Solution Brief

PacketXpress™
High-Speed Packet Capture

Protect IT Operations from Information Loss and Network Infiltration

With security and network operations collecting increasing amount of network and device information across a growing number of monitoring and analysis applications, forensic analysis teams are still left with not enough detail to get to root cause and mitigation. Furthermore, this expensive infrastructure is still vulnerable to traffic overload situations due to significant traffic growth in the network that overloads the analysis and monitoring infrastructure.

Axellio developed PacketXpress to provide detailed packet data for any event and buffer the monitoring and analysis infrastructure from traffic spikes, which extends the useful life of the diverse security, network, and application operations infrastructure while reducing operation costs.

PacketXpress captures and indexes at a sustained 100 Gbps rate with zero packet loss across a variety of high-speed ethernet interfaces. It simultaneously allows for real-time traffic distribution and data analysis at sustained 100 Gbps rates with no impact on capture performance. Furthermore, rather than requiring racks of equipment, PacketXpress is a 3-rack unit solution.

CURRENT MONITORING APPROACH LEAVES ORGANIZATIONS VULNERABLE

To assure security, services, and application delivery, IT operations over many years have optimized the real-time analysis of network traffic and device information as the most economical approach to address infrastructure availability and performance. Collecting statistical information such as NetFlow, events, or aggregated data allows for use of less storage and analysis for event detection, alarming, performance analysis and planning for network, application, and security operations.

As cost-effective as this approach might seem, it is really insufficient when it comes to detecting security vulnerabilities, getting to root cause, and validating mitigation attempts:

- **Detect –** When traffic spikes, capturing and indexing may not be able to keep up. Even though this has a limited impact on performance and traffic statistics, analysis and monitoring solutions such as Intrusion Detection Systems (IDS) can miss 10% of all IDS events with only 3% packet loss[1]. Knowing that many intrusions are often masked by Denial of Service attacks, this is particularly troublesome.
- **Resolve –** For root cause analysis of security, network, or application events, statistics and logs can provide proof that an event happened, or an intrusion took place, but often by themselves are insufficient to determine the exact circumstances to mitigate the situation. Pre- and post-event information is essential to determine how an intruder was able to get into the network and what information was compromised. This requires packet data that is often not available and capturing it after an incident requires the event to happen again. This is like putting security cameras in place after a break-in happened.

[1] É. Leblond/P. Manev, Stamus Networks, Nov 2019

- **Validate –** After implementing the mitigation or fix, it is essential to validate whether the issue has been resolved. Given the complexity of today's networks, simulations are often difficult to generate, but without the original packet data pre- and post-event, a validation of the fix is difficult at best.

These issues have tangible impact on the organization:

- IBM-Security stated in their "2019 Cost of a Data Breach Report" that a data breach to the average US company results in over 25,000 data records stolen, costing the company as much as $8.2M per data breach. Loss of customer trust and the resulting loss of business contributed 36% of the overall cost.
- Network and applications operations are not far behind: The cost of network downtime varies widely between organizations, but in even conservative estimates can amount to over $14M per year even as reported[2].

Therefore, it is essential that the monitoring infrastructure avoids data loss due to traffic spikes while providing instantaneously detailed packet data for vulnerability and root cause analysis, and validation of mitigation steps taken.

PACKETXPRESS – AN ECONOMIC APPROACH TO MANAGE MONITORING TRAFFIC LOADS AND CAPTURE ESSENTIAL PACKET DATA

PacketXpress captures and records sustained 100 Gbps with no packet loss across a variety of high-speed ethernet interfaces while also being able to provide sustained 100 Gbps real-time data analysis and traffic distribution to other analysis applications with no impact on capture performance. Furthermore, rather than requiring racks of equipment, PacketXpress is a single box, 3U high solution.

This addresses the above-mentioned issues:

- **Detect** – With 100 Gbps intake rate without loss, traffic spikes become a non-issue as PacketXpress buffers the packets, distributing them to analysis applications at their consumable rate.
- **Resolve** – Being able to continuously capture data from the network provides pre- and post-event information for root-cause analysis.
- **Validate** – With the actual packet data being available for any event, replay is viable to validate that the mitigation or fix has resolved the issue.

