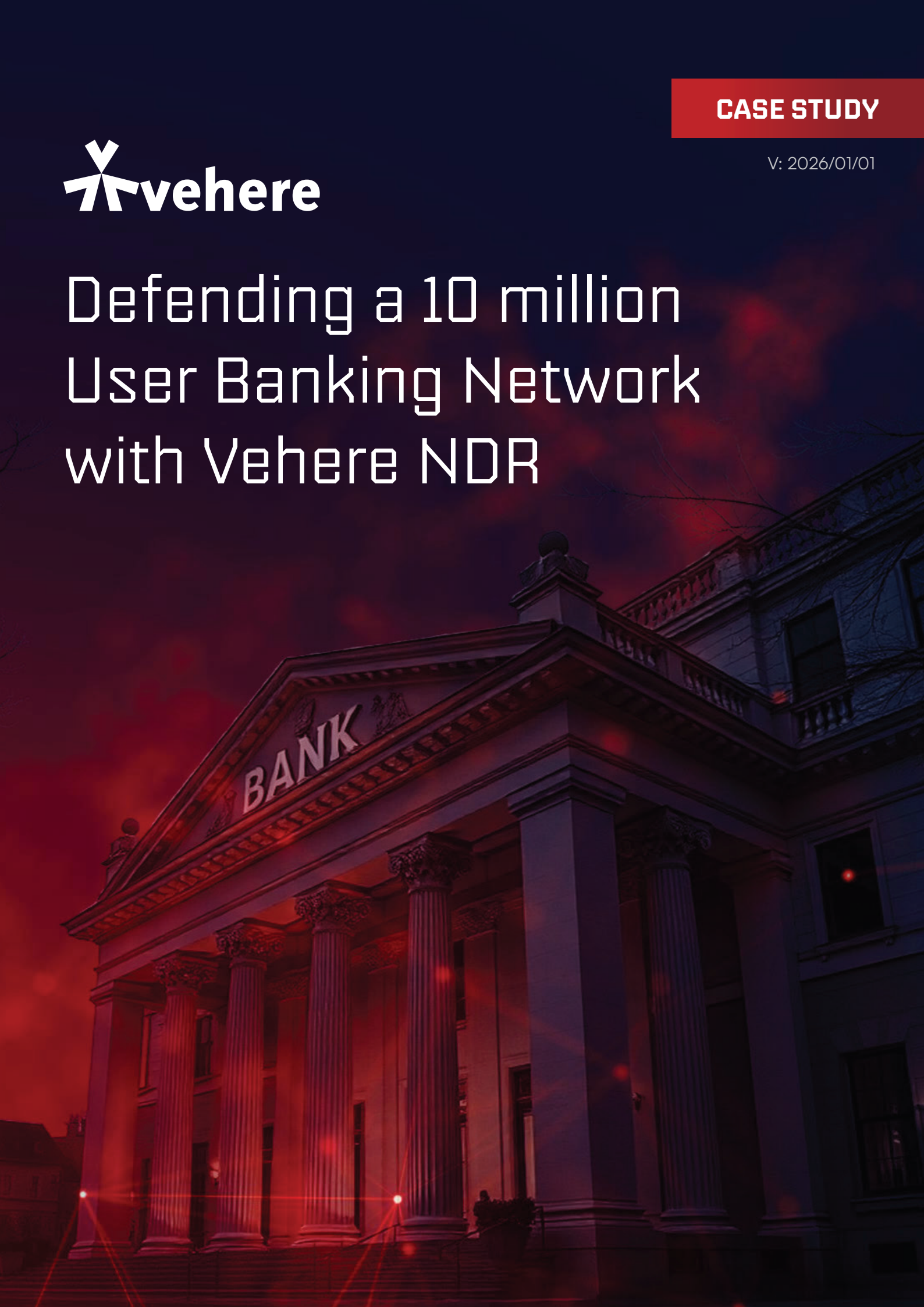
CASE STUDY

V: 2026/01/01

vehere

Defending a 10 million User Banking Network with Vehere NDR



Customer Overview

One of India's largest universal banks, operating one of the country's most expansive branch networks, initiated a cyber security modernization program to elevate the foundation for a future ready cyber resilient environment across a nationally distributed, high-volume financial infrastructure.

Architected to process **~ 180 Million** transactions per day	Caters to **10 Million +** users everyday
A nationwide network of **2,100 +** branches	Connected to a web of **3,700 +** ATMs

Serving millions of retail, corporate, and government customers, the bank operates a nationwide ecosystem spanning branches, ATMs, digital banking platforms, and hybrid infrastructure environments. Public disclosures indicate that its core technology platforms are architected to process millions of transactions per day across reconciliation engines and back-end financial workflows, reflecting enterprise-grade throughput, high availability requirements, and mission-critical performance standards.

