EXTRAHOP

CUSTOMER STORY

Retail Leader Secures Mission-Critical Operations and Streamlines Global Membership Services

A leading operator of membership warehouse clubs faced critical visibility gaps. The organization struggled to detect active ransomware. Manual data gathering processes were inefficient. These technical hurdles caused soaring labor costs and slow incident resolution. This threatened the global supply chain and millions of cardholders. To modernize its defense, the retailer deployed ExtraHop RevealX™ NDR. This implementation provided real-time monitoring and automated forensic analysis across the entire retail footprint.

The organization selected the ExtraHop RevealX platform to achieve strategic alignment between security and network operations, reaching the following outcomes:

- **Proactive threat detection:** The organization successfully deployed machine learning to identify ransomware, data staging, and exfiltration in real time, preventing potential disruptions to high-volume transaction flows.
- **Automated forensics and rapid insights:** The deployment eliminated manual post-incident data gathering, enabling security teams to reconstruct past network events and identify root causes in minutes rather than hours or days.
- **Operational efficiency and labor savings:** By automating data analysis, the retailer significantly reduced labor costs associated with manual troubleshooting and streamlined global infrastructure management.
- **Unified source of network truth:** The platform bridged cross-functional silos, providing a shared diagnostic environment that enhanced team coordination and established the network as the definitive source of truth.

The Challenge: Securing Global Membership Operations and Digital Growth

Operating international retail requires high-performance network reliability. The existing technical landscape presented several core challenges:

Lack of Real-Time Visibility

Prior to using ExtraHop, the organization lacked a centralized system for automated network data analysis. This created “blind spots” where active ransomware and data exfiltration could remain undetected until after an impact occurred.

Reactive and Costly Troubleshooting

The organization relied on manual, post-incident data gathering that slowed issue resolution. Without the ability to perform PCAP replay, engineers could not effectively reconstruct past network events, leading to extended mean time to resolution (MTTR) and increased operational overhead.

Fragmented Forensic Processes

Technical teams functioned in isolation due to siloed data sources. This lack of integration made it difficult to establish a single source of truth for global operations, particularly during high-traffic shopping periods where transaction stability is vital.

