Axellio PacketXpress®

Modernize Your Packet Capture Without Starting Over

Suricata. Zeek. Wireshark. tcpdump. Your team didn't just install these tools, they tuned them, built dashboards around them, and trained analysts to trust what they show. That's the real investment in your SOC, and it's exactly what's at risk every time someone proposes a new capture platform. PacketXpress was designed around a different idea: what if modernizing didn't mean starting over?

With PacketXpress, every tool your team already relies on keeps running exactly the way it does today, no reinstalling, no retraining, no rebuilding dashboards from scratch. The only thing that's different is what's happening underneath: faster, more reliable, more complete data flowing into the tools you already trust.

The Risk Nobody Talks About

Most SOCs aren't slow to replace an aging capture platform because of the technology, they're slow because of what they'd have to rebuild. Years go into tuning Suricata and Snort rules, writing custom Zeek scripts, and building the dashboards analysts rely on every shift. Pull the capture layer out from under all of that, and you're not just installing new hardware, you're re-earning trust in every alert it generates.

In practice, that risk shows up in three places:

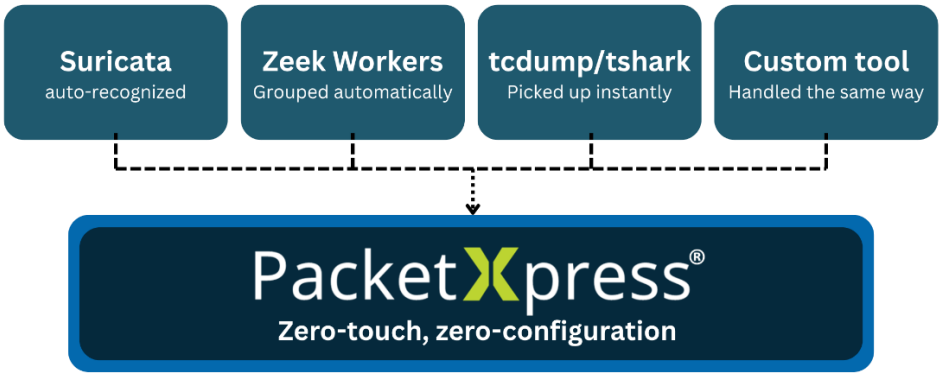
- **Detection logic you've already built:** years of custom rules, scripts, and dashboards shaped around your specific traffic.
- **Workflows your analysts already trust:** the playbooks and alert triage steps built around today's tools, and the training that goes with them.
- **The cutover itself:** weeks or months of running two systems side by side just to prove the new one can be trusted.

It's often easier to keep an oversubscribed, aging packet broker that’s dropping traffic than to take on that risk, even when everyone knows it's holding the team back.

PacketXpress: A Different Kind of Upgrade

PacketXpress takes that risk off the table. Every rule, every signature, every script, every dashboard, and every playbook keeps working after the switch, because the upgrade happens beneath your tools, not inside them.

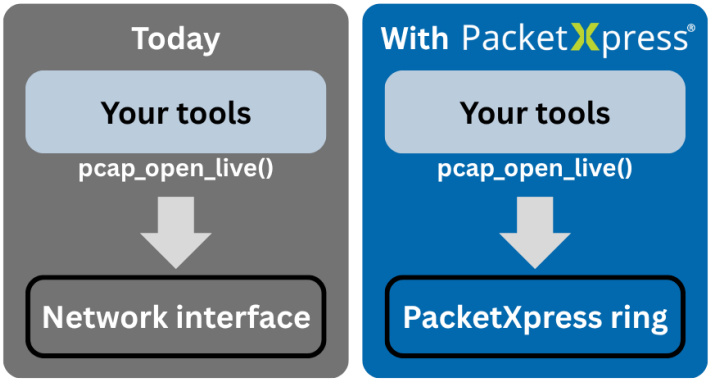
New Tool In, No Setup Required



- **What actually changes**: the data flowing into your tools is now filtered, flow-controlled, and pulled from lossless capture, so nothing is missed. What each tool sees on its end: no difference at all.

Same Connection Your Tools Already Trust

Every tool in your stack already knows how to read from a capture source, that's how it talks to the network today. PacketXpress simply becomes that source. There's nothing new to install on the tool side and no integration project to run, because as far as your tools can tell, nothing about how they connect has changed.



No Bottlenecks, No Blind Spots

Behind that familiar connection is a delivery system built to keep up with real SOC traffic volumes, without the slowdowns that come from moving packets through extra layers of copying and processing. Even under heavy load, timing stays precise down to the nanosecond, which is exactly what your team needs when reconstructing a fast-moving incident or spotting a timing-based attack.

Nothing for Your Team to Maintain

Spin up a new tool, and PacketXpress recognizes it and starts feeding it the right traffic immediately, no configuration required.

One setup covers your entire tool fleet. Suricata is picked up automatically, including additional instances as you scale. Zeek's worker processes are grouped and connected without any manual mapping. An analyst spinning up tcpdump or tshark for a quick look is recognized on the spot. Even a custom, in-house tool is handled the same way, and its resources are freed up automatically the moment it's no longer running.

Improve the Platform Without Rebuilding Around It

PacketXpress exists because of a simple idea: the platform underneath your tools should never be what's stopping you from improving it. Your SOC gets a faster, more capable capture and distribution layer, and every rule, script, and dashboard your team has already built keeps working, untouched. That's what separates an upgrade from a migration, your analysts spend their time using better data, not rebuilding around it.

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. www.Axellio.com