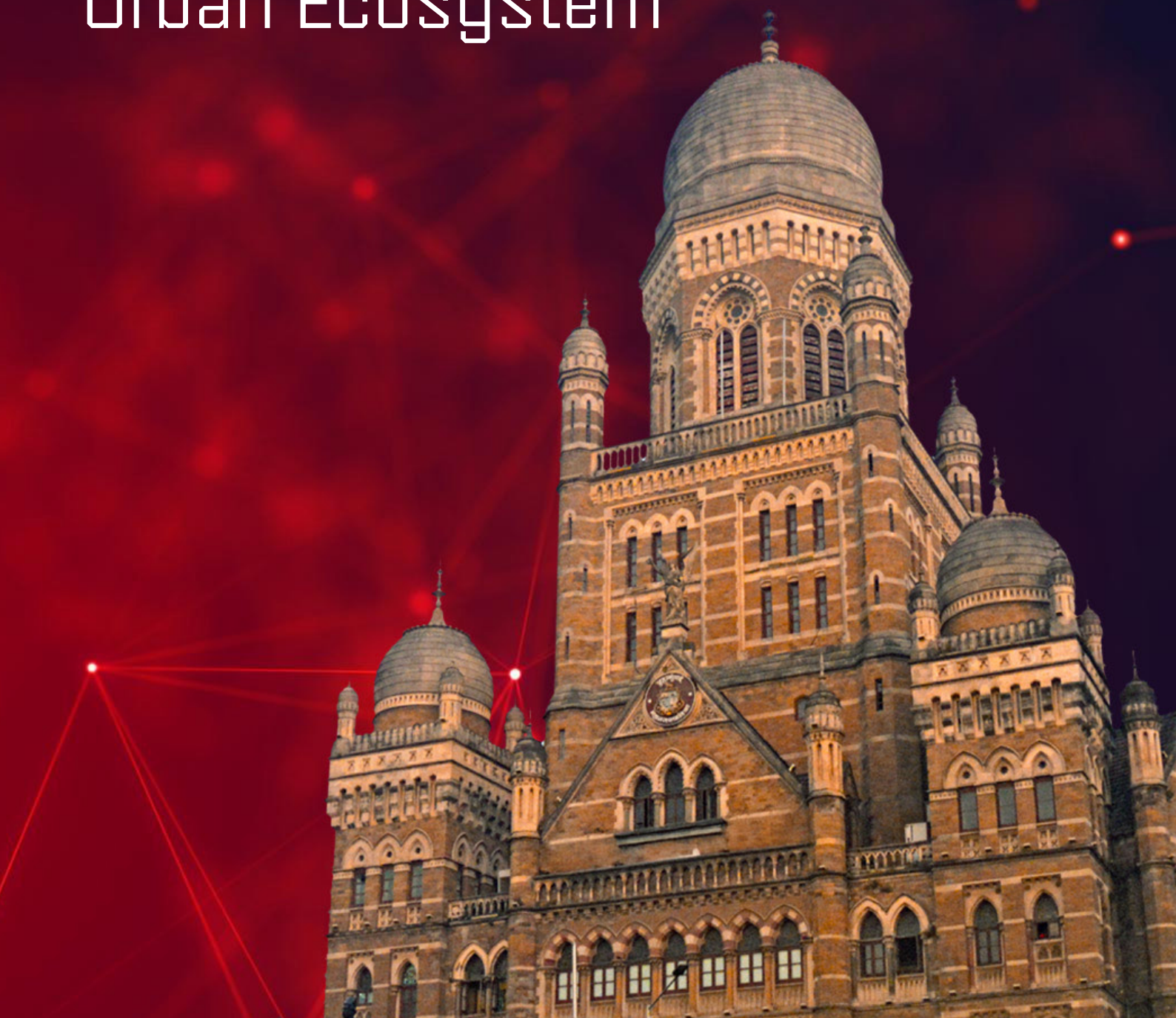
CASE STUDY

V: 2026/03

vehere

Vehere NDR Secures the Municipal Corporation Powering India's Largest Urban Ecosystem



Customer Overview

A leading Tier-1 urban governance authority in Asia, serving over 27 million citizens and managing thousands of municipal services and digital applications, operates one of the region's most complex public-sector IT environments. As a backbone of critical urban infrastructure, its network must remain continuously available with zero tolerance for downtime, supporting millions of daily digital transactions across data centers, cloud workloads, smart-city platforms, and interdepartmental systems.

Serves
~27 million
People

Responsible for
11%
of the National GDP

Contributes to
30%
of National Income Tax Collection

Handles
40%
of India's Foreign Trade

> ***To protect this high-volume, high-sensitivity environment, the authority required deep network visibility, long-term forensic retention, and real-time threat detection, capabilities that extended beyond traditional SIEM-first security models.***

Business Challenges and requirements

The organization faced increasing pressure from regulatory, operational, and cyber-risk perspectives and required an NDR solution capable of delivering:

- 180-day network metadata retention for compliance, audits, and long-tail threat hunting
- 90-day full packet capture (PCAP) to support deep forensic investigations
- Multi-protocol file and session reconstruction (HTTP, SMTP, FTP)
- Real-time threat visibility across L2-L7, including encrypted traffic
- Faster root-cause analysis across network, application, and user activity

Existing tools, primarily SIEM-centric platforms, lacked native packet-level visibility, were limited in protocol reconstruction, and could not deliver the forensic depth required for such a large and distributed environment.

Solution Delivered

The authority selected Vehere Network Detection and Response (NDR) with integrated Full Packet Capture as the foundational visibility and detection layer for its SOC.

Vehere delivered a purpose-built NDR + PCAP architecture that provided:

- Native 180-day metadata retention and 90-day PCAP at scale
- Full session and file reconstruction across multiple protocols
- Real-time L2 - L7 analytics with encrypted traffic visibility
- Forensic-grade evidence for investigations and audits
- Integration with existing SOC tools, including SIEM and response platforms

Vehere NDR's Win Areas

Native Long-Term Retention at Scale: Vehere NDR uniquely met the requirement for extended metadata and PCAP retention natively, without relying on external storage, bolt-ons, or architectural compromises.

Full Session Reconstruction Beyond SIEM Limitations: Unlike SIEM-first platforms with limited protocol visibility, Vehere enabled full multi-protocol session and file reconstruction, providing investigators with complete context.

Real-Time Network Analytics Across Encrypted Traffic : Vehere delivered L2-L7 visibility, behavioral analytics, and encrypted traffic insights-restoring visibility lost to traditional tools as encryption volumes increased.

Architecture-Led Differentiation: Through focused technical discussions and demonstrations, Vehere clearly articulated the limitations of SIEM-centric detection and positioned NDR + PCAP as the primary visibility layer.

Demonstrated Value Through Hands-On Evaluation: Live demonstrations and POVs showcased deep forensic workflows, protocol reconstruction, and threat detection, clearly differentiating Vehere from legacy and add-on models.

Outcome for Customer

With Vehere NDR deployed, the authority has strengthened its SOC operations with:

- Unified network detection and forensic visibility in a single platform
- Reduced dependency on multiple point tools
- Long-term evidence retention supporting compliance and audits
- Accelerated investigations using session-and packet- level data
- Improved detection confidence across encrypted and east-west traffic.

The platform now serves as a scalable visibility backbone across municipal IT, citizen services, and critical backend systems.

Delivering Strategic Value

Vehere NDR has been enabling the organization 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 large-scale civic infrastructure.

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