At this scale, daily transaction processing translates into multi-billion-dollar monetary flows across diverse banking channels. The sheer velocity, volume, and distribution of network traffic position the institution among the most operationally complex financial environments in emerging markets: demanding continuous cyber security, forensic-grade telemetry, and real-time threat detection capabilities.

> ***Our priority was to achieve continuous threat visibility and forensic readiness across an environment that processes transactions at a massive scale. Vehere enabled us to meet stringent regulatory requirements while simplifying SOC operations.***

Business Requirements

The SOC modernization initiative was driven by the following global grade requirements:

- Alignment with RBI regulatory mandates, supporting 7 days of full packet capture and 180 days of indexed network metadata retention for audit and compliance needs.
- Real-time security across north-south and east-west traffic, enabling early detection of advanced and stealthy threat activity.
- Deep packet level insight to reconstruct incidents, support investigations, and withstand regulatory scrutiny.
- National-level scalability to sustain high-volume traffic across data centers, branch networks, digital banking platforms, and hybrid cloud environments.
- Operational and cost efficiency through elimination of per-decoder licensing, reduced hardware footprint, and simplified security operations.

Key Challenges

The bank required a single, unified security platform capable of delivering real-time network threat detection and forensic-grade packet visibility. It also needed to support regulatory -mandated long-term data retention across a geographically distributed, high-transaction -volume environment. At the same time, the solution had to avoid cost escalation, and the operational complexity typically associated with traditional global OEM security platforms.

Solution Delivered:

Deployment of Vehere Network Detection Response (NDR) integrated with high performance Full Packet Capture (PCAP) and long term metadata retention, delivering:

- 7 day full packet capture retention,
- 180 day indexed metadata storage,
- AI driven behavioral analytics for early threat detection, and
- Centralized SOC visibility optimized for national scale banking infrastructure.

Vehere NDR – Key Win Areas

- **Compliance First Architecture:** Purpose built to meet regulated industry retention mandates without add on modules or third party dependencies.
- **Deep Packet and Metadata Visibility:** Native integration of full packet capture and metadata analytics delivers packet level insights at scale.
- **Unified and Scalable SOC Operations:** Centralized management and analytics simplify security operations across distributed, highvolume environments.
- **Battle-Tested Performance at Scale:** Proven to operate at petabyte-scale data environments and terabit network speeds, delivering continuous, lossless packet capture for mission-critical networks.
- **Regional Expertise with Global Applicability:** Strong local support and regulatory understanding combined with architecture suitable for global financial institutions.
- **No Per Decoder Licensing Model:** Predictable, flat licensing that scales with traffic growth avoiding cost escalation common with global OEMs.

Solution Architecture Overview

The deployed architecture consisted of:

AI-powered NDR: Advanced behavioral analytics and machine learning models to detect reconnaissance, lateral movement, and data exfiltration attempts in real time.

Full Packet Capture: Scalable, high-throughput continuous lossless packet capture enabling complete reconstruction of network events.

Metadata Retention and Analytics: Long-term retention of enriched network metadata for rapid search, correlation, and threat hunting.

Centralized SOC Operations: Unified dashboards and investigation workflows, reducing mean time to detect and respond.

Vehere NDR delivered deep network visibility, ensured compliance alignment, and simplified security operations across the bank's SOC environment.

Outcomes and Business Impact

Regulatory Compliance and Audit Readiness: The bank achieved full alignment with RBI network data retention mandates, strengthening regulatory posture and audit confidence.

Improved Threat Detection and Response: Real time behavioral analytics combined with packet level evidence significantly improved detection accuracy and accelerated incident response.

Deep-packet Investigation Capability: SOC teams gained the ability to reconstruct incidents with packet level fidelity, supporting root cause analysis, legal defensibility, and regulatory reporting.

Predictable Costs and Simplified Operations: By eliminating per decoder licensing and minimizing hardware dependency, the solution delivered predictable economics and reduced SOC operational overhead.

Delivering Strategic Value

By modernizing its SOC with Vehere NDR, the bank established a future ready security foundation for balancing regulatory compliance, deep network security, and operational efficiency. The deployment demonstrates how large, regulated financial institutions can achieve enterprise scale cyber resilience without the complexity and cost traditionally associated with legacy global security platforms.

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 Institutions, 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