EXTRAHOP

Securing the Global Media Pipeline: Protecting Content Integrity and Creative Innovation

Keep Critical Media Production Workflows and IP Pipelines Free from Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: Securing the All-IP Production Frontier

In 2026, the media and entertainment industry has fully embraced the "seismic shift to IP," moving production facilities and broadcast centers onto massive, high-bandwidth 100 Gbps Ethernet networks. While uncompressed 8K workflows and cloud-integrated editing have enabled unprecedented creative agility, they have also transformed the media pipeline into a high-value target for sophisticated digital adversaries. Studios and broadcasters now face a new reality where a network disruption can silence a global broadcast or leak a blockbuster before it hits theaters:

- **The Vulnerability of the All-IP Control Plane:** As traditional SDI cables are replaced by SMPTE ST 2110 and AMWA NMOS protocols, the production floor has inherited the vulnerabilities of standard IT. In 2026, we see a rise in attacks targeting the NMOS control plane to reroute live media streams or launch multicast floods that cause frame-drops and jitter. These "silent" disruptions can take a premier live event off the air without a single piece of malicious code, exposing a critical gap where traditional security tools fail to understand media-specific traffic.
- **"Recovery Denial" and Content Extortion:** Ransomware has moved beyond simple encryption. Modern threat actors now focus on "silent exfiltration" followed by recovery denial. This is the targeted destruction of backups to maximize leverage. In this era, the "day-and-date" release of a season finale or a $200M feature film is the ultimate bargaining chip. Protecting these crown jewels requires the ability to detect lateral movement and staging behaviors within the high-speed production network before the exfiltration begins.
- **The Crisis of "Shadow AI" IP Leakage:** Creative teams are increasingly utilizing generative AI for VFX, color grading, and automated dubbing. However, this has created a massive leak in the media supply chain. Without visibility, proprietary scripts, unreleased footage, and raw voice files are being uploaded to unvetted third-party AI platforms. These shadow AI leaks not only compromise intellectual property but can also lead to the loss of TPN Gold Star Shield certification, rendering a studio ineligible for major distribution partnerships.
- **Precision Timing and the "Time-Slamming" Threat:** Frame-accurate synchronization relies entirely on precision time protocol (PTP). In 2026, adversaries are targeting PTP Grandmaster clocks to desynchronize audio and video streams. This is a technique known as "time-slamming." Because most security solutions lack protocol-level awareness of PTP, these timing anomalies often go undetected until the moment of broadcast failure, turning a synchronization issue into a catastrophic outage.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all network interactions by decrypting and decoding over 90+ protocols at 100 Gbps to protect uncompressed 8K media streams and high-speed production pipelines.

The Definitive Data Source for the AI-Enabled SOC

Powers M&E SOC automation with unalterable network data, providing the context for AI agents to stop content exfiltration at machine speed.

AI-Powered Cyber Threat Detection

Uses cloud-scale machine learning to detect lateral movement and ransomware targeting unreleased scripts and high-value creative IP.

Unified Agentless Visibility

Discovers all production assets, including SDI-to-IP gateways and cloud suites, without installing software or impacting rendering performance.

Strategic Line-Rate Decryption

Analyzes encrypted traffic to expose threats in NMOS control plane commands, preventing adversaries from rerouting live feeds.

High-Fidelity Performance Metrics

Troubleshoots disruptions and verifies SLAs using wire data metrics for deep insight into PTP sync jitter and media stream performance.

Continuous Forensic Capture

Maintains unalterable network records to satisfy audit requirements for TPN Gold Shield and MPA content security standards.

