PacketXpress: Turning Network Visibility from a Cost Center into an Advantage

Reducing the Cost of Network Visibility

Enterprise network visibility teams face increasing performance demands alongside rising infrastructure costs. Network speeds and east–west traffic continue to grow, while AI-driven datacenter expansion is driving up server, memory, and NVMe storage costs. Traditional Network Data Recorder (NDR) architectures scale linearly with traffic and peak bandwidth, forcing tradeoffs between retention, analytic coverage, and cost. PacketXpress® was engineered to eliminate this tradeoff by redesigning how packets are captured, stored, and consumed

The Cost Problem with Traditional NDR Architectures

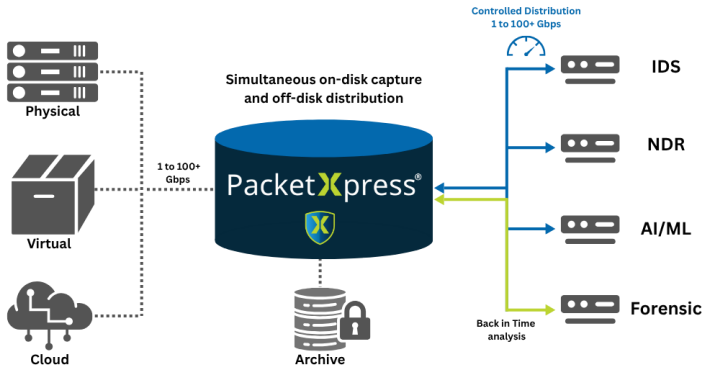
Conventional NDR deployments rely on packet brokers feeding live traffic directly into downstream analytics and dedicated PCAP storage appliances. Each tool must process packets at wire speed, requiring systems to be sized for peak traffic conditions rather than normal operating loads. As network speeds increase to 40 Gbps and higher, this architecture drives rapid growth in:

- NVMe storage capacity to maintain retention
- RAM requirements to sustain lossless capture
- CPU cores to analyze traffic in real time
- Physical appliances to avoid packet loss

The result is escalating capital and operational expense, fragmented visibility, and underutilized infrastructure during non-peak periods.

PacketXpress: Designed to Reduce Cost

PacketXpress introduces a data-centric visibility architecture where packets are captured once, optimized at ingest, and shared through controlled, software-defined interfaces. By improving storage efficiency, analytic efficiency, and hardware utilization together, PacketXpress reduces costs across the visibility stack without sacrificing fidelity or performance.



Axellio PacketXpress - The Network Intelligence Platform

XpressFS™: High Performance File System

At the core of PacketXpress is XpressFS, a purpose-built file system optimized for high-throughput packet capture and time-series data. Unlike general-purpose file systems, XpressFS is designed for low-latency, high-bandwidth streaming and extreme concurrency.

XpressFS decouples packet ingest from downstream consumption using built-in buffering, enabling concurrent reads and writes without impacting capture performance. The file system scales to many petabytes across multiple servers while maintaining consistent performance.

XpressFS supports stream- and time-addressable access through standard APIs and direct mount, while performing compression, deduplication, filtering, and encryption at speed to reduce storage footprint without sacrificing analytic fidelity.

PacketXpress – System Sizing Chart

Typical PacketXpress Deployment Characteristics

Sustained Capture Rate	CPU Cores	System Memory	NVMe SSDs
10+ Gbps	16-24 cores	~64 GB RAM	2+ NVMe SSDs
40+ Gbps	10-16 cores	~128 GB RAM	3+ NVMe SSDs
100 Gbps	28-32 cores	~256 GB RAM	6+NVMe SSDs

** This chart provides general system-sizing guidance based on typical PacketXpress deployments. Actual requirements vary depending on traffic composition, enabled features such as compression or encryption, retention goals, and extraction workloads. Axellio works with customers to validate performance on their specific hardware platforms.*

Intelligent Payload Slicing: Eliminating Low-Value Storage

Encryption is now pervasive across enterprise and mission-critical networks, extending beyond HTTPS to include machine-to-machine TLS, encrypted file transfers, east–west service communications, and proprietary protocols. Most security and performance analytics tools do not decrypt payloads, rendering encrypted payload data unusable while still consuming significant storage capacity.

PacketXpress Intelligent Payload Slicing identifies encrypted payloads at capture and removes just the payload portion, retaining packet headers, flow metadata, and relevant session attributes. This eliminates low-value data while maintaining analytic fidelity for detection and investigation. While heavily dependent on the type of network traffic, we typically see a 60-95% reduction in packet storage volume allowing up to 20x longer PCAP history storage.

Supported protocols include TLS 1.1, 1.2, and 1.3; SSL 3.0; DTLS 1.0 and 1.2; SSH-2.0; QUIC v1, v2, and draft implementations; WireGuard; IPsec ESP; SMB3; MsgType 1–4; and Veem. This ensures consistent storage reduction and analytic fidelity across both enterprise and mission-critical encrypted traffic.

