

Comprehensive Network Detection and Response at Scale

Capture and Transform High Volume Traffic Into High Fidelity Security Insights

Virtually all cyberattacks cross the network, which is why high-fidelity network traffic is essential for effective security operations. However, while many security teams monitor traffic going in and out of their organizations, analysts are often blind to the traffic within the organization, leaving them vulnerable to attackers hiding inside or at the network edge.

These hidden threats inside the network in many cases have already established malicious connections to external command and control systems to exfiltrate sensitive data and/or deploy malware at a moment's notice. Without a reliable and cost-effective way to capture and transform raw network packets into insightful network evidence, organizations won't know they've been breached until it's too late.

Corelight and Garland Technology address this problem with a solution that can be deployed in minutes to give organizations the network insight they need to provide a stronger defense.

INTEGRATION HIGHLIGHTS

Delivers full-fidelity packets to Corelight sensors, enabling improved visibility and threat detection

Combines rich, correlated network logs with evidence-based detections to accelerate investigations and response

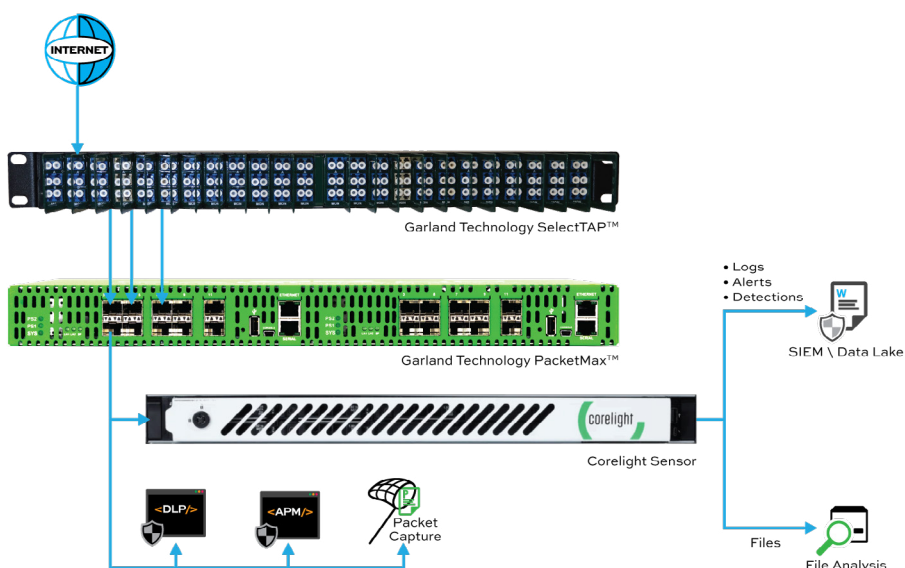
Reduces cloud costs with Garland's efficient packet capture and Corelight data aggregation

Provides real-time analytics and rich security context for faster incident response

Scales seamlessly across hybrid and multi-cloud environments

HOW IT WORKS

1. Garland Technology Network TAPs deployed at any links in a network create a 100% copy of the network traffic.
2. The tapped network traffic is then sent to a Network Packet Broker for traffic grooming, using features such as aggregation, load balancing, and deduplication.
3. The groomed traffic is then mirrored to the out-of-band Corelight sensor for analysis. Traffic is captured and converted to rich, correlated protocol logs and detections, providing users with critical security context of their network traffic.
4. Additional ports on the Garland Packet Broker can also send the same copies of the network traffic to additional security and monitoring tools as needed.



Transforming Network Traffic Into Comprehensive, Detailed Evidence

Combining Garland Technology's packet broker solutions with Corelight's Open NDR Platform gives organizations the rich and actionable network evidence they need to identify both external and internal threats, accelerate investigations, and respond effectively.

Garland's reliable, economical, and easy to deploy network TAP and packet broker solutions deliver precise, lossless traffic to Corelight sensors, enabling organizations to disrupt sophisticated attackers hiding inside or at the network edge. The integrated solution offers a variety of scalable deployment options to capture and efficiently make sense of all network traffic, regardless of what your environment looks like.

KEY BENEFITS

Corelight integration with Garland Technology empowers security teams to accelerate incident response, simplify security operations, and enhance enterprise resilience against cyber threats with complete, multi-cloud network visibility, high-fidelity network data, and best in class network detections.



GET COMPLETE VISIBILITY

The integrated Corelight and Garland Technology solution delivers complete network visibility by providing full-fidelity packet access, enriched security insights, and flexible encrypted traffic analysis across hybrid and multi-cloud environments.



ACCELERATE RESPONSE

Establish a network baseline and spot anomalies quickly with correlated alerts, evidence, and packets so SOC analysts can respond accurately with the scope and severity of adversary activity.



IMPROVE NETWORK DETECTION AND COVERAGE

Combining Garland Technology's leading network TAPs, packet brokers, and cloud visibility solutions with Corelight's advanced analytics, organizations have an optimal solution for identifying and responding to threats quickly and easily.



INCREASE OPERATIONAL EFFICIENCY

Garland Technology's flexible solution supports both cloud and on-premise environments, while Corelight consolidates legacy tools like traditional network monitoring and IDS, streamlining security and reducing tool sprawl across infrastructures.

About Corelight

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.

About Garland Technology

Garland Technology is an industry leader of IT and OT network solutions for enterprise, critical infrastructures, and government agencies worldwide. Since 2011, Garland Technology has been engineering and manufacturing simple, reliable, and affordable Network TAPs and Network Packet Brokers in Richardson, TX. For help identifying the right IT/OT network visibility solutions for projects large and small, or to learn more about the inventor of the first bypass technology, visit GarlandTechnology.com.



Have Questions?

sales@garlandtechnology.com | +1 716.242.8500

GarlandTechnology.com/corelight



See every bit, byte, and packet®