EXTRAHOP

CUSTOMER STORY

Diversified Industrial Leader Closes Visibility Gaps and Unifies Security

A major EMEA industrial conglomerate displaced legacy tools with ExtraHop to gain 100 Gbps visibility across global manufacturing sites. By integrating ExtraHop RevealX™ with key applications, the organization eliminated critical blind spots, stopped credential harvesting attacks, and replaced alert noise with high-fidelity detections and automated response workflows.

The implementation enabled the detection of lateral movement and closed critical security gaps, allowing the infrastructure and systems team to respond to threats with surgical precision. The conglomerate selected the ExtraHop RevealX platform after a rigorous evaluation, achieving the following strategic outcomes:

- **Strategic Ecosystem Integration:** By switching to CrowdStrike and integrating it with ExtraHop, the team achieved a unified defensive posture that feeds high-value network telemetry into their EDR and SIEM for rapid, automated response.
- **Unrestricted 100 Gbps Visibility:** ExtraHop eliminated blind spots across global manufacturing sites, providing native, line-rate decryption and deep protocol analysis (parsing over 90 protocols) without impacting performance.
- **High-Fidelity Phishing Detection:** The platform's integration with Microsoft 365 allowed the team to immediately detect and block a credential harvesting attack, preventing further compromise of the corporate portal.
- **Maximized SOC Focus:** The security team achieved a substantial reduction in alert noise, shifting their focus from manual tuning to high-priority incident investigation and proactive threat hunting.

The Challenge: Industrial Complexity and Critical Visibility Gaps

As a diversified global industrial leader, this organization manages a substantial technical footprint where uptime and intellectual property protection are paramount. Its expansive manufacturing sites and hybrid-cloud environment presented several core challenges:

Critical Visibility Gaps and Blind Spots

The incumbent environment suffered from unacceptable blind spots. It lacked the native, line-rate decryption capabilities required to inspect communications between global manufacturing sites. Consequently, threats hidden in critical east-west traffic and communications with unmanaged IoT and industrial assets were missed entirely, leaving sensitive intellectual property vulnerable.

Operational and Integration Friction

The organization's initial endpoint strategy lacked the deep synergy required for modern defense. The disconnect between their legacy network tools and previous legacy EDR solutions created silos, making it difficult to correlate network anomalies with endpoint behavior. This gap hindered the team's ability to quickly contain risks without resorting to blunt, manual interventions.

Inadequate Performance at Scale

With an annual turnover exceeding hundreds of millions of euros, the organization required a solution capable of monitoring 100 Gbps traffic volumes without introducing latency. The incumbent tools failed to scale across the group's diverse hybrid enterprise, resulting in inconsistent coverage that threatened to compromise the continuous operation of high-value production lines.

Alert Fatigue and High-Noise Environment

The security team was overwhelmed by noisy, low-fidelity alerts from legacy systems. This alert fatigue obscured true post-compromise threats, forcing analysts to spend valuable time tuning filters and managing false positives rather than focusing on high-priority incident investigation and strategic threat hunting.

