CASE STUDY

V: 2026/04

vehere

Eliminating Blind Spots at Scale: Vehere NDR Secures a $20B Banking Environment

About the Organization

One of India's leading public sector banks operating a vast, highly distributed digital ecosystem supporting millions of customers across urban and rural regions. Its infrastructure spans:

- Thousands of branch locations and service points
- A dense network of ATMs and self-service kiosks
- Core banking systems, payment gateways, and mobile platforms
- Data centers, DR sites, and hybrid cloud workloads
- Tens of thousands of endpoints including employee devices, servers, and network-connected systems

With the rapid expansion of digital banking, the environment processes millions of transactions daily, making it a high-value target for advanced cyber threats.

While endpoint security remains critical, modern attackers increasingly bypass or "blend into" endpoints, leveraging encrypted traffic, lateral movement, and stealth techniques. This creates blind spots that only network-level visibility (NDR) can address making it essential for ensuring continuous, resilient operations in a zero-downtime banking environment.

Total Revenue of	Total Assets of	Has a Market Cap of	Total Business value crossed
~$1.6 billion	**~$19 billion**	**~$1.74 billion**	**$20.4 billion**
in 2025	*in 2025*		*in 2025*

> ***Our environment operates on a massive scale, where threats can easily hide within encrypted and internal traffic. Endpoint security alone was no longer sufficient - we needed deep, continuous network visibility with high detection confidence and minimal noise.***

Business Challenges and Requirements

The bank faced increasing complexity in securing its expanding digital footprint:

- Operational and Security Challenges
  - Highly distributed infrastructure across branches, ATMs, and data centers
  - Increasing reliance on encrypted traffic, limiting visibility for traditional tools
  - Sophisticated threats leveraging lateral movement within internal networks
  - Alert fatigue due to high noise from existing security tools
  - Need for zero downtime, where even minor disruptions impact customer trust.
- Detection and Visibility Gaps
  - Endpoint-based controls alone were insufficient for detecting network-borne threats
  - Lack of deep packet-level visibility across east-west traffic
  - Limited ability to investigate incidents with full context

- Key Requirements
  - 180-day indexed network metadata retention and 90-day full PCAP for long-trail threat hunting, compliance, audit, and deep forensics
  - Multi-protocol (HTTP, SMTP, FTP) file extraction and full-session reconstruction for precise investigation and evidentiary analysis
  - Real-time L2-L7 visibility across encrypted traffic for complete network coverage
  - High-confidence, low-noise detection with contextual insights to reduce alert fatigue and improve SOC efficiency
  - Accelerated root-cause analysis across network activity to reduce MTTD and MTTR
  - Simple, dependency-free architecture enabling fast deployment and rapid time-to-value

Solution Delivered

Vehere NDR was deployed to deliver continuous, high-fidelity network visibility, advanced threat detection, and deep forensic capabilities, fully aligned to the bank's operational and compliance requirements.

- Extended retention with continuous, lossless full PCAP and indexed metadata, enabling long-tail threat hunting, compliance, and deep forensic analysis
- L2-L7 Deep Packet Inspection (DPI) with multi-protocol support (HTTP, SMTP, FTP), enabling file extraction and full-session reconstruction for precise investigations
- Real-time visibility across encrypted north-south and east-west traffic, ensuring complete coverage of internal and external network activity
- High-confidence, low-noise detection powered by behavioral analytics and context-rich insights, reducing alert fatigue and improving SOC efficiency
- Contextual alert rationale with playbook-driven response recommendations, accelerating root-cause analysis and reducing MTTD and MTTR
- Full-session reconstruction and rapid search capabilities, enabling faster, evidence-backed incident investigations
- Lightweight, dependency-free architecture, ensuring seamless deployment, minimal disruption, and rapid time-to-value
- The solution was deployed in alignment with the bank's existing infrastructure, ensuring minimal operational disruption and rapid validation within the proof-of-concept phase.

> ***The NDR platform has transformed our security operations. We now have complete visibility across our network, faster detection of sophisticated threats, and the confidence to investigate incidents with precision - without overwhelming our SOCs***

Vehere NDR's Win Areas

The bank faced increasing complexity in securing its expanding digital footprint:

- Purpose-built NDR with deep protocol analytics, delivering high-fidelity, low-noise detection and reduced SOC fatigue
- Comprehensive visibility across encrypted, east west, and stealth threat vectors
- On-premises architecture with full control over sensitive network telemetry
- Petabyte-scale storage and terabit-speed processing with continuous, lossless full PCAP
- Smart indexed storage enabling rapid search, investigation, and full-session reconstruction
- Built-in alert rationale with playbook-driven response recommendations for faster, consistent SOC action
- Lightweight, scalable design with rapid deployment and strong field execution

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