Axellio PacketXpress – The Network Intelligence Platform

Scalable, Simultaneous, Always-On
Recording and Distribution at over 100 Gbps

AXELLIO®

Founded: 2018, US owned and operated

HQ: Colorado Springs, CO, USA

Background: 20 years in high-performance enterprise storage solutions

Target Market: Network and Security Operations in:

- Defense
- Intelligence
- Commercial Enterprise

Product: PacketXpress®
High-speed network packet data capture, storage, distribution, control, and analysis platform

Applications:

- Cyber security threat detection and response
- Financial trading & market data analysis
- Low SWaP, high-speed capture, and distribution
- Other inline packet assessment & control

US Government Contracts:

- GWACs include NASA SEWP and CIO CS
- Under contract with DoD/Army since 2020 delivering cyber solutions

ISO 9001:2015 Certified

Axellio® PacketXpress® is the network intelligence platform to capture, store, analyze, and distribute all network traffic in an extremely small footprint at over 100 Gbps. It is designed to enhance the performance, efficiency, and accuracy of your existing security analysis applications.

PacketXpress provides an open, scalable platform capable of handling over 100 Gbps traffic with no loss, while simultaneously providing access to all data directly from disk at over 100 Gbps for real-time or forensic analysis applications. For real-time analysis, it increases the performance and accuracy by avoiding overload situations and the resulting blind spots. For historical forensic analysis as well as mitigation validation, PacketXpress replays any pre- and post-event packet data at any speed for in-depth analysis.

PacketXpress is scalable and extensible from mobile deployments to multi-rack datacenter and distributed solutions. It complements any existing security analysis infrastructure, making any network analysis application more resilient while reducing licensing costs.

Today's Network Security Monitoring Approach – Complex, Costly, Ineffective

Visibility of network traffic across the perimeter and the core of the infrastructure is more important than ever in times when advanced threat actors circumvent traditional perimeter and endpoint protection. Once inside, attackers are spending months performing reconnaissance to map out the target infrastructure and defenses, preparing material for exfiltration, and planting additional malware.

Many security organizations are overwhelmed by the current monitoring solutions, the resulting operational costs, and the expertise needed to quickly triage, prioritize, and respond to an ever-increasing number of threats. This has driven many organizations to limit their traffic monitoring to the ingress and egress points of their infrastructure. Internal network traffic, virtual, and cloud traffic is then not being monitored or just analyzed using a more limited metadata approach, relying on event logs and traffic flow data from infrastructure devices, routers, and switches.

Although metadata is efficient to detect suspicious activities, it is often insufficient for triage, assessing the spread of the intrusion, determining the required incident response techniques, or to perform forensic analysis. In addition to increasing the time to detection and mitigation, it also allows threat actors to maintain persistence longer, increasing their chances of success and the impact of their attacks.

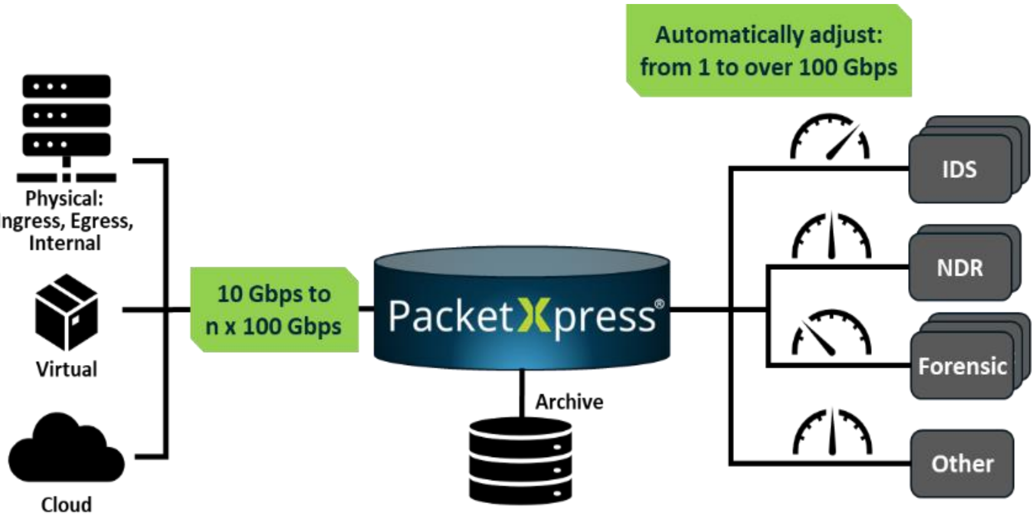
To identify and handle threats in the infrastructure, security teams must have better network visibility. But monitoring and analyzing all network traffic is considered complex and costly and therefore often quickly dismissed. Network Detection and Response (NDR) solutions entered the market over the last few years to address some of those concerns, but they also are focused primarily on threat detection. Consequently, the traffic that was analyzed is quickly discarded, and only the event-relevant information is maintained to minimize data storage requirements. However, this degrades the effectiveness of incident analysis.

