EXTRAHOP

CUSTOMER STORY

Automotive Parts Supplier Modernizes Global Security Infrastructure

A global automotive parts leader faced internal visibility gaps because legacy tools only monitored north-south traffic. To protect proprietary research, they deployed ExtraHop RevealX™ NDR for high-scale east-west visibility. This modernization enabled the detection of lateral movement and closed critical security gaps without disrupting production or next-generation engineering designs.

The company selected the ExtraHop RevealX platform after a rigorous head-to-head proof of concept (POC) against an NDR competitor, achieving the following outcomes:

- **Enterprise-wide internal visibility:** The company successfully gained deep visibility into east-west traffic, closing critical gaps that previously allowed lateral movement to go undetected.
- **Strategic legacy displacement:** ExtraHop replaced an underperforming legacy network forensics platform, delivering significantly higher forensic depth and real-time detection for the security operations center.
- **Scalable global rollout:** The platform demonstrated the capacity to operate across a massive worldwide footprint, securing every organizational location with a unified detection architecture.
- **Proprietary privacy compliance:** The deployment was customized to align with the supplier's internal data privacy mandates, ensuring high-fidelity analysis met the company's unique regulatory requirements.

The Challenge: Securing East-West Traffic and Global Engineering Assets

The company's existing architecture presented several foundational hurdles that prevented effective threat detection:

Ineffective Legacy Solutions

The company relied on an outdated security stack, which failed to generate actionable intelligence from its high volume of network traffic. This lack of return on investment (ROI) prevented the security team from decommissioning redundant tools and streamlining their technical environment.

Internal Blind Spots

While the perimeter was monitored, the team lacked the specialized tools to inspect lateral traffic. This left the company blind to internal movement, making it difficult to stop threats that had already bypassed north-south defenses to target sensitive manufacturing segments.

Complexity at Scale

With a mature network team managing thousands of endpoints worldwide, any new solution had to integrate seamlessly into a high-volume, high-stakes environment. The company needed a platform that could scale globally without introducing performance risk.

Stringent Data Privacy Standards

As an engineering giant, the company maintains proprietary data privacy standards that exceed standard regulations. Any network-based detection platform had to provide deep forensic evidence while respecting these strict internal data-handling rules.

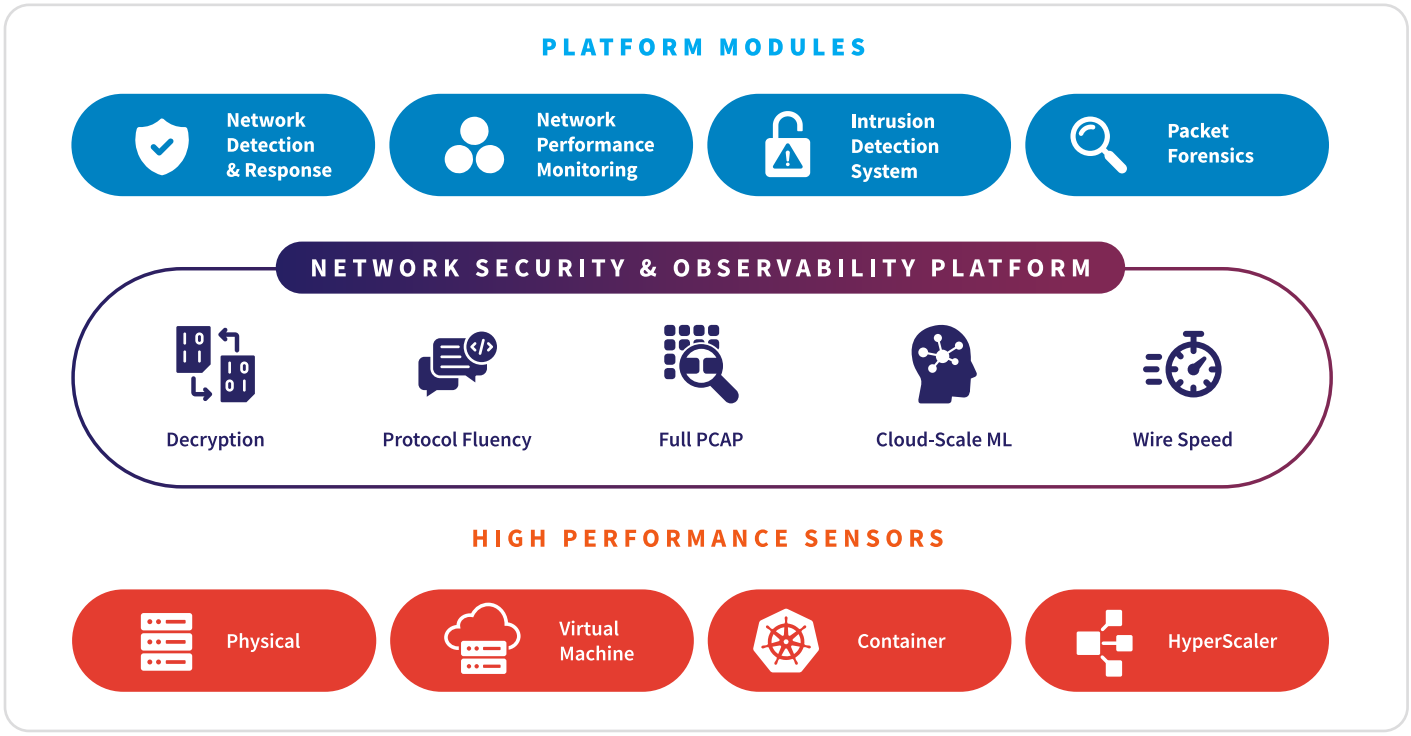
The Solution: Unified Detection with ExtraHop NDR

ExtraHop proved its technical superiority during the competitive POC, demonstrating a unique ability to handle the complexity of an automotive manufacturing environment. The modern NDR platform enabled the SOC to gain definitive evidence of threats that were previously invisible.

The key outcomes and advantages delivered to the company include:

- **Unrestricted visibility and decryption:** The automotive parts 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 company 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 parts 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 parts leader achieved transformative security improvements and operational stability following the worldwide rollout of the ExtraHop NDR platform.

Verified Competitive Strength

By outperforming a competitor in a live environment, ExtraHop proved it was the only solution capable of meeting the forensic and scale requirements of a global engineering leader. This validation gave the company confidence in their long-term security roadmap.

Unified Global View

The implementation across all global sites provided the first ever unified view of the company's entire network. This rollout simplified the management of complex traffic flows and ensured consistent protection for every manufacturing site.

Successful Tool Decommissioning

The company realized significant ROI by rationalizing its product stack. By displacing multiple legacy vendors with a single platform, the company simplified its technical environment and reduced the costs required to manage disparate security tools.

Compliance with Proprietary Standards

The implementation was successfully mapped to the company's internal privacy standards. This allowed the security team to perform deep forensic analysis and establish a shared source of truth while remaining fully compliant with proprietary data protection mandates.

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