EXTRAHOP

CUSTOMER STORY

Leading US Healthcare Insurance Provider

Health Insurer Ends Upgrade Instability and Reduces SOC Costs

A leading global health insurance provider faced significant operational and security risks due to the instability of its incumbent network detection and response (NDR) platform. The organization relied on a legacy NDR tool originally marketed to them as a network traffic analysis tool to monitor its complex enterprise network, but recurring software updates caused the system to lose all custom tuning rules every quarter. This instability led to alert fatigue and a lack of reliable forensic data for proactive threat hunting, and unnecessarily consumed valuable SOC engineering time.

The company selected the ExtraHop RevealX™ platform after a competitive review, replacing its legacy incumbent to achieve:

- **Stable forensic continuity:** The organization eliminated the quarterly loss of tuning rules, ensuring that detection logic remained intact across system updates.
- **Reduced alert fatigue:** The SOC moved from high-noise environments to high-fidelity data, focusing on useful insights rather than repetitive false positives.
- **Enhanced threat hunting:** Analysts gained the deep level of forensic data required to initiate proactive hunting and investigate exfiltration attempts.
- **Seamless ecosystem integration:** The platform established proven integrations with NetSkope, CrowdStrike, and the customer's SIEM. These integrations provide a unified defensive posture.

The Challenge

As a major health insurance provider, this organization manages vast amounts of sensitive patient data across on-premises and cloud environments. The highly regulated and data-intensive nature of its business presented several critical challenges:

Unstable Tool Infrastructure: Every quarterly update to the incumbent legacy tool caused the system to lose all previously established tuning rules, forcing the security team to rebuild hundreds of their detection logic rules repeatedly.

Operational Burnout from Alert Fatigue: The lack of persistent tuning resulted in a constant stream of low-value alerts, overwhelming the SOC and obscuring real threats.

Forensic Visibility Gap: The incumbent system, which functioned as a NetFlow aggregator, provided insufficient data. This gap prevented sophisticated threat hunting or detailed investigations into potential data exfiltration.

Inflexible Data Ingestion: The team required a solution that could simultaneously accommodate NetFlow and full packet analysis without sacrificing performance or depth.

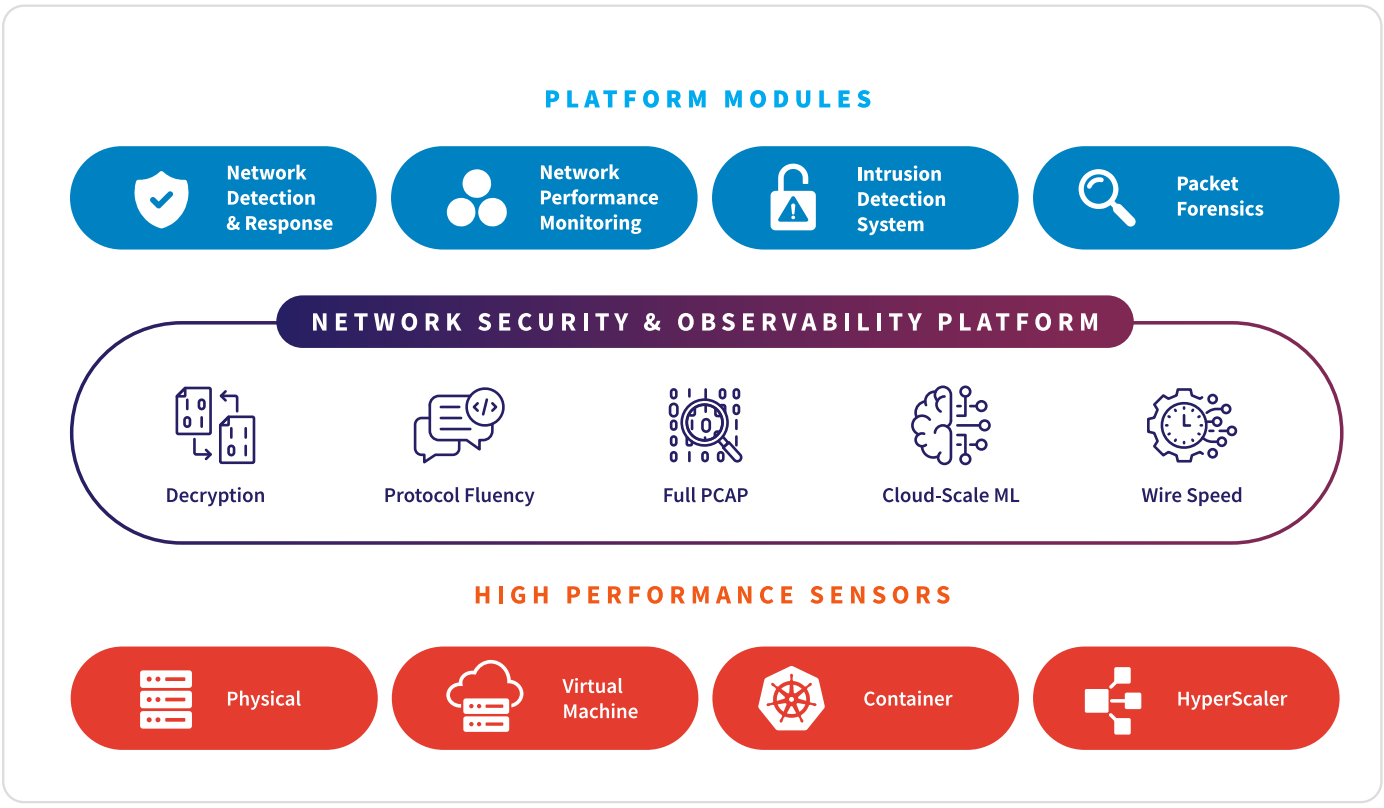
The Solution: Unified Detection with ExtraHop NDR

