Case Study

Enabling Digital Transformation at Scale:

Unified Visibility for Security Delivery and Digital Services for Telecom

Agility with Peak Performance Network Security at 100Gbps

CUSTOMER

Customer is a large multinational telecommunication operator and multi-play service provider focused on digital infrastructure and services, and aims to enrich lives and stimulate human growth through technology. It has market share in domestic and international telecommunication markets and in business and residential domains.

Operating across ten countries in the Middle East, North Africa, and Southeast Asia, the customer offers services including mobile and fixed-line connectivity, broadband internet, cable television, and corporate managed services. It has been among the early movers in launching commercial 5G networks in its regions and is increasingly positioning itself not just as a telecom operator but as a provider of digital services. infrastructure and transformation investing in subsea cables, data centers, API platforms, cloud, and AI partnerships, private 5G for enterprise, and expanded business services offerings.

CHALLENGE

Customer faces several critical challenges as it continues to strengthen its position as a leading digital infrastructure provider. A key priority is achieving unified visibility across its multi-tenant data centers, which requires centralized 100Gbps high-speed network packet data capture, based on security IOC triggers, and processing logs to ensure both performance and security. Equally important is proactive security, with a demand for a dependable Network Detection and Response (NDR) solution capable of handling scalable and secure logs as well as packet data record archives, while seamlessly integrating with Elastic Search database management to support advanced analytics.

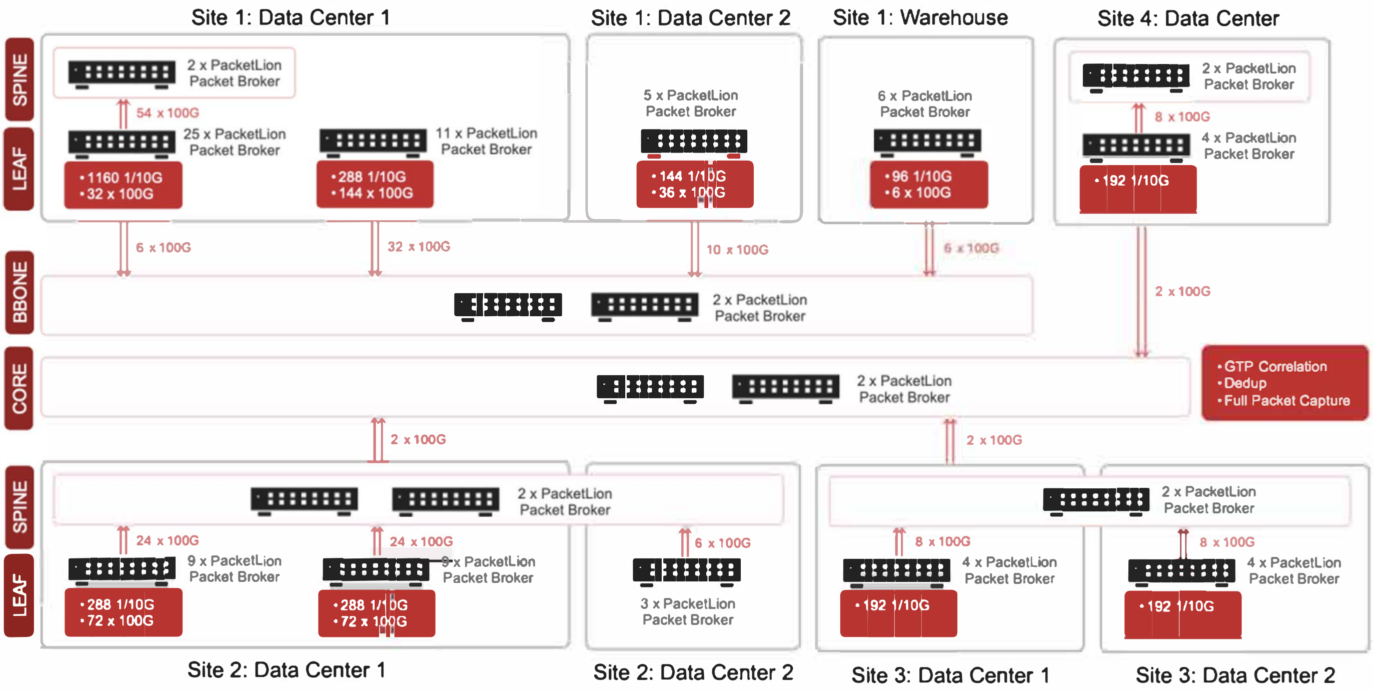
Customer also requires robust policy control, allowing its security teams to define, customize, and manage rulesets easily while ensuring smooth integration with existing SOC workflows and tools such as SIEM platforms. In addition, the customer must guarantee high availability of its systems through active/standby high-availability provisioning across data center sites, minimizing downtime and ensuring uninterrupted services for its end customers.
Finally, service and support remain essential, as the customer depends on highly personalized support that extends through deployment and

