EXTRAHOP

CUSTOMER STORY

EMEA Government Tech Hub Secures New Centralized Data Center and Protects Critical Public Applications

A leading EMEA government technology hub deployed ExtraHop to secure its new centralized data center. By consolidating NDR and IDS into a single console and integrating natively with F5, Splunk, and Palo Alto Networks, the organization eliminated encrypted traffic blind spots while dramatically reducing storage overhead.

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

- **Consolidated NDR and IDS Operations:** ExtraHop unified network detection and response alongside deep intrusion detection capabilities within a single management console, reducing infrastructure complexity.
- **Pervasive Encrypted Application Visibility:** The platform provided granular visibility into all SSL traffic for government applications published on F5 LTM/ASM, eliminating critical blind spots without needing separate decryption tools.
- **Frictionless Ecosystem Synergy:** Natively integrated telemetry automated workflows across the hub's existing technical stack, seamlessly feeding data to Splunk SIEM and Palo Alto Networks SOAR.
- **On-Premises TCO Optimization:** By storing comprehensive network transaction records locally on-premise, the organization eliminated massive licensing and data ingestion fees associated with alternative architectures.

The Challenge: Centralized Infrastructure Expansion and Integration Complexity

As a leading public sector technology provider in the EMEA region, this organization supports critical government applications demanding absolute uptime and flawless security. Mandated to construct a new centralized data center, the hub faced sophisticated architectural and security hurdles that legacy point solutions could not resolve.

Pervasive Application Encryption Gaps

The data center relied heavily on applications published via F5 LTM/ASM. The massive volume of encrypted SSL/TLS traffic created critical blind spots, leaving analysts unable to inspect traffic for hidden post-compromise behaviors.

Stringent Multi-Capability Requirements

The team required a single solution that natively delivered both signature-based intrusion detection (IDS) and behavior-based network detection and response (NDR). Deploying separate products threatened to introduce tool sprawl and complex operational workflows.

Complex Ecosystem Integration

The new platform had to align tightly with existing investments, integrating seamlessly with Gigamon packet brokers, Splunk SIEM, and Palo Alto Networks SOAR without increasing configuration overhead or breaking traffic workflows.

Prohibitive Data Ingestion Costs

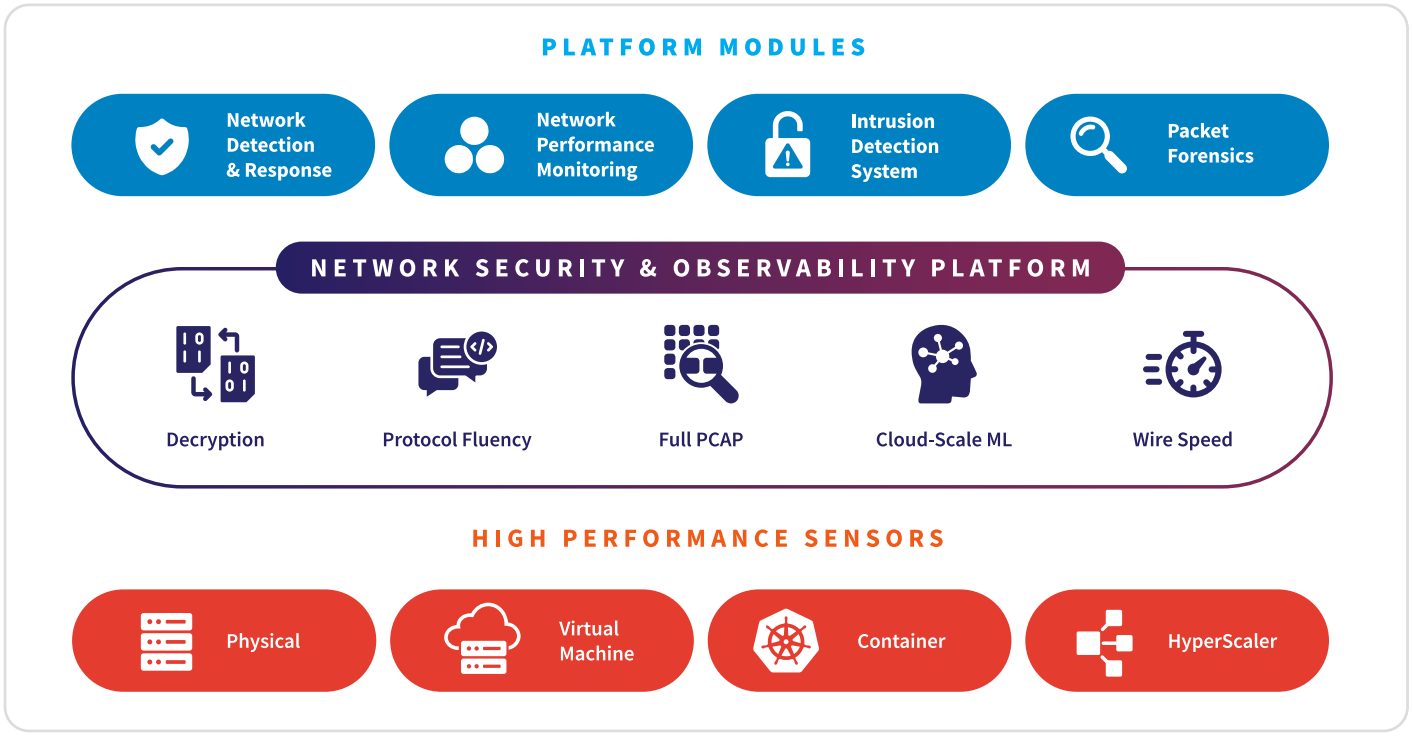
Alternative NDR tools selected for evaluation presented a financial bottleneck by forcing all network records into Splunk SIEM. This architecture would trigger skyrocketing data ingestion fees and unsustainably inflate the total cost of ownership.

The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully provided the agentless network security solution required for a high-stakes government data center environment, proving its ability to provide unified security coverage that met the organization's strict performance, integration, and scalability requirements with the proven benefits of a modern NDR platform. 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: Scalable Visibility and Cost-Optimized Security

The EMEA government tech hub achieved immediate, transformative security improvements following the deployment of the ExtraHop modern NDR platform across its new centralized data center infrastructure.

Unified Platform Consolidation

Delivering NDR and IDS within a single console eliminated the friction of managing separate point solutions. Analysts now maintain complete oversight of network behavior and signature alerts from one interface to maximize hunting efficiency.

Total F5 Application Visibility

The platform eliminated encrypted blind spots by inspecting SSL traffic for applications published on F5 LTM/ASM. This line-rate decryption provided operational clarity into core public-facing systems without introducing latency.

Seamless Multi-Vendor Integration

ExtraHop aligned with Gigamon brokers without redundant decryption while feeding network truth to Splunk SIEM and triggering automated responses within Palo Alto Networks SOAR, entirely erasing technical silos.

Substantial TCO Optimization

ExtraHop's on-premises record store avoided the skyrocketing ingestion fees of architectures that require storing records in Splunk SIEM. Local metadata storage enabled deep investigations while dramatically reducing licensing overhead.

Sovereign Network Control

The tech hub established a scalable layer of network truth that protects critical government applications, ensuring robust compliance with cyber resilience frameworks while future-proofing its centralized digital footprint.

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