EXTRAHOP

Strengthening Operational Resilience and Protecting Policyholder Trust in the Insurance Sector

Keep Critical Insurance Applications and Processes Free from Threats and Disruption with ExtraHop RevealX™

Industry Challenges: From Actuarial Risk to Digital Fragility

The insurance sector is the ultimate arbiter of risk, yet it faces an era where digital infrastructure is a primary target for systemic disruption. As insurers pivot toward active insurance models and cloud-native processing, the attack surface has expanded. By 2026, cybersecurity will be a core component of solvency and trust. As the digital and physical worlds of insurance merge, institutions face several critical friction points:

- **The Escalation of Nation-State and Destructive Attacks:** Geopolitically motivated actors have moved beyond data theft to the active paralysis of financial safety nets. In early 2026, a coordinated campaign targeted global reinsurance settlement networks, attempting to manipulate underwriting algorithms and suppress historical claims data. These adversaries target the integrity of core ledger systems, which can trigger liquidity crises. Protecting these transactions requires absolute internal visibility to contain lateral movement before destructive commands execute across the underwriting core.
- **The GenAI-Powered Fraud and Identity Crisis:** Generative AI has reached a tipping point for claims integrity. In 2026, an estimated 25% of digital claims involve synthetic media, including deepfake witness statements or fabricated medical reports. These "perfect lies" bypass traditional document-level security and authentication. Insurance firms must identify this post-compromise behavior on the wire to prevent mass fraudulent payouts or the exfiltration of policyholder NPI before they enter the global banking network.
- **The Visibility Gap in Legacy and Hybrid Infrastructures:** Modern insurance firms rely on a mix of legacy mainframes, cloud workloads, and autonomous AI agents. These environments use unmanaged assets and third-party API connections that cannot host security agents, leaving them invisible to standard EDR defenses. This agent blind spot is a primary target for ransomware groups who exploit edge vulnerabilities to move toward sensitive actuarial records. Maintaining sub-second quote speeds requires a unified approach that secures the entire transaction path.
- **Regulatory Rigor and the Mandate for Operational Resilience:** Regulatory mandates have shifted focus from data privacy to impact tolerance. The Digital Operational Resilience Act (DORA) and the April 2026 certification deadline for NYDFS Part 500 now require insurers to prove continuous behavioral monitoring across their entire infrastructure. Meeting these standards while processing high-volume claims requires a definitive source of truth that can reconstruct security events. Carriers must provide verifiable proof of monitoring to maintain insurance-grade security and protect their solvency.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all interactions by decrypting and decoding 90+ protocols at 100 Gbps to protect high-volume underwriting engines and claims processing platforms.

The Definitive Data Source for the AI-Enabled SOC

Provides high-fidelity wire data to power the next generation of insurance SOC automation and defenses, delivering unalterable ground truth to eliminate investigative friction.

AI-Powered Cyber Threat Detection

Identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting actuarial databases and policyholder NPI using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers every asset, from legacy mainframes to autonomous AI agents and cloud workloads, without installing software or impacting transaction latency.

Strategic Line-Rate Decryption

Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats within secure underwriting transfers and proprietary claims APIs.

High-Fidelity Performance Metrics

Troubleshoots service disruptions using 5,000+ wire data metrics for deep operational insight into network latency and digital distribution application performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy audit requirements for DORA, NYDFS 500, and the NAIC Model Data Security Law.

