EXTRAHOP

Protecting the Modern Retail Ecosystem and Scaling Global eCommerce with Confidence

Keep Critical Retail and eCommerce Applications and Processes Free From Threats and Disruption With ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: From Digital Friction to Operational Fragility

The retail sector's shift toward unified commerce has created a hyper-connected ecosystem where digital friction translates to immediate cart abandonment. In 2026, retail and ecommerce leaders face critical points of failure that threaten both brand reputation and financial solvency. As the digital shelf becomes the primary revenue engine, the attack surface has expanded into a complex web of APIs and third-party logistics.

- **The Escalation of Nation-State Sabotage:** Geopolitical actors moved from stealing data to erasing brand availability by paralyzing global supply chains. In early 2026, the Handala group targeted payment switches and 3PL providers to freeze just-in-time fulfillment. Countering these threats requires internal visibility to stop lateral movement before it triggers a collapse of inventory management systems or automated warehouse robotics.
- **The API and Headless Commerce Crisis:** Sophisticated attackers exploit the shift toward headless commerce by targeting order management APIs and loyalty wallets. Using AI-driven credential stuffing, they bypass traditional perimeters to stage mass fraudulent shipments and steal stored value. Retailers must detect this post-compromise behavior on the wire to prevent PII exfiltration before it enters the last-mile delivery network.
- **The Visibility Gap in Smart Retail Infrastructure:** Modern storefronts and distribution centers rely on unmanaged assets like POS controllers, handheld scanners, and autonomous picking robots that cannot support security agents. These agent blind spots allow attackers to pivot undetected across the retail edge. This gap violates PCI DSS 4.0.1 and NIS2 directives, jeopardizing the integrity of the physical-to-digital transaction path.
- **Regulatory Rigor and Conversion Integrity:** 2026 mandates require retailers to prove continuous monitoring across the cardholder data environment. Satisfying these standards during high-velocity events like Black Friday requires a unified SOC and NOC approach. Real-time visibility into the transaction path ensures resilience against systemic events without introducing the latency that drives cart abandonment and erodes customer lifetime value.

KEY CAPABILITIES

Depth and Breadth of NDR Performance: Monitors all network interactions by decrypting and decoding over 90+ protocols, including native support for HTTP/S, SQL, and API traffic, at speeds up to 100 Gbps.

The Definitive Data Source for the AI-Enabled SOC: RevealX powers unified commerce SOC automation with unalterable network data, eliminating investigative friction during seasonal peak volumes to accelerate detection and remediation.

AI-Powered Cyber Threat Detection: RevealX NDR utilizes machine learning and behavioral baselining to detect sophisticated attacks, lateral movement, and ransomware targeting critical business services and applications.

Unified Agentless Visibility: Automatically discovers every asset, from BOPIS kiosks to autonomous warehouse robotics and cloud workloads, without installing software.

Strategic Line-Rate Decryption: Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats in payment integrations and APIs without adding latency.

High-Fidelity Performance Metrics: Troubleshoots complex disruptions using over 5,000 wire data metrics for deep insight into storefronts and inventory systems.

Continuous Forensic Capture: RevealX maintains unalterable PCI DSS 4.0 and CCPA audit trails, accelerating root-cause analysis for transaction integrity.

The Solution: RevealX Network Intelligence

ExtraHop RevealX delivers the network intelligence needed to protect customer PII and ensure commerce continuity. By providing a unified view of hybrid environments, RevealX helps security teams detect sophisticated threats while ensuring service availability. Real-time transaction path visibility is a requirement for operational resilience, where downtime costs millions. This ground truth is essential as digital innovation must outpace sophisticated adversaries.

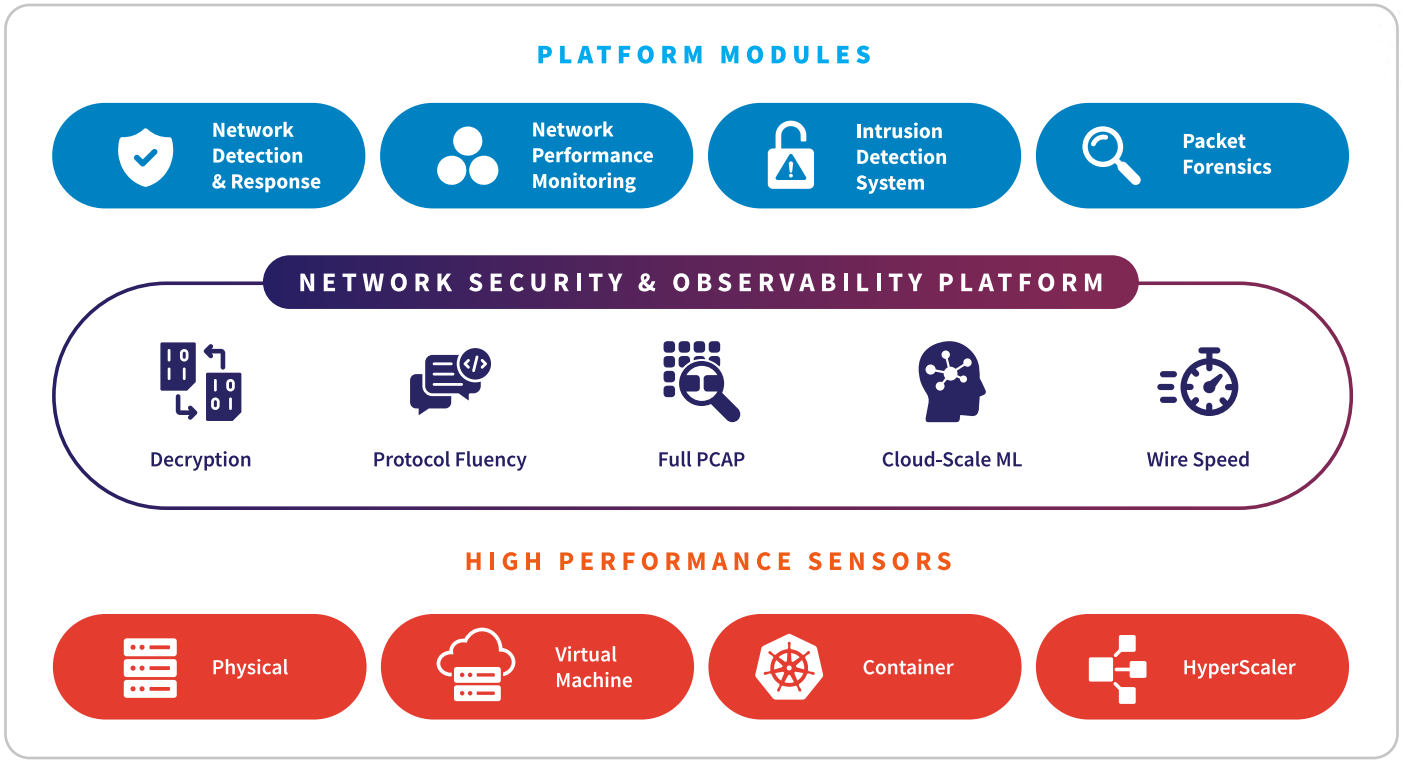
Neutralizing nation-state campaigns requires stopping actors before they execute commands. By monitoring wire data instead of vulnerable agents, RevealX identifies lateral movement and credential abuse used for ransomware or skimming. This agentless approach ensures that if a logistics provider or edge gateway is compromised, the platform identifies anomalies in real time. Teams can then isolate segments, preserving fulfillment centers and protecting assets from disruption.

Meeting retail regulations requires complete visibility. A real-time view across on-premises, hybrid cloud, and edge-powered stores allows teams to stay ahead of outages. Because logs can be modified, the network provides the only immutable source of truth. RevealX decrypts and decodes 90+ protocols at 100 Gbps, providing persistent visibility across unmanaged POS terminals and warehouse robotics where security agents cannot be installed.

ExtraHop uses machine learning to identify attacks that evade signature tools. By establishing behavioral baselines, the AI identifies living-off-the-land tactics targeting headless commerce APIs. Line-rate decryption of TLS 1.3 prevents attackers from hiding lateral movement within encrypted payment integrations. This provides the independent observation required for Zero Trust while maintaining the fast checkout speeds expected in modern retail.

Integrating NDR and NPM eliminates silos, allowing teams to troubleshoot storefront latency or ransomware before exfiltration. This unified approach allows retailers to enforce segmentation and manage compliance with PCI DSS 4.0, CCPA, and the Digital Services Act. Wire data provides the proof to validate security controls and ensure revenue streams remain uninterrupted. RevealX deconstructs IT complexity without tool sprawl friction.

ExtraHop NDR Platform



NDR Technology Use Cases for the Retail/eCommerce Institutions

Nation-State Attacks	Provides deep visibility into lateral movement and data exfiltration, enabling the detection of subtle, long-term campaigns targeting global supply chains, JIT logistics, and cross-border payment settlements.
Threat Detection & Response	Enables proactive investigation into hidden threats across hybrid environments to find what logs and agents miss within omnichannel payment ecosystems, headless commerce engines, and third-party API integrations.
Threat Hunting	Uncovers stealthy, signature-less threats by leveraging behavioral baselines to find anomalies that evade automated alerts before they impact seasonal peak volumes, BFCM flash sales, or automated fulfillment centers.
SOC Modernization	Unifies SOC and NOC workflows to eliminate data silos. It uses AI-powered prioritization to improve operational efficiency for unified commerce orchestration and high-frequency SKU inventory updates.
Incident Response & Investigation	Provides forensic-level visibility and "one-click" investigations to determine the root cause of an incident. It offers an unalterable record of all network transactions for PCI audit trails, protecting sensitive customer PII and order history.
Lateral Movement	Detects attackers moving internally using peer-group clustering and protocol decoding to catch pivots that bypass perimeter security toward PCI-DSS scoped segments, order management systems (OMS), or warehouse management systems (WMS).
Cloud Workload Security	Delivers agentless, full-spectrum visibility to defend critical shopping cart services and serverless checkout functions while discovering unmanaged assets across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask Account Takeover (ATO) and loyalty point draining in real time, providing deep visibility into identity-based threats targeting digital wallets.
Ransomware Attacks	Identifies early-stage ransomware activity, such as file staging and encryption patterns. This provides the visibility needed to isolate infected hosts before the exfiltration of nonpublic consumer information or JIT supply chain disruption occurs.
Unmanaged Devices	Fills the visibility gap for unmanaged retail devices like BOPIS kiosks, handheld scanners, smart shelving, and point-of-sale (POS) terminals by monitoring their network traffic directly.
EDR Evasion Detection	ExtraHop's out-of-band monitoring identifies malicious activity even if endpoint agents are disabled. This ensures persistent visibility across embedded POS systems and automated distribution center hardware where agents cannot be installed.
AI Security	Monitors interactions with generative AI platforms and autonomous logistics agents that might be used for dynamic pricing engines or automated customer support bots within containerized cloud workloads.
Operationalizing Zero Trust	Acts as the independent observer in the Zero Trust Architecture loop. It detects policy drift and provides empirical proof that PCI DSS 4.0 segmentation and guest Wi-Fi isolation are effective.

NPM Technology Use Cases for the Retail/eCommerce Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot complex disruptions. It provides clear visibility into latency and throughput to prevent shopping cart abandonment on high-volume storefronts.
Operational Resilience	Reduces disruption impact by resolving infrastructure degradation before it hits retail continuity. It ensures availability through proactive service-level monitoring during flash sales and promotional events.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow from metrics to packets, eliminating friction between network teams and ecommerce application developers.
Migrate Workloads to the Cloud	Maintains performance during core retail migration by auto-mapping dependencies and assets, using on-premises baselines to validate successful cloud delivery of SaaS-based storefronts.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes environments. This ensures performance for critical business services like real-time API inventory lookups.
Forensic-Grade Investigations	Combines long-term metadata with scalable PCAP for an unalterable record of events, enabling deep-dive analysis into past checkout outages or intermittent last-mile logistics degradations.
Application Performance Monitoring	Complements APM by filling network-layer visibility gaps, decoding 90+ protocols to provide real-time insights into database response times for product searches versus network latency.

Retail/eCommerce Industry Compliance & Regulatory Use Cases

Continuous Compliance Monitoring	Global	PCI DSS 4.0	Enables continuous CDE monitoring to detect unauthorized payment script changes (Requirement 6.4.3) or exposed Primary Account Numbers (PAN).
Data Privacy & Governance	EU, UK, USA (CA), Brazil	GDPR, CCPA, LGPD	Maps sensitive personal information (SPI) across headless commerce APIs to prevent loyalty PII leaks into advertising trackers.
Supply Chain & Third-Party Risk	EU / Germany	NIS2, Supply Chain Act	Monitors 3PL and SaaS payment providers to identify vendor anomalies and prevent systemic logistics paralysis.
Audit Readiness & Incident Forensics	China / EU / USA	PIPL, GDPR, CCPA	Supports 72-hour regulatory windows and Magecart event reconstruction to prove due diligence and avoid turnover-based fines.
Security Control Validation	Global / USA	PCI DSS 4.0, CCPA	Validates internal segmentation, such as isolating guest Wi-Fi from POS networks, and ensures MFA is active across payment environments.
Marketplace Transparency & Safety	EU	Digital Services Act (DSA)	Ensures trader traceability for platform transparency and monitors third-party seller interactions to protect data integrity.
Critical Infrastructure Protection	China	MLPS 2.0	Tracks unauthorized cross-border data transfers to meet Grade 3 "proactive defense" and continuous monitoring requirements.

Customer Benefits: Safeguarding Brand Trust and Operational Velocity Across the Omnichannel Landscape

ExtraHop RevealX delivers the network intelligence needed to protect brand trust and operational velocity across omnichannel environments. Using cloud-scale machine learning and line-rate TLS 1.3 decryption, RevealX detects anomalies like Magecart-style skimming and credential stuffing that evade traditional tools. By monitoring the wire, retailers protect customer PII and loyalty programs during peak volumes, preserving long-term customer value.

The shift to headless commerce and hybrid clouds creates blind spots in the transaction path. RevealX secures these architectures and legacy storefronts by observing actual traffic flows instead of modifiable logs. This provides the definitive forensic evidence required for PCI DSS 4.0, GDPR, and DSA audits without compromising sub-second checkout speeds.

RevealX also secures unmanaged devices from BOPIS kiosks to warehouse robotics that agent-based security cannot reach. It identifies lateral movement and account takeovers before they trigger supply chain disruptions. With continuous discovery of every network entity, RevealX helps retailers operationalize Zero Trust and resolve storefront latency, ensuring high-value revenue streams and consumer trust remain uninterrupted.

> "Visibility at our remote locations provides insight that is critical to delivering a seamless and secure experience for our customers and associates. ExtraHop allows for a much deeper understanding and more accurate representation of what's happening at every store."
>
> **DAVID NARAYAN**
> Distinguished Engineer
> Home Depot

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 retail and ecommerce:
Home Depot
Ulta Beauty

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