[2] Aberdeen Research 2019: $163,674/hour; Gartner 2018: Average downtime per year: 87 hours

Solution Brief

PacketXpress™
Highspeed Packet Capture

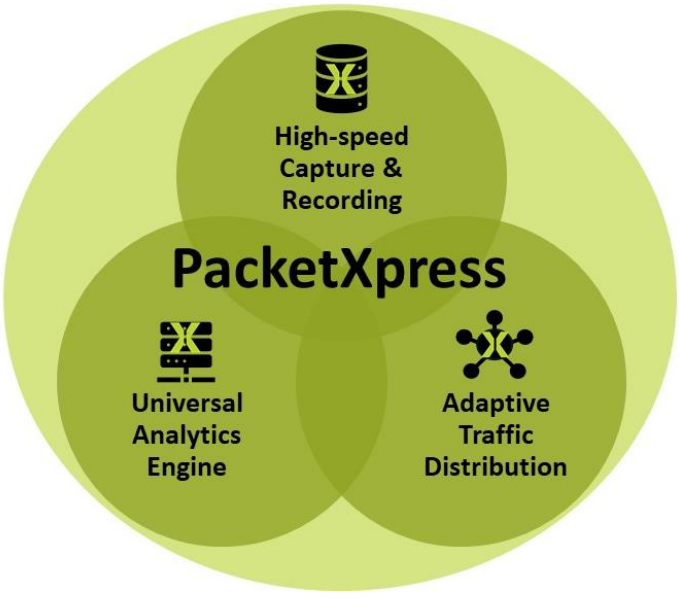
Axellio has optimized off-the-shelf hardware components through its unique Xpress Fabric software to optimize capture, storage, analysis, and packet extraction to overcome the issues that have prevented economic packet capture in the past:

- **Sustained 100 Gbps packet capture** with no packet loss
- **725 Terabyte of onboard storage** for back-in-time pre- and post-event analysis
- **Real-time data indexing and analysis** sustained at 100 Gbps with no impact on capture performance
- **Extract based on any information** – no indexing needed
- **Adaptive traffic distribution** sustained at up to full 100 Gbps to your existing onboard and offboard analysis applications while avoiding overload by automatically adjusting traffic to rates that applications can handle
- **Compact formfactor** - 3U standard industry rack formfactor provides a small footprint in size, weight, and power consumption - keeping CAPEX and OPEX costs low

PACKETXPRESS – PRIMARY FUNCTIONALITY

PacketXpress protects your investment in monitoring and analysis applications while reducing time-to-root-cause, cost of downtime, and data-breaches through:

- **High-speed capture and recording** - Accelerates time-to-root-cause:
  - Streamlining your analysis process and shortening time to resolution
  - Accelerating access to all pre- and post-event packet data
- **Adaptive Traffic Distribution -** Extend the useful life of your monitoring and analysis infrastructure while keeping up with network speed and traffic growth
- **Universal Analytics Platform -** For all your analysis and monitoring applications for efficient operation and investment protection



2375 Telstar Drive, Suite 150 | Colorado Springs, CO 80920 | 1.800.463.0297 | 1.719.309.3370 | www.axellio.com

Solution Brief

PacketXpress™
Highspeed Packet Capture

HIGH-SPEED CAPTURE & RECORDING – REMOVING THE CONSTRAINTS

Existing packet capture infrastructure is often complex and hardware intensive. This leads to a trade-off decision of when and where to record traffic, often only reactively deployed after an event happened. This creates additional complexity by often not knowing where to deploy the capture devices to ensure capture of all relevant packets.

Packet capture solutions on the market today require a lot of hardware to reliably capture, store, and analyze at rates significantly above 10 Gbps. Those solutions rely on expensive packet brokers to distribute the load across racks of servers and storage to keep up with the traffic. There are additional architectural constraints that further limit the simultaneous operation of indexing and storage:

- Realtime Indexing – Necessary to later extract relevant information, indexing has to be pre-configured and limited in scope to avoid consuming too many processing resources, which can negatively impact capture performance by up to 25%.
- SATA drives are used, which are inexpensive but only allow for either read or write operations at any given time. This means with today's solutions, capturing at high rates requires the user to only slowly extract data, delaying the analysis, or to perform packet analysis offline after capturing has been stopped.

