EXTRAHOP

CUSTOMER STORY

# Construction Leader Unifies SecOps and NetOps

A leading U.S. homebuilder deployed ExtraHop to unify security across its hybrid-cloud enterprise and remote offices. By closing visibility gaps and aligning with CIS standards, the organization reduced tool sprawl and accelerated response times, creating a single source of truth for its security, IT, and cloud teams.

The organization selected the ExtraHop RevealX™ platform to serve as the unified source of network truth, successfully delivering:

- **Unified Hybrid Detection:** ExtraHop eliminated visibility gaps across the organization's diverse cloud and on-premises footprint, providing a consistent security posture for both centralized and remote operations.
- **Cross-Functional Collaboration:** By providing a single solution with flexible storage options, the platform broke down silos between NetOps, SecOps, and cloud teams, significantly reducing tool sprawl.
- **Behavior-Based Threat Detection:** The security team moved away from manual investigation efforts toward automated, high-fidelity detections, drastically cutting the mean time to respond (MTTR) to potential incidents.
- **CFO-Aligned Cost Optimization:** Through a strategic business justification focused on total cost of ownership (TCO), the organization achieved a consolidated defensive architecture that delivered higher value than disconnected legacy point solutions.

## The Challenge: Fragmented Visibility and Compliance Pressure

For a national leader in the construction industry, operational efficiency is tied directly to network uptime and security. As the organization expanded its digital footprint to support modern home-building technologies, its existing security architecture began to struggle with the complexities of a hybrid environment.

| | |
|---|---|
| **Incomplete Coverage and Remote Office Risk** | The organization faced unacceptable blind spots across regional datacenters and numerous remote construction trailers and sales offices. This created an environment where incidents could go undetected in the "cracks" between locations, leading to delayed response times. |
| **Alignment with CIS Standards** | A growing need to align with Center for Internet Security (CIS) standards placed significant pressure on internal teams. Their current toolset lacked the unified detection approach necessary to meet these benchmarks and demonstrate a strengthened security posture to executive leadership. |
| **Siloed Workflows and Tool Sprawl** | The organization was plagued by "siloed" workflows where security, IT, and application teams used disparate data sources. This fragmentation led to inefficient troubleshooting, duplicated efforts, and a high TCO as the company managed multiple niche tools that failed to communicate. |

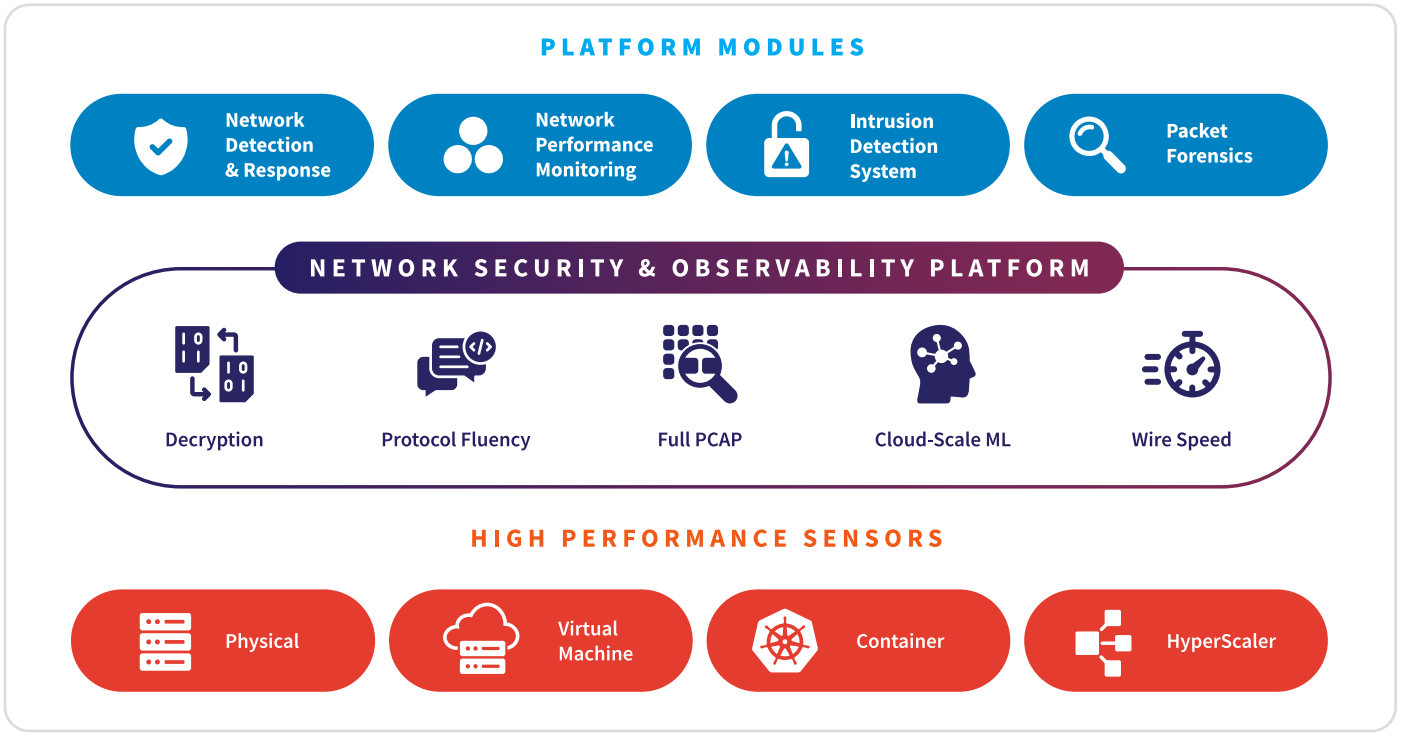
## The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully provided the agentless network security solution required for a sprawling national footprint, proving its ability to provide unified coverage across both corporate and remote construction environments.

The key outcomes and advantages delivered to the organization include:

- **Unrestricted visibility and decryption:**
  The oranization 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: Unified Defense and Accelerated Response

By deploying ExtraHop RevealX, the homebuilder transformed its security operations into a proactive, high-performance center of excellence.

### A Single Source of Truth for NetOps and SecOps

ExtraHop provided the deep protocol analysis needed to support multiple departments. By using the same network data for both security and performance, the organization successfully fostered a culture of collaboration.

### Consistent Hybrid Network Security

The platform established a unified visibility layer that treats cloud and on-premises traffic with the same level of scrutiny, eliminating the “cloud blind spots” that previously slowed down operations.

### Reduced Manual Investigation Effort

With behavior-based threat detection, the team moved away from the “noise” of traditional alerts. The high-fidelity intelligence allowed analysts to focus on true threats, cutting manual investigation time and ensuring rapid response to potential ransomware.

### Executive and TCO Alignment

The success of the project was driven by a strong alignment between technical requirements and business outcomes. By justifying the investment through core pillars of value for the CFO and CIO, the organization secured a future-proof solution that lowered the long-term TCO of their infrastructure.

## 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**