ExtraHop provides the agentless network security solution required for the healthcare insurance provider. This platform delivers unified security coverage that meets the healthcare insurance provider's security requirements. The modern NDR platform permits the SOC to achieve transformative efficiency. ExtraHop passively monitors network traffic without requiring software deployment on sensitive patient data infrastructure.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:** The organization secured the required forensic depth and network control when it deployed ExtraHop. The platform 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 reduces the SOC's operational burden with high-fidelity, low-noise detections. This shift permits analysts to move focus from low-value false positives to highly reliable network activity.
- **Actionable context and identity:** The security team gains comprehensive insight by using identity-based investigation. This feature links malicious network activity directly to user and service accounts.
- **Streamlined incident response via ecosystem integration:** ExtraHop simplifies incident response workflows. The platform establishes itself as the definitive source of network truth, automatically feeding high-value contextual data to NetSkope, CrowdStrike, and the customer's SIEM.
- **Unified security platform:** The organization improves efficiency and reduces complexity by consolidating NDR, NPM, and IDS capabilities into one unified, integrated solution.
- **Deep protocol coverage for core assets:** The healthcare insurance provider mitigates risk by gaining deep fluency. The sensor parses over 90 protocols to allow for accurate decoding of all traffic, including sensitive database communications.

ExtraHop NDR Platform



The Results: ROI and Operational Stability

The healthcare insurance provider realized security improvements following the transition to the ExtraHop NDR platform:

Deep Forensic Fidelity: The organization retains a significantly deeper level of forensic data compared to its previous solution. This data enables high-confidence investigations into exfiltration and lateral movement.

Detection Stability: The SOC removes the quarterly "reset" of tuning rules. This stability permits the team to mature their detection logic over time rather than constantly troubleshooting system updates.

Hybrid Data Flexibility: The platform integrates both packet-level data and NetFlow. This integration provides comprehensive visibility across the entire hybrid infrastructure.

Proven Integration Ecosystem: Integrations with NetSkope and CrowdStrike deliver the cross-platform telemetry necessary to stop threats at the edge and the endpoint.

Reclaimed SOC Engineering Time: The elimination of the need to rebuild lost configurations every quarter reduces the labor costs associated with tool maintenance.

Reduced Investigation Costs: Analysts expend less time manually piecing together evidence and more time executing high-value threat hunts.

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