EXTRAHOP

CUSTOMER STORY

Leading Global Payments and Financial Technology Provider

Payments Leader Cuts Incident Response from Hours to Minutes

A leading global payments and financial technology provider that moves trillions of dollars and processes a large percentage of all credit card transactions, confronted a critical security gap in its infrastructure. The organization maintained no network detection and response (NDR) solution in place for its core payment infrastructure, which left it blind to internal threats like lateral movement and privilege escalation. This lack of visibility resulted in extremely long Level 4 incident investigations, averaging three hours, severely delaying the Security Operations Center's (SOC) ability to respond.

The organization selected the ExtraHop modern NDR platform to secure its critical assets, successfully delivering:

- **First-ever NDR for core payments:** The organization gained NDR capability for critical payment infrastructure, securing assets vital to the national economy.
- **Rapid incident response:** The team cut Level 4 incident investigation response time from **three hours to less than 15 minutes** to maximize SOC efficiency.
- **High-fidelity internal threat detection:** The platform enabled high-fidelity detection of lateral movement, privilege escalation, and unusual authentication on the network.
- **Accelerated deployment & ROI:** Dedicated ExtraHop residents ensured success and mitigated project stall risk, which accelerated deployment and delivered rapid ROI.

The Challenge

As a global leader in payments and financial technology that operates infrastructure critical to the national economy, this organization demands flawless security execution against high-level threats like nation-state actors. However, the existing security architecture presented several critical challenges:

Critical Blind Spots on Payment Infrastructure
The lack of an NDR solution left critical payment infrastructure completely blind to internal threats. The organization could not detect sophisticated attacks such as lateral movement, privilege escalation, or unusual authentication at the network level.

Inadequate Incumbent Security and Core NDR Gap
While the incumbent NDR vendor provided network data, it failed to deliver the required security depth. This existing solution lacked the deep security detections necessary to stop high-level threats, including sophisticated nation-state attacks. The absence of a proper NDR function meant the organization remained blind to critical internal threats like lateral movement, privilege escalation, and unusual authentication at the network level.

Extremely Long Incident Response Times

Extremely long Level 4 incident investigations hindered the SOC. These investigations took approximately **three hours** and delayed the team's ability to quickly contain and neutralize threats. Reducing this time was a key organizational goal.

Risk of Stalled Deployment

Due to heavy operational workloads on internal security and engineering teams, the organization faced a significant risk of a stalled or low-ROI NDR deployment.

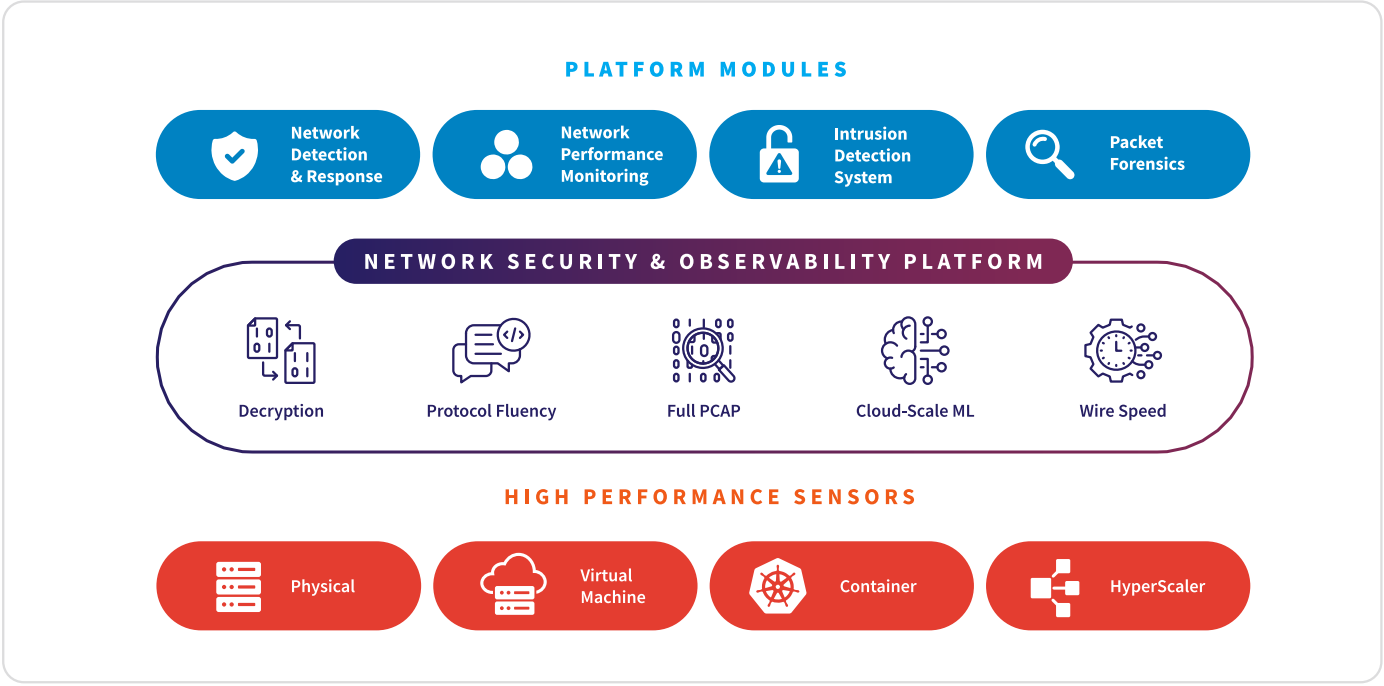
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully displaced the incumbent vendor, proving its ability to provide unified security coverage that met the organization's high-stakes security requirements. The modern NDR platform enabled the SOC to achieve transformative efficiency.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:** The organization 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 organization 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 organization 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 payments leader achieved immediate, transformative security improvements following the deployment of the ExtraHop NDR platform.

Transformed Incident Response Time: The organization dramatically cut Level 4 incident investigation time from **three hours to less than 15 minutes**. This improvement allows the SOC to respond to threats and maintain their competitive advantage in the payment space.

Gained Critical Security Visibility: For the first time, the organization gained NDR capability for its critical payment infrastructure. This visibility enables high-fidelity detection of key internal threats such as privilege escalation and lateral movement.

Displaced Incumbent and Ensured ROI: ExtraHop displaced the incumbent vendor. The organization ensured a high-ROI deployment by leveraging dedicated ExtraHop residents to accelerate the project and mitigate stall risk.

Enhanced Ecosystem Integration and Automation: ExtraHop successfully closed integration gaps. The team now sends alerts and performance detections to **Moogsoft**, while **Google Chronicle** pulls security detections via REST API to strengthen defense in depth.

Future-Ready Security Operations: The networking and security teams now collaborate more closely to build out the future SOC operations. These teams leverage ExtraHop's platform for comprehensive network performance monitoring, plus detection and response on one platform to thwart nation-state attacks.

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