Enterprise NDR Transformation for a Leading Indian Organization

Network Detection & Response (NDR) Transformation with Central Manager, Flow Collectors, Sensor Data Store, Hybrid Traffic Visibility, and 24x7 Support

EXECUTIVE CONTEXT

COMnet partnered with a leading Indian enterprise to implement a Network Detection & Response (NDR) program focused on hybrid network visibility, real-time threat detection, and sustained operational support. The engagement delivered a central manager, flow collectors, and sensor data store in a high-availability DC/DR design, with telemetry sourced from Internet, DMZ, ACH internal networks, and cloud firewalls hosted in AWS, GCP, and Azure.

DC/DR
HA architecture

3 Zones+
Traffic sources

24x7
Support

IMPACT

- Established centralized NDR visibility across internet-facing, DMZ, internal ACH, and multi-cloud traffic paths, reducing monitoring blind spots.
- Improved incident detection and investigation by consolidating traffic telemetry into a unified platform for real-time analytics and forensic review.
- Strengthened the enterprise's ability to identify anomalous behavior and lateral movement through network behavior analytics and anomaly detection.
- Enhanced operational resilience with a DC/DR high-availability deployment model for the NDR management and data collection stack.
- Enabled sustained cyber operations with a three-year, 24x7 remote support construct covering platform monitoring, tuning, and issue management.

MAJOR ISSUES

- The client required deeper visibility into east-west and north-south traffic flows across both on-premises and cloud-connected environments.
- Traditional perimeter controls alone were insufficient to provide forensic-quality network visibility and early detection of advanced threats.
- Traffic originating from multiple trust zones—Internet, DMZ, internal ACH, and cloud firewalls—created complexity in telemetry normalization and event correlation.
- The organization needed an NDR architecture that could operate in a resilient DC/DR model without compromising availability or data retention.
- Operational teams required a support framework capable of sustaining detection quality, rule tuning, and platform health over the long term.

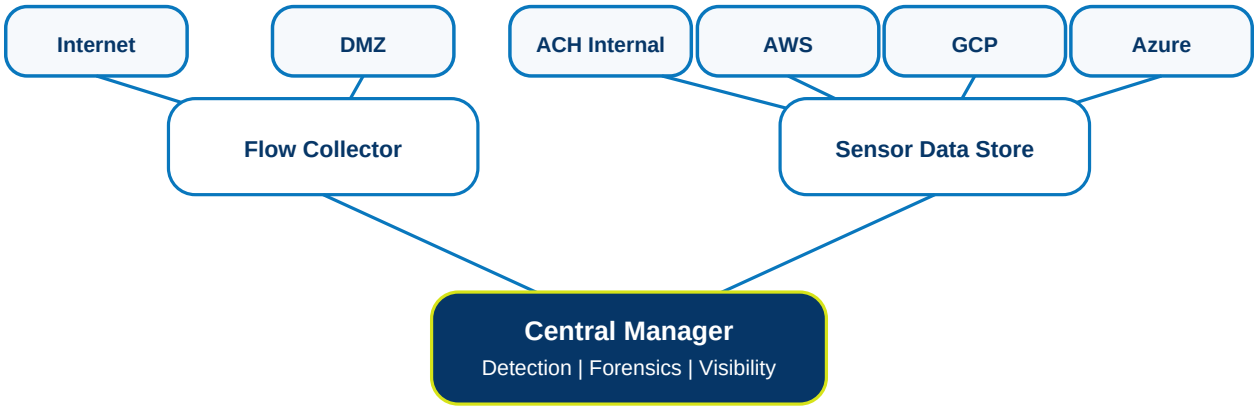
Enterprise NDR Transformation for a Leading Indian Organization

Network Detection & Response (NDR) Transformation with Central Manager, Flow Collectors, Sensor Data Store, Hybrid Traffic Visibility, and 24x7 Support

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

REFERENCE SECURITY ARCHITECTURE



DC/DR high-availability deployment | 24x7 remote support | continuous monitoring and tuning

- Designed and deployed Central Manager, Flow Collector, and Sensor Data Store components for the NDR platform.
- Implemented deployment across DC and DR environments in a high-availability architecture.
- Integrated traffic telemetry from three major network domains—Internet, DMZ, and ACH internal network.
- Extended visibility into cloud-connected environments by ingesting relevant telemetry from cloud firewalls hosted in AWS, GCP, and Azure.
- Enabled capabilities spanning real-time threat detection, incident response, forensics, network behavior analytics, anomaly detection, and traffic visibility.
- Delivered three years of platform support through a 24x7 remote operations model.

- Telemetry Ingestion Layer: Flow and network telemetry were collected from Internet, DMZ, ACH internal networks, and cloud firewall environments.
- Collection and Storage Layer: Flow Collectors and Sensor Data Store components were deployed to aggregate, retain, and normalize traffic evidence for detection workflows.
- Central Management Layer: A Central Manager provided unified visibility, alert review, forensic investigation, and platform administration.
- Detection Analytics Layer: The NDR stack supported behavioral analytics, anomaly detection, traffic inspection, and incident investigation use cases.
- High-Availability Deployment Scope: Core NDR components were implemented across DC and DR locations to support resilience and service continuity.
- Operational Support Layer: 24x7 remote support covered monitoring, troubleshooting, platform maintenance, and response coordination over a three-year support period.

Enterprise NDR Transformation for a Leading Indian Organization

Network Detection & Response (NDR) Transformation with Central Manager, Flow Collectors, Sensor Data Store, Hybrid Traffic Visibility, and 24x7 Support

KEY STRATEGIES

- Visibility-First Security Design: The engagement prioritized deep network observability as the foundation for threat detection, investigation, and executive-level risk visibility.
- Hybrid Telemetry Normalization: Data from on-premises trust zones and multi-cloud firewall estates was normalized to improve correlation quality and investigative context.
- Resilient Architecture Planning: DC/DR deployment patterns were used to align NDR services with the client's availability and continuity requirements.
- Behavioral Detection Focus: The solution emphasized anomaly detection and network behavior analytics to identify suspicious activity that signature-only approaches may miss.
- Operationalization of Forensics: The NDR stack was positioned not only for alerting, but also for structured incident response and forensic reconstruction.
- Continuous Support and Tuning: A 24x7 remote support model ensured sustained platform health, rule optimization, and rapid issue handling throughout the support lifecycle.
- Scalable Enterprise Readiness: The architecture was designed to scale across additional traffic sources, environments, and investigative requirements as the organization matures.

EXECUTIVE TAKEAWAY

COMnet translated a fragmented network-visibility challenge into a structured NDR program with high-availability deployment, multi-zone telemetry ingestion, behavioral analytics, and round-the-clock operational support. The result is a stronger enterprise detection posture with greater visibility, investigative depth, and long-term operational sustainability

OUTCOME SNAPSHOT

- Broader traffic visibility across enterprise and cloud-connected environments.
- Faster detection, triage, and evidence-led investigation of suspicious network activity.
- A resilient, supportable NDR foundation aligned to enterprise-scale cyber operations.

TRANSFORMATION SUMMARY

NDR platform with Central Manager, Flow Collectors, Sensor Data Store, DC/DR HA design, and 24x7 support