EXTRAHOP

IT and Telecommunications: Securing the Digital Backbone from Global Core to Enterprise Edge

Defend Critical Connectivity and Maximize Operational Uptime with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: Securing the Architecture of Global Connectivity

IT and telecommunications represent the converged global architecture of carriers, cloud providers, and managed services that facilitate the movement and processing of data. In 2026, this industry acts as the nervous system for the modern economy, where the distinction between the physical transport of bits and the software that manages them has entirely vanished. While this convergence accelerates innovation, it also creates a high-stakes environment where digital fragility can lead to societal-scale disruption:

- **The Persistence of Nation-State Sabotage on Core Infrastructure:** Geopolitically motivated adversaries have moved beyond simple espionage to the active sabotage of global routing and signaling. By targeting the border gateway protocol (BGP) or hijacking signaling protocols like SS7 and Diameter, nation-state actors can reroute global traffic or isolate entire regions. Protecting this digital backbone requires deep visibility into the core network to detect unauthorized path changes or lateral movement before an adversary can disable critical communication links or undersea cable landing stations.
- **The Managed Service and API Ripple Effect:** Telecommunications providers and IT firms now function as the primary supply chain for the global enterprise. Attackers increasingly target managed service providers (MSPs) and cloud gateways to gain "trusted" access to thousands of downstream customers simultaneously. Using compromised API tokens or hijacked administrative sessions, they can move from a provider environment into a customer core. Traditional endpoint security often fails here because the attack originates within the infrastructure itself, requiring a network-centric approach to identify identity abuse and unauthorized data staging.
- **The Blind Spots of 5G, 6G, and Distributed Edge Computing:** The rollout of 5G and early 6G has pushed compute power to the network edge, creating a massive, unmanaged attack surface of IoT devices and small-cell stations. These edge components frequently lack the resources to host security agents, leaving a significant visibility gap in the "last mile" of connectivity. To maintain operational integrity, providers must have the ability to analyze traffic directly on the wire to identify protocol anomalies and malicious command and control (C2) traffic across highly distributed, high-speed environments.
- **Strict Compliance and the Mandate for National Resilience:** 2026 regulations, such as the NIS2 Directive and CIRCIA, have classified IT and telecommunications as "essential" infrastructure with zero tolerance for prolonged outages. Manufacturers and carriers must now provide verifiable proof of continuous monitoring and rapid incident reporting for any event that impacts service availability. Meeting these standards while adhering to data residency and ePrivacy requirements requires a definitive source of truth that can reconstruct security events across hybrid cloud and multi-vendor environments.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all interactions by decrypting and decoding 90+ protocols at 100 Gbps to protect high-volume core networks and distributed edge environments.

The Definitive Data Source for the AI-Enabled SOC

Provides high-fidelity wire data to power telecommunications SOC automation. This delivers unalterable ground truth to eliminate investigative friction and accelerate remediation across critical infrastructure.

AI-Powered Cyber Threat Detection

Identifies lateral movement and ransomware targeting 5G signaling, core routing, and managed service portals using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers unmanaged infrastructure such as small cells, IoT gateways, and edge compute nodes without installing software or risking network availability.

Strategic Line-Rate Decryption

Analyzes TLS 1.3 and PFS traffic to expose hidden threats within encrypted management traffic without adding latency to high-speed data planes.

High-Fidelity Performance Metrics

Troubleshoots service disruptions using 5,000+ wire data metrics for deep operational insight into network latency and BGP/DNS performance.

Continuous Forensic Capture

Maintains unalterable transaction records to satisfy NIS2, CIRCIA, and ePrivacy audit requirements while accelerating root-cause analysis for service outages.

