EXTRAHOP

Transportation and Logistics: Protecting the Global Flow from Port to Last Mile

Keep Critical Transportation Networks and Supply Chains Free from Threats with ExtraHop RevealX™

Industry Challenges: Protecting the Global Flow from Port to Last Mile

Global transportation and logistics operate at the epicenter of commerce, where digital friction triggers a cascade of economic delays. By 2026, the industry will have evolved into a hyper-connected web of automated ports, autonomous fleets, and AI-driven sortation centers. While this transformation maximizes efficiency, it creates a massive attack surface where one compromised sensor can paralyze a national supply chain. Transportation and logistics leaders face several critical friction points:

- **The Escalation of Nation-State Sabotage and Kinetic Risk:** Geopolitically motivated adversaries have moved beyond data theft toward functional destruction of physical trade routes. These actors target the integrity of automated port cranes and railway signaling to create artificial bottlenecks. Protecting the global flow requires internal visibility to stop lateral movement before destructive commands can execute on critical transport controllers or navigation systems.
- **The Crisis of Interconnected 3PL and API Sprawl:** Modern logistics relies on thousands of API integrations between shippers, carriers, and third-party logistics providers. Attackers exploit these trusted connections as a backdoor to move from a partner environment into the core of a global logistics network. Using stolen credentials or hijacked service tokens, they can manipulate cargo manifests and reroute high-value shipments undetected by traditional perimeters.
- **The Visibility Gap in Automated Logistics Environments:** Distribution centers and shipping terminals run on thousands of unmanaged endpoints, including handheld scanners, smart telematics, and autonomous vehicles, that cannot host security agents. These agent blind spots allow attackers to move laterally while disabling traditional IT security tools. Organizations must have off-the-box visibility to detect anomalies directly on the wire before they escalate into systemic outages or safety incidents.
- **Regulatory Rigor and the Mandate for Rapid Disclosure:** 2026 mandates like CIRCIA and the EU NIS2 Directive have compressed the timeline for incident reporting. Transportation leaders must now disclose material incidents within 72 hours of determination. Meeting these standards requires an immutable source of truth that provides a definitive record of every network interaction, ensuring supply chain integrity while maintaining the precision required for last-mile delivery.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all network interactions by decrypting and decoding over 90 protocols at speeds up to 100 Gbps to protect high-velocity logistics hubs and automated distribution operations.

The Definitive Data Source for the AI-Enabled SOC

RevealX provides the high-fidelity wire data required to power next-generation logistics SOC automation. By delivering unalterable ground truth, RevealX eliminates investigative friction and accelerates the path from detection to remediation.

AI-Powered Cyber Threat Detection

Identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting critical transport services and supply chain systems using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers every asset, including unmanaged IoT devices like port cranes, telematics, and sortation robots, along with hybrid cloud workloads, without installing software or risking operational stability.

Strategic Line-Rate Decryption

Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats and unauthorized data staging without adding latency to time-sensitive transportation operations.

High-Fidelity Performance Metrics

Troubleshoots complex disruptions and verifies service level agreements using over 5,000 wire data metrics for deep operational insight into network latency and logistics application performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy audit requirements for CIRCIA and NIS2, accelerating root-cause analysis and incident reconstruction.

