Complete Network Traffic Analysis and Visibility at Scale

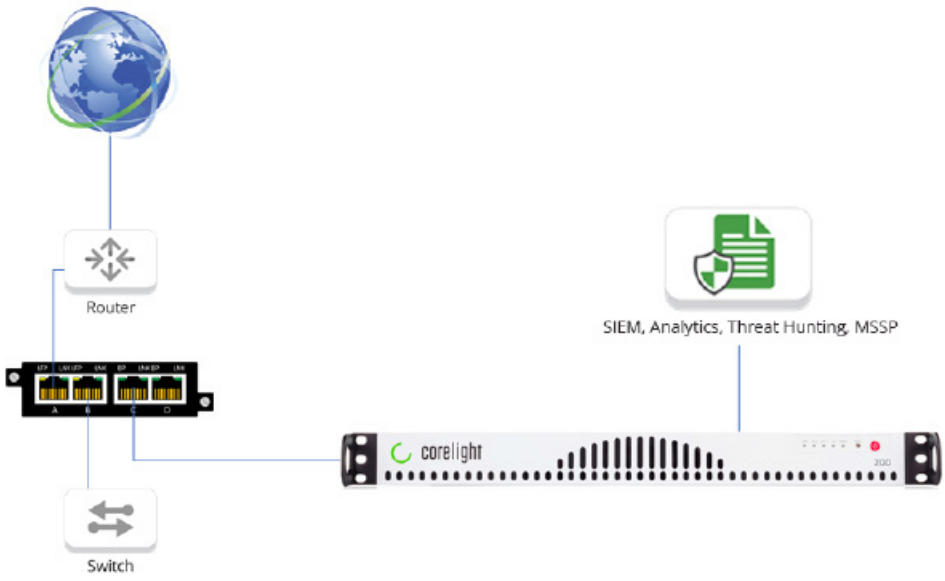
A Joint Solution from Corelight and Garland Technology

Scalably capture all data on the wire, transforming high volume traffic into high fidelity security data and insights

Since nearly all cyber attacks must cross the network, extracting security-relevant data from network traffic is essential across a wide range of security operations including incident response, threat hunting, and threat detection. Finding a way to reliably and cost-effectively capture all traffic and transform it into usable security data, however, can be challenging, especially in environments with limited data center space and high throughput traffic.

Garland Technology and Corelight have partnered to offer an integrated solution to this problem via Garland Technology's compact, high performance network TAPs and aggregators that can deliver a complete copy of network traffic to out-of-band Corelight Sensors, which transform the captured traffic into comprehensive network logs, extracted files, and custom security insights via the power of the open-source Zeek Network Security Monitor (formerly known as "Bro").

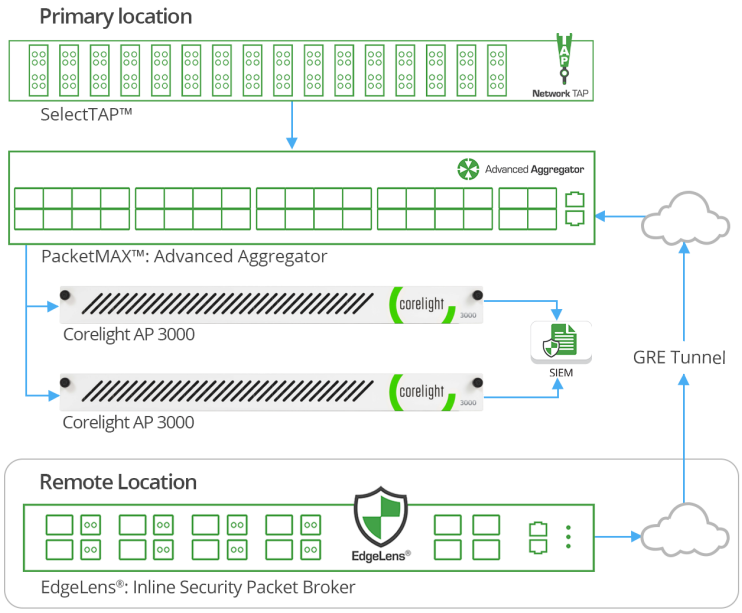
Both companies draw on deep, historical domain expertise to deliver best-in-class technologies: Garland Technology was founded by the inventor of the first Bypass TAP and Corelight was founded by the inventor and key developers of open-source Zeek. This joint solution offers customers a scalable way to capture and make fast sense of *all* of their network traffic no matter the environment, reducing risk by dramatically accelerating network security operations and insights.



Deployment To Ensure Full Line-rate Traffic Analysis

Many security teams today have limited to no security visibility into their DNS traffic at the perimeter, leaving them blind to attackers who hide in DNS traffic and use it to establish malicious C2 server communications, deploy malware, and exfiltrate sensitive data. For lean security teams, Garland Technology's Copper TAP and Corelight's AP 200 Sensor provide a fast, affordable way to capture DNS traffic and get quick, comprehensive insights into potentially malicious DNS activity.

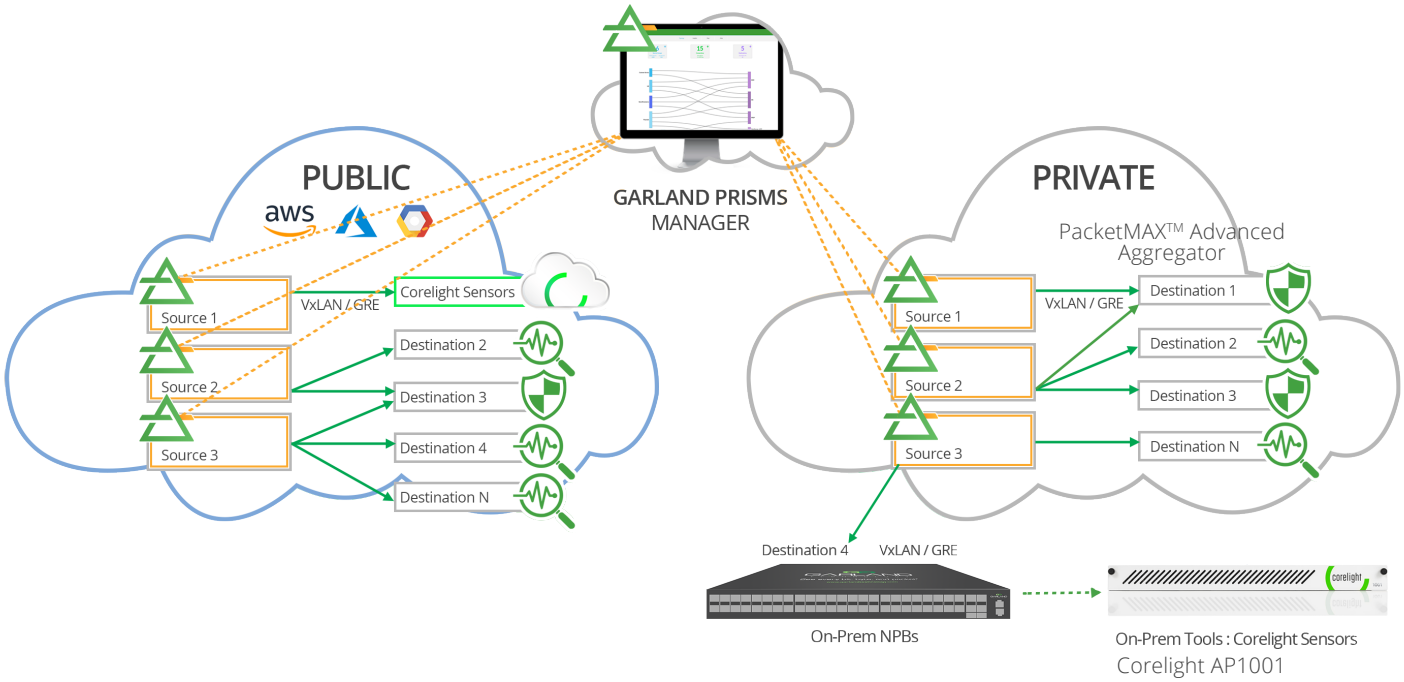
Garland Technology's Copper TAP provides complete network visibility by passing and capturing all live wire data to active, inline security devices. Corelight's AP 200 Sensor then transforms the captured traffic into protocol comprehensive logs, including rich DNS logs that provide critical security context missing from typical DNS server records, such as the content of the response. Corelight can also fork and filter the logs so you can send a complete copy of the logs to a SIEM for incident response, while sending a separate, DNS-only stream to a security analytics tool like the Real Intelligence Threat Analytics (RITA) to detect threats like DNS tunneling and send those alerts on to your SIEM.



A Co-Location Deployment That Scales with Your Network

The scalable design of multi-network environments with satellite locations allows for easy deployment and management of remote sensors along with other monitoring and inline devices. At the primary location, Garland's SelectTAP™: Fiber Modular Chassis is tapping multiple links, sending traffic through the PacketMAX™ Advanced Aggregator for aggregation and the PacketMAX Advanced Features box for deduplication.

The remote location of Garland's Edgelens® sends traffic back to the primary's Advanced Aggregator using GRE tunnels to load the traffic to the two Corelight AP3000 devices.



Threat Detection in Hybrid Cloud Environments

For Hybrid cloud solutions, traffic from a public cloud environment is being sent through a Nubeva Prism into Garland's PacketMAX™ Advanced Aggregator. The traffic from a private cloud environment is output using the Corelight Virtual sensor also into the Advanced Aggregator. Both environments traffic is then sent to a Corelight AP1000 for threat detection, data enrichment, and operational insight.

Garland Technology Network TAPs and Packet Brokers

Garland Technology provides a full platform of