The Solution: RevealX Network Intelligence

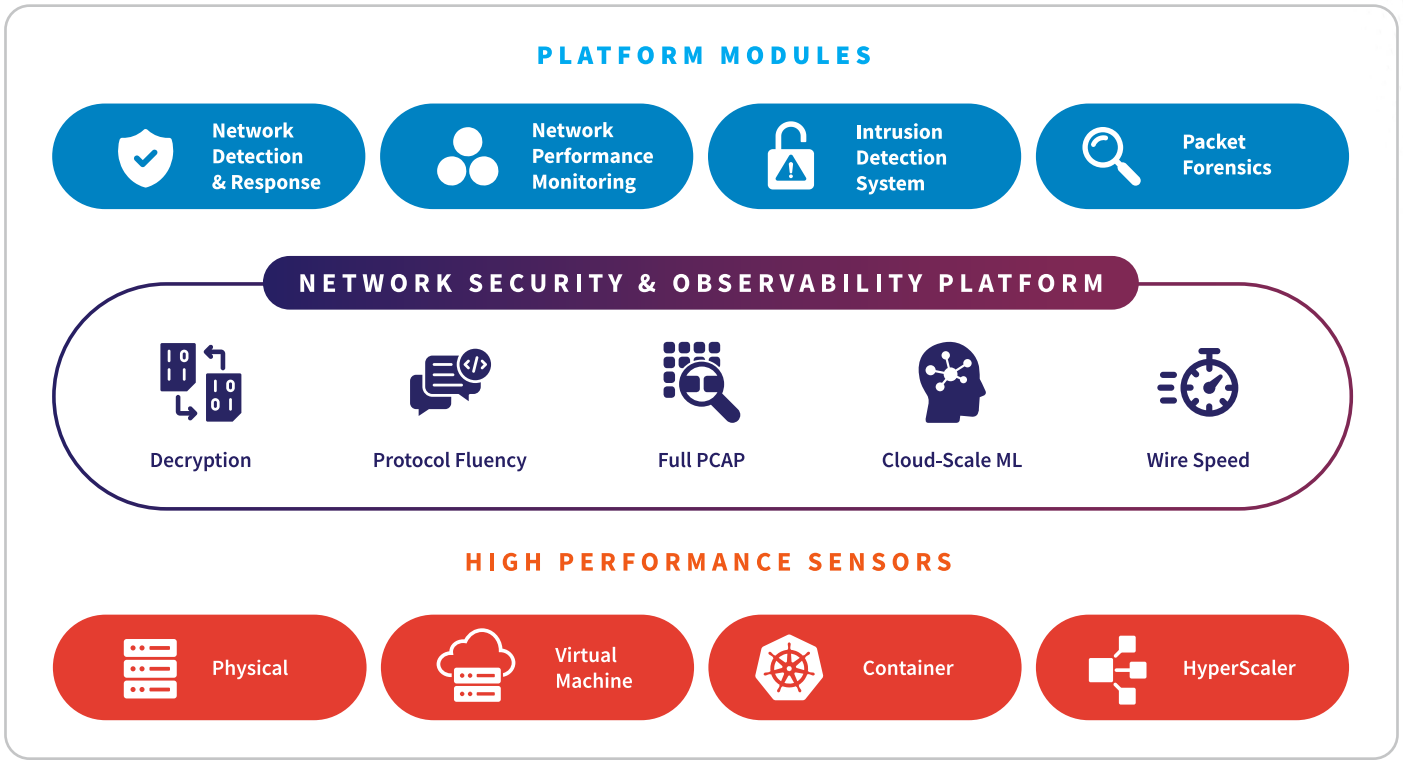
ExtraHop RevealX provides the unalterable ground truth required to secure and optimize the global digital backbone. By analyzing every packet at line rate up to 100 Gbps, RevealX eliminates the visibility gaps that traditional security tools ignore in high-velocity carrier and cloud environments. In an industry where a single second of latency or a core network outage can impact millions of users and disrupt national infrastructure, RevealX delivers the real-time insights needed to maintain service availability and institutional trust.

The platform solves the agent blind spot by providing agentless, passive monitoring of over 90+ protocols. This ensures that critical infrastructure components like 5G small cells, edge compute nodes, and specialized telecommunications hardware are fully visible without risking system stability or introducing performance overhead. By baselining normal behavior across these unmanaged devices, security teams can instantly detect anomalies that indicate an adversary has established a foothold within the signaling plane or a distributed cloud gateway.

To counter geopolitically motivated sabotage, RevealX identifies subtle shifts in network behavior that signify lateral movement from corporate IT into the core routing heart of the network. By exposing hidden threats within encrypted management traffic using strategic decryption, the platform stops attackers before they can manipulate BGP tables or compromise DNS integrity. This visibility extends to the managed service ecosystem, where RevealX monitors the integrity of provider-to-client connections to prevent administrative hijacks and supply chain contagion from reaching downstream enterprise customers.

Beyond threat detection, RevealX accelerates incident response to meet the rigorous continuous monitoring and reporting requirements of NIS2 and CIRCIA. It provides a definitive forensic record of all network transactions, which eliminates the guesswork during investigations and allows for rapid root-cause analysis of both security breaches and performance degradations. This unified approach bridges the gap between the SOC and the NOC by combining security detection with deep performance metrics. By monitoring the health of critical transaction paths, RevealX ensures that security measures do not introduce latency, protecting the speed and reliability of the global IT and telecommunications architecture.

