EXTRAHOP

# Secure and Accelerate Healthcare Experiences

Keep critical applications and processes free from threats and disruption with ExtraHop RevealX™


## Industry Challenges: From Data Security to Patient Safety

Healthcare Delivery Organizations (HDOs) operate where digital downtime translates directly to patient risk. By 2026, the hospital perimeter has dissolved into a hyper-connected ecosystem of telemedicine, cloud-integrated EHRs, and surging IoMT. This evolution makes cybersecurity a core component of clinical reliability. As digital and physical worlds merge, HDOs face several critical friction points:

- **The Escalation of Nation-State and Destructive Attacks:** Geopolitically motivated actors have shifted from data theft to functional destruction. A 2026 attack on a global medical device company saw threat actors exploit endpoint management to wipe hundreds of thousands of devices. By striking trusted vendors, these actors disrupt surgical logistics and clinical continuity. Protecting patient lives now requires absolute internal visibility to contain east-west movement before destructive commands execute.
- **The Identity and Lateral Movement Crisis:** The adoption of FHIR and HL7 interoperability standards has expanded the attack surface for cloud-integrated EHRs. Modern actors prioritize the long-term theft of PHI using "living off the land" tactics to subvert IAM/PAM controls and blend with legitimate behavior. By using stolen credentials to move laterally, they navigate undetected to clinical databases. HDOs must detect this post-compromise activity on the wire before exfiltration begins.
- **The Visibility and EDR Evasion Gap:** Millions of life-critical IoMT assets, such as infusion pumps, cannot host security agents. This agent blind spot leaves DICOM imaging and PACS traffic invisible to traditional tools. Furthermore, sophisticated attackers now prioritize disabling EDR agents immediately after gaining a foothold. This creates hurdles for HIPAA, HITECH, and FDA 524B frameworks, which mandate strict auditing of patient data access.
- **Operational and Regulatory Convergence:** 2026 mandates make technical safeguards non-negotiable, yet IT teams face record tool fatigue. Fragmented tools often lead to silos between security and network teams during outages. To maintain 100% uptime, HDOs must unify SOC and NOC workflows within a Zero Trust Architecture. This requires clinical-grade segmentation to isolate medical devices and robust DLP to protect the patient journey from on-premises data centers to the cloud.

## KEY CAPABILITIES

**Depth and Breadth of NDR Performance**
Monitors all network interactions by decrypting and decoding over 90+ protocols, including native support for HL7, FHIR, and DICOM, at speeds up to 100 Gbps.

**The Definitive Data Source for the AI-Enabled SOC** RevealX powers healthcare SOC automation with unalterable network data, eliminating investigative friction 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 applications.

**Unified Agentless Visibility**
Automatically discover every asset, including unmanaged medical devices and cloud workloads, without installing software.

**Strategic Line-Rate Decryption**
Analyze modern encrypted traffic, including TLS 1.3, Kerberos, NTLM, SMB3, and MSRPC to expose hidden threats without adding latency.

**High-Fidelity Performance Metrics**
Troubleshoot complex disruptions using over 5,000 wire data metrics for deep clinical and operational insight.

**Continuous Forensic Capture**
RevealX maintains unalterable HIPAA and HITECH audit trails, accelerating root-cause analysis for patient safety.

## The Solution: RevealX Network Intelligence

ExtraHop RevealX provides the network intelligence required to secure patient data, maintain patient safety, and help ensure clinical continuity. By delivering a unified view of the hybrid environment, RevealX enables security and network teams to detect sophisticated threats and ensure service availability.

