol isolation, access governance, session recording, and emergency lockbox capabilities.**
IEC 62443	**Platform tested against ISA/IEC 62443 requirements including identification and authentication (SR 1.x), use control (SR 2.x), data confidentiality (SR 4.x), and network segmentation (SR 5.x).**
SOC 2	**Platform provider maintains SOC 2 Type 2 attestation, providing independent assurance of security controls.**

With the USCG's cyber incident reporting requirements effective July 2025 and full cybersecurity plan submissions due by July 2027, the operator is well ahead of compliance timelines.

Looking Ahead

The operator's zero-trust access infrastructure is now a foundational element of its maritime cybersecurity program. Looking forward, the organization is pursuing several strategic initiatives:

- **Expansion of the Xona platform to additional shoreside hospitality facilities and corporate infrastructure**
- **Integration with SIEM and SOAR platforms for automated incident response workflows**
- **Enhanced vendor scoring and risk-based access policies leveraging session analytics**
- **Preparation for full USCG cybersecurity plan submission ahead of the July 2027 deadline**
- **Evaluation of cellular backup modules for emergency access during satellite link outages**

In an industry where a single cyber incident can disrupt operations for thousands of passengers and crew across multiple vessels, the operator's investment in purpose-built OT secure access is not merely a compliance exercise — it is a strategic capability that strengthens operational resilience across the world's largest cruise fleet.

About Xona Systems

Xona Systems is the secure access platform purpose-built for OT and critical infrastructure. Recognized as an Overall, Product, Innovation, and Market Leader in KuppingerCole's 2025 Leadership Compass for Secure Remote Access for OT/ICS, Xona is deployed in 40+ countries across energy, utilities, manufacturing, oil & gas, maritime, water, defense, and mining.

*Learn more at **xonasystems.com**.*