EXTRAHOP®

CUSTOMER STORY

Global Electronics Provider Secures High-Risk Labs and Gains 100% Agentless Visibility

A global electronics technology provider of products, services, and solutions for industrial and commercial customers faced a severe, high-risk security challenge within its 11 global IT labs. These labs, essential for presales testing, were constantly under cyberattack and contained a rotation of unmanaged devices, many owned by customers. Traditional security tools like EDR could not be deployed on these unmanaged assets, creating a significant visibility gap and putting sensitive customer data at risk. The business impact was severe, including **2–3 significant breaches per year**, negatively impacting customer trust.

The company selected the ExtraHop modern NDR platform after a competitive review against Darktrace and Vectra, achieving the following:

- **Financial risk mitigation:** The organization protected its bottom line by eliminating the heavy costs associated with 2–3 annual breach remediations and potential regulatory penalties.
- **Infrastructure cost savings:** By deploying a 100% agentless solution, the provider avoided the massive labor and software costs required to manage security on constantly rotating, unmanaged devices.
- **Consolidated global efficiency:** The provider achieved a lower total cost of ownership (TCO) by replacing disparate lab-monitoring tools with a single, centralized global platform.
- **Asset lifecycle ROI:** The platform maximized the value of high-speed lab infrastructure by providing line-rate visibility and decryption without introducing performance bottlenecks.

The Challenge

As a technology provider, this organization utilizes 11 global IT labs for crucial presales testing of its products, services, and solutions. The highly dynamic and high-risk nature of these lab environments presented several critical challenges:

Unique High-Risk Environment

The 11 global IT labs faced regular cyberattacks due to their function in presales testing.

Lack of Control over Devices

The labs contained a constantly changing rotation of unmanaged devices, often owned by customers, which made traditional security control impossible.

Significant Visibility Gap

Traditional security tools like EDR could not be deployed on these constantly rotating, unmanaged devices, leaving the environment blind to threats.

Severe Business Impact from Breaches

This visibility gap resulted in 2–3 significant security breaches annually, which damaged customer relationships, eroded trust, and put sensitive customer data on test devices at risk of exposure or regulatory penalties.

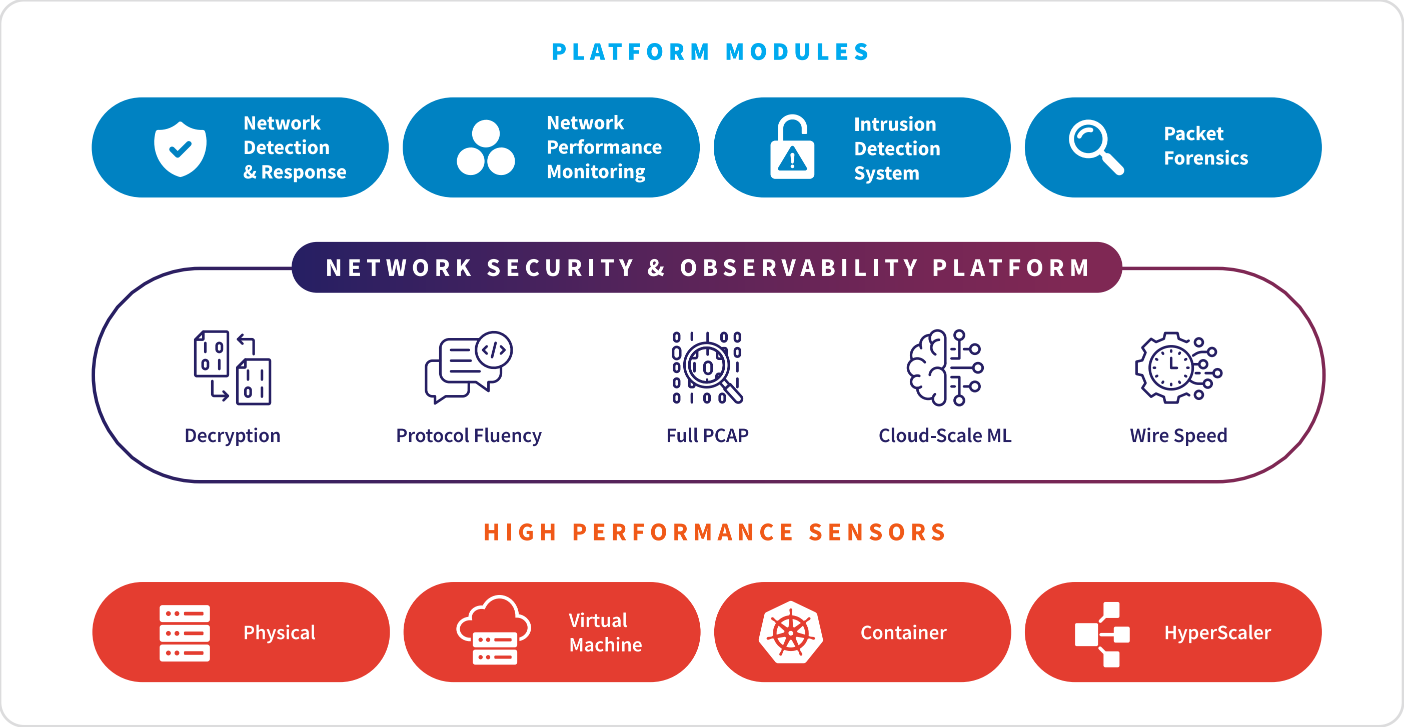
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully provided the agentless network security solution required for the global labs, proving its ability to provide unified security coverage that met the organization's high-stakes security requirements. The modern NDR platform enabled the SOC to achieve transformative efficiency. ExtraHop was uniquely compelling due to its ability to passively monitor network traffic without requiring software deployment on the constantly rotating, unmanaged devices.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:** The global electronics technology provider 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 global electronics technology provider 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 electronics technology provider achieved immediate, transformative security improvements across its high-risk IT labs following the deployment of the ExtraHop NDR platform.

Security Gap Closure: The platform delivered the critical ability to monitor for malicious activity in the lab environments where EDR deployment was not possible.

Breach Elimination: The organization successfully eliminated the 2–3 significant breaches it was experiencing annually, proactively protecting sensitive customer data and key business relationships.

Agentless and Complete Visibility: The company gained 100% agentless visibility and achieved complete, passive monitoring of all network activity across its 11 labs, including unmanaged customer-owned devices.

Centralized Control: A single, easy-to-use platform now provides centralized global monitoring across all 11 disparate lab locations.

Enhanced Security Ecosystem: The platform seamlessly integrated with the Microsoft SIEM and EDR platform, feeding high-accuracy detections to accelerate existing security workflows.

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