EXTRAHOP

Strengthening Operational Resilience and Protecting Innovation in the Medical Device Industry

Keep Critical Medical Device Applications and Processes Free From Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: From Life-Critical Design to Systemic Vulnerability

The medical device industry drives healthcare innovation through the Internet of Medical Things (IoMT). As devices move to hyper-connected cloud platforms, they have become prime targets for systemic disruption. Medical device manufacturers share high-stakes challenges with hospitals and pharmaceutical firms, including destructive ransomware and intellectual property theft. In 2026, cybersecurity is a core component of clinical reliability and patient safety. As digital and physical medical technology merge, institutions face several critical friction points:

- **The Escalation of Nation-State Sabotage and IP Theft:** Geopolitically motivated actors have moved beyond data theft to the paralysis of healthcare supply chains and the theft of R&D. In early 2026, campaigns targeted medical device firms to exfiltrate surgical robotics designs and manipulate clinical trial data. Adversaries target the device lifecycle, from engineering to the production floor. Protecting these assets requires absolute internal visibility to contain lateral movement before sensitive IP is exfiltrated.
- **The Crisis of IoMT Proliferation and the Agent Blind Spot:** Modern medical technology relies on wearables, legacy diagnostic imaging, and autonomous AI monitors. These devices represent a massive visibility gap because they cannot host traditional security agents and rely on unmanaged API connections. This agent blind spot is a primary target for ransomware groups who exploit firmware vulnerabilities to move laterally toward sensitive patient records or clinical databases.
- **The Convergence of Cybersecurity and Patient Safety:** In 2026, digital downtime translates directly to clinical risk. Security failures in medical devices can force hospital diversions or the postponement of life-critical procedures. Securing these environments requires real-time detection that identifies anomalous behavior within the digital transaction path without introducing latency or impacting device performance.
- **Regulatory Rigor and the Mandate for Lifecycle Resilience:** 2026 mandates have shifted the focus from data privacy to mandatory lifecycle resilience. Section 524B of the FD&C Act and the EU Medical Device Regulation (MDR) require manufacturers to prove continuous vulnerability monitoring and maintain a complete software bill of materials (SBOM). Meeting these standards requires a definitive source of truth that provides verifiable proof of security throughout the product lifecycle.

KEY CAPABILITIES

Depth and Breadth of NDR Performance: Decrypts and decodes 90+ protocols at 100 Gbps to protect proprietary device designs and high-precision manufacturing operations.

The Definitive Data Source for the AI-Enabled SOC: Powers SOC automation with unalterable network data, accelerating detection and remediation across clinical and production environments.

AI-Powered Cyber Threat Detection: Uses ML to detect lateral movement and ransomware targeting device firmware, surgical robotics, and patient PHI.

Unified Agentless Visibility: Automatically discovers all assets, including unmanaged IoMT and legacy imaging, without software or impacting device performance.

Strategic Line-Rate Decryption: Analyzes TLS 1.3 traffic to expose threats without adding latency to time-critical cloud telemetry or medical APIs.

High-Fidelity Performance Metrics: Uses 5,000+ metrics to troubleshoot disruptions, ensuring the availability and reliability of critical manufacturing and clinical operations.

Continuous Forensic Capture: Maintains unalterable audit trails for FDA 524B and EU MDR, providing the independent record needed for device integrity and patient safety.