The Solution: RevealX Network Intelligence

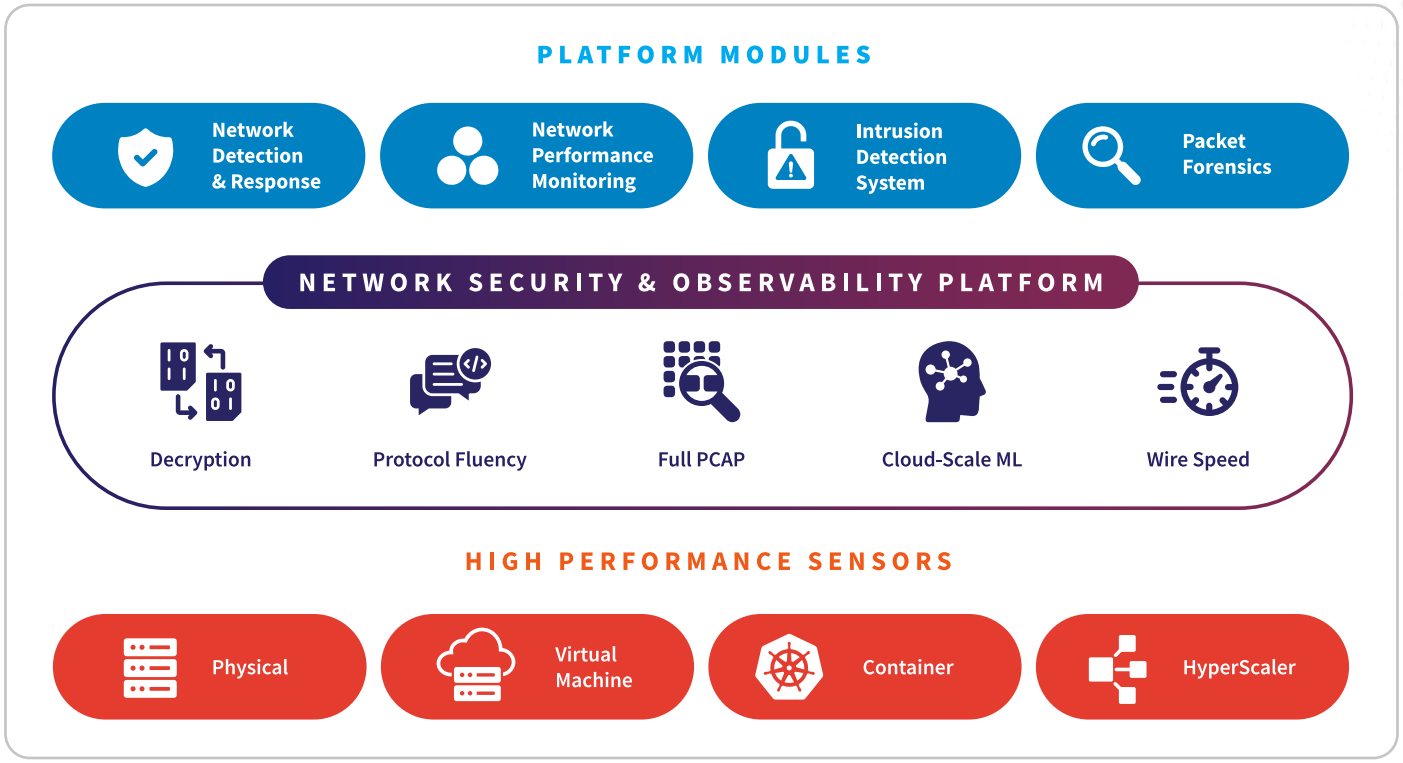
ExtraHop RevealX provides the unalterable ground truth required to secure the modern transportation and logistics ecosystem. By analyzing every packet at line rate, RevealX eliminates the visibility gaps that traditional security tools ignore. In a sector where a single minute of downtime results in systemic supply chain collapse, RevealX delivers the real-time insights needed to maintain operational uptime and national infrastructure stability.

The platform solves the agent blind spot by providing agentless, passive monitoring of over 90 protocols. This ensures that critical logistics assets like automated port cranes, warehouse robots, and fleet telematics are fully visible without risking system stability. By baselining normal behavior across these unmanaged IoT and OT devices, security teams can instantly detect anomalies that indicate an adversary has established a foothold on the warehouse floor or within a shipping terminal.

To counter geopolitically motivated sabotage, RevealX identifies subtle shifts in network behavior that signify lateral movement from corporate IT into the operational heart of the logistics network. By exposing hidden threats within encrypted traffic using strategic decryption, the platform stops attackers before they can manipulate cargo manifests or freeze automated fulfillment lines. This visibility extends to the sprawling 3PL and API ecosystem, where RevealX monitors the integrity of third-party integrations to prevent partner-borne contagion from reaching core transport systems.

Beyond threat detection, RevealX accelerates incident response to meet the compressed disclosure windows of 2026 mandates like CIRCIA and NIS2. It provides a definitive forensic record of all network transactions, eliminating the guesswork during investigations and allowing for rapid root-cause analysis. This unified approach bridges the gap between the SOC and the NOC by combining security detection with performance metrics. By monitoring the health of critical transaction paths, RevealX ensures that security measures do not introduce latency, protecting the precision of just-in-time logistics from port to last mile.