Integrated Flow Generation: Faster Insight, Less Data Movement

PacketXpress generates network flow records in parallel with full packet capture, providing immediate, queryable visibility without requiring access to raw PCAP data. By enabling flow-based pivots, filtering, and targeted packet extraction, PacketXpress:

- Accelerates threat detection and triage
- Reduces unnecessary data reads from storage
- Lowers downstream compute and I/O utilization
- Shortens investigation timelines

Flows and packets remain tightly correlated, allowing analysts to move seamlessly from high-level trends to precise packet-level evidence only when needed.

PacketXpress provides integrated indexing, long-term archiving, and real-time visualization. Indexed packet and flow data enables rapid search and retrieval, while Grafana dashboards provide visibility into traffic behavior, protocol activity, and system performance.

Buffered Analytics: Decoupling Capture from Analysis

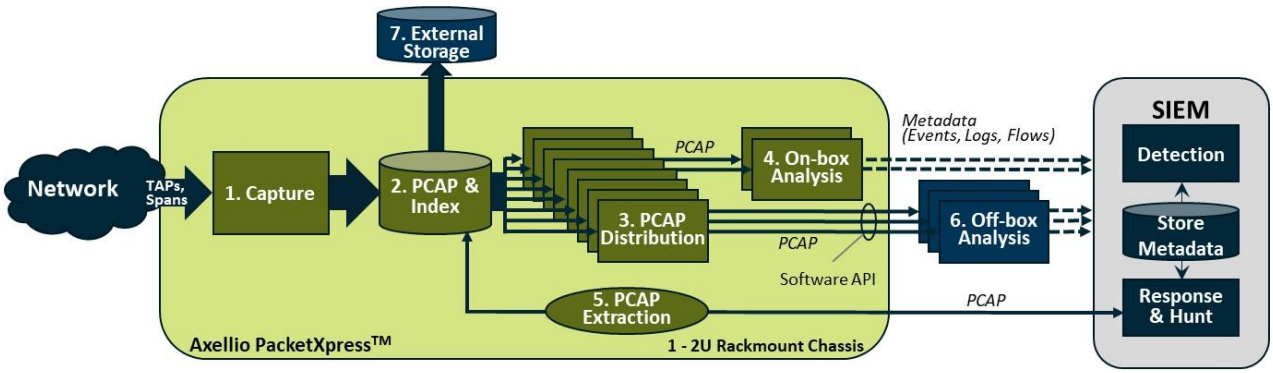
Traditional NDR environments must size analytics for peak traffic, resulting in oversized systems that remain underutilized most of the time.

PacketXpress decouples packet capture from packet analysis by buffering traffic in high-speed storage. Analytics consume data at their own rate rather than at line rate, allowing infrastructure to be sized for sustained workloads instead of worst-case bursts.

This architecture:

- Reduces CPU and memory requirements
- Lowers the number of required analytic servers
- Eliminates idle capacity during normal operation
- Maintains deterministic, lossless capture

PacketXpress is composed of multiple integrated software services that operate together to manage capture, storage, indexing, analytics access, and system orchestration. These components are tightly coupled through the PacketXpress software stack, ensuring consistent performance, reliability, and operational simplicity as deployments scale.



Virtualized and Containerized Analytics Deployment

PacketXpress enables analysis applications to run as virtual machines or containers, either directly on the capture node or on external virtualization platforms. This virtualization-first approach increases application density per server, simplifies scaling, and allows new tools to be deployed without additional physical hardware.

As server, memory, and storage costs fluctuate due to AI and hyperscale demand, PacketXpress provides a flexible and future-proof way to control infrastructure spend while maintaining full visibility coverage.

Flexible Deployment Models: On-Premises and Cloud

PacketXpress supports flexible deployment across on-premises, private cloud, and public cloud environments. The platform deploys in traditional datacenters as well as cloud-based infrastructures, enabling organizations to align visibility architectures with operational, security, and cost requirements.

PacketXpress delivers consistent capture, storage, and analytics across dedicated hardware, virtualized infrastructure, and cloud platforms—enabling hybrid deployments without workflow redesign.

Designed for High-Speed, Mission-Critical Environments

PacketXpress has been deployed in environments requiring Risk Management Framework (RMF) and STIG alignment, supporting secure configuration, controlled access, and auditability in regulated and mission-critical networks. The PacketXpress secure development lifecycle includes automated Fortify Static Code Analysis to identify common software weaknesses such as injection flaws, insecure data handling, and improper error management. Early detection and remediation of these issues improves software resilience, reduces downstream patching requirements, and provides additional assurance for security assessment and authorization processes.

PacketXpress is purpose-built for modern, high-speed networks supporting:

- 40/100/400 Gbps links
- East–west and north–south traffic
- Hybrid, multi-cloud, and containerized environments
- Security operations, forensics, and performance analysis

By capturing once, optimizing early, and enabling controlled consumption of packet data, PacketXpress allows organizations to extend retention, reduce hardware growth, and respond faster—without redesigning their architecture as traffic scales.

PacketXpress changes the economics of network visibility by capturing once, optimizing early, and decoupling capture from analysis—allowing organizations to scale visibility without scaling cost.

AXELLIO

Axellio mission is to control data overload in timeseries analysis systems that monitor for threats to our infrastructure through innovative storage and distribution solutions. Axellio innovative software solutions simultaneously capture, store, analyze, and distribute any streaming data exceeding 100 Gbps in a scalable but extremely small footprint.

www.Axellio.com