EXTRAHOP

CUSTOMER STORY

Logistics Giant Secures Critical Maritime Infrastructure and Eliminates Blind Spots by Replacing Legacy Competitor

A global port operator displaced a legacy NDR competitor with ExtraHop to secure critical maritime infrastructure. By gaining visibility into agentless devices and east-west traffic, the organization mitigated ransomware risks. Seamless CrowdStrike and other critical application integrations now provide a unified, 100% visible defensive posture across all ports.

The organization selected the ExtraHop modern NDR platform to displace the incumbent, successfully delivering:

- **Unified Visibility:** ExtraHop eliminated critical east-west traffic and unmanaged asset blind spots. It provides native, line-rate decryption and broad protocol support for devices that cannot host agents.
- **Resilient Port Protection:** The operator secured sensitive maritime infrastructure against ransomware. It did this without introducing performance impacts to high-volume shipping and logistics flows.
- **High-Fidelity Detection:** The Security Operations Center (SOC) achieved a massive reduction in alert noise. This allowed the team to shift from manual data collection to high-priority threat hunting.
- **Scalable Integration:** ExtraHop provided a comprehensive, scalable security solution. It integrated seamlessly with the existing CrowdStrike platform via API, overcoming previous integration failures.

The Challenge: Port Security and Invisible Ransomware Risks

As a maritime logistics leader, this organization manages critical infrastructure where downtime ripples through the global supply chain. Protecting these hubs is vital, yet the organization faced severe visibility gaps across port environments that legacy tools and endpoint security could not address.

Critical Visibility Gaps and Network Blind Spots

The organization lacked visibility into port devices. Many mission-critical assets were unable to support endpoint agents, leaving the team blind to device-to-device communication. This lack of east-west visibility meant that lateral movement and network-based threats could propagate undetected across the infrastructure.

Ransomware and Operational Downtime Risk

The urgency for a modern NDR solution peaked in 2024 when a competitor's port was hit with ransomware, resulting in a two-week shutdown. This wake-up call proved that the organization's existing security posture could not ensure the continuous operation of its global shipping sites.

Troubleshooting and Fragmented Workflows

The network team lacked in-depth visibility into how port devices connected back to the central datacenter. Without high-fidelity network records or packet capture, troubleshooting performance and security issues remained a manual, time-consuming process. Additionally, a legacy NDR competitor failed to provide confident integration. Without a unified view or streamlined integration with key applications like CrowdStrike, the organization faced significant operational burdens correlating data from disparate systems.