The Solution: RevealX Network Intelligence for Media Production

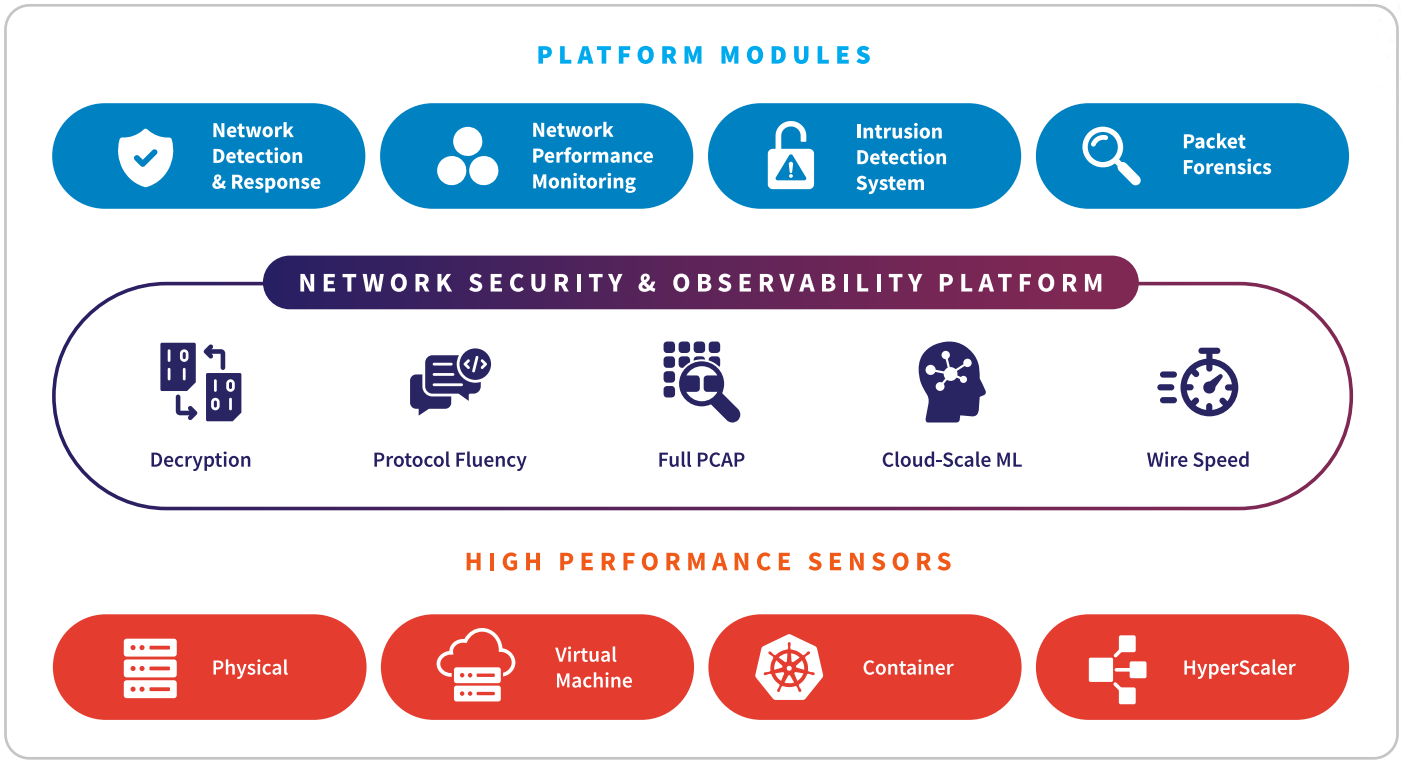
ExtraHop RevealX provides the unalterable ground truth required to secure the high-speed media pipeline and protect the creative assets that define global entertainment. By analyzing traffic at 100 Gbps, it eliminates visibility gaps across hybrid production clouds and uncompressed 8K broadcast zones. In a sector where a single content leak can cost hundreds of millions in projected revenue or compromise a studio's TPN Gold Shield status, RevealX maintains production integrity. The platform turns the network into a definitive record of truth, allowing security teams to see every interaction without the need for intrusive agents that could disrupt frame-accurate rendering or live transmission.

RevealX resolves the all-IP blind spot through passive monitoring of specialized broadcast protocols. Critical infrastructure, including SMPTE ST 2110 media streams, NMOS control plane commands, and SDI to IP gateways, remains fully visible without risking stability. By baselining normal behavior, RevealX detects the subtle anomalies that indicate an adversary is attempting to reroute live feeds via unauthorized IS-05 commands or launch time-slamming attacks against the PTP Grandmaster clock. This visibility is vital for stopping sophisticated actors who use legitimate media protocols to blend with high-bandwidth production traffic.

To counter content extortion and IP theft, RevealX identifies the network shifts that signal data staging for exfiltration. By exposing threats within encrypted command and control channels, the platform stops attackers before they can pivot from office zones into restricted post-production segments or digital asset management systems. This visibility extends to the modern supply chain, monitoring the behavior of shadow AI agents and third-party VFX partners to prevent unauthorized uploads of unreleased footage. Line rate decryption ensures that attackers cannot hide malicious exfiltration within the massive encrypted streams typical of a 2026 hybrid cloud workflow.

Finally, RevealX accelerates the transition to permanent audit readiness. It provides the unalterable record necessary for MPA Best Practices and TPN Gold Shield verification, moving firms from periodic assessments to continuous evidence collection. This ground truth satisfies the rigorous demands of day-and-date release security and facilitates the 72-hour reporting windows now common in global media contracts. By bridging the gap between the SOC and the live production floor, RevealX ensures that security never becomes a bottleneck for creative velocity or broadcast reliability.