beyond, ensuring that solutions are not only effectively implemented but also maintained and optimized over time.

Collectively, these challenges highlight customers' focus on building a resilient, secure, and scalable infrastructure that underpins its mission to deliver world-class digital services across its global markets.

SOLUTION

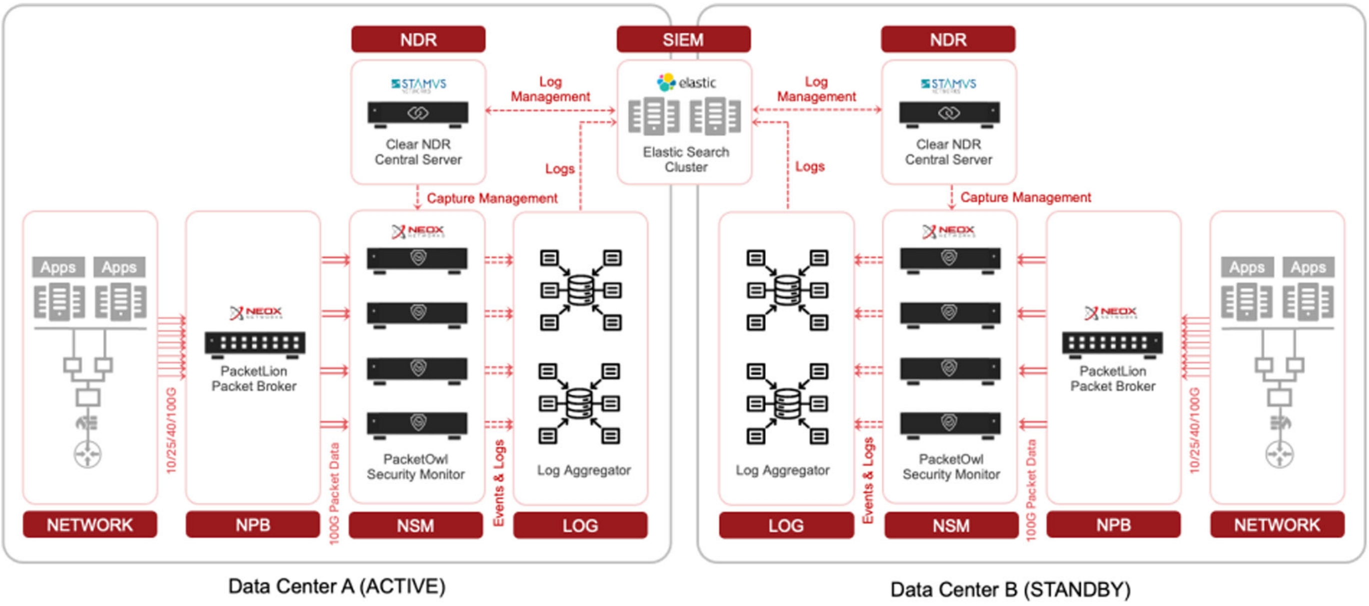
NEOX Networks is the expert in providing advanced Network Visibility solutions for IT and OT observability and security. Stamus Networks delivers the next generation transparent network defense through Clear NDR – cyber defense to uncover and stop serious threats and unauthorized network activity before they harm organizations. The solution for the customer comprises building a highly scalable multi-tier network visibility architecture based on the NEOX PacketLion series of Network Packet Brokers, which aggregates and consolidates the network packet and flow data for centralized processing (such as deduplication, filtering, GTP correlation, and packet capture) and forwards it to the security infrastructure.