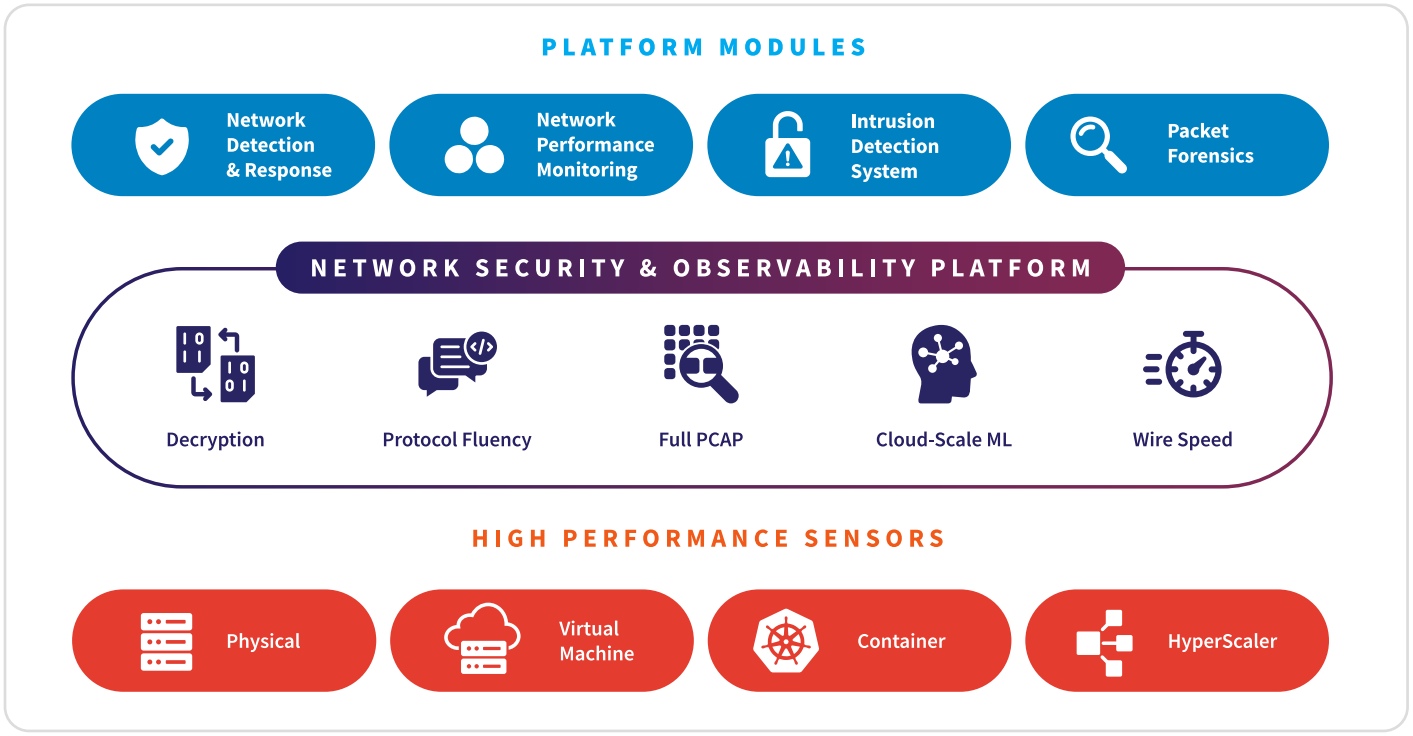
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully displaced the incumbent NDR vendor by proving its ability to provide unified security coverage. The platform met the organization's strict performance and scalability requirements.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:** The organization secured the required forensic depth and network control when it deployed ExtraHop. The platform analyzes 100 Gbps of east-west traffic and uses **high-speed decryption** to immediately find threats previously hidden within encrypted flows.
- **Reduced alert fatigue via high-fidelity detection:** The **cloud-scale machine learning** built into the ExtraHop platform lifted the SOC's operational burden. High-fidelity, low-noise detections allowed analysts to move focus from false positives to highly reliable network activity. This signals true post-compromise threats and **endpoint detection and response (EDR) evasion tactics**.
- **Actionable context and identity:** The security team achieved comprehensive insight by using **identity-based investigation**. This links malicious network activity directly to user and service accounts. It finally enables the detection of all missed lateral movement attacks.
- **Streamlined incident response via ecosystem integration:** ExtraHop fundamentally simplified incident response workflows. It established itself as the definitive source of network truth. The platform automatically feeds high-value contextual data to the customer's existing SIEM and EDR platforms.
- **Unified security platform:** The organization gained efficiency and reduced complexity by consolidating NDR, NPM, and IDS capabilities. This created **one unified, integrated solution** for comprehensive network security and observability.
- **Deep protocol coverage for core assets:** The organization mitigated major risk by gaining deep fluency. Parsing over **90+ protocols** allowed for accurate decoding of all traffic, including sensitive database communications, without introducing performance risk. This was critical for detecting hidden AD attacks and lateral movement.

ExtraHop NDR Platform



The Results: Resilient Maritime Operations and Unified Defense

The port operator achieved immediate, transformative security improvements and closed critical infrastructure gaps following the deployment of the ExtraHop RevealX™ NDR platform.

Decisive Platform Selection

The organization successfully selected ExtraHop over an NDR competitor after a long competitive POC. This fixed critical east-west visibility and unmanaged asset blind spots. The implementation also solved long-standing integration and technical support issues.

Gained Global Supply Chain Protection

ExtraHop provided essential visibility for sensitive port devices that were unable to host endpoint agents. This allowed the organization to proactively protect core logistics operations from ransomware events. This security was achieved without compromising the movement of high-volume maritime traffic.

Maximized SOC Focus

The organization achieved a substantial improvement in operational efficiency through high-fidelity detections and granular network records. This empowered the security team to shift from manual troubleshooting to high-priority incident investigation. The team now conducts proactive threat hunting across all port sites.

Closed Integration Gaps

The new platform closed all ecosystem gaps via a comprehensive API and CrowdStrike integration. This established a single source of network truth. It provides seamless, high-value data feeds to the managed service provider application and existing internal security platforms.

Unified Port-to-Datacenter Control

For the first time, the organization gained a scalable and holistic security solution across its entire global maritime enterprise. By providing deep protocol analysis and the option for full packet capture, ExtraHop overcame the limitations of previous tools. This ensures the continuous protection of mission-critical port assets.

ABOUT EXTRAHOP

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response (NDR).

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance monitoring (NPM), intrusion detection (IDS), and packet forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit **extrahop.com** or follow us on **LinkedIn**.

EXTRAHOP®

info@extrahop.com
extrahop.com