ExtraHop NDR Platform



NDR Technology Use Cases for the IT and Telecommunications Industry

Nation-State Attacks	Detects lateral movement and exfiltration in long-term campaigns targeting global core routing, BGP stability, and undersea cable landing stations.
Threat Detection & Response	Investigates hidden threats across converged IT and carrier environments, filling visibility gaps in the Signaling Plane and OSS/BSS where agents cannot be deployed.
Threat Hunting	Leverages behavioral baselining to find signature-less threats and protocol anomalies before they impact 5G/6G core availability or roaming interconnects.
SOC Modernization	Unifies SOC and NOC workflows with AI prioritization to manage carrier-grade telemetry, accelerating response times for critical infrastructure service delivery.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of signaling and management protocols like SS7, Diameter, and DNS for one-click root-cause analysis.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots from corporate IT environments toward critical core network segments and signaling gateways.
Cloud Workload Security	Provides agentless visibility for virtualized and cloud-native network functions (VNF/CNF), discovering shadow IT and unmanaged assets across multi-cloud environments.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value administrative portals, jump hosts, and network management systems.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of subscriber data or total paralysis of billing and provisioning systems.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including 5G small cells, IoT edge gateways, and specialized hardware that cannot host security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy infrastructure, routers, and carrier-grade switches.
AI Security	Monitors generative AI and autonomous agents used for network optimization, traffic engineering, or predictive maintenance in containerized workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that 5G network slicing, micro-segmentation, and hardware-security-zone policies are effective.

NPM Technology Use Cases for the IT and Telecommunications Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for factory floor automation and PLC-to-HMI sessions.
Operational Resilience	Resolves infrastructure degradation before it hits production continuity, ensuring availability through proactive monitoring of mission-critical SCADA services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between plant operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during MES or ERP migration by auto-mapping dependencies and using OT baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for IIoT gateways and supply chain APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past production outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols (e.g., Modbus, EtherNet/IP), providing real-time insights into command processing time vs. network latency.

IT and Telecommunications Industry Compliance & Regulatory Use Cases

Operational Resilience	EU	NIS2 Directive	Resilience Validation: Maps dependencies for essential IT and telco services and validates impact tolerance during cyber events to ensure service continuity.
Incident Reporting	US	CIRCIA	Mandatory Reporting: Powers the ability to identify, scope, and report covered cyber incidents within the 72-hour window using unalterable forensic evidence.
Infrastructure Security	US	SEC Cybersecurity Disclosure	Materiality Assessment: Provides the wire data evidence needed to determine the materiality of an incident and satisfy public disclosure requirements.
Data Privacy	Global	ePrivacy / GDPR	Signaling Privacy: Audits access to signaling metadata and subscriber records, providing the forensic documentation required for rigorous privacy compliance audits.
5G Security Excellence	Global	GSMA FS.31 / NESAS	Audit Compliance: Provides continuous monitoring of the 5G core to detect unauthorized changes and confirm the integrity of 3GPP-defined security functions.
National Security	Global	NIST SP 800-53	System Integrity: Identifies lateral movement and unauthorized remote access, bypassing traditional perimeter gates in critical communication infrastructure.

Customer Benefits: Ensuring Service Resilience and Operational Continuity Across the Digital Backbone

ExtraHop RevealX delivers tangible business outcomes for IT and telecommunications leaders by transforming complex network data into actionable intelligence. Organizations achieve immediate ROI through the consolidation of security and performance monitoring into a single platform. This reduces operational overhead and improves collaboration between the SOC and NOC teams responsible for maintaining global connectivity.

A primary benefit is the significant reduction in mean time to detect (MTTD) and mean time to respond (MTTR) to infrastructure threats. By providing unalterable ground truth across core networks and distributed edge environments, RevealX ensures that security teams can identify lateral movement before it impacts critical signaling or subscriber services. This proactive stance protects brand reputation and prevents the massive financial losses associated with service outages or nation-state sabotage of core routing infrastructure.

Furthermore, RevealX simplifies the complexity of 2026 regulatory compliance. The platform automates the data collection required for NIS2, CIRCIA, and SEC reporting, allowing organizations to meet strict 72-hour incident notification windows with confidence. By maintaining continuous visibility into unmanaged 5G nodes and edge compute assets, providers can prove the integrity of their digital perimeters to auditors and partners. Ultimately, RevealX secures the global flow of data by ensuring that the digital infrastructure supporting the modern economy remains resilient and visible.

> "You can't secure what you can't see. With ExtraHop, we've got eyes on every interaction that takes place on our network. That is the first step to protecting our environment."
>
> **SENIOR CYBER SECURITY ENGINEER**
> Large Wireless Telecommunications Company

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 the IT and telecommunications industry: Global Telecommunications Provider

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