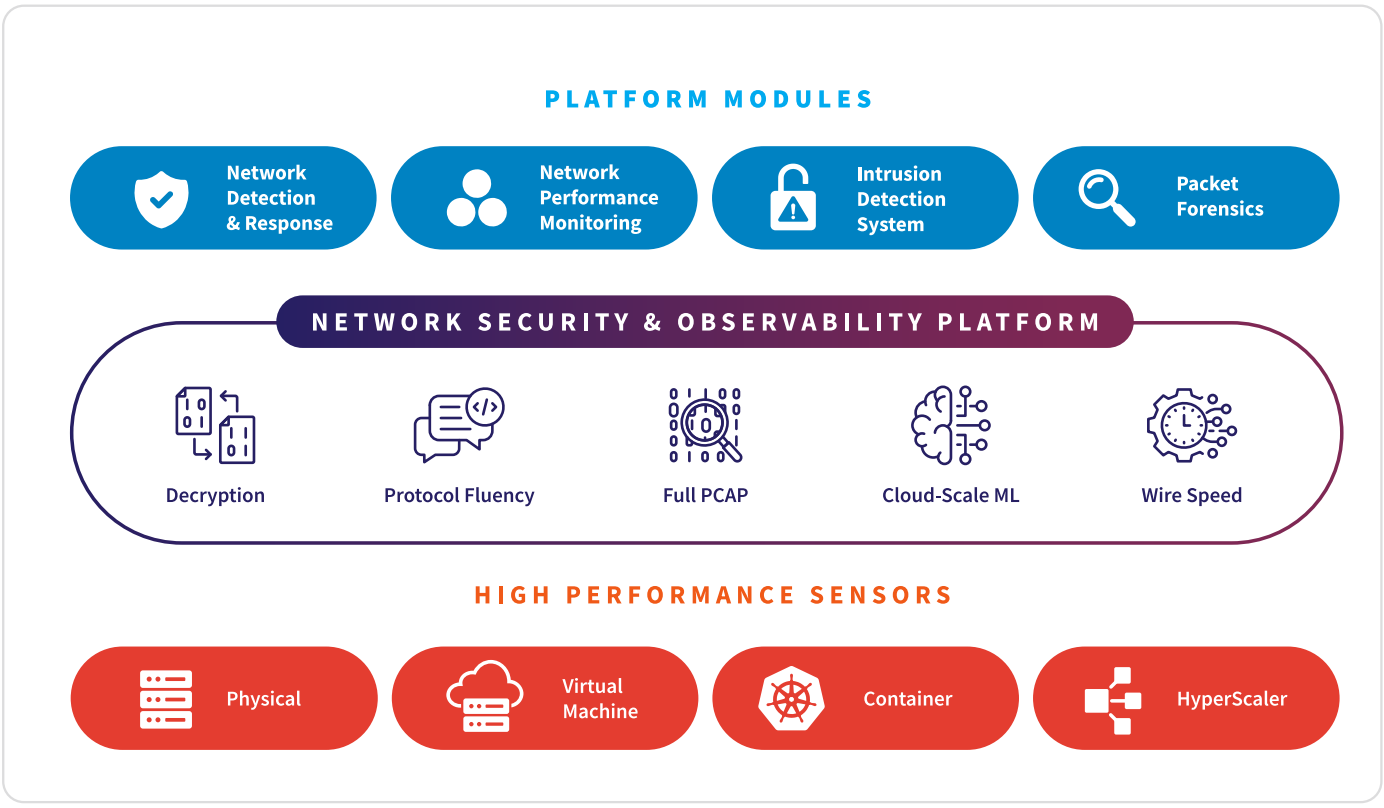
The Solution: Unified Detection with ExtraHop NDR

The successful deployment of ExtraHop enabled the retail leader to modernize its defensive and operational posture. The modern NDR platform provided the specialized inspection required to manage complex retail data protocols and high-speed traffic.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:** The retail leader secured the required forensic depth and network control when it deployed ExtraHop, which 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 reduced the SOC's operational burden by providing high-fidelity, low-noise detections. This shift allowed analysts to move their focus from low-value false positives to highly reliable network activity, signaling 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, which links malicious network activity directly to user and service accounts, finally enabling the detection of all missed AD and lateral movement attacks.
- **Streamlined incident response via ecosystem integration:** ExtraHop fundamentally simplified incident response workflows because it established itself as the definitive source of network truth, automatically feeding 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 into one unified, integrated solution for comprehensive network security and observability.
- **Deep protocol coverage for core assets:** The retail leader mitigated major risk by gaining deep fluency (parsing over 90 protocols) that 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. This was critical for detecting hidden AD attacks and lateral movement.

ExtraHop NDR Platform



The Results: Performance and Protection

The membership warehouse leader achieved immediate, transformative improvements in operational agility and threat defense following the deployment of the ExtraHop NDR platform.

Enhanced Ransomware Defense

The organization now possesses real-time ML threat detection capabilities that protect core retail infrastructure. This visibility ensures that ransomware and data-staging activities are neutralized before they can impact membership services.

Significant Labor Cost Reduction

By rationalizing the troubleshooting process, the organization realized a notable reduction in labor costs. The move from manual data collection to automated forensics has saved thousands of work hours and streamlined global operations.

Rapid Forensic Analysis

The platform delivers analysis and forensic results in minutes. The ability to reconstruct past network events via automated insights ensures that the security team can perform exhaustive root-cause analysis with unprecedented speed.

Global Operational Consistency

The retail leader successfully implemented the platform across its international sites. This rollout provided the first-ever unified view of the global membership network, ensuring consistent security and performance standards worldwide.

Continuous Critical Monitoring

The deployment successfully unified disparate technical teams. These groups now collaborate using a single source of network truth, allowing for proactive risk reduction and continuous monitoring of vital telemetry and applications.

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