EXTRAHOP

Securing Global Engagements and Safeguarding Client Trust in the Professional Services Sector

Keep Critical Professional Services and Client Engagements Free from Threats with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: Protecting the Intellectual Capital and Client Trust Ecosystem

Global professional services firms operate where intellectual property and client trust are the primary products. In this high-stakes sector, digital friction does not simply slow operations. It erodes the foundational confidence required for legal, financial, and strategic consulting. By 2026, the industry will have shifted toward proprietary AI models and API-first collaboration that accelerates innovation but creates an opaque attack surface. A single vulnerability in a partner portal or a compromised OAuth token can now jeopardize sensitive data across thousands of global clients simultaneously.

As lines between professional services firm networks and client environments disappear, several critical failure points emerge:

- **The Escalation of Nation-State and Destructive Attacks:** Geopolitically motivated actors have moved beyond simple data theft toward functional destruction and strategic paralysis. These adversaries target the integrity of M&A negotiations, proprietary legal strategies, and lobbying intel to manipulate market outcomes. Protecting these assets requires internal visibility to contain lateral movement before destructive commands reach document management systems or sensitive case files where the firm's most valuable client secrets reside.
- **The Reality of Conduit Risk and Identity Sprawl:** Consulting firms face significant conduit risk, where attackers compromise the firm to gain trusted, privileged access to downstream client environments. This is exacerbated by project-specific cloud sprawl and the explosion of service accounts that often remain overprivileged and unmonitored after an engagement ends. Attackers exploit these unmonitored lateral paths to navigate from employee office suites into high-value customer environments, using the firm's legitimate connectivity as a Trojan horse.
- **The Visibility Gap in Distributed Architectures:** Modern firms rely on thousands of third-party APIs and work-from-anywhere workflows that traditional security agents cannot monitor. This gap is exacerbated as attackers prioritize disabling EDR tools immediately upon entry to hide their movements. Organizations must now detect post-compromise activity, such as token abuse or unauthorized data staging, directly on the wire before client exfiltration or service disruption begins.
- **Regulatory Rigor and Contractual Liability:** 2026 mandates have compressed the timeline for incident response. Beyond SEC rules requiring 4-day material disclosure, firms face increasingly strict master service agreements (MSAs) from clients that demand proof of continuous, real-time behavioral monitoring. Meeting these standards requires a unified approach that provides a definitive forensic record of all network interactions to prove data integrity and maintain compliance.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors network interactions by decrypting and decoding 90+ protocols at 100 Gbps to protect high-volume document management and client portal operations.

The Definitive Data Source for the AI-Enabled SOC

Powers professional services SOC automation with unalterable wire data, eliminating investigative friction to accelerate detection and remediation.

AI-Powered Cyber Threat Detection

Uses machine learning to detect attacks and lateral movement targeting critical client data, M&A strategies, and intellectual property.

Unified Agentless Visibility

Discovers every asset, including unmanaged IoT and cloud workloads, without installing software or risking billable system stability.

Strategic Line-Rate Decryption

Analyzes TLS 1.3 and PFS to expose hidden threats without adding latency to time-sensitive client transactions and advisory services.

High-Fidelity Performance Metrics

Troubleshoots complex disruptions using 5,000+ metrics for deep insight into application latency and billable service performance.

Continuous Forensic Capture

Maintains an unalterable record to satisfy SOC 2, ISO 27001, and NIS2 mandates, accelerating root-cause analysis for confidentiality.

The Solution: RevealX Network Intelligence

ExtraHop RevealX provides the network intelligence required to secure sensitive client data, protect high-value intellectual property, and ensure the continuity of global engagements. By delivering a unified view of the hybrid environment, RevealX enables security and network teams to detect sophisticated threats and ensure service availability for mission-critical applications such as document management systems and partner portals.

