EXTRAHOP

CUSTOMER STORY

Media Leader Secures Critical Broadcast Infrastructure and Ends East-West Blind Spots

A leading diversified media company in the Asia-Pacific region, with extensive holdings in television, digital, publishing, and radio, confronted critical security and visibility challenges across its vast and complex network. The company struggled with a significant lack of east-west visibility and blind spots between its segmented broadcast, media, and corporate networks. Additionally, the absence of proactive behavior monitoring contributed to delayed threat identification and obscured IT hygiene issues.

The company selected the ExtraHop RevealX™ platform after a competitive review, achieving the following strategic outcomes:

- **Financial protection of critical assets:** The company secured critical broadcast infrastructure against downtime and high-level threats. This protection safeguarded core revenue-generating operations.
- **Operational ROI through multicast automation:** ExtraHop resolved a unique visibility challenge by implementing specialized filtering for high-bandwidth multicast traffic. This deployment eliminated the need for a costly packet broker.
- **Unified global efficiency:** The SOC gained complete east-west visibility across siloed broadcast, media, and corporate segments. This unified perspective decreased the manual effort required to manage disparate network environments.
- **Ecosystem ROI and value realization:** The platform bridged critical security gaps by feeding high-value contextual data to existing investments, including CrowdStrike and Google Chronicle. These integrations maximized the effectiveness of the total security stack.
- **Proactive risk reduction:** By enabling high-fidelity detection of unusual device and user behavior, the team transitioned from reactive response to proactive threat identification. This shift decreased the potential impact of network-level attacks.

The Challenge

As one of the world's largest diversified media companies, this company operates a vast, segmented network that handles high-bandwidth media traffic and houses critical broadcast infrastructure. Securing this complex environment presented several core challenges:

Critical Visibility Gaps in East-West Traffic

The company struggled with a critical lack of east-west visibility and pervasive blind spots between its siloed broadcast, media, and corporate network segments.

Lack of Proactive Detection

The company lacked a mechanism for proactive detection of unusual device or user behavior, which routinely led to delayed threat identification and obscured IT/cyber hygiene issues.

Unsecured Critical Infrastructure

The limited visibility into key traffic flows prevented the team from adequately securing broadcast infrastructure. This vulnerability posed a major risk to core operations.

Multicast Traffic Complexity

Analyzing the high-bandwidth media traffic that utilized multicast posed a specialized visibility challenge. The team required a specialized ERSPAN deployment to filter and analyze the traffic at the switch level because the environment lacked a packet broker.

Integration and Coverage Issues

The large network maintained minimal EDR coverage and experienced integration issues with existing tools, including CrowdStrike EDR, CrowdStrike SIEM, and Google Chronicle SIEM, further limiting centralized security control.

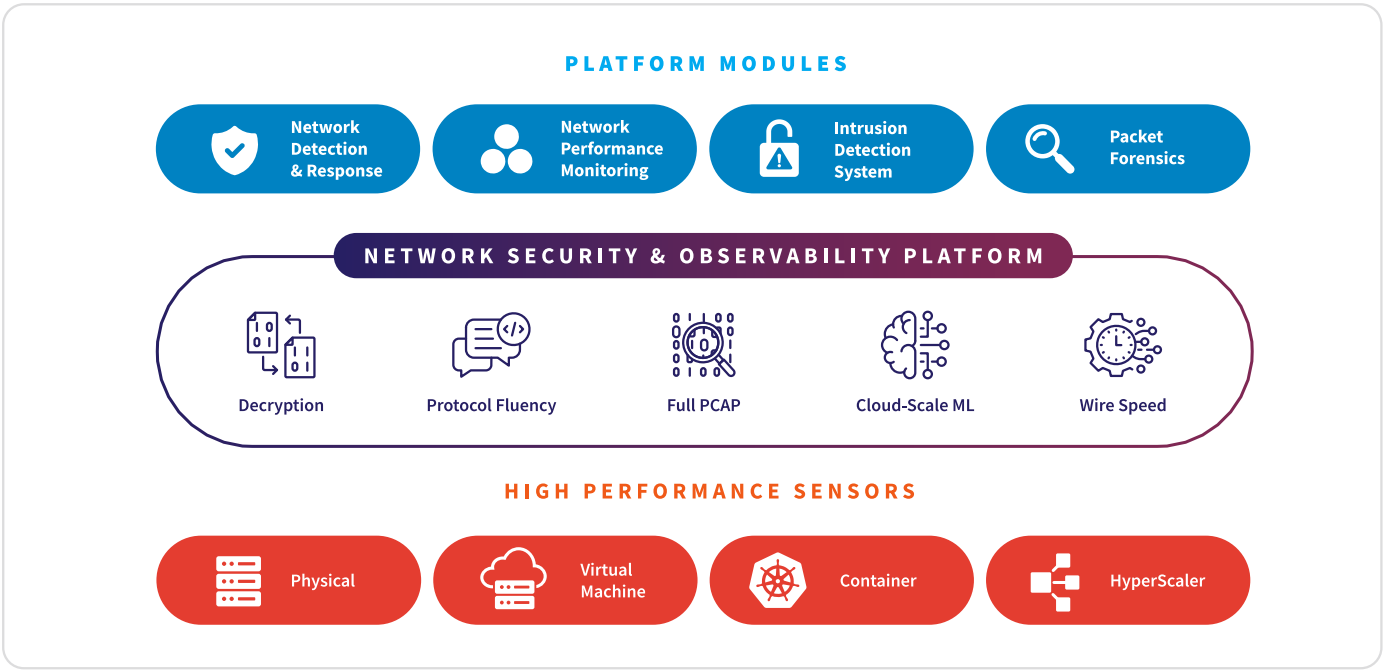
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully proved its ability to provide unified security coverage that met the company's unique security requirements to address corporate, media, and broadcast networks. The modern NDR platform enabled the SOC to achieve transformative efficiency. ExtraHop was selected as the sole proof-of-concept (POC) vendor, ultimately winning the selection over an NDR competitor.

The key outcomes and advantages delivered to the company include:

- **Unrestricted visibility and decryption:** The company 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 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 company 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 diversified media leader achieved transformative visibility and security improvements across its highly complex environment following the deployment of the ExtraHop NDR platform.

Unified Network Security: The company gained crucial east-west visibility across its formerly siloed broadcast, media, and corporate network segments.

Secured Critical Broadcast Infrastructure: The solution secured critical broadcast infrastructure and provided proactive threat detection. This deployment addressed the lack of visibility into key traffic flows.

Solved Multicast Visibility Challenge: ExtraHop successfully analyzed high-bandwidth multicast traffic, solving a unique visibility challenge required by the nature of media operations.

Enhanced Ecosystem Integration: The platform closed integration gaps and successfully fed contextual data to existing security tools, including CrowdStrike and Google Chronicle.

Decisive Platform Selection: ExtraHop displaced the competition. This selection demonstrated the platform's ability to handle the company's complex NDR requirements

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