EXTRAHOP

CUSTOMER STORY

Major Exchange Solves Scalability and Visibility Gaps by Replacing Incumbent NDR

A leading global multi-asset exchange, which provides listing, trading, clearing, and data services for critical financial instruments, faced severe scalability and visibility gaps with its incumbent network detection and response (NDR) vendor. The existing solution failed to provide comprehensive coverage across its diverse, high-speed hybrid environment, resulting in critical blind spots, excessive alert noise, and hindered SOC operations.

The exchange selected the ExtraHop modern NDR platform to displace the incumbent, successfully delivering:

- **Unified visibility:** ExtraHop eliminated critical east-west traffic and unmanaged asset blind spots; it provides native, line-rate decryption and broad protocol support.
- **Zero-latency protection:** The exchange secured sensitive, time-critical trading databases without introducing performance impact to core revenue streams.
- **High-fidelity detection:** The Security Operations Center (SOC) achieved a massive reduction in alert noise, shifting from tuning false positives to focusing on high-priority threat hunting.
- **Scalable integration:** ExtraHop provided a robust, scalable security solution that seamlessly integrated with the exchange's existing CrowdStrike, Active Directory (AD), SIEM, and SOAR platforms, overcoming the incumbent's integration and scalability failures.

The Challenge: Critical Visibility Gaps and Performance Risks

As a leading multi-asset exchange, this organization operates at the absolute cutting edge of the financial world, requiring zero downtime, zero performance degradation, and an imperative for flawless security execution. Its expansive and critical hybrid/multi-cloud environment, housing time-sensitive trading databases, presented a significant challenge to the existing security architecture and incumbent NDR solution.

Critical Visibility Gaps and Blind Spots

The incumbent NDR vendor left unacceptable blind spots in the network. It lacked native, line-rate decryption capabilities, meaning threats hidden in critical east-west traffic and communications with unmanaged assets it missed completely.

Performance and Latency Risk

Due to the exchange's high-speed operational demands, the security tool had to provide zero-latency monitoring for time-sensitive trading databases to avoid compromising trade execution speed or affecting core revenue streams. The incumbent failed to meet this demand.

Poor Scalability and Hybrid Support

The incumbent solution failed to scale across the organization's diverse hybrid/multi-cloud environment, resulting in inadequate coverage and performance issues that risked a security failure as the exchange scaled its operations.

Alert Fatigue and Hindered SOC Automation

The incumbent tool's noisy, low-fidelity alerts caused significant SOC alert fatigue, obscuring critical threats and forcing analysts to tune filters instead of responding to incidents. Furthermore, poor SIEM and SOAR integration limited automation and centralized visibility, hindering efficient response efforts.

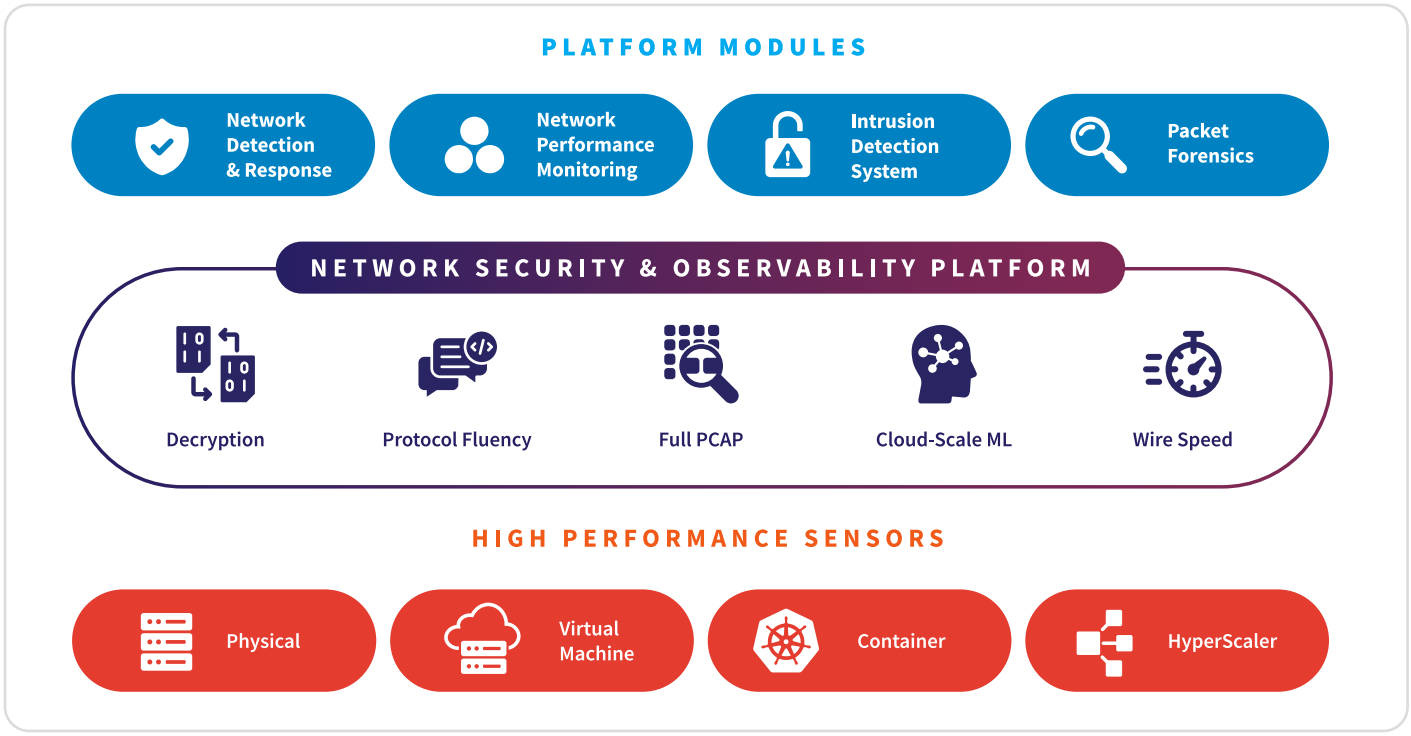
The Solution: Unified Detection with ExtraHop NDR

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

The key outcomes and advantages delivered to the exchange include:

- **Unrestricted visibility and decryption:**
  The global exchange 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 exchange 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 exchange achieved immediate, transformative security improvements following the deployment of the ExtraHop NDR platform.

Decisive Platform Selection

The exchange successfully replaced the incumbent, fixed east-west visibility and unmanaged asset blind spots, and solved long-standing scalability and integration issues.

Gained Revenue Stream Protection

ExtraHop provided essential visibility for sensitive trading databases, allowing the organization to proactively protect core revenue streams without compromising crucial trade execution speed.

Maximized SOC Focus

The organization achieved a substantial reduction in alert noise with high-fidelity detections, empowering analysts to shift their focus from tuning and noise reduction to high-priority incident investigation and threat hunting.

Closed Integration Gaps

The new platform closed all integration gaps, providing seamless, high-value data feeds to CrowdStrike, Active Directory, and their centralized SIEM/SOAR systems.

Unified Hybrid-Cloud Control

For the first time, the organization gained a scalable and holistic security solution across its entire hybrid/multi-cloud enterprise, overcoming the incumbent's inability to keep up with the technical footprint.

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