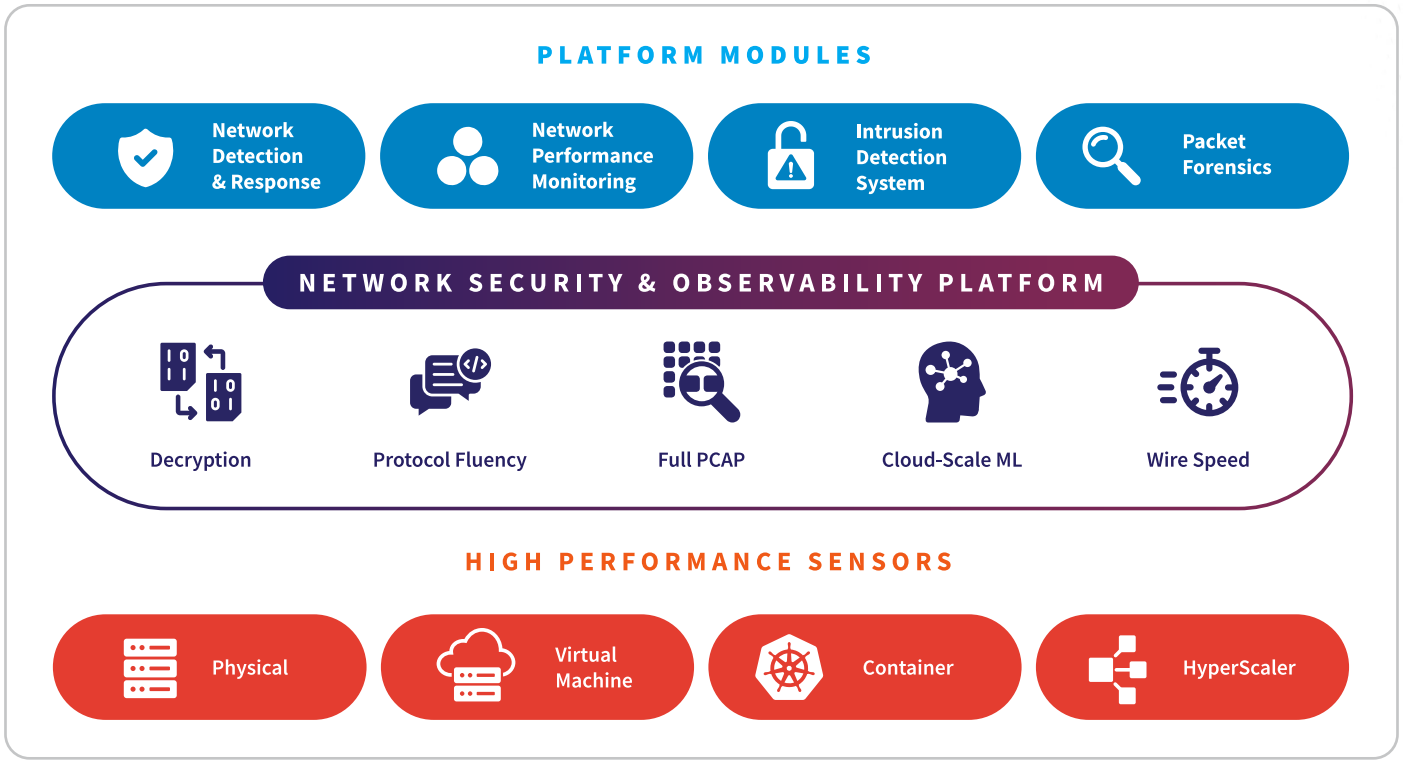
Neutralizing destructive nation-state threats requires intercepting actors before they execute malicious commands on high-value assets. By monitoring the wire instead of relying on vulnerable agents, RevealX detects the subtle lateral movement and credential abuse used to pivot from corporate offices into production environments. This agentless approach identifies anomalous behavior in real time, even if a third-party maintenance connection or an unmanaged IoT device is compromised. Security teams can quickly isolate affected segments to preserve engagement continuity and protect sensitive client strategies from large-scale disruption.

Securing workloads across the edge, core, and cloud requires RevealX to monitor all network interactions by decrypting and decoding over 90 protocols at speeds up to 100 Gbps. This delivers complete visibility and intelligent response. Because RevealX utilizes out-of-band monitoring, it remains a persistent source of truth even when attackers disable or evade EDR agents. This strategy is essential for securing unmanaged devices and legacy infrastructure that cannot host traditional security software.

As a leader in AI-driven NDR, ExtraHop utilizes cloud-scale machine learning to identify sophisticated attacks that evade signature-based tools. By establishing baseline behavior for every entity and user, our AI identifies living-off-the-land tactics. A key differentiator is the ability to perform line-rate decryption of TLS 1.3, ensuring attackers cannot hide lateral movement or credential abuse within encrypted traffic. This allows RevealX to provide the independent observation required for a zero trust architecture.

By integrating NDR and NPM, RevealX helps eliminate the silos between SOC and NOC workflows. Teams can troubleshoot issues ranging from portal latency to active ransomware staging before data exfiltration occurs. This unified approach allows firms to enforce strict segmentation policies and manage a robust security posture across distributed environments. With high-fidelity wire data, organizations ensure continuous compliance with 2026 mandates, including SOC 2 Type II, ISO 27001, and NIS2 updates.