The Solution: RevealX Network Intelligence

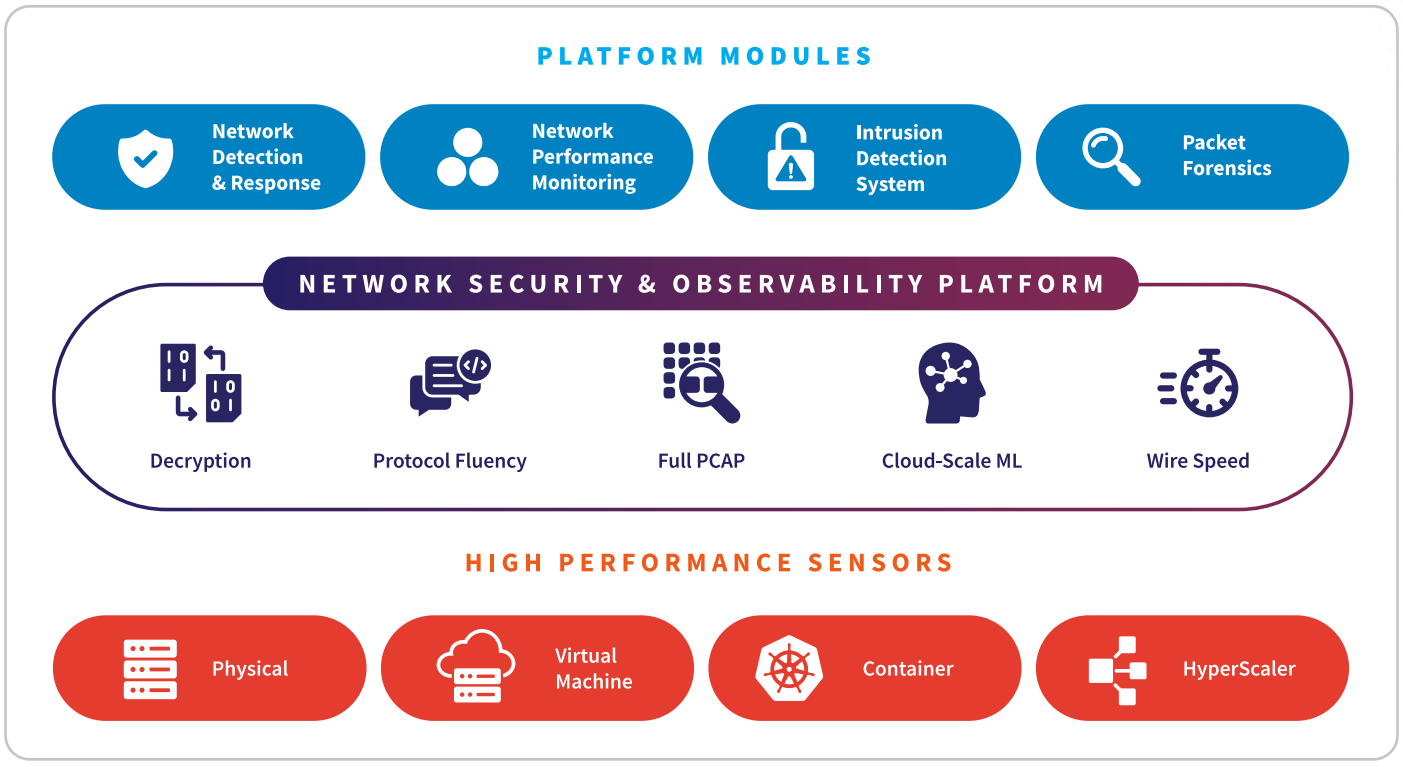
ExtraHop RevealX provides the unalterable ground truth required to secure the global medical device lifecycle. By analyzing every packet at line rates up to 100 Gbps, RevealX eliminates visibility gaps in cloud-integrated device management and high-precision manufacturing. In an industry where security failures lead to patient harm or multi-billion dollar R&D losses, RevealX maintains operational continuity. The platform turns the network into a definitive record of truth, allowing security teams to see everything across their infrastructure without intrusive agents.

RevealX solves the agent blind spot by providing agentless, passive monitoring of over 90 protocols. Critical infrastructure, from autonomous surgical robots and infusion pumps to legacy imaging systems, is fully visible without risking system stability or clinical safety. By baselining normal behavior, security teams can instantly detect anomalies indicating an adversary is manipulating telemetry or establishing a foothold in the engineering pipeline. This visibility is essential for identifying "living off the land" tactics that blend with legitimate clinical traffic.

To counter nation-state sabotage and IP theft, RevealX identifies subtle shifts in network behavior signifying the staging of design data for exfiltration. By exposing threats within encrypted management traffic via strategic decryption, the platform stops attackers before they pivot from office zones into restricted engineering or clinical segments. This extends to the broader supply chain, monitoring connections to third-party diagnostic services and cloud-integrated monitors to prevent contagion. Line-rate inspection of TLS 1.3 ensures attackers cannot hide malicious payloads within device-to-cloud streams.

Beyond detection, RevealX accelerates incident response to meet the rigorous reporting requirements of FDA 524B, EU MDR, and NIS2. It provides a definitive forensic record of all network transactions, eliminating guesswork and allowing rapid root-cause analysis of security breaches and performance drops. This unified approach bridges the gap between SOC and clinical engineering teams, combining security detection with deep performance metrics. By monitoring critical transaction paths, RevealX ensures security measures do not introduce latency, protecting the speed and reliability of modern patient care.

