AI for Networks
Networks for AI

Deliver High-Fidelity Network Detection and Response

with Aviz Networks and OpenText™ Network Detection & Response

Executive Overview

Organizations rely on Network Detection and Response (NDR) platforms to identify advanced threats that evade traditional security controls. However, **the effectiveness of NDR depends entirely on the quality, completeness, and context of the network traffic it analyzes.**

As enterprise networks expand across on-premises data centers, campus environments, edge locations, and hybrid multi-cloud infrastructures, security teams struggle to deliver the right traffic to detection platforms. Capturing all traffic overwhelms NDR sensors with noise, while incomplete visibility creates blind spots—particularly in East–West traffic where lateral threats commonly occur.

The joint solution from **Aviz Networks** and **OpenText™ Network Detection & Response** ensures that OpenText™ NDR sensors receive **optimized, enriched, and high-quality network traffic**, enabling more accurate detections, faster investigations, and reduced alert fatigue across modern enterprise networks.

High-fidelity NDR starts with intelligent network traffic.

The Challenge: Detection Is Only as Good as the Traffic

Despite investments in NDR technologies, organizations continue to face detection gaps due to the limitations of how network traffic is captured and delivered.

Key challenges include:

- Fragmented traffic across data center, campus, edge, and cloud environments
- Excessive traffic volume with insufficient filtering and deduplication
- Blind spots in East–West, overlay, and encrypted traffic
- Limited context from logs alone
- Alert fatigue caused by noisy and redundant data

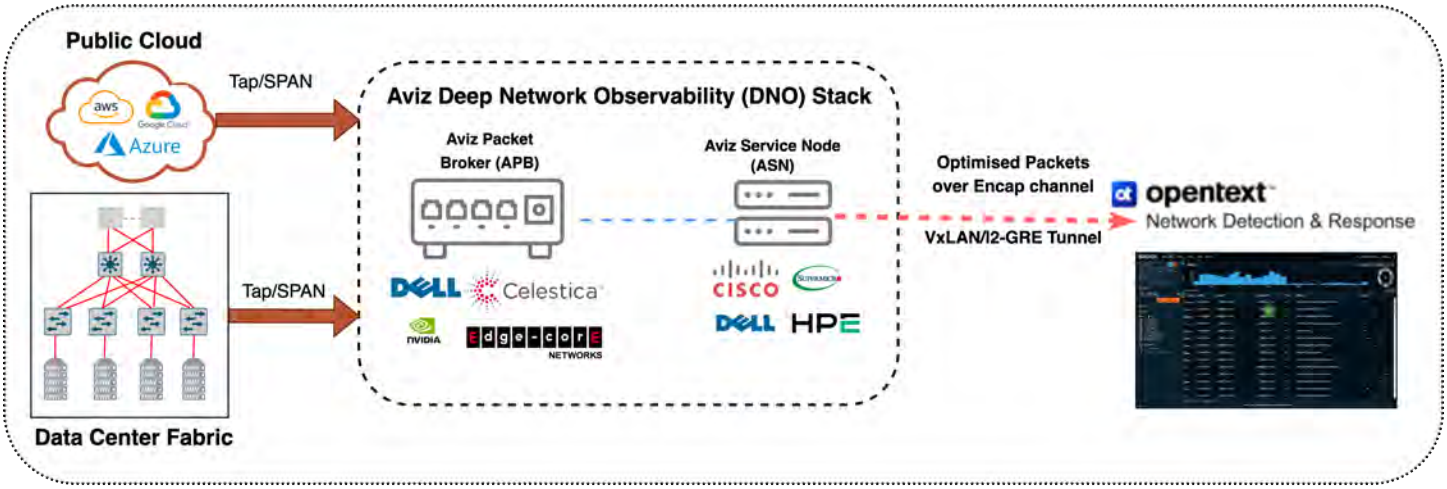
Without intelligent traffic optimization, NDR platforms cannot consistently deliver high-confidence detection outcomes.

Copyright 2025. All rights are reserved

The Joint Solution: Intelligent Traffic for High-Fidelity NDR

The Aviz Networks and OpenText™ Network Detection & Response joint solution introduces an intelligent traffic intelligence layer between enterprise networks and OpenText™ Network Detection & Response sensors. This ensures that only relevant, optimized, and context-rich traffic is delivered for analysis and evaluation.

Aviz Deep Network Observability (DNO) Stack



Aviz Packet Broker (APB)

Provides traffic acquisition and first-level optimization by tapping and aggregating traffic across data center, campus, edge, and cloud environments. APB applies centralized filtering and overlay-aware processing (VXLAN, ERSPAN) to remove noise before analysis.

Aviz Service Node (ASN)

Delivers advanced traffic intelligence, including packet deduplication, L4–L7 application identification, and metadata generation. Optional NVIDIA DPU acceleration enables high-performance processing at scale.

OpenText™ Network Detection & Response

OpenText™ Network Detection & Response consumes optimized traffic and enriched metadata from Aviz DNO to deliver high-fidelity Network Detection & Response, detecting lateral movement, insider threats, encrypted attacks, and both known and unknown

Key Outcomes

- Improved detection accuracy through high-quality traffic
- Reduced alert fatigue by eliminating noise
- Faster threat investigation and response
- Lower infrastructure and tooling costs
- Scalable NDR across hybrid and multi-cloud environments

Together, Aviz Networks and OpenText™ Network Detection & Response deliver confident, high-fidelity threat detection by unifying deep network observability with advanced NDR analytics.

Copyright 2025. All rights are reserved