EXTRAHOP

CUSTOMER STORY

Leading Global Financial Services Provider

Financial Services Leader Ends Operational Silos and Modernizes Global Security Infrastructure

A leading financial services provider faced critical operational inefficiencies driven by a fragmented security and networking architecture. Relying on a patchwork of legacy tools, the organization operated in isolated silos, resulting in visibility gaps that increased both risk and mean time to resolution (MTTR). As part of an aging infrastructure renewal, the company deployed ExtraHop RevealX NDR to break down these silos and modernize its environment. By providing a single source of truth across the entire hybrid network, RevealX consolidated disparate operations into a unified system. This transition empowered security and IT teams with line-rate decryption and real-time network intelligence, closing critical detection gaps and streamlining compliance in a highly regulated financial landscape.

The company selected the ExtraHop RevealX platform after an extensive proof of concept (POC) involving multiple internal teams, achieving the following strategic outcomes:

- **Platform consolidation and tool rationalization:** The company successfully decommissioned and replaced multiple legacy solutions, including an XDR and SIEM platform, an IDS/IPS, a first-generation NDR solution, and a network performance monitoring and diagnostics (NPMD) product into a single integrated platform.
- **Unified operations and visibility:** The deployment bridged the networking and security teams for the first time, establishing a shared culture of rapid incident resolution and providing enterprise-wide visibility across multiple locations worldwide.
- **Enhanced card transaction integrity:** ExtraHop provided specialized inspection for custom card transaction protocols, securing core financial flows against sophisticated, high-level threats.
- **Optimized customer and user experience:** The platform reduced troubleshooting latency for the customer support experience (CSX), accelerating response times for critical internal applications.

The Challenge: Eliminating Visibility Gaps and Operational Silos

As one of the world's most successful financial services providers, this company operates a high-volume environment that demands flawless execution against high-level threats. However, the existing technical landscape presented several core challenges:

Disparate Solution Fragmentation: The company struggled with multiple different legacy tools to support its primary use cases. This fragmentation led to product redundancy and high maintenance costs, preventing the team from achieving a simplified technical environment through product rationalization.

Siloed Operating Teams: Network and security operations functioned in disparate silos with minimal communication. This lack of integration delayed incident response and made it difficult to establish a single source of truth during critical outages or security events.

Visibility Gaps in Critical Infrastructure: The legacy architecture lacked adequate coverage for east-west traffic, leaving the company blind to internal lateral movement. Furthermore, troubleshooting the hundreds of backend systems supporting the Customer Care Professional (CCP) applications took too much time, negatively impacting the customer journey.

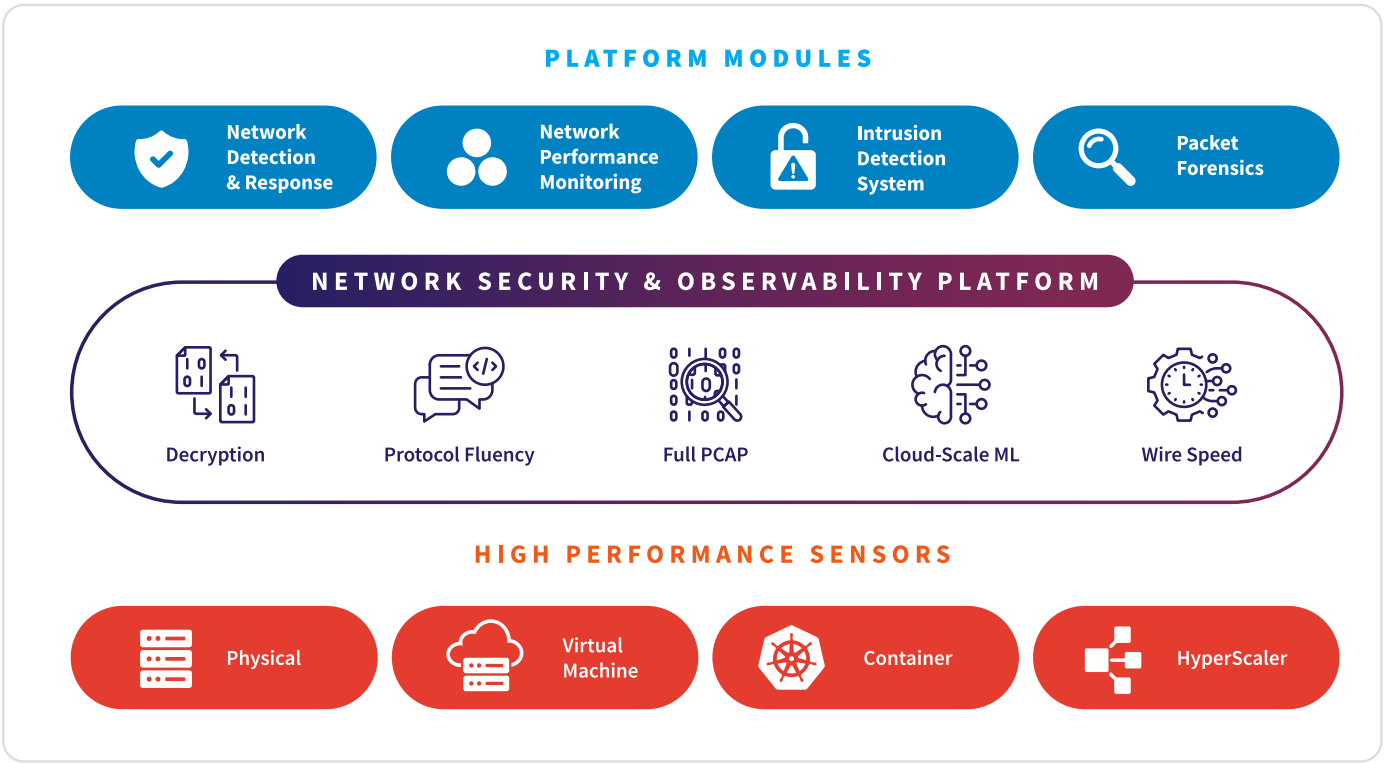
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully provided the agentless network security solution required for global deployments, proving its ability to provide unified security coverage that met the company's high-stakes security requirements. The modern NDR platform enabled the SOC to achieve transformative efficiency. ExtraHop was uniquely compelling due to its ability to passively monitor network traffic without requiring software deployment on constantly rotating, unmanaged devices.

The key outcomes and advantages delivered to the company include:

- **Unrestricted visibility and decryption:** The financial services leader 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 reduced the SOC's operational burden by providing high-fidelity, low-noise detections. This shift allowed analysts to move their 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 financial services leader 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 financial services leader achieved immediate, transformative security improvements and operational stability following the deployment of the ExtraHop NDR platform.

Deep Global Deployment Excellence: The company successfully completed a massive implementation across multiple global sites, including key financial centers worldwide. This rollout provided the first-ever unified view of the global network.

Accelerated Mean Time to Resolution: By reducing latency for the internal applications used for the CSX, the team dramatically improved the efficiency of support journeys. The platform provides immediate evidence of detected threats and performance bottlenecks, enabling improvement of the CSX for the network team.

Successful Tool Decommissioning: The company realized significant ROI by rationalizing its product stack. By displacing multiple legacy vendors with a single platform, the company simplified its technical environment and reduced the labor and software costs required to manage disparate security tools.

Bridged Organizational Divide: The deployment successfully unified the network and security teams. These groups now collaborate using a single source of network truth, allowing for proactive risk reduction and more effective threat hunting across the entire enterprise.

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