ExtraHop NDR Platform



NDR Technology Use Cases for the Transportation and Logistics Industry

Nation-State Attacks	Detects lateral movement and exfiltration in nation-state campaigns targeting global trade routes, port automation, and maritime navigation systems.
Threat Detection and Response	Investigates hidden threats across converged IT and OT environments, filling visibility gaps in automated warehouses and sortation centers where agents fail.
Threat Hunting	Leverages behavioral baselining to find signature-less threats and protocol anomalies before they impact JIT fulfillment, vessel safety, or fleet schedules.
SOC Modernization	Unifies SOC and NOC workflows with AI prioritization to reduce alert fatigue, accelerating response times for critical logistics and 3PL service delivery.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of DNP3, IEC 60870, and MQTT commands for one-click root-cause analysis of terminal outages.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots from corporate IT toward critical port controllers, railway signaling, and gantry crane SIS.
Cloud Workload Security	Provides agentless visibility for cloud-integrated transportation management systems (TMS), discovering shadow IT across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value dispatcher workstations and bridge navigation systems.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of manifests or total paralysis of last-mile delivery networks.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including handheld scanners, smart telematics, and autonomous vehicles that cannot host security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy terminal operating systems (TOS) and rail assets.
AI Security	Monitors generative AI and autonomous agents used for route optimization, predictive maintenance, or warehouse automation in containerized workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that IEC 62443 zone/conduit policies and Purdue Model segmentation are effective.

NPM Technology Use Cases for the Transportation and Logistics Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for automated sortation and port crane control sessions.
Operational Resilience	Resolves infrastructure degradation before it hits supply chain continuity, ensuring availability for mission-critical TMS and WMS services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between warehouse/terminal operations and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during WMS or ERP migration by auto-mapping dependencies and using OT baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for 3PL gateways and logistics supply chain APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past terminal outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into transaction processing time versus network latency in high-volume hubs.

Transportation and Logistics Industry Compliance & Regulatory Use Cases

Incident Disclosure	United States	CIRCIA	72-Hour Reporting: RevealX provides the immutable forensic record and "ground truth" evidence required to meet mandatory CISA reporting timelines for critical logistics.
Critical Infrastructure	European Union	NIS2 Directive	Network Continuity: Identifies unauthorized pivots and “living-off-the-land” attacks. RevealX satisfies mandates for continuous monitoring of maritime and rail networks.
Transport Security	United States	TSA Security Directives	Lateral Movement Detection: Supports rail and aviation compliance by monitoring OT segments. RevealX identifies unauthorized commands targeting signaling or safety systems.
Maritime Integrity	Global	IMO Cyber Risk (2021)	Shipboard Security: Audits IT/OT gateways to prevent data breaches from moving into navigation or propulsion systems. RevealX ensures port-to-ship communication integrity.
Supply Chain Risk	Global	ISO 28000	Vendor Access Auditing: Monitors 3PL and maintenance connections for unauthorized access to core logistics data. RevealX ensures JIT fulfillment and cargo manifests remain untampered.

Customer Benefits: Ensuring Supply Chain Resilience and Operational Continuity Across the Transportation and Logistics Network

ExtraHop RevealX delivers tangible business outcomes for transportation and logistics leaders by transforming network data into actionable intelligence. Organizations achieve immediate ROI through the consolidation of security and performance monitoring tools, which reduces operational overhead while improving cross-team collaboration between the SOC and NOC.

A primary benefit is the significant reduction in mean time to detect and respond to systemic threats. By providing unalterable ground truth across the entire supply chain, RevealX ensures that security teams can identify lateral movement before it impacts fulfillment or last-mile delivery. This proactive stance protects brand reputation and prevents the massive financial losses associated with port closures or warehouse standstills.

Furthermore, RevealX simplifies the complexity of 2026 regulatory compliance. The platform automates the data collection required for CIRCIA and NIS2 reporting, allowing organizations to meet 72-hour disclosure windows with confidence. By maintaining continuous visibility into unmanaged IoT and OT assets, logistics providers can prove the integrity of their digital perimeters to partners and insurers. Ultimately, RevealX secures the global flow of goods by ensuring that the digital infrastructure supporting the physical world remains resilient, visible, and under control.

> "With ExtraHop, we're not spending time looking for a needle in a haystack. That means we can spend more time on projects that are strategically valuable to the business. It's a win-win."
>
> **IT SECURITY MANAGER**
> American Transportation Manufacturer

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments in transportation and logistics: American Transportation Manufacturer

Or contact us to schedule your personalized demo and security assessment.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com