Therefore, many organizations have reverted to an on-demand traffic capture and analysis or have limited deployments only at strategic points in the network, such as ingress and egress points. This leaves many visibility gaps especially when Packet Capture (PCAP) devices are only capturing limited conversations of interest.

Axellio PacketXpress - the Network Intelligence Platform

Rethinking Network Traffic Analysis

Leveraging the latest storage and server architecture technologies, Axellio developed a high-speed, high-intake network visibility platform for packet capture, storage, analysis, and distribution in an extremely small footprint. Designed for the needs of defense and intelligence agencies and global security operations, PacketXpress combines the benefits of network packet capture and network packet broker solutions. PacketXpress buffers incoming traffic, allowing monitoring and analysis tools to ensure they never drop a packet even under high traffic conditions. As a result, analysis applications can be deployed as software-only solutions, virtualizing the previously hardware-centric approach while storing all packets.



Axellio PacketXpress - The Network Intelligence Platform

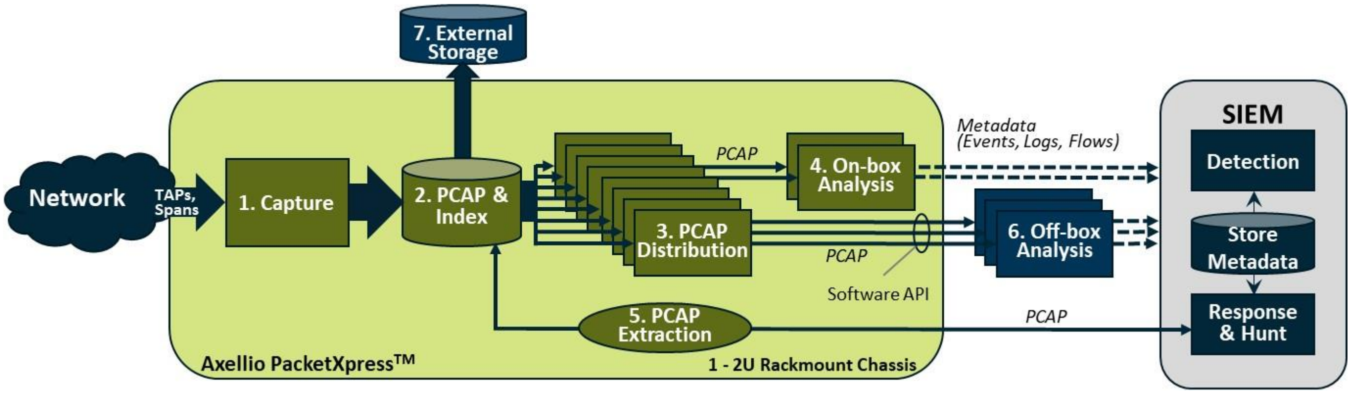
- **Collect anywhere** – at any speed:
  - Collect traffic from the physical ingress-egress, the internal network, to virtual, and cloud.
  - No loss capture at any speed – from 10 Gbps to well over 100 Gbps sustained simultaneous data ingest, recording, and distribution.
- **Adaptive traffic distribution** – to any analysis application:
  - Reliable software APIs – distribute traffic at controlled, application consumable rates with no loss.
  - Rewind, replay, re-analyze – for repeated in-depth analysis, mitigation validation, and training.
  - Multiple data extraction streams can be individually configured for speed and content.

