CASE STUDY

V: 2026/01/01

vehere

World's Largest Passenger Railway Network Operator Deploys Vehere NDR to Strengthen Cyber Defense

Customer Overview

A large national critical infrastructure operator managing the world's second-largest railway network under a single management, supporting high-volume, mission-critical applications across a highly distributed environment, required enhanced enterprise security. With rising encrypted traffic and expanding digital services, its SOC needed deeper analytics and forensic capability without increasing operational complexity.

Business Requirement

The customer required an advanced Network Detection and Response solution that could deliver:

- 30-day metadata retention
- 5-day full packet capture (PCAP)
- Real-time L2 - L7 analytics
- Multi-protocol session reconstruction (HTTP, SMTP, FTP)
- Improved SOC visibility, investigation capability and threat detection across sensitive national infrastructure

Solution Delivered

The customer deployed Vehere Network Detection and Response (NDR) with integrated Full Packet Capture (PCAP) to deliver deep visibility, real-time threat detection, and forensic-grade retention across critical network segments. Vehere provided native metadata retention of up to 180 days, multi-day PCAP for byte-level investigations, encrypted-traffic analytics without decryption, advanced DPI and protocol analysis (including custom and legacy protocols), full multi-protocol session reconstruction, and MITRE ATT&CK-aligned detection models, while seamless SIEM and SOAR integration enabled automated investigation and response workflows across the SOC.

> ***"We sought a unified Network Detection and Response (NDR) solution that delivers deep network visibility, forensic readiness, and long-term investigative capabilities, while effectively securing sensitive, legacy, and mission-critical railway infrastructure where endpoint agents cannot be deployed"***

Key challenges

- Blind spots in east-west traffic limited forensic depth and delayed root-cause analysis.
- EDR agents could not be deployed across all endpoints due to the presence of diverse operating environments.
- Requirement for a fully on-premises security platform with no dependence on cloud telemetry.
- SOC teams struggled to justify alerts and present defensible evidence during compliance audits.

Vehere NDR's Win Areas

Complete technical compliance: Native support for 180-day metadata and 5-day PCAP retention, meeting all governance and technical requirements without customization.

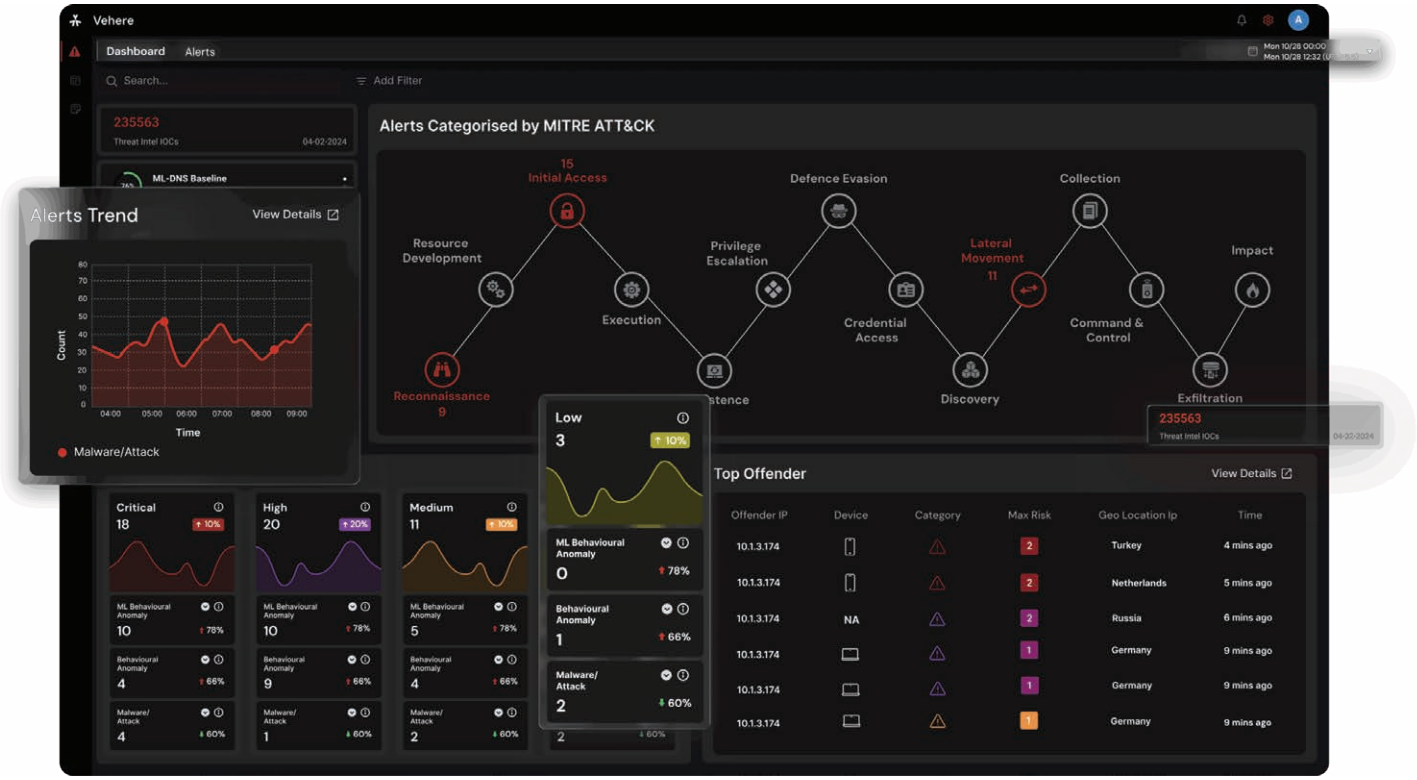
Comprehensive network visibility: Real-time L2 - L7 analytics, enriched metadata, and encrypted-traffic visibility without decryption, enabling deep SOC investigations.