ExtraHop NDR Platform



NDR Technology Use Cases for the Media & Entertainment Industry

Nation-State Attacks	Detects lateral movement and exfiltration in long-term campaigns that may be targeting unreleased feature films, proprietary VFX workflows, and creative IP.
Threat Detection and Response	Investigates hidden threats across converged IP production environments, filling visibility gaps in edit bays and media asset management (MAM) where agents fail.
Threat Hunting	Leverages behavioral baselining to find signature-less threats and anomalies before they impact broadcast continuity, content integrity, or frame-accurate quality.
SOC Modernization	Unifies studio and broadcast engineering workflows with AI prioritization to reduce alert fatigue, accelerating response times for digital content distribution.
Incident Response and Investigation	Delivers forensic visibility and unalterable records of NMOS (IS-04, IS-05, IS-08) and SMPTE ST 2110 control plane commands for rapid root-cause analysis.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots bypassing perimeters toward restricted playout segments, rendering farms, and creative labs.
Cloud Workload Security	Provides agentless visibility for cloud-integrated production workloads, discovering shadow IT and unmanaged assets across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value broadcast controllers and editor workstations.
Ransomware Attacks	Identifies ransomware staging and “recovery denial” patterns to isolate hosts before exfiltration of creative IP or disruption of live broadcast feeds.
Unmanaged Devices	Monitors network traffic for unmanaged broadcast cameras, intercom systems, and hardware encoders that cannot support traditional security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy playout servers and master control stations.
AI Security	Monitors generative AI agents used for VFX, automated dubbing, or content recommendation, to prevent unauthorized uploads of proprietary scripts or raw footage.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that TPN Gold Shield micro-segmentation and media network zone policies are effective.

NPM Technology Use Cases for the Media & Entertainment Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for 8K uncompressed video and IP-media production sessions.
Operational Resilience	Resolves infrastructure degradation before it hits broadcast continuity, ensuring availability through proactive monitoring of critical playout and delivery services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between broadcast engineering and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during MAM or DAM migration by auto-mapping dependencies and using production baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for media gateways and content distribution APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past broadcast outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding media protocols (e.g., NMOS, SMPTE ST 2110), providing real-time insights into command processing time vs. network latency.

Professional Services Industry Compliance & Regulatory Use Cases

Operational Resilience	Global	SMPTE ST 2110-10	Sync Assurance: Supports secure implementation of PTP (IEEE 1588) by detecting unauthorized “time-slamming” or grandmaster hijacking attempts.
Cybersecurity Maturity	Global	TPN Gold Shield	Audit Readiness: Provides the continuous behavioral monitoring and unalterable records required for MPA-verified TPN assessments and “gold star” status.
Audit and Forensics	Global	MPA Best Practices	Control Verification: Satisfies mandates for protecting creative assets by offering a definitive source of network truth for access to production segments.
Best Practice Framework	US	CIRCIA	Incident Disclosure: Enables compliance with 72-hour reporting windows by providing instant forensics into the scope and blast radius of a content breach.
Data Security and Privacy	EU / US	CPRA / GDPR	DTC Protection: Audits access to subscriber PII within direct-to-consumer platforms to prevent unauthorized data transfers and ensure privacy compliance.
Regulatory Best Practices	Global	AI Authorship Laws	Evidentiary Support: Maintains a persistent record of AI agent network behavior to document human-led creative workflows and defend intellectual property rights.

Customer Benefits: Empowering Creative and Operational Excellence

ExtraHop RevealX provides a definitive defense against modern content extortion by detecting the silent staging and exfiltration of high-value media files before attackers can leak intellectual property or destroy backups. By continuously monitoring network behavior, the platform exposes sophisticated adversaries who have already bypassed perimeter defenses and are "living off the land" inside your production environment.

The industry transition to all-IP production via SMPTE ST 2110 and NMOS introduces a massive new attack surface that traditional endpoint security agents cannot reach. RevealX decodes these specialized media protocols at 100 Gbps to ensure all routing instructions are legitimate, preventing adversaries from hijacking the control plane, rerouting live feeds, or disrupting broadcast integrity.

To mitigate the risks of generative AI, the platform prevents shadow AI leakage by monitoring the network for unauthorized uploads of proprietary scripts and raw footage to unvetted third-party platforms. This continuous visibility safeguards your intellectual property and ensures strict compliance with 2026 AI authorship mandates across the entire high-speed media supply chain.

Finally, RevealX acts as a strategic business enabler by transitioning your organization to a state of permanent audit readiness for the TPN Gold Shield. By providing the continuous network telemetry and forensic evidence required by the Motion Picture Association, it delivers the zero-trust verification needed to accelerate contract approvals with major studio partners.

> "We strive to provide the best customer experience possible, so excellent network performance is a must. RevealX provides more accurate and detailed detection information than other solutions, which means we can resolve network and application performance issues before they impact customers, and detect threats before attackers can achieve their goals."
>
> **CHIEF OF CYBERSECURITY ARCHITECTURE**

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments in media and entertainment: Leading Diversified Media Company

Or contact us to schedule your personalized demo and security assessment.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com