- **Universal platform for any application** – tailored to your specific needs:
  - Flexible form factor – from mobile to multi-rack data center configurations delivered on common-off-the-shelf (COTS) hardware.
  - Expandable storage – from hours to months – local or external.
  - Customizable – from the software to off-the-shelf hardware to fit your environment.
  - Dense footprint – offered from 1U and up, depending on capacity & intake rates.

PacketXpress provides a flexible architecture with speed at its core, allowing Axellio to quickly add new capabilities to meet almost any use case that utilizes network packets.

PacketXpress - An Open Platform

Built as a dense, high-performance platform, PacketXpress integrates leading-edge server and storage technologies and a patent pending file system for a diverse set of use cases and analysis applications. PacketXpress provides the industry's highest sustained performance in the smallest footprint:



PacketXpress Architecture

High-speed capture & recording – from 10 Gbps to multiple 100 Gbps without losing a packet:

- Ability to monitor across physical, virtual, containerized, and cloud environments using commercially available TAPs (Test Access Points), SPANs (Switched Port Analyzer) and R-SPANs (Remote SPAN), virtual TAPs, and cloud service offered mirroring services.
- Hardware-based traffic filtering, deduplication, and slicing allows for selective traffic capture as necessary while time stamping every packet with nano-second accuracy.

Storage – simultaneous read and write at over 100Gbps for on-disk-storage for days, weeks, or months:

- Scalable storage – NVMe SSD drives with an onboard storage capacity of several petabytes in just a single 1U or 2U server.
- Long-term, off-box archival and compression to further extend storage capacity at reduced cost.
- Secure data through data at rest encryption.

Adaptive traffic distribution – near real-time, content- and rate-controlled traffic distribution directly from disk via standard software APIs:

- Multiple data extraction streams can be flexibly and individually configured in both speed and content, based on a 5-tuple configuration (source/destination address, protocol, and port number) or via the rich filter capabilities of the Berkeley Packet Filter (BPF).
- Automatically adjusting traffic to rates the analysis applications can reliably consume.
- Open web API for PCAP retrieval for onboard and offboard analysis applications in either physical or virtual environments.

Analysis application agnostic – software-based, hardware-agnostic access to packets anytime for any event, with direct integration in your existing workflow:

- Application agnostic – deploy any analysis application on-board using any standard OS or distribute to any outside analysis applications.
- Ability for dynamic queries without the need to pre-define indexing at time of capture, offering more flexible and dynamic analysis capabilities for the unexpected.
- Multi-pass analysis – The ability to rewind, replay, re-analyze for repeated in-depth analysis and mitigation validation.

Open platform – scalable and economical – lowest footprint and cost to performance ratio in the industry while scaling from mobile to distributed datacenter deployments:

- Economical – Delivered on COTS technology from any major vendor to reduce maintenance and procurement costs.
- Small form factor – Offered in 1U to 2U depending on capacity and intake rates, reducing Size, Weight, and Power (SWaP) for mobile deployment and easy transportation.
- Scalable – Multiple instances of PacketXpress can be deployed for even higher performance in data center type applications or for distributed deployment.

PacketXpress – The Analysis Edge You Need for Your Environment

Close the visibility gap – go beyond the metadata:

- Broaden the view – extend visibility into external, internal on-prem, virtual, and cloud.
- Provide immutable evidence – immediate access to any pre- and post-event packet data.
- Avoid going blind when traffic spikes – keep up and increase analysis accuracy.

Increase operational effectiveness – for rapid and informed decisions:

- Fast access to all pre- and post-event packet data – for all events, anytime, anywhere.
- Local and remote access – wherever your experts are located.
- Validate mitigation – Ensure that the corrective measures are effective.

Reduce total cost of ownership & complexity – monitor your entire infrastructure:

- Centralize hardware intensive processing and reduce hardware sensor proliferation and complexity.
- Manage traffic rates to your analysis applications, avoiding licensing for peak traffic rates and efficiently managing network and traffic growth.
- Integrate seamlessly and leverage your existing analysis infrastructure – no retraining or workflow changes, just better data.

Contact us

Find out how PacketXpress can make a difference for your application:

www.axellio.com	**+1 (800) 463-0297**
contactus@axellio.com	**+1 (719) 309-3370**

The above specifications are based on the configuration supported as of the date of the publication and may change without notice. Axellio shall not be liable for technical or editorial errors or omissions contained herein. Please contact us for the latest information.