Proven POC performance: Outperformed alternative solutions across multiple POCs with SI partners, delivering higher detection accuracy, better scalability, and deeper forensic reconstruction.

Strong partner alignment: Seamless integration with the lead system integrator's SOC architecture, ensuring smooth deployment, operational efficiency, and long-term support fit.

Clear technical differentiation: Demonstrated superior network visibility, ATT&CK aligned detection, multi-protocol reconstruction, and automated response via SIEM/SOAR integrations.

On-Premises by Design: Fully on-premises architecture with no cloud telemetry, ensuring sensitive traffic, metadata, and forensic evidence never leave the critical infrastructure environment.



Outcome for Customer

With Vehere NDR and PCAP, the critical infrastructure operator now benefits from:

Unified Detection and Forensics: Single on-premises platform delivering NDR with 5 days of lossless packet capture and 180 days of metadata retention

Improved Detection Accuracy: High-confidence alerts driven by real network behavior and MITRE ATT&CK-aligned analytics

Faster Investigations: Reduced MTTR through instant access to historical metadata and byte-level packet evidence

Audit Readines: Compliance-grade packet and metadata retention supporting audits and post-incident analysis

Reduced SOC Load: Lower false positives and clearer attack narratives through session reconstruction

Stronger Security Posture: Continuous visibility across encrypted, hybrid, and east-west network traffic

This deployment significantly strengthened cyber resilience across the operator's national infrastructure footprint.

Delivering Strategic Value

Vehere has been enabling the operator to detect advanced threats through ATT&CK-aligned analytics, reconstruct complete attack paths with forensic precision, automate response actions across SOC tooling, meet stringent audit and retention mandates, and build a future-ready detection architecture for national critical infrastructure.

About Vehere

Backed by over 18 years of battle-tested experience supporting national defense and critical security programs across the globe, Vehere NDR unifies advanced threat detection, deep network visibility, and forensic-grade packet analytics into a single, scalable platform. With native multi-day PCAP retention, enriched metadata, encrypted-traffic analytics, and MITRE ATT&CK aligned detection, it equips SOC teams with precise real-time insight and rapid investigative depth. Seamless SIEM/SOAR integration accelerates response workflows, enabling security leaders to strengthen resilience, reduce operational overhead, and build a future-ready detection architecture for high-sensitivity environments.

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