EXTRAHOP

CUSTOMER STORY

Financial Institution Secures Critical Assets and Streamlines SOC Operations by Replacing Legacy Network Tools

A leading commercial bank replaced legacy security tools with ExtraHop RevealX™ to close critical east-west visibility gaps. By automating ransomware detection and integrating with CrowdStrike, the bank transformed manual forensics into real-time insights. This modernization protected mission-critical financial assets and significantly increased SOC efficiency across all branches and data centers.

The bank selected the ExtraHop RevealX NDR platform over two other leading NDR competitors to modernize its security posture, successfully delivering:

- **Real-Time Ransomware Defense:** ExtraHop uses advanced machine learning to identify ransomware activity, data staging, and theft in real time.
- **Streamlined SOC Operations:** By eliminating manual forensic data collection, the security team achieves insights in minutes rather than days.
- **Push-Button Ecosystem Integration:** The platform provides a seamless integration with CrowdStrike to create a unified source of truth.
- **Complete Asset and Protocol Visibility:** The bank achieved continuous monitoring of assets, including the ability to auto-discover devices and track expiring certificates.

The Challenge: Automated Protection and Operational Efficiency

Operating a leading commercial bank requires high-performance network reliability and flawless execution. However, the existing technical landscape presented several core challenges that left financial services vulnerable.

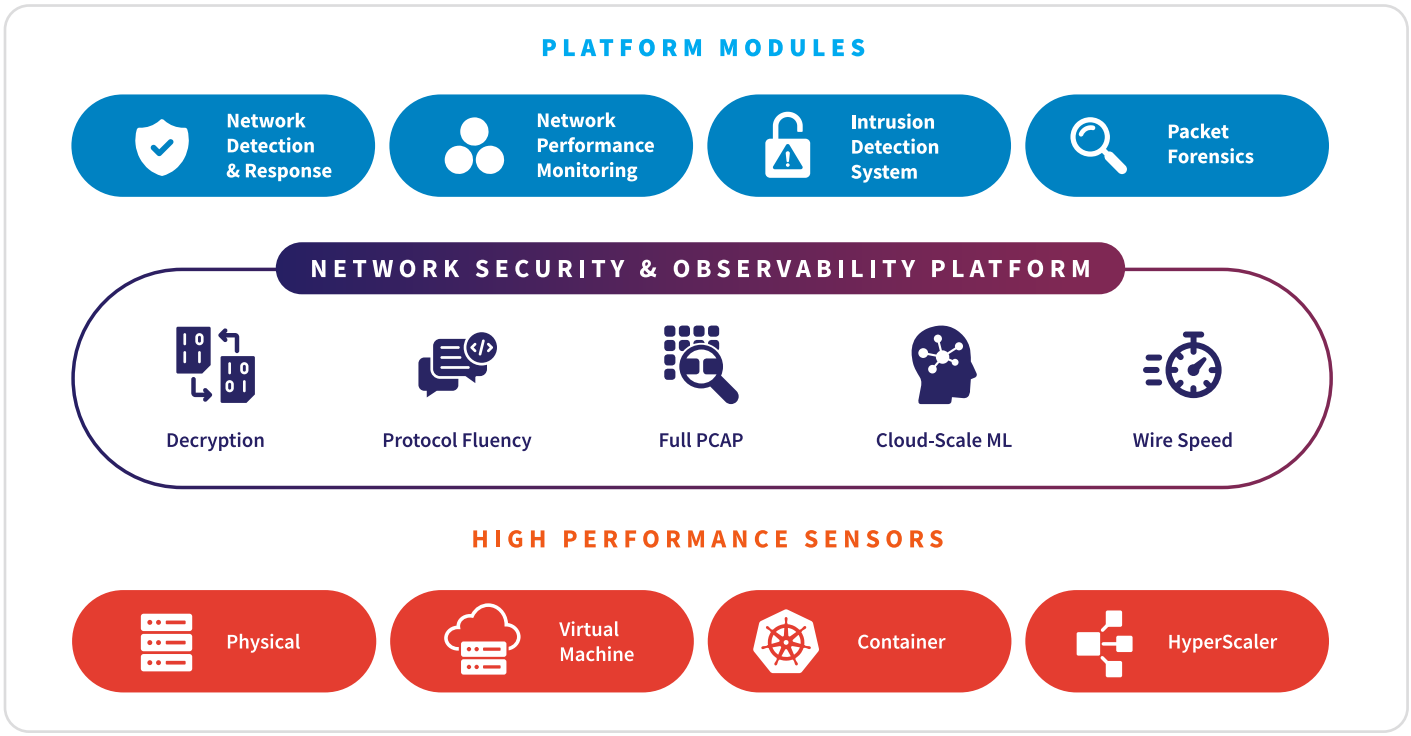
Critical Visibility Gaps and Reactive Defense	The bank lacked east-west visibility into real-time network threats. It relied on a legacy approach that required manual data collection only after issues were detected. This delay left the bank vulnerable to network-based ransomware, data exfiltration, and lateral movement across its critical data center services.
Invisible Vulnerabilities and Insecure Protocols	The security team had no insight into insecure protocols or the specific servers using them. There was no centralized system to track expiring certificates. These architectural gaps hid potential vulnerabilities that could be exploited to compromise the branch and data center network.
Manual Forensic Burdens and Fragmented Workflows	Investigating threats was a slow process involving complex data collection across various networks and virtualization tools. These fragmented workflows hindered coordination between security and operations teams. The bank needed a unified platform to correlate network anomalies and reduce the labor costs associated with manual troubleshooting.

The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully displaced the incumbent NDR vendor by proving its ability to provide unified security coverage. The platform met the bank's strict performance and scalability requirements while delivering the following advantages:

- **Unrestricted visibility and decryption:** The bank 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 lifted the SOC's operational burden because it provided high-fidelity, low-noise detections. This shift allowed analysts to move 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 bank 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 bank 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: Automated Protection and Operational Efficiency

The bank achieved immediate, transformative security improvements and significant labor savings following the deployment of the ExtraHop RevealX NDR platform.

Decisive Platform Selection

The bank successfully selected ExtraHop over two other leading NDR vendors. This move fixed critical east-west visibility gaps and unmanaged asset blind spots while solving long-standing manual forensic issues.

Gained Mission-Critical Asset Protection

ExtraHop provided essential visibility for sensitive financial databases and applications. This allowed the bank to proactively protect core banking services and identify ransomware activity, data staging, or theft without compromising system performance.

Maximized SOC Focus

The bank achieved a substantial reduction in manual labor with machine learning detections. This empowered analysts to shift focus from manual data collection to high-priority incident investigation and proactive threat hunting in minutes rather than days.

Closed Integration Gaps

The new platform closed all coordination gaps via a push-button CrowdStrike integration. This established a single source of network truth that provides seamless data feeds and transactional record retention for the bank's security and operations teams.

Unified Operational Control

For the first time, the bank gained a scalable and holistic security solution across its entire branch and data center network. This provided continuous monitoring of all devices and insecure protocols to ensure that hidden network threats are identified in real time.

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