EXTRAHOP

CUSTOMER STORY

Global Retirement Fund: Securing a Hybrid Multicloud Enterprise

A leading global retirement fund, operating in a high-volume, hybrid-cloud environment, faced critical visibility and detection failures with its existing network detection and response (NDR) vendor. The incumbent created massive cloud blind spots and low-fidelity alerts, hindering the security operation center's (SOC) ability to detect sophisticated threats like Active Directory (AD) attacks.

The ExtraHop modern NDR platform displaced the incumbent and won a head-to-head competitive proof of concept (POC) by delivering:

- **Unified visibility:** ExtraHop eliminated the critical hybrid-cloud blind spot (Azure/AWS), providing full visibility at 100 Gbps.
- **High-fidelity detection:** The retirement fund was able to immediately detect advanced AD attacks, such as **Golden Ticket**, and lateral movement that the incumbent missed by switching to the ExtraHop modern NDR platform.
- **Operational efficiency:** By shifting focus from low-value tuning to high-priority threat hunting, ExtraHop helped to reduce SOC alert fatigue.

The Challenge

A leader in its industry, the global retirement fund manages more than $100 billion in assets, employs 1,000+, and operates with an absolute imperative for zero-risk tolerance given its high-value status. Its expansive technical environment spanned multiple data centers and a hybrid multicloud footprint (including Azure and AWS), hosting high-volume trading and administrative systems. This combination of a vast technical footprint and strict compliance demands introduced significant challenges to the fund's security operations and incumbent NDR solution.

Critical visibility and performance gaps

The organization struggled with a critical hybrid-cloud blind spot. The existing NDR product failed to provide coverage for a significant portion of their public cloud infrastructure and was incapable of analyzing high-speed internal encrypted east-west traffic at up to 100 Gbps, meaning threats hidden in encrypted flows were entirely missed.

Missed detections

The incumbent NDR vendor consistently failed to detect critical post-compromise activities: AD attacks, command and control (C2), and lateral movement, as these activities were hidden within encrypted communications and legitimate protocols that the tool could not properly decode.

Alert fatigue

The SOC was severely impacted by excessive, low-fidelity detections from the incumbent NDR tool, wasting valuable analyst time on false positives and excessive tuning.

Technical gaps and future imperative

The incumbent solution could not meet the operational demands of the fund's expansive technical environment, which risked a security failure as the environment scaled. The replacement had to provide deep protocol fluency, particularly for database communications, to decode internal traffic that the incumbent had failed to analyze. Furthermore, seamless integration with existing tools like CrowdStrike and Microsoft AD was mandatory to maintain a cohesive, functional security ecosystem.

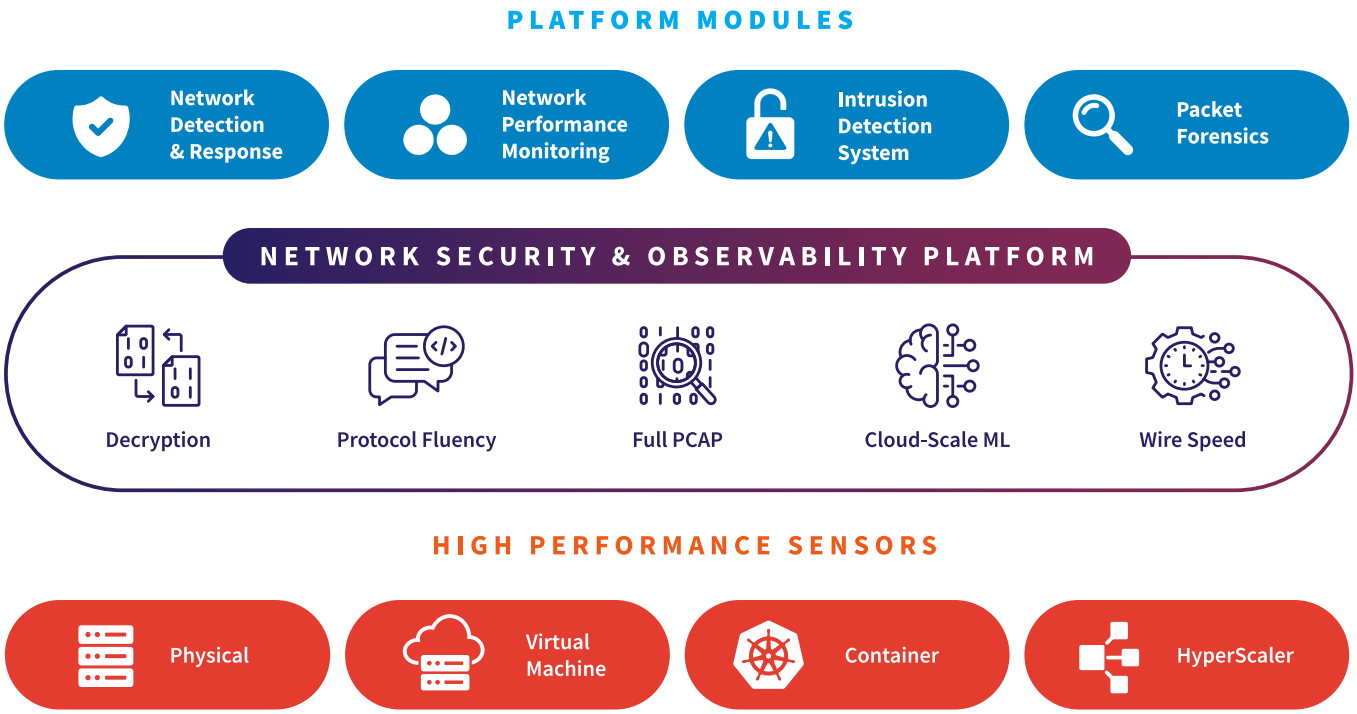
The Solution: Unified Detection with ExtraHop NDR

Following a rigorous head-to-head POC against two leading competitors, the global retirement fund selected ExtraHop as its preferred NDR vendor, finally securing their hybrid environment with the proven benefits of a modern NDR platform.

The key outcomes and advantages the ExtraHop platform delivered to the retirement fund include:

- **Unrestricted visibility and decryption:** The fund secured the required forensic depth and network control by deploying 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 leveraging 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 fund 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: Security Excellence

The global retirement fund achieved immediate, transformative security improvements following the deployment of their new NDR platform.

Decisive platform selection

The retirement fund successfully displaced the incumbent NDR vendor, validating their selection of the modern platform with immediate, tangible results. The fund proved it could achieve superior technology and visibility by instantly eliminating the public-cloud blind spot and enabling the detection of high-fidelity AD attacks.

Unified hybrid-cloud control

For the first time, the organization gained holistic visibility across the entire hybrid enterprise after the new NDR platform entirely eliminated the critical public-cloud blind spot (Azure/AWS).

High-value threat mastery

The SOC immediately achieved the capability to detect high-fidelity, advanced AD attacks, such as the **AD Delegation Enumeration Activity** and domain enumeration, even over encrypted communication.

Maximized SOC focus

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

Accelerated incident response

The fund fundamentally streamlined the SOC's incident response workflow, greatly reducing the time and effort required for investigations by leveraging centralized, contextualized data from the NDR platform.

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