Unifying Network Visibility and Intelligent Threat Detection with VLI and Axellio

Today's cyber threats demand more than traditional defenses. Organizations face massive data volumes, rising storage costs, and advanced attackers. This brief explains how **VLI's "network black box" and Axellio's high-performance PacketXpress® Platform** work together to provide deep security insights and cost-effective threat detection.

Axellio: The Foundation for Comprehensive Network Visibility

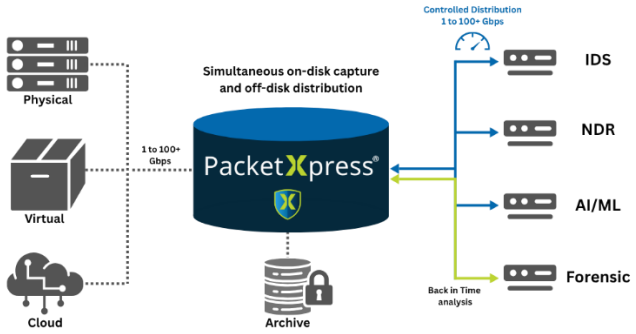

Figure 1: Axellio PacketXpress

Axellio's PacketXpress is a patented, compact, and scalable software platform for high-speed packet capture, storage, and distribution. Designed for COTS hardware, it integrates easily with existing security tools.

- **High-Speed Performance:** Captures and stores full PCAP traffic at 200 Gbps in a COTS 1U server with no data loss—using the smallest footprint in its class.
- **Deep Packet Visibility:** Enables full packet inspection for advanced threat detection and forensics.
- **Scalable & Efficient:** Customizable to fit small to large deployments, offering top-tier cost-to-performance.
- **Easy Integration:** Open APIs support seamless integration into current security environments.

Trusted by Fortune 500 companies and the U.S. Military, PacketXpress enhances visibility, speeds up threat response, and strengthens overall security operations.

VLI: Intelligent Data Filtering and Advanced Threat Detection

VLI, a Georgia Tech spinout backed by DARPA and the DOD, specializes in advanced threat attribution using unique "gray space" data to map APT infrastructure and malware campaigns. Its "network black box" enhances intelligence capabilities through:

- **Real-Time Filtering:** Captures only cyber-relevant traffic at line-rate speeds, cutting data volume significantly
- **Cost Savings:** Reduces storage and analysis costs by up to 70%
- **Improved Detection:** Delivers cleaner data to better identify APTs, IoT threats, and third-party malware
- **Passive Operation:** Analyzes traffic without active probing—ideal for sensitive environments

VLI is piloting this capability with the DoD at key Internet exchange points.

The Combined Advantage: Unparalleled Security and Efficiency

Axellio's PacketXpress® provides the foundational capability for full-fidelity capture, storage, and dissemination of all your network data at enterprise scale, ensuring comprehensive visibility without compromise. This patented software platform excels at high-speed packet capture (over 200 Gbps) and distribution (over 200 Gbps) from disk, preventing data loss even during traffic spikes or DDoS attacks. Unlike solutions limited to metadata, PacketXpress offers immutable evidence through full PCAP data, allowing for "Packet DVR" functionality to rewind, replay, and re-analyze any pre- and post-event data for rapid forensic analysis and triage. Operating on commercial-off-the-shelf (COTS) hardware, it offers cost efficiency and scalability, extending visibility into external, internal on-premise, virtual, and cloud environments with extensible storage for long-term retention.

Building upon this, VLI's cutting-edge platform intelligently sifts through that network data, ensuring customers retain cybersecurity-relevant data and then can provide actionable threat intelligence on that data and other proprietary gray space data sources. VLI's XDP-based solution efficiently assigns a security value score to each packet, filtering benign traffic and preserving critical, high-impact data for long-term storage, which significantly reduces storage needs and costs. Leveraging unique "gray space" data sources and advanced algorithms from its DARPA-originated Enhanced Attribution project, VLI's Pythia platform proactively maps adversary infrastructure and attributes threats to virtual actors, tracking thousands of active APT (Advanced Persistent Threat) and commodity malware campaigns continuously and automatically. The output focuses on prioritized lists of Indicators of Compromise (IOCs) with clear context and explainability, transforming raw data into actionable insights and reducing the manual burden on security analysts. This synergy delivers unparalleled network visibility and proactive threat defense for large enterprises and critical infrastructure.

Key Benefits of Our Integrated Solution:

- **Complete Network Visibility:** Capture every packet, even during high-volume events, ensuring no blind spots.
- **Intelligent Data Optimization:** Drastically reduce data storage costs by retaining only cybersecurity-relevant traffic for long-term analysis.
- **Proactive Threat Intelligence:** Automatically map adversary infrastructure and identify active APT and commodity campaigns before they fully manifest.
- **Actionable Insights:** Receive prioritized IOCs with clear context and explanations, enabling rapid response and reducing analyst workload.
- **Cost Efficiency & Scalability:** Optimize existing security investments by feeding relevant data to analysis tools and reducing licensing costs, all on flexible, COTS hardware.
- **Rapid Forensics & Validation:** Rewind and replay full packet data to analyze incidents deeply and validate countermeasures with real traffic

Conclusion

The partnership between VLI and Axellio represents a leap forward in cyber defense. By synergizing Axellio's robust, high-speed data capture and storage with VLI's intelligent filtering and advanced threat attribution capabilities, organizations can achieve a more effective, efficient, and proactive security posture. This collaboration provides the critical balance of comprehensive network visibility and precise, actionable threat intelligence needed to outpace today's adversaries. Contact us today to learn more.