ExtraHop NDR Platform



NDR Technology Use Cases for the Medical Device Industry

Nation-State Attacks	Detects lateral movement and exfiltration in campaigns targeting proprietary device firmware, surgical robotics designs, and clinical trial results.
Threat Detection & Response	Proactively investigates hidden threats across hybrid environments to find what logs miss in engineering platforms and device management systems.
Threat Hunting	Uncovers stealthy threats using behavioral baselines to stop anomalies before they impact clinical reliability or device integrity.
SOC Modernization	Unifies SOC and clinical engineering workflows and uses AI prioritization to accelerate response times for global device production and maintenance.
Incident Response & Investigation	Provides forensic visibility and maintains unalterable records of medical protocol transactions (DICOM, HL7) for rapid root-cause analysis of device failures.
Lateral Movement	Identifies internal pivots via peer group clustering to catch movement toward restricted engineering zones, firmware update servers, or patient data segments.
Cloud Workload Security	Delivers agentless visibility to defend cloud-integrated device telemetry platforms and discover shadow IT across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates behavior with IAM to unmask credential abuse in real time, protecting high-value developer, clinician, and system administrator accounts.
Ransomware Attacks	Identifies early-stage ransomware patterns to isolate hosts before exfiltration of IP or the disruption of life-critical device availability.
Unmanaged Devices	Monitors traffic directly to fill the visibility gap for unmanaged IoMT and robotic controllers where traditional security agents cannot be installed.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity even if agents are disabled, ensuring visibility across legacy diagnostic and manufacturing workstations.
AI Security	Monitors generative AI and autonomous agents used for clinical decision support or device design to prevent data leaks and unauthorized manipulation.
Operationalizing Zero Trust	Acts as an independent observer to detect policy drift and validate internal segmentation between clinical device zones and corporate office networks.

NPM Technology Use Cases for the Medical Device Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions. Provides visibility into latency and throughput for remote patient monitoring and telemedicine platforms.
Operational Resilience	Resolves infrastructure degradation before it hits clinical continuity. Ensures availability for mission-critical device APIs and production monitoring services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between IT teams and Clinical Engineering during device or application outages.
Migrate Workloads to the Cloud	Maintains performance during core system migration by auto-mapping dependencies and using baselines to validate successful cloud delivery for PACS or EHR.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps. Ensures performance for crown jewel services like surgical robotics telemetry and patient intake portals.
Forensic-Grade Investigations	Combines metadata with scalable PCAP for an unalterable record, enabling deep-dive analysis into past clinical service outages or device telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols. Provides real-time insights into database response times versus network latency for medical imaging systems.

Medical Device Industry Compliance & Regulatory Use Cases

Lifecycle Resilience	US	FDA 524B	Postmarket Monitoring: Satisfies mandates by providing continuous behavioral monitoring and audit trails required for mandatory postmarket pre-submissions.
Product Safety	EU	EU MDR	Clinical Investigation: Delivers forensic evidence and transaction records needed to prove device safety and cybersecurity throughout the operational lifecycle.
Critical Infrastructure	EU	NIS2 Directive	Essential Service Security: Validates the security of device manufacturing and supply chains. Provides forensic evidence required for mandatory incident disclosure.
Data Protection	Global	HIPAA / GDPR	PHI/NPI Safeguarding: Speeds up notification by attributing data access paths. Provides forensic proof of breach scope to protect patient data and minimize fines.
Quality Management	Global	ISO 13485	Control Verification: Provides technical proof of continuous monitoring for unauthorized activity, ensuring the integrity of device quality management records.
Intellectual Property Audit	Global	WIPO Standards	IP Protection: Validates the security of proprietary device designs by maintaining a persistent record of all data transfers involving patent-pending technology.

Customer Benefits: Safeguarding Clinical Innovation and Patient Safety

ExtraHop RevealX counters nation-state sabotage by containing lateral movement before actors can manipulate clinical data or steal proprietary designs. By monitoring wire data instead of vulnerable agents, the platform identifies subtle indicators of compromise that precede intellectual property theft. This proactive defense ensures that core research algorithms and high-precision production lines remain intact.

To mitigate ransomware and IoMT risks, RevealX establishes behavioral baselines to flag anomalies bypassing traditional perimeters. Real-time detection of unusual interactions with diagnostic systems or telemetry prevents unauthorized firmware changes, ensuring life-critical devices remain available for patient care.

RevealX eliminates visibility gaps in legacy hardware and modern cloud platforms by automatically discovering assets without intrusive agents. This provides oversight of specialized workstations and unmanaged edge devices invisible to standard defenses.

Meeting FDA 524B and EU MDR demands becomes a streamlined process through continuous monitoring and unalterable forensic recording. RevealX provides empirical proof of security maturity to satisfy global authorities and maintain market access. Ultimately, these capabilities transform cybersecurity into a strategic asset, protecting brand reputation and clinical reliability in a life-critical market.

> "ExtraHop RevealX is a critical tool to help us protect data in transit and at rest. We have to see and understand how data is moving from point to point so we can quickly identify unusual or problematic patterns."
>
> **GARY GOODEN**
> CISO, Seattle Children's 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 medical devices:
Seattle Children's Hospital

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