PacketXpress, on the other hand, provides fast access to all packets anytime, pre- and post-event, with no need to filter down due to system performance limitations:

- Capture – High-speed intake, processing, and storage – sustained 100 Gbps intake with zero packet loss for all frame sizes.
- Simultaneous, high-speed read and write at intake speed – no need to wait for data, analysis can happen simultaneously while capturing data.
- Extract based on any information – with no indexing required, you can extract based on any information necessary. No need to anticipate what to index before you start the capture or having to perform lengthy post-capture filtering procedures.

ADAPTIVE TRAFFIC DISTRIBUTION – EXTEND THE USEFUL LIFE OF YOUR MONITORING & ANALYSIS INFRASTRUCTURE

Even though packet brokers have offloaded processing-intensive activities from your monitoring and analysis appliances, traffic growth and traffic spikes are still propagated from the network to the monitoring and analysis infrastructure, potentially overloading your analysis environment.

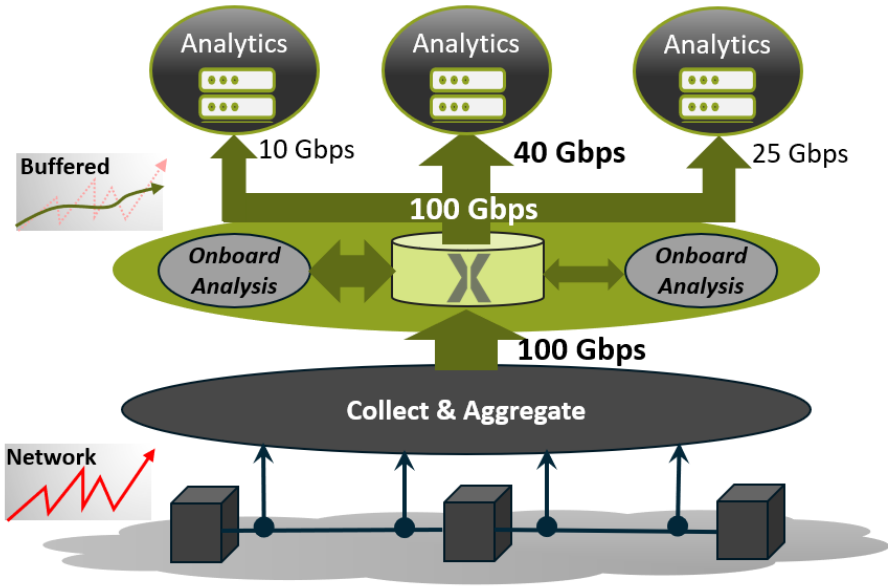
2375 Telstar Drive, Suite 150 | Colorado Springs, CO 80920 | 1.800.463.0297 | 1.719.309.3370 | www.axellio.com

PacketXpress™
Highspeed Packet Capture

This either leads to data loss, as traffic cannot be processed, or sampling of information resulting in an incomplete picture of the situation. This problem will become more pressing for many organizations with over 40% of US enterprises expecting 50% or more traffic growth over the next 12 months[3] in their networks.

Traffic spikes and growth may be acceptable for performance measurements and traffic statistic generation, but it has a devastating impact on security intrusion detection and root cause analysis. Even 3% packet loss can lead to 10% missed alerts, and 25% packet loss resulting in missing half of all intrusion alerts[4]. Furthermore, missing packets can seriously impact your ability to analyze root cause.

PacketXpress' ability to simultaneous perform read and write on up to 100 Gbps allows for real-time storage while distributing the captured traffic at controlled rates to other applications matching their intake rates. This "buffering" smooths out traffic spikes that would otherwise overload applications and lead to data loss. Furthermore, PacketXpress can filter traffic to reduce volume for each application as well.



Even more important, you are now able to go-back in time and re-run analysis after an event was detected.

This allows data analysis post-event via different applications or different analysis settings repeatedly and full validation of mitigations developed and deployed in your environment or test bed.

UNIVERSAL ANALYTICS PLATFORM – FOR ANY ANALYSIS & MONITORING APPLICATION FOR EFFICIENT OPERATION AND INVESTMENT PROTECTION

PacketXpress is a reliable, high-performance compute platform that allows for on-board operation of your analysis and monitoring applications. This provides better throughput and lower delay while avoiding dedicated, costly appliances. Its modular hardware and software configuration allow for extensible storage, memory, and processing (CPU and GPU) while offering standard OS environments in either bare metal, virtual, or in a hybrid environment.