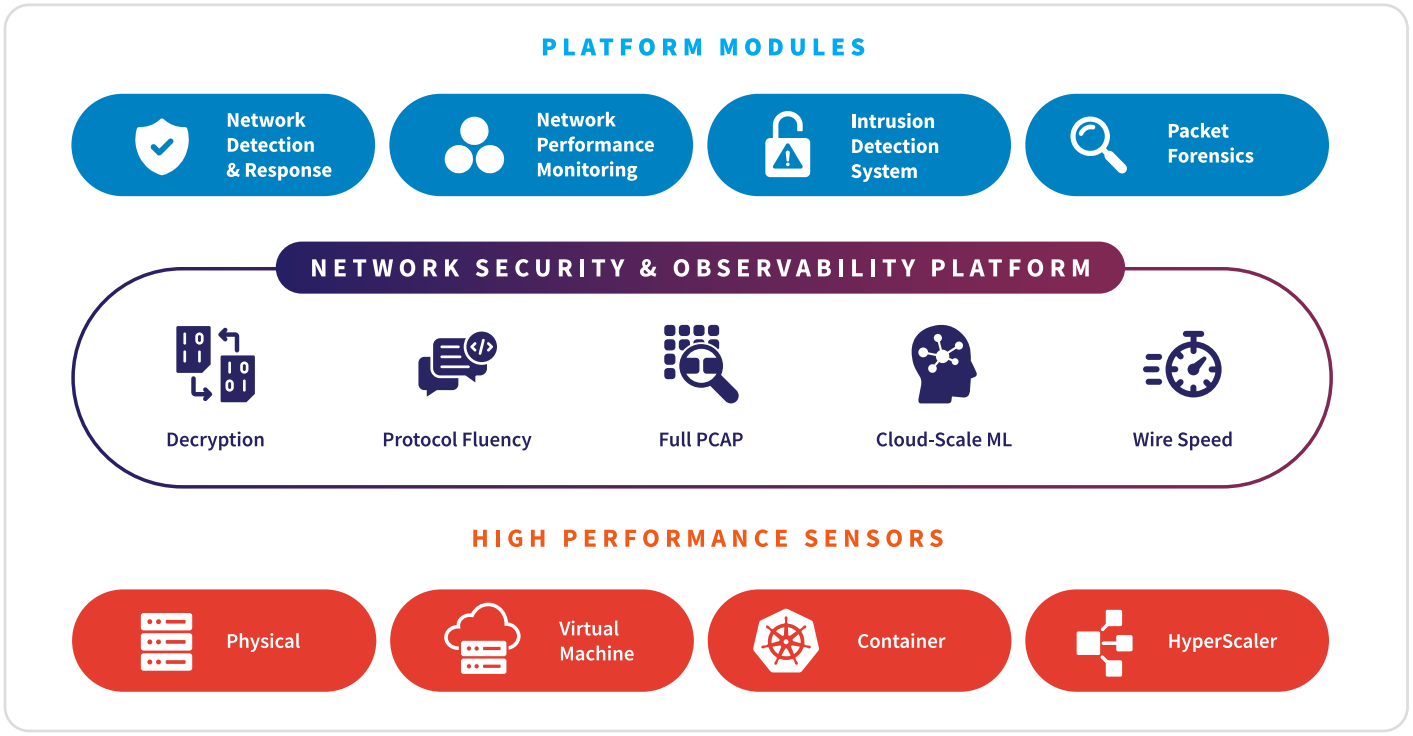
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully displaced the incumbent NDR vendor by proving its ability to provide unified security coverage that met the conglomerate's strict performance and scalability requirements with the proven benefits of a modern NDR platform.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:**
  The global conglomerate 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 lifted the SOC's operational burden because it provided high-fidelity, low-noise detections. This shift allowed analysts to move 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 global conglomerate mitigated major risk by gaining deep fluency (decrypting and decoding over 90+ protocols) that allowed for accurate analysis 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: Scalable Visibility and Unified Defense

This industrial leader achieved immediate and transformative security improvements following the deployment of the ExtraHop RevealX platform.

Decisive Platform Selection

The organization successfully displaced legacy solutions and fixed critical east-west visibility and unmanaged asset blind spots. This transition solved long-standing scalability issues across global manufacturing sites and diverse business units.

Protected Critical Intellectual Property

ExtraHop provided essential visibility for sensitive industrial databases and 100 Gbps traffic flows. This allowed the conglomerate to proactively protect core intellectual property and manufacturing secrets without introducing performance risks to high-speed production lines.

Maximized SOC Focus

The security team achieved a substantial reduction in alert noise through high-fidelity detections. This shift empowered the group's 10-person team to stop managing false positives and instead focus on high-priority incident investigation and proactive threat hunting.

Closed Integration Gaps

The new platform closed all integration gaps by providing seamless, high-value data feeds to CrowdStrike, Active Directory, and their centralized SIEM and SOAR systems. This synergy allowed for rapid response to threats like credential theft without unnecessary automatic containment.

Unified Hybrid-Cloud Control

For the first time, the organization gained a scalable and holistic security solution across its entire hybrid enterprise. This overcame the previous vendor's inability to keep pace with a technical footprint spanning mining, energy, and chemical operations.

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