CASE STUDY

V: 2026/03

vehere

Securing a Petabyte-Scale National Intelligence Network with Vehere NDR

Customer Overview

The organization is a leading national intelligence and homeland security agency responsible for safeguarding one of the world's largest democratic nations from internal and cross-border security threats. The agency operates a highly classified digital ecosystem supporting intelligence gathering, secure communications, and coordination across multiple government departments and operational units.

Its infrastructure spans across distributed operational centers, secure data facilities, and interconnected intelligence networks, handling large volumes of sensitive data and mission-critical communications. These networks support intelligence operations, secure inter-agency collaboration, advanced analytical platforms, and highly sensitive investigative workflows.

The intelligence agency is responsible for the safety of a nation that:

Has a population of **~1.5 billion**

Is a **$ 4 trillion** economy

Has one of the largest internet-using populations globally.

Given the scale and sensitivity of these operations, the agency requires continuous security and visibility across high-throughput networks to enable proactive threat detection and deep packet-level visibility for investigations.

Business Challenges and Requirements

Operating in a national security environment, the agency required continuous monitoring NDR Platform capable of supporting real-time threat detection and network forensics across a large, high-throughput infrastructure. Existing monitoring tools, however, introduced critical visibility and operational gaps.

Limited Network Visibility: Security monitoring relied on logs, NetFlow, and metadata, offering only partial visibility into network activity. This limited detection of APTs, covert command-and- control traffic, and data exfiltration over legitimate protocols. Without full packet capture, analysts lacked session-level visibility for effective investigations.

On-Premises Architecture: Given the sensitivity of national intelligence traffic, the agency required a fully on-premises NDR platform to ensure packet data and network telemetry remain within controlled infrastructure, eliminating the risk of sensitive information being transmitted to external cloud environments.

Extended Data Retention: The environment required the ability to retain up to 1 year of extracted and indexed network metadata and 7 days of raw packet capture (PCAP) to enable retrospective threat hunting, historical traffic analysis, and packet-level incident investigations.

Absence of Historical Packet Evidence: Existing solutions lacked continuous packet retention, preventing reconstruction of historical network sessions. This limited the ability to investigate breaches, reconstruct attacker timelines, and analyze suspicious communications at the packet level.

High-Speed Traffic Monitoring: The environment requires line-rate monitoring across high-throughput networks. Traditional tools struggled to maintain lossless visibility at scale, resulting in gaps in detection and forensic analysis.

Fragmented Security Architecture: Detection and packet capture operated on separate platforms, increasing integration overhead and slowing investigations. The agency required a unified architecture combining real-time NDR analytics with deep packet-level forensics.

Our environment operates on a massive scale, where even a single missed packet can hide a threat. We needed a fully on-premises NDR platform delivering continuous lossless packet visibility, deep packet-level analytics, and investigative certainty across high-throughput networks.

Solution Deployed

To address these challenges, the agency deployed a Vehere Network Detection and Response (NDR) platform, enabling comprehensive network security, visibility and forensic investigation across high-throughput environments.

AI-Powered Network Detection and Response (NDR): Behavioral analytics continuously monitor east-west and north-south network traffic to detect anomalies, suspicious communication patterns, and advanced threats.

Continuous Full Packet Capture (PCAP): The platform performs line-rate packet acquisition, capturing complete network packets across monitored segments to ensure lossless traffic visibility.

Unified Detection and Investigation Platform: The integrated architecture combines real-time detection with forensic packet analysis, eliminating the need for separate tools and simplifying security operations.

Deep Packet Inspection (DPI): Advanced DPI engines analyze protocol behavior and communication patterns, enabling analysts to detect malicious activity embedded within legitimate traffic.

Network Forensics and Session Reconstruction: Security teams can reconstruct complete network sessions, files, and communication flows, providing detailed insights during investigations.

Metadata and Packet Storage: The deployment includes scalable storage to retain up to 1 year of extracted and indexed network metadata and 7 days of raw packet capture (PCAP), enabling retrospective analysis and historical investigations.

Vehere NDR's Win Areas

- Native integration of Network Detection and Response with continuous, lossless full packet capture (PCAP) ensuring complete traffic visibility
- On premises by design NDR architecture that keeps all packet data and network telemetry within the organization's infrastructure, eliminating reliance on external cloud environments and ensuring complete data sovereignty and operational control.
- Advanced Deep Packet Inspection (DPI) for granular protocol decoding and behavioral traffic analysis
- High-fidelity packet retention with full-session reconstruction enabling detailed threat investigation and packet-level evidence analysis
- Battle-tested proven performance in mission-critical environments, supporting high-throughput networks with sustained reliability

Outcome for the Organization

- **Comprehensive Network Security:** Security teams gained full packet-level visibility into network traffic, enabling deeper threat detection capabilities.
- **Faster and More Accurate Investigations:** With full session reconstruction and historical packet access, analysts can quickly trace attacker activity and determine root causes.
- **Reduced Operational Complexity:** By combining NDR analytics and packet capture on a single platform, the organization simplified its security monitoring architecture and reduced operational overhead.
- **High-Performance Monitoring at Scale:** The deployed solution supports continuous lossless packet capture across high- throughput network environments, ensuring complete visibility even under heavy traffic loads.

> *After evaluating multiple solutions, Vehere NDR clearly stood out. It's fully on-premises architecture ensures our sensitive telemetry never leaves our environment, while continuous lossless packet capture, deep network analytics, and full-session reconstruction provide the visibility we need across high-throughput networks. Our analysts now operate with complete packet-level evidence to detect and investigate sophisticated threats with confidence.*

Strategic Impact

By deploying the Vehere NDR platform, the agency significantly enhanced its cyber defense, situational awareness, threat hunting, and investigative capabilities, enabling security teams to detect sophisticated threats earlier, conduct detailed packet-level investigations, maintain historical network evidence for intelligence analysis, and better protect critical national security infrastructure from advanced cyber threats.

About Vehere

Vehere is a new-age software company specializing in AI Cyber Network Intelligence. For more than a decade, Vehere has been supporting criminal investigation analysts in Defense and Intelligence communities. Vehere is now trusted by cyber-analysts in Fortune 500 companies, including Telecom, Financial agencies, and Smart cities to protect critical infrastructure against advanced cyber threats and nation-state attacks.

Vehere preserves fundamental principles of privacy and civil liberties. We proactively defend your cyberspace by cross leveraging our expertise between national security and enterprise security.

Address:
1390 Market Street
Suite 200, San Francisco, CA 94102

Unit No. 5, 1st Floor, Andaz, Asset Area 1
Aerocity, New Delhi-110037

E: sales@vehere.com

W: www.vehere.com