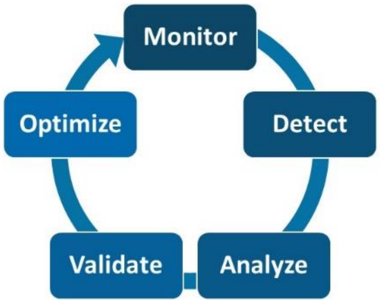
Axellio PacketXpress

Use Cases Across the Network & Security Operational Lifecycle

PacketXpress® addresses many challenges across the network and security operational life cycle in commercial enterprises and defensive cyber operations teams in government agencies:



- Monitor more traffic economically for complete visibility.
- Detect events reliably and prevent false or missed events under high traffic load.
- Triage, analyze, and resolve incidents with the complete event details that alarm and event notifications do not provide.
- Validate countermeasures before deployment with actual event traffic.
- Optimize the stability, speed, scalability, and responsiveness of network & security infrastructure even under high traffic load.

Monitor for Complete Visibility

Current Situation	Many organizations consider traffic monitoring complex and expensive, and in response they limit their monitoring to strategic points in the network, focusing mainly on ingress and egress points. The remainder of the infrastructure is monitored via alarms, event logs, and traffic flow data. However, with threats penetrating any perimeter defense, no matter how secure, failing to monitor internal traffic makes organizations vulnerable.
PacketXpress Capabilities	Monitor more traffic via your existing network infrastructure while providing richer insight for forensic analysis. It collects, tags, and immediately stores all traffic from multiple network sources while simultaneously distributing directly from disk packets to analysis systems at speeds they can reliably ingest.
Benefits	• Analysis tools can now be sized and licensed for the average intake speed, not for peak traffic rate, saving hardware and software licensing costs. • Free up monitoring and analysis capacity to monitor additional points in the network (e.g., adding East-West traffic to the already monitored North-South traffic).

Detect Events Accurately in High Traffic

Current Situation	Monitoring and analysis applications are easily overwhelmed in high-traffic situations, such as traffic spikes or DDOS events. This results in not analyzing all traffic and letting attacks slip through undetected.
PacketXpress Capabilities	• Capture and buffer all incoming traffic and distribute time-stamped packets to analysis systems at speeds they can reliably ingest. • Time-stamp, deduplicate, filter, slice, or tag network traffic, allowing for the removal of non-essential traffic – further offloading the analysis applications.
Benefits	• No packets are ever dropped before the analysis, even when data rates are high (e.g., in case of a DDoS attack). This ensures that analysis systems are provided 100% of the traffic for analysis and never lose a packet due to overload.

Analyze and Resolve Quickly

Current Situation	Triage, prioritizing, and resolving the increasing number of threats is difficult when alarms and event logs are often difficult to correlate and lack detail.
PacketXpress Capabilities	• Find and replay any pre-and post-event packet data at any speed for in-depth analysis. • Scale to retain network traffic for days, months, or years cost-effectively.
Benefits	• Simplify and accelerate forensic and historical analysis through easy access to recreate not just the events but also what happened before and after the event.

Validate Countermeasures before Deployment

Current Situation	Validating the successful implementation of security mitigation is difficult in today's complex infrastructure and is often deployed without any validation at all. This leaves infrastructures vulnerable to repeated exploitation.
PacketXpress Capabilities	• Find and replay any pre-and post-event packet data at any speed up to over 100 Gbps to validate countermeasures or stress test the monitoring infrastructure. • Scale to retain network traffic for days or months cost-effectively.
Benefits	• Reliably validate whether threats will now be detected based on the new signatures, classification rules, or other improvements made by rerunning actual event traffic. • Determine whether newly identified threats occurred previously that might have been missed prior to the updates.

Optimize Network & Security Infrastructure Under High Traffic Load

Current Situation	• Predicting and optimizing the stability, speed, scalability, and responsiveness of any network & security infrastructure under high traffic load is often difficult or even impossible in today's complex infrastructure. • Recreating real-life situations in a limited lab set-up often lacks the complexity and dynamic behavior of our network and security infrastructure and does not generate the required data for a reliable assessment.
PacketXpress Capabilities	• Find and replay any pre-and post-event packet data and the surrounding traffic at any speed up to over 100 Gbps to validate countermeasures or to stress test the monitoring infrastructure.
Benefits	• Validate new devices, software loads, and fixes in a secure environment under real-live traffic conditions. • Ensure that your infrastructure provides the speed, performance, and reliability your organization relies upon before operational deployment. • Optimize your infrastructure to lower cost and ensure a reliable and efficient network and security monitoring environment.

About Axellio

Axellio provides extreme high-performance, scalable, compact, economical, and simultaneous time-series data ingest, storage, and distribution solutions for the defense and intelligence community at speeds exceeding 100 Gbps for cybersecurity and for intelligence, surveillance, and reconnaissance (ISR) applications.
Contact us at: contactus@axellio.com **or +1 (719) 309-3370**