The Solution: RevealX Network Intelligence

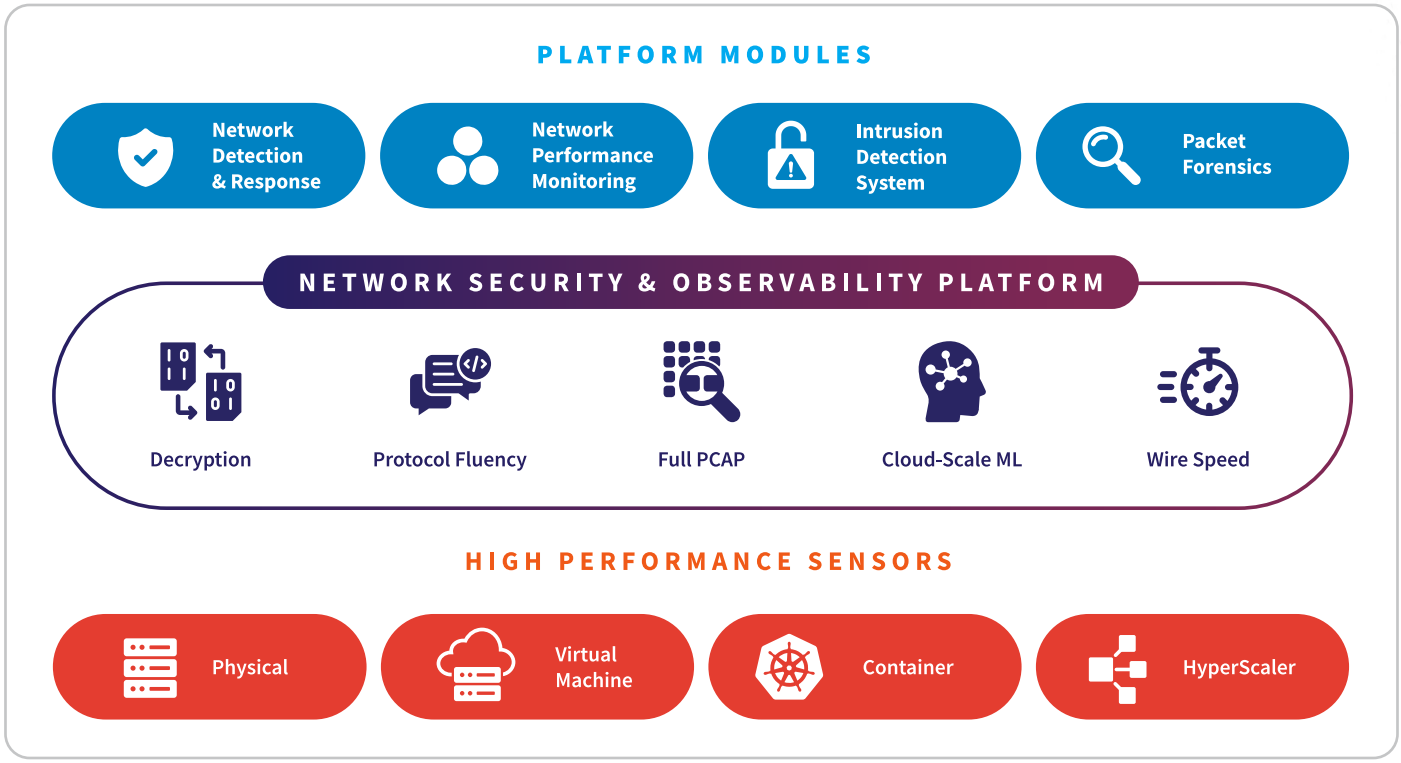
ExtraHop RevealX provides the unalterable ground truth required to secure the global insurance ecosystem. By analyzing every packet at line rate up to 100 Gbps, RevealX eliminates the visibility gaps in both modern cloud-native underwriting platforms and legacy claims systems. In an industry where trust is the core product and a service outage can trigger immediate policyholder churn, RevealX delivers the real-time insights needed to maintain operational continuity and defend the "Insurance Promise." The platform turns the network into a definitive record of truth, allowing security teams to see everything happening across their infrastructure without the need for intrusive agents.

The platform solves the agent blind spot by providing agentless, passive monitoring of over 90 protocols. This ensures that critical infrastructure, from the autonomous AI agents used for risk assessment to the legacy back-office systems that still power core policy administration, is fully visible without risking system stability. By baselining normal behavior across these diverse environments, security teams can instantly detect anomalies that indicate an adversary is attempting to manipulate actuarial data or has established a foothold in the claims settlement pipeline. This level of visibility is essential for identifying the "living off the land" tactics used by sophisticated actors who seek to blend in with legitimate administrative traffic.

To counter strategic extortion and GenAI-powered fraud, RevealX identifies subtle shifts in network behavior that signify the staging of sensitive policyholder data for exfiltration. By exposing hidden threats within encrypted management traffic using strategic decryption, the platform stops attackers before they can pivot from general office zones into the high-value underwriting core. This visibility extends to the broader insurance supply chain, where RevealX monitors the integrity of connections to reinsurers and third-party administrators to prevent supply-chain-borne contagion. The ability to inspect TLS 1.3 traffic at scale ensures that attackers cannot hide malicious payloads within encrypted API calls or secure cloud-integrated claims workflows.

Beyond threat detection, RevealX accelerates incident response to meet the rigorous 72-hour reporting requirements of DORA, NYDFS 500, and the NAIC Model Law. 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 digital operations teams 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 modern insurance experience.

