EXTRAHOP

ExtraHop RevealX™ for Ports

Secure Port Infrastructure and Ensure Supply Chain Continuity



Challenges

Ports keep regional and global trade moving, making them prime targets for cybercriminals and nation-state actors. A single cyberattack that halts terminal operations can stall supply chains within hours. Maritime cyberattacks doubled in 2025, and researchers expect AI-driven attacks to push that number higher.[1] Critical challenges include:

High costs of service disruptions

- The 2024 Rhysida ransomware attack on the Port of Seattle, a public port authority, knocked out ticketing kiosks, display boards, and Wi-Fi at Seattle-Tacoma International Airport and exposed the personal data of about 90,000 people.[2]
- Any amount of system downtime leaves containers unprocessed, idles truck fleets and rail networks, and drives up overtime and rerouting costs.

Operational blind spots

- Legacy systems, IoT and ITS devices, and smart port initiatives have expanded the attack surface. With terminal operators, drayage carriers, CBP, and rail all connected to port networks, one vulnerability can put the whole port at risk.
- Limited visibility into unmanaged assets and lateral movement between terminals slows threat detection.
- Public port authorities often have small IT and security teams stuck working through alert backlogs instead of proactive work like threat hunting or preparing their Cybersecurity Plans.

Regulatory compliance burden

- The USCG final rule, Cybersecurity in the Marine Transportation System (33 CFR Part 101, Subpart F), took effect July 16, 2025, for MTSA-regulated facilities. By July 16, 2027, each must designate a Cybersecurity Officer, complete a Cybersecurity Assessment, and submit a Cybersecurity Plan.
- The USCG rule requires reporting cyber incidents to the National Response Center without delay, and EO 14116 adds reporting to the FBI, CISA, and the Captain of the Port, so ports need fast detection and response backed by defensible evidence.

KEY OUTCOMES

By deploying ExtraHop RevealX to provide real-time network visibility and performance monitoring across all assets, ports can drive measurable improvements in the following areas.

Consolidated visibility

- Increased network context, control, and forensic capabilities without tool sprawl. Handle NPM and NDR through a single platform.
- Pervasive visibility across users, devices, applications, workloads, APIs, and machine identities, equipping security teams with decision-grade intelligence.

Stronger compliance

- Reduce the time and costs associated with preparing evidence for federal audits and incident reports.
- Leverage continuous monitoring and recording capabilities to qualify for lower premiums or better eligibility on cyber insurance policies.

Improved resilience

- Shrink mean time to detect and respond (MTTD/MTTR) for security incidents, containing threats before they disrupt terminal operations.
- Resolve performance and availability issues faster, avoiding costly downtime and returning capacity to lean IT teams.
- Increase analyst productivity by shifting time from chasing false alarms to proactive defense.

Unified Visibility and Resilient Port Protection

ExtraHop RevealX enables ports to gain full visibility across all assets, secure critical infrastructure against ransomware, and streamline security operations for faster threat detection and response through the following capabilities.

Network Detection and Response
Protect critical maritime infrastructure with real-time visibility into agentless IT, IoT, and Intelligent Transportation System (ITS) devices and east-west traffic to identify and combat machine-speed attacks.

Network Performance Monitoring
Minimize costly terminal downtime with high-fidelity performance and latency monitoring across IT applications, IoT endpoints, and ITS networks.

Flexible Deployment
Deploy NDR, NPM, IDS, or all three on a single passive architecture to eliminate tool sprawl and support separate module licensing based on port priorities.

AI-Ready SOC/NOC Operations
Accelerate investigations and achieve more confident determinations with real-time network context for analysts, plus APIs and an MCP server ready for AI agents, so lean port teams can operationalize around-the-clock triage.

Operational Technology (OT) Protection
Monitor OT protocols such as Modbus across automated cranes, SCADA networks, and smart grids. ExtraHop uses IDS signatures to catch malware, command-and-control threats, and known exploits before sabotage halts cargo.

Continuous Monitoring and Incident Reporting
Network records and precision packet capture help ports scope incidents fast, report to the National Response Center without delay, and give investigators the forensic evidence they need.

FedRAMP™

ExtraHop is trusted across the public sector, and RevealX Federal is FedRAMP® Class C certified, independently assessed against NIST SP 800-53 control requirements.

Learn More

See how ExtraHop can help your port meet EO 14116 and USCG cyber requirements and stop cyberattacks before they disrupt operations.

Talk to an expert about your priorities, including projects that may qualify for FEMA Port Security Grant Program (PSGP) funding, and get a full **demo**.

1. Cytur, via The Maritime Executive, "Report: Maritime Cyberattacks Doubled in 2025," February 24, 2026.
2. Port of Seattle, "Port Cyberattack Archive," updated April 2, 2025.

ABOUT EXTRAHOP

ExtraHop is a leader in real-time network intelligence, giving organizations the high-fidelity context to power security and IT AI automation, detect risks faster, and respond with confidence. AI agents rely on ExtraHop's real-time, ground-truth data to operate reliably in the SOC and NOC. For security teams, that means surfacing threats and definitive evidence to investigate them at machine speed. For IT operations, it means resolving performance issues in seconds. Engineered for unmatched scale, the ExtraHop RevealX platform delivers a unified view of the network across data centers, campus, branch, cloud, and AI environments. To learn more, visit **extrahop.com** or follow us on **LinkedIn**.

EXTRAHOP®

info@extrahop.com
extrahop.com

© 2026 ExtraHop Networks, Inc., RevealX and ExtraHop are registered trademarks or trademarks of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners. 1238A 11.06.26