EXTRAHOP

CUSTOMER STORY

Automotive Leader Secures Global Security Infrastructure

A global automotive leader faced visibility gaps when a legacy NDR suffered packet loss and untrustworthy data. By deploying ExtraHop RevealX™ NDR, the manufacturer restored data integrity with lossless, line-rate decryption. This modernization provided reliable real-time monitoring and evidence-based detection, securing high-stakes operations across North America, EMEA, and APJ.

The organization selected the ExtraHop RevealX platform after an evaluation of the incumbent legacy NDR vendor and multiple potential new vendors, achieving the following outcomes:

- **Primary source for threat protection:** The organization successfully established ExtraHop as the primary source of truth, enabling the SOC to protect against advanced threats with high-fidelity data.
- **Evidence-based detections and forensics:** The deployment of PacketStore enabled full packet capture, providing the granular detail and evidence required to understand the "why" behind threats and track lateral movement.
- **Global operational efficiency:** By consolidating security controls and replacing legacy IDS, the manufacturer streamlined global infrastructure management across its worldwide sites.
- **Unified security ecosystem:** The platform integrated seamlessly with Netskope, bridging technical gaps and accelerating the resolution of complex system dependencies.

The Challenge: Restoring Data Trust and Securing Global Manufacturing

Operating a global automotive brand requires flawless execution and high-performance network reliability against constant challenges from threat actors. However, the existing technical landscape presented several core challenges:

Inadequate Legacy Visibility

Prior to using ExtraHop, the organization relied on a legacy NDR vendor that suffered from lost packets. This meant the SOC was unable to fully trust the information provided, relegating the solution to a secondary checking role that was insufficient for the scale of the business.

Lack of Actionable Context

The manufacturer struggled with detections that failed to provide the detail as to "why" a threat occurred. Without this level of information, the team could not effectively track lateral movement, which was a major concern for the organization.

Complexity at Global Scale

With manufacturing operations spread across three major regions, the customer needed a solution that could deploy globally and handle the challenge of encrypted traffic without introducing performance risk.

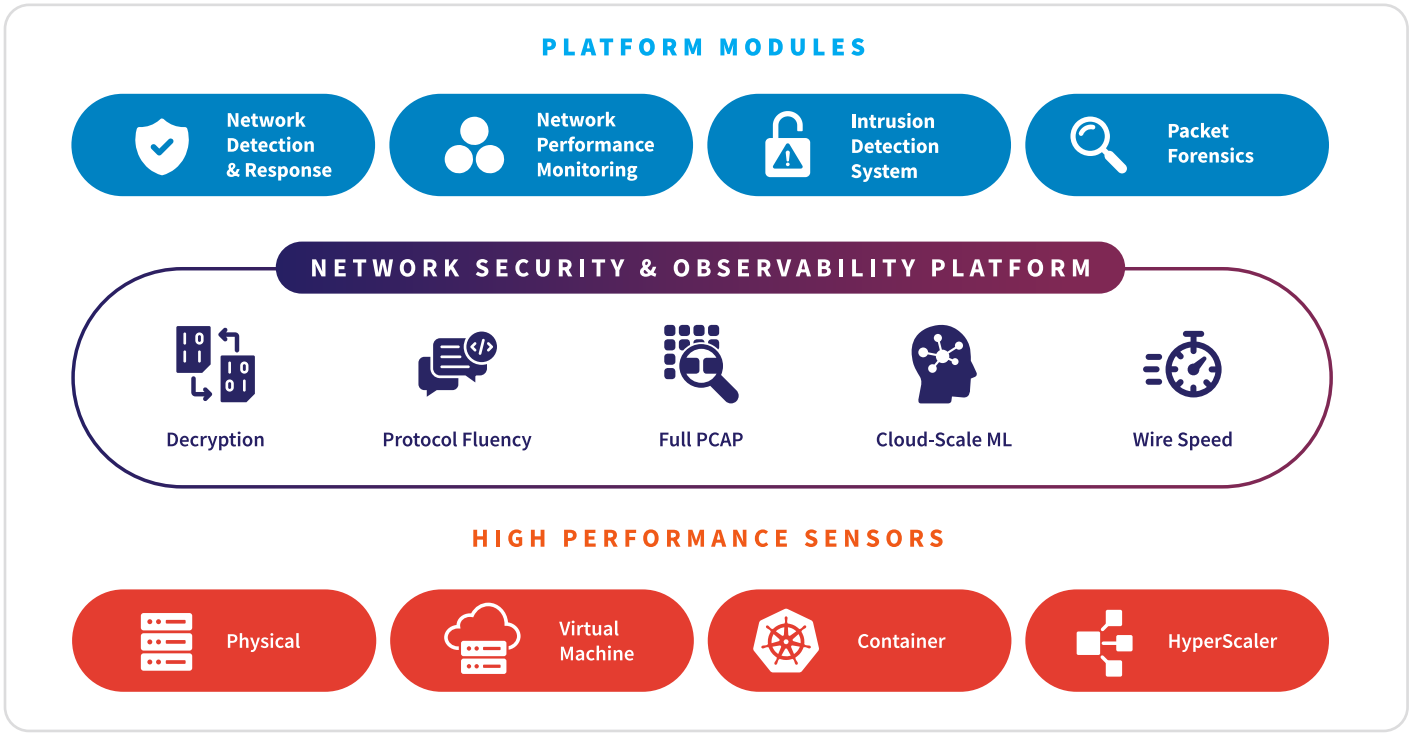
The Solution: Unified Detection with ExtraHop NDR

The successful deployment of ExtraHop enabled the automotive leader to modernize its defensive and operational posture. The platform provided the specialized inspection and granularity required to manage a mature and technical SOC environment.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:**
  The automotive 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 automotive manufacturing 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.

ExtraHop NDR Platform



The Results: Performance and Protection

The global automotive manufacturer achieved immediate, transformative improvements in security posture and operational agility following the deployment of the ExtraHop NDR platform.

Enhanced Threat Success

The organization now possesses a primary source of information to protect against advanced threats across its global manufacturing operations.

Deeper Investigation Capabilities

By moving to automated forensics and full packet capture through PacketStore, the engineering team can now perform the deep investigation work required for a mature SOC.

Global Operational Consistency

The rollout provided a unified view of the global network across North America, EMEA, and APJ, ensuring consistent security and performance standards worldwide.

Strategic Partnership Foundation

The selection of ExtraHop was based on a desire for a vendor that wanted to build a relationship and grow together, a partnership that continues to this day.

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