[3] EMA "Network Management Megatrends 2020" – March 2020

[4] É. Leblond/P. Manev, Stamus Networks, Nov 2019

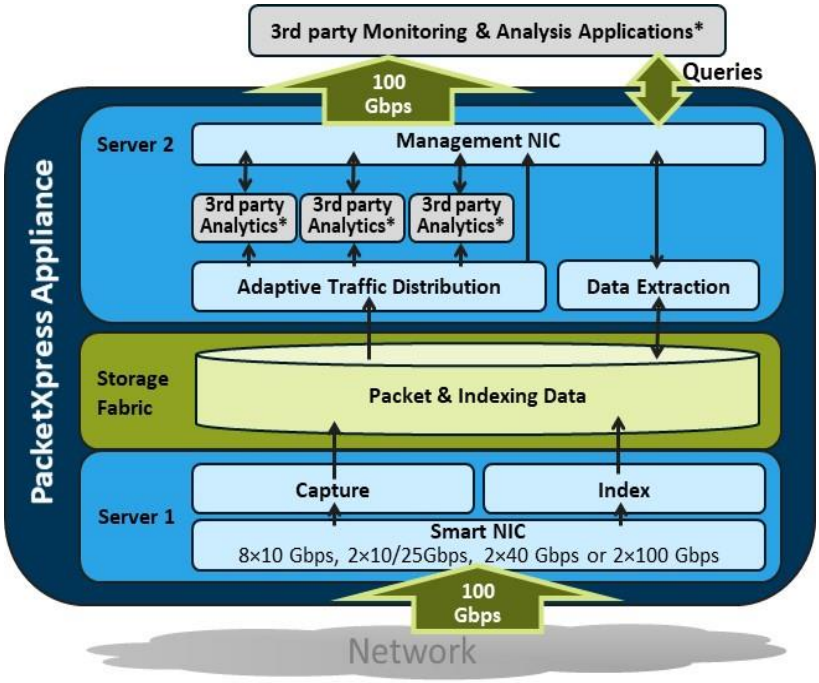
Solution Brief

PacketXpress™
Highspeed Packet Capture

PACKETXPRESS APPLIANCE – SPECIFICATIONS

PacketXpress has three primary components:

1. Server 1 with its high-speed smart NIC
2. The Xpress Fabric-enabled storage component to retain and access packet data
3. Server 2 for adaptive traffic distribution and onboard analysis via third-party analysis applications such as IDS (e.g. Zeek), SIEMS (e.g. Splunk) or forensics (e.g. Security Onion), NPM or APM (e.g. Solarwinds) or packet analysis (e.g. Wireshark), or any other application.



DATASHEET

Network Connectivity	•	Inline or Tap/Span port connect
	•	Ethernet connectivity via two QSFP28: 8×10 Gbps, 2×10/25Gbps, 2×40 Gbps or 2×100 Gbps
	•	Tunneling: GTP, IP-in-IP, GRE and NVGRE
Hardware Accelerated	•	Zero packet loss for all frame sizes (including Jumbos)
	•	Filtering: L2 - L4 with stateful flow management
	•	Deduplication, slicing (fixed or dynamic offset), multi-port packet merge, IP fragment handling
Time Sync	•	IEEE 1588-2008 PTP and PPS – PCAP and UNIX
	•	1 ns time stamp resolution
Storage	•	Up to 725 Terabytes via 48 hot-swappable solid state drives
Distribution Connectivity	•	Up to 16 streams of up to 100 Gbps adaptive traffic distribution to feed external applications across different interface configurations
Processing	•	20 Million IOPS, 240 GBps system throughput
	•	Two servers per chassis each with two Intel Xeon Cascade Lake Servers: up to 56 cores/112 threads per server, up to 2TB of RAM
Extensible	•	Additional PCIe slots for GPUs, for NVMe SSDs, or other PCIe cards
Formfactor	•	3U high, 30-inch deep for Industry Standard Rack mounting
	•	N+2 Redundant power supply

2375 Telstar Drive, Suite 150 | Colorado Springs, CO 80920 | 1.800.463.0297 | 1.719.309.3370 | www.axellio.com