PacketXpress: Intelligent Payload Slicing

Reducing Network Visibility Cost Without Sacrificing Insight

What is PacketXpress

PacketXpress® is Axellio's network intelligence platform designed to reduce the cost of network visibility. Traditional Network Detection & Response (NDR) architectures scale linearly with traffic and peak bandwidth, forcing tradeoffs between retention, performance, and cost. PacketXpress eliminates this tradeoff by optimizing packet data at ingest and enabling controlled, software-defined access to packet and flow data—allowing visibility to scale without scaling infrastructure cost.

At the core of the platform is XpressFS™, a purpose-built, high-performance file system for packet and time-series data. XpressFS delivers lossless, deterministic capture at high speeds while supporting compression, deduplication, filtering, and encryption without impacting capture performance.

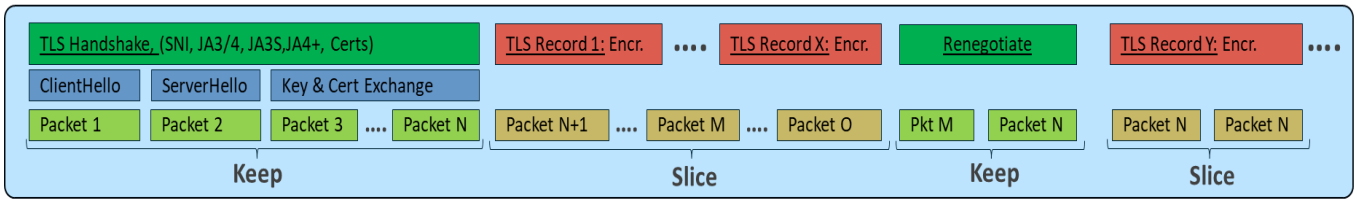
The Visibility Cost Challenge in Encrypted Networks

Encryption is now the default across enterprise and mission-critical networks, with HTTPS, east–west services, machine-to-machine TLS, QUIC, VPNs, and proprietary protocols dominating traffic. While essential for security, encryption creates a visibility cost problem because most security and performance tools do not decrypt payloads, encrypted payloads provide little analytic value, and the data still consumes significant storage, I/O, and retention capacity. Traditional systems capture and store encrypted payloads in full, driving rapid growth in storage and infrastructure costs without improving detection or investigation outcomes.

Intelligent Payload Slicing

Intelligent Payload Slicing is a PacketXpress ingest-time capability that removes low-value encrypted payload data while preserving the information that analytics actually use. PacketXpress identifies encrypted sessions during capture and selectively removes payload content while retaining:

- Full packet headers
- Flow metadata and session attributes like TLS handshakes, renegotiation, etc.
- Transport headers (Eth, IP, TCP/UPD, original byte count, and preserves all flow information
- Timing, sequencing, and behavioral context



By retaining Handshake metadata while dropping bulk encrypted payload, the Intelligent Payload Slicing provides continued ability to detect encrypted malware traffic and preservation of high-fidelity indicators for SOC and threat hunting teams.

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.

TLS Handshake metadata which spans multiple packets is critical for threat detection; Most security tools extract the following metadata from this Handshake:

- SNI (Server Name Indication) for domain identification
- ALPN (Application-Layer Protocol Negotiation)
- Cipher suites and extensions
- Certificate chain, issuer details, public key length
- JA4/JA4+, JA3/JA3S fingerprints
- Version negotiation, record sizes, and timing patterns

This approach dramatically reduces storage consumption while maintaining analytic fidelity for threat detection, forensics, and performance analysis.

Currently Supported Encrypted Protocols

PacketXpress Intelligent Payload Slicing Supports a wide range of modern encrypted protocols, including:			
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)	WireGuard	IPsec ESP	SMB3

New protocols including proprietary protocols are being added all the time, so please reach out if you have questions on specific protocols that you're interested in.

Why Payload Slicing Matters

By eliminating encrypted payloads that tools cannot use, PacketXpress delivers measurable benefits:

- Reduced storage requirements without shortening retention
- Lower I/O and read amplification for downstream analytics
- Improved analytic efficiency by focusing computing on high-value data
- Predictable scaling as encrypted traffic volumes grow

Integrated Flows and Buffered Analytics

Intelligent Payload Slicing works with the integrated flow generation and buffered analytics already included in PacketXpress. Flow records are created in parallel with packet capture, enabling fast, query-driven analysis without accessing raw packet data until needed. High-speed buffering decouples capture from analysis, letting tools consume data at their own pace and allowing systems to be sized for sustained workloads rather than peak bursts—reducing CPU, memory, and server requirements.

Axellio's mission is to control data overload in timeseries analysis systems that monitor for threats to our infrastructure through innovative storage and distribution solutions. Axellio's 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**