ExtraHop NDR Platform



NDR Technology Use Cases for the Insurance Industry

Nation-State Attacks	Detects lateral movement and exfiltration in long-term campaigns targeting actuarial IP, policyholder portfolios, and reinsurance settlement networks.
Threat Detection & Response	Investigates hidden threats across converged IT and legacy environments, filling visibility gaps in claims management systems (CMS) and policy administration systems (PAS).
Threat Hunting	Leverages behavioral baselining to find signature-less threats and anomalies before they impact underwriting integrity, claims processing, or actuarial modeling.
SOC Modernization	Unifies SOC and claims operations workflows with AI prioritization to reduce alert fatigue, accelerating response times for critical financial infrastructure.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of API transactions and database queries for one-click root-cause analysis of system outages or fraudulent payouts.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots bypassing perimeters toward restricted actuarial zones, NPI segments, and core ledgers.
Cloud Workload Security	Provides agentless visibility for cloud-hosted underwriting simulations and subscriber portals, discovering shadow IT across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value administrative portals, policy administration systems, and jump hosts.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of policyholder NPI or total paralysis of claims settlement.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including digital signage, IoT sensors in telematics-enabled vehicles, and unauthorized edge gateways.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled or missing on legacy mainframes and specialized actuarial workstations.
AI Security	Monitors generative AI agents used for claims triage, fraud detection, and autonomous underwriting to ensure they remain within defined security parameters.
Operationalizing Zero Trust	Acts as the independent observer in the Zero Trust Architecture loop. It detects policy drift and provides empirical proof that internal network segmentation policies are effective.

NPM Technology Use Cases for the Insurance Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for time-critical underwriting engines and claims processing.
Operational Resilience	Resolves infrastructure degradation before it hits service continuity, ensuring availability through proactive monitoring of mission-critical CMS and PAS applications.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between digital operations (app owners) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during core system migration, such as Guidewire to Cloud, by auto-mapping dependencies and using baselines to validate delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for subscriber portals and claims intake 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, providing real-time insights into transaction processing time versus network latency in high-volume hubs.

Insurance Industry Compliance & Regulatory Use Cases

Rapid Materiality Assessment	EU	DORA	Resilience Validation: Maps dependencies between critical insurance services and validates impact tolerance during cyber events to ensure continuity.
Continuous Security Monitoring	Global	NIST CSF 2.0 (DORA Support)	Detection & Response: Powers Detect (DE) and Respond (RS) functions to spot anomalies and scope "blast radius" within insurance networks in real time.
Personal Data Attribution	US (NY)	NYDFS Part 500	Mandatory Certification: Provides the continuous monitoring and audit trails required for 72-hour reporting and the annual certification deadline.
Technical Proof of Monitoring	Global	NIST SP 800-53 (NYDFS Alignment)	Control Verification: Provides continuous monitoring (CA-7) to detect unauthorized changes and confirm the integrity of insurance security operations.
Risk Detection and Response	US	NAIC Model Law	NPI Safeguarding: Audits access to nonpublic information (NPI) and provides forensic documentation required for state insurance commissioner audits.
Operational Resilience	Global	NIST SP 800-53 (NAIC Alignment)	System Integrity (SI): Identifies lateral movement and unauthorized remote access, bypassing traditional perimeters to protect policyholder records.

Ensuring Operational Resilience and Protecting Policyholder Trust

ExtraHop RevealX delivers tangible business outcomes for insurance leaders by transforming network noise into a definitive record of truth. 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 digital operations teams responsible for maintaining underwriting integrity and claims processing velocity.

A primary benefit is the protection of the industry's most critical assets, policyholder trust and actuarial IP. By providing unalterable ground truth across hybrid environments, RevealX ensures that security teams can identify GenAI-powered fraud and destructive attacks before they impact the bottom line. This proactive defense helps insurers maintain favorable loss ratios and secure better terms in the 2026 reinsurance market.

Furthermore, RevealX simplifies the complexity of global regulatory compliance. The platform automates the data collection required for DORA and the strict April 15, 2026, certification deadline for NYDFS Part 500. By maintaining continuous visibility into unmanaged assets and agentic AI workflows, carriers can prove operational resilience to regulators and policyholders alike. Ultimately, RevealX transforms cybersecurity into a strategic asset that protects brand reputation while supporting the solvency and reliability required in a competitive market.

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 insurance industry:
Leading US Healthcare Insurance Provider

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

> "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**

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