Site 1: Data Center 1
Site 1: Data Center 2
Site 1: Warehouse
Site 4: Data Center
SPINE
LEAF
2 x PacketLion Packet Broker
54 x 100G
25 x PacketLion Packet Broker
•1160 1/10G •32 x 100G
11 x PacketLion Packet Broker
•288 1/10G •144 x 100G
5 x PacketLion Packet Broker
•144 1/10G •36 x 100G
6 x PacketLion Packet Broker
•96 1/10G •6 x 100G
2 x PacketLion Packet Broker
8 x 100G
4 x PacketLion Packet Broker
•192 1/10G
6 x 100G
32 x 100G
10 x 100G
6 x 100G
2 x 100G
BBONE
2 x PacketLion Packet Broker
CORE
2 x PacketLion Packet Broker
•GTP Correlation •Dedup •Full Packet Capture
2 x 100G
2 x 100G
SPINE
LEAF
2 x PacketLion Packet Broker
24 x 100G
9 x PacketLion Packet Broker
•288 1/10G •72 x 100G
24 x 100G
9 x PacketLion Packet Broker
•288 1/10G •72 x 100G
6 x 100G
3 x PacketLion Packet Broker
2 x PacketLion Packet Broker
8 x 100G
4 x PacketLion Packet Broker
•192 1/10G
8 x 100G
4 x PacketLion Packet Broker
•192 1/10G
Site 2: Data Center 1
Site 2: Data Center 2
Site 3: Data Center 1
Site 3: Data Center 2

The security infrastructure consists of NEOX PacketOwl Network Intrusion Detection (NIDS) and Security Monitoring (NSM) appliances, an advanced, high-performance network packet-data-based network security platform, designed to identify, analyze, log, and alert in real-time, as well as capture the event-triggered packet data (PCAP) for forensics and incident response. With its lossless, high-throughput design, the PacketOwl can capture and analyze up to 100Gbps of sustained network traffic, making it the highest-performance Suricata-based open platform in the industry at the time.

Stamus and NEOX Clear NDR solution delivers actionable insights with guided threat hunting and automated alert triage, including high-fidelity Declarations of Compromise™ (DoC) and Declarations of Policy Violations™ (DoPV). Clear NDR is a proactive cybersecurity defense solution designed to detect, analyze, and respond to emerging threats within customers' networks. It uses advanced analytics, machine learning, and behavioral analysis to monitor network traffic, detect threats, and unauthorized activity in real-time.



In the customer data center environment, PacketLion(s) aggregate north-south and east-west traffic to be fed into a cluster of PacketOwl(s), which pre-process the traffic for Clear NDR. PacketOwl(s) also serve as event-triggered capture points based on Clear NDR central server signals. The event logs generated are fed into log-aggregation systems and then into an Elastic Search cluster for analysis and management. The solution, therefore, fully meets customer requirements.

VALUE

The customer selected the NEOX and Stamus solution because of the clear value and superiority it offered, as below:

> "With NEOX and Stamus solution, we have gained the confidence that our critical digital infrastructure is secure, resilient, and future-ready. The unified visibility and advanced detection capabilities not only strengthen our defenses against evolving threats but also empower our teams to act proactively. This has reduced operational risk, improved compliance, and ultimately allow us to focus on delivering advanced services and greater value to our customers while driving our digital growth strategy."
>
> **Anonymous**
> Head of Security Operations & Architecture

Unified Visibility

- Visibility and security from a single source with pre-integrated Stamus Clear NDR and NEOX PacketLion and PacketOwl visibility solutions
- High-performance FPGA architecture of NEOX appliances with conditional-PCAP and encrypted SED storage

Proactive Security

- Intuitive, scalable, and easy-to-use Clear NDR for threat hunting and incident response
- Seamless integration with Elastic Search database
- On-premises solution with no cloud or internet dependency

Policy Control

- Open-source architecture with free definable and adjustable rulesets, no restrictions

- Easy integration with third-party SIEM or other SOC systems

High Availability

- Active/Standby HA provisioning across sites

Service and Support

- Personalized service with on-site deployment and ongoing technical support

NEOX Networks provides Next Generation Network Visibility for IT & OT Observability and Security. The result is strengthened cybersecurity, hybrid-cloud application observability, and business continuity, by integrating the network intelligence and real-time data-in-motion. Learn more at neoxnetworks.com

Stamus Networks delivers the next generation of open and transparent network defense. Trusted by security teams at the world’s most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Learn more at stamus-networks.com