ExtraHop NDR Platform



NDR Technology Use Cases for the Professional Services Industry

Nation-State Attacks	Detects lateral movement and exfiltration to stop campaigns targeting M&A strategies, litigation drafts, and intellectual property.
Threat Detection and Response	Proactively investigates hidden threats across hybrid environments to find what logs miss in document management systems and partner portals.
Threat Hunting	Uncovers stealthy threats using behavioral baselines to stop anomalies before they impact high-value engagements or proprietary consulting models.
SOC Modernization	Unifies SOC and NOC workflows and uses AI-powered prioritization to accelerate response times for global professional service delivery teams.
Incident Response and Investigation	Provides forensic-level visibility for root-cause analysis and maintains unalterable records of sensitive client files and privileged communications.
Lateral Movement	Identifies internal movement via peer-group clustering to catch pivots toward document repositories or sensitive financial databases.
Cloud Workload Security	Delivers agentless visibility to defend cloud-integrated productivity workloads and discover shadow IT across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates behavior with IAM to unmask credential abuse in real time, protecting high-value partner and administrator accounts.
Ransomware Attacks	Identifies early-stage ransomware patterns to isolate hosts before exfiltration of sensitive client data or proprietary source code.
Unmanaged Devices	Monitors traffic directly to fill the visibility gap for unmanaged assets, like conference systems, where agents cannot be installed.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity even if agents are disabled, ensuring visibility across legacy infrastructure and unmanaged workstations.
AI Security	Monitors generative AI platforms used for document review and contract analysis to prevent exploitation and service disruption.
Operationalizing Zero Trust	Acts as an independent observer in the zero trust loop to detect policy drift and validate internal segmentation for client files.

NPM Technology Use Cases for the Professional Services Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions. Provides clear visibility into latency and throughput for global collaboration platforms and remote client advisory sessions.
Operational Resilience	Reduces disruption impact by resolving infrastructure degradation before it hits billable service continuity. Ensures availability through proactive monitoring of mission-critical document management services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow from metrics to packets, eliminating friction between global IT teams and application developers.
Migrate Workloads to the Cloud	Maintains performance during DMS migration by auto-mapping dependencies and using on-premises baselines to validate successful cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps. Ensures performance for crown-jewel services like API-driven billing systems and client-facing portals.
Forensic-Grade Investigations	Combines metadata with scalable PCAP for an unalterable record, enabling deep-dive analysis into past service outages or intermittent portal degradations.
Application Performance Monitoring	Complements APM by filling network-layer gaps. Decodes 90+ protocols to provide real-time insights into database response times versus network latency for rapid search.

Professional Services Industry Compliance & Regulatory Use Cases

Materiality Assessment	US	SEC / CIRCIA	Enables rapid forensics into SaaS and token abuse to assess breach materiality within mandatory 4-day (SEC) or 72-hour (CIRCIA) disclosure windows.
Continuous Security Oversight	Global	SOC 2 (Type II)	Satisfies CC7.2 and CC7.3 criteria by providing 24/7 monitoring of production environments and providing unalterable audit trails for security and confidentiality audits.
Supply Chain Resilience	EU	NIS2	Supports critical digital service providers by monitoring update channels and detecting lateral movement. Provides forensic evidence required for rapid regulatory incident disclosure.
Data Privacy Attribution	Global	GDPR / CCPA	Speeds up notification by attributing data access paths. Provides forensic proof of breach scope to protect client PII and minimize potential fines.
Information Security Management	Global	ISO 27001	Provides technical proof of continuous network monitoring for unauthorized activity and internal data movement, addressing Annex A 8.16 and 8.12 requirements.
Professional Confidentiality	US / Regional	ABA 477R	Validates the integrity of electronic communications. Monitors for unauthorized access to privileged client information to meet professional ethics and confidentiality mandates.

Customer Benefits: Ensuring Resilience and Client Trust

Visibility into network truth is the foundation for modern professional services protection. ExtraHop RevealX provides the real-time insights required for global collaboration, secure client portals, and sub-second transaction speeds. By monitoring the wire, firms safeguard against threats and protocol anomalies that jeopardize engagement uptime, billable productivity, and brand reputation.

The shift to cloud-native architectures and AI-integrated workflows creates agility but introduces exploitable blind spots. RevealX secures distributed microservices and complex supply chains by observing actual traffic instead of modifiable logs. This provides the definitive forensic evidence needed to satisfy global mandates like SOC 2 Type II, ISO 27001, and the SEC four-day disclosure rule.

RevealX also protects the unmanaged ecosystem of IoT devices and non-human identities that agent-based tools miss. It identifies lateral movement and credential abuse before they compromise sensitive case files or exfiltrate proprietary M&A strategies. Through continuous, real-time discovery and classification, RevealX ensures that critical advisory services and high-value client data remain uninterrupted.

> "ExtraHop has fundamentally changed the way that we monitor and manage the business."
>
> **DIRECTOR OF IT**
> Leading Professional Services 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:
Home Depot
Ulta Beauty
Seattle Children's Hospital

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