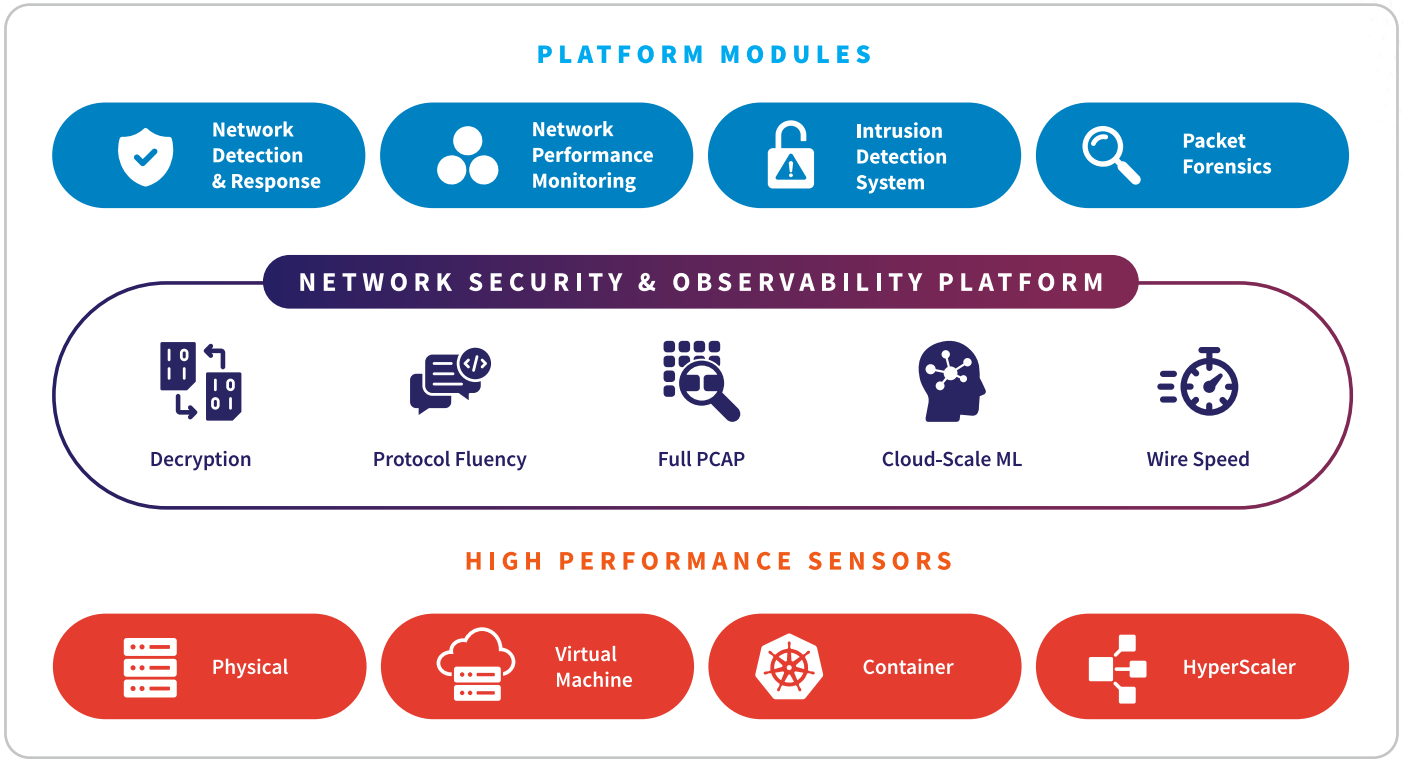
Neutralizing destructive nation-state threats requires intercepting actors before they can execute malicious commands. By monitoring the wire instead of vulnerable agents, RevealX detects the lateral movement and credential abuse used to deploy wiper malware. This agentless approach identifies the anomalous behavior in real time, even if medical devices are compromised. Clinical teams can quickly isolate affected segments to preserve clinical continuity and protect patient lives from large-scale disruption.

Securing workloads across the edge, core, and cloud requires RevealX to monitor all network interactions by decrypting and decoding over 90+ protocols, including native support for HL7, FHIR, and DICOM, at speeds up to 100 Gbps. This delivers complete visibility and intelligent response. Because RevealX utilizes out-of-band monitoring, it remains a persistent source of truth even when attackers disable or evade EDR agents. This strategy is essential for securing unmanaged IoMT devices and legacy PACS systems that cannot host traditional security software.

As a leader in AI-driven NDR, ExtraHop utilizes cloud-scale machine learning to identify sophisticated attacks that evade signature-based tools. By establishing baseline behavior for every device and user, our AI identifies "living off the land" tactics. A key differentiator is the ability to perform line-rate decryption of TLS 1.3, ensuring attackers cannot hide lateral movement or IAM/PAM credential abuse within encrypted clinical traffic. This allows RevealX to provide the independent observation required for a Zero Trust Architecture.

By integrating NDR and NPM, RevealX helps to eliminate the silos between SOC and NOC workflows. Teams can troubleshoot issues ranging from EHR latency to active ransomware staging before PHI exfiltration occurs. This unified approach allows HDOs to enforce clinical Segmentation policies and manage a robust Vulnerability Disclosure Program (VDP) for connected medical devices. With high-fidelity wire data, organizations can ensure compliance with 2026 HIPAA and HITECH updates.

### ExtraHop NDR Platform



## NDR Technology Use Cases for Healthcare & Life Sciences

| | |
|---|---|
| Nation-State Attacks | Provides deep visibility into lateral movement and data exfiltration, enabling the detection of subtle, long-term nation-state campaigns that target healthcare. |
| Threat Detection & Response | Enables proactive investigation into hidden threats across hybrid environments using intuitive, query-based workflows and over 5,000 wire data metrics to find what logs and agents miss with the EHR ecosystem. |
| Threat Hunting | Uncovers stealthy, signature-less threats and persistent actors by leveraging behavioral baselines and historical metadata to find anomalies that evade automated alerts before they can impact patient care. |
| SOC Modernization | Unifies SOC and NOC workflows to eliminate data silos. It uses AI-powered prioritization to reduce alert fatigue, accelerating response times and improving overall operational efficiency for healthcare delivery. |
| 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, including access to sensitive PHI. |
| Lateral Movement | Detects attackers as they move internally by utilizing peer-group clustering and protocol decoding (SMB, RDP, etc.) to catch pivots that bypass perimeter security. It catches pivots toward PACS or clinical databases that bypass perimeter security. |
| Cloud Workload Security | Delivers agentless, full-spectrum visibility to defend critical cloud-integrated EHR workloads and discover "shadow IT" or unmanaged assets across AWS, Azure, and Google Cloud. |
| Identity-Based Attacks | Correlates network behavior with Identity and Access Management (IAM) to unmask credential abuse, token theft, and privilege escalation in real time, providing deep visibility into identity-based threats. |
| 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 PHI occurs. |
| Unmanaged Devices | Fills the visibility gap for unmanaged healthcare devices like CT scanners and centrifuges by monitoring their network traffic directly, since these specialized systems may not support EDR agents. |
| EDR Evasion Detection | ExtraHop's out-of-band monitoring identifies malicious activity even if endpoint agents are disabled. This ensures persistent visibility across IoMT devices and other hardware where agents cannot be installed. |
| AI Security | AI security includes AI workloads and other containerized cloud workloads. This use case monitors interactions with generative AI platforms and autonomous agents that might be used for Clinical Decision Support. |
| Operationalizing Zero Trust | Acts as the independent observer in the Zero Trust Architecture loop. It detects policy drift and provides empirical proof that clinical Segmentation policies are effective. |

## NPM Technology Use Cases for Healthcare & Life Sciences

| | |
|---|---|
| Performance Monitoring | Uses high-fidelity telemetry to troubleshoot complex disruptions. It provides clear visibility into latency and throughput for telemedicine and remote care sessions. |
| Operational Resilience | Reduces disruption impact by resolving infrastructure degradation before it hits clinical continuity. It ensures availability through proactive service-level monitoring. |
| Troubleshooting & Resolution | Accelerates root-cause analysis via a 3-click workflow from metrics to packets, eliminating friction between network and clinical application teams. |
| Migrate Workloads to the Cloud | Maintains performance during EHR migration by auto-mapping dependencies and assets, using on-premises baselines to validate successful cloud delivery. |
| Monitor Critical Workloads | Provides deep L2-L7 visibility into high-value apps and Kubernetes environments. This ensures performance for crown-jewel services like HL7 gateways and FHIR APIs. |
| Forensic-Grade Investigations | Combines long-term metadata with scalable PCAP for an unalterable record of events, enabling deep-dive analysis into past outages or intermittent degradations. |
| Application Performance Monitoring | Complements APM by filling network-layer visibility gaps, decoding 100+ protocols, including DICOM, to provide real-time insights into response and processing time versus latency. |

## Healthcare & Life Sciences Compliance & Regulatory Use Cases

| | | | |
|---|---|---|---|
| Healthcare | United States | HIPAA / HITECH | 2026 HIPAA Security Rule Update. These acts protect patient privacy (ePHI). NDR assists by auditing all database access, and logging the who, what, and where data of interactions to provide the forensic documentation required for compliance audits. |
| Medical Devices | United States | FDA 524B | This regulation focuses on the cybersecurity of medical devices (IoMT). NDR profiles device behavior to find anomalies and identifies vulnerabilities in connected equipment before they can impact patient safety. |
| Healthcare | United States | CIRCIA | Starting in 2026, healthcare organizations must report substantial cyber incidents to CISA within 72 hours and any ransomware payments within 24 hours. |
| Pharmaceuticals | United States / Global | GxP / 21 CFR 11 | These regulations ensure data integrity in drug manufacturing. NDR provides audit trails for access to lab and batch records, preventing “cyber-tampering” that could lead to dangerous product recalls. |

## Customer Benefits: Achieving Strategic Healthcare Goals

With unified network intelligence, AI-powered threat detection, and streamlined workflows, ExtraHop RevealX enables security and IT teams to investigate incidents and troubleshoot performance issues across complex healthcare environments. RevealX utilizes cloud-scale machine learning and line-rate TLS 1.3 decryption to detect anomalous network, application, and IoMT activity that evades tools relying on static signatures.

Healthcare organizations use RevealX to safeguard EHR systems and PHI while significantly reducing the risk of ransomware. According to recent 2025 and 2026 industry benchmarks, this unified approach can reduce unplanned downtime by up to 86% and accelerate threat resolution by 87%. These efficiencies ensure continuous compliance with mandates, including the HIPAA Security Rule, HITECH requirements, and HITRUST frameworks.

Whether on-premises or in the cloud, RevealX reduces operational friction by consolidating NDR and NPM into a single source of truth. It provides the empirical data needed to operationalize a Zero Trust Architecture and validate internal Segmentation policies. Forensic-level data and associated packets are just a click away. This allows healthcare teams to resolve disruptions in HL7 or PACS data flows and close security gaps with unprecedented speed.

> "Without ExtraHop, the investigation would have taken days or weeks, exposing the hospital to potentially catastrophic risk. Even the FBI was impressed when they found out how quickly we identified and contained the threat."

**JOANNE WHITE**
CIO, Wood County Hospital

## 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 healthcare:
Prisma Health
Seattle Children's Hospital
Leading U.S. Healthcare Insurance Provider
Wood County Hospital
Hill Physicians

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**