Gain Powerful Network Visibility to Disrupt Attacks Early

Corelight and Axellio PacketXpress® deliver unprecedented network visibility and comprehensive attack evidence for faster response. Reliable & cost-effective at any speed.

Security engineers are inundated with ever-increasing mountains of abstracted event data. Without valuable evidence and insight to evaluate this information against, security engineers lack the context to quickly triage, prioritize and respond to an increasing number of threats. Furthermore, visibility is often limited to endpoint and network ingress/egress points, leaving adversaries plenty of infrastructure to hide in.

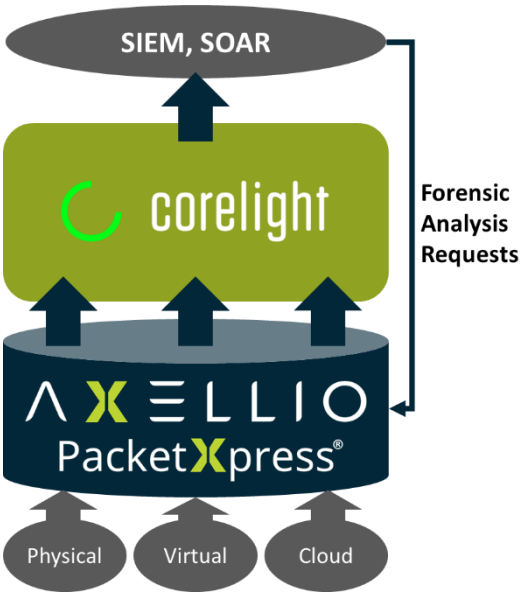
Corelight and Axellio are integrating their solutions to provide a cost-effective, open, and comprehensive network detection and response (NDR) solution for broader visibility across physical, virtual, and cloud infrastructure. This solution provides the network evidence needed to make faster decisions and prevent those lingering threats in your network. Axellio and Corelight translate network and cloud activity into evidence to proactively hunt for threats, quickly investigate cyber incidents, gain visibility into the networks, and leverage analytics powered by machine learning.

Unlike other NDR solutions, the Corelight and Axellio solution keeps up with any amount of traffic you need to analyze, never missing a packet even in extreme high load situations that intruders try to hide behind. For faster triage and more insightful forensics, Axellio PacketXpress' provides comprehensive pre- and post-event network packet data for detailed analysis of every event – not just the events you had the foresight to create a packet capture trigger for!

The Corelight & Axellio PacketXpress – the Open NDR platform

To accelerate your network threat detection and response, we've integrated two powerful open platforms that enhance your existing security monitoring infrastructure, providing complete visibility and insightful analytics – scalable, reliable, and economical:

- **Corelight**'s open network detection and response (NDR) platform based on Zeek and Suricata defends some of the world's most sensitive, mission-critical organizations.
- **Axellio PacketXpress**, is the highest performing, smallest form factor network traffic capture, storage, and distribution platform. PacketXpress provides an open, scalable security platform that can handle over 100 Gbps in a 2U formfactor with no loss and provides direct access to data for any of your existing security applications.



Axellio PacketXpress is an application-agnostic, open platform that captures, stores, and forwards traffic reliably and without loss. PacketXpress' ability to simultaneously store to disk and distribute from disk at over 100 Gbps allows the Corelight analysis to keep up with any traffic load. PacketXpress buffers the traffic and plays it out as fast as the analysis application can consume it, avoiding overload situations due to licensing or processing performance limitations. Furthermore, by storing the incoming traffic for days, weeks, or even months, you can access all packets anytime for pre- and post-event analysis, integrated into the Corelight workflow. Built entirely on off-the-shelve hardware, PacketXpress integrates easily with your current network monitoring infrastructure.

- Up to 100Gbps capture sustained for no-loss capture and distribution to meet the capture needs of any network size and speed.
- Always-on, long-term on-disk-storage for days, weeks, or months - scalable up to 1.5 Petabyte onboard storage in a single 2U server, extendable for higher performance or distributed deployment.
- Adaptive traffic distribution - Over 100 Gbps simultaneous traffic distribution with rate control. This allows for traffic buffering for any onboard and offboard analysis application to ensure reliable no-loss, real-time analysis that keeps up with traffic growth. Unlike other solutions in the market, traffic capture is not impacted by writing data from disk for distribution or analysis.

Corelight helps customers stay ahead of ever-changing cyber-attacks, by making evidence the heart of security strategy. Our open NDR platform transforms network and cloud activity into evidence that elite defenders use to drive complete visibility, next-level analytics, faster investigations, and expert threat hunting.

- NDR coverage for every device on the network: Understand and manage risk across the entire IoT and OT landscape including high-value assets, managed and unmanaged endpoints, IoT devices, and cloud environments.
- Single platform for NDR: Corelight provides everything security operations teams need for detection and response, built on open standards including Zeek® for telemetry, Suricata for alerts, and Smart PCAP for packets.
- Faster answers for analysts and hunters: Rich, structured network data from 35+ protocols, and 400+ data fields captured in real-time provides additional context for alerts, accelerating incident response and dramatically expanding threat hunting capabilities.
- Integration with existing SOC toolsets: Correlate rich network telemetry with threat intelligence feeds for sending to multiple destinations simultaneously, including Microsoft Sentinel, Splunk, and other analytic tools.
- Deeper insights: Unique insights to hunt for attackers without compute-intensive practices that compromise privacy, find command-and-control (C2) activity using Corelight content developed by Corelight Labs. The content contains unique insights that cover C2, Encrypted Traffic, and Entity collections mapped to the MITRE ATT&CK framework.
- Complete visibility of the network, both on-premise and in the cloud, with evidence that spans months and years, not days and weeks. Customers can leverage machine learning, behavioral analysis, threat intelligence and signatures to enable broad coverage of network-centric threats.

Reducing Risks & Expenses

This joint solution accelerates your response and awareness to attacks by creating insightful event information and correlating the data with the traffic surrounding any event. It provides the clear and complete information you need to avoid long attacker dwell time, leaving them no place to hide. This economical solution also integrates into your existing security infrastructure, extending your visibility without extending your budget.

Reduce Risk	Manage Expenses, Increase Visibility
• Close visibility gaps – never lose a packet – in your physical, virtual, and cloud environment • Improve productivity and reduce Mean-Time-to-Detect (MTTD) and Mean-Time-to-Repair (MTTR) • Identify the early stages of a ransomware attack • Fingerprint or even decrypt encrypted connections • Provide immutable evidence – immediate access to any pre- and post-event information • Validate mitigations - Ensure that mitigations are effective	• Replace a standalone IDS • Reduce hardware sensor proliferation and complexity • Simplify your network visibility fabric and reduce cost and complexity • Extend the life cycle of your existing monitoring infrastructure and delay expensive upgrades • Virtualize your analysis applications or operate on less costly servers, avoiding costly proprietary analysis hardware

Corelight transforms network and cloud activity into evidence so that data-first defenders can stay ahead of ever-changing attacks. Delivered by our open NDR platform, Corelight's comprehensive, correlated evidence gives you unparalleled visibility into your network. This evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks. Our on-prem and cloud sensors go anywhere to capture structured, industry-standard telemetry and insights that work with the tools and processes you already use.

Contact us

www.corelight.com

fed-team@corelight.com

+1(888) 547-9497

Axellio® is an innovator in network intelligence platforms, closing the security visibility gap for any network security application, reducing risk and security infrastructure cost, while increasing operational effectiveness. Axellio PacketXpress® provides an analysis-agnostic platform for our solution partners. It enhances the performance and analysis capabilities for real-time and historical network traffic analysis, addressing the needs of security and network operations of defense, intelligence, and commercial enterprises.

Contact us

www.axellio.com

contactus@axellio.com

+1 (800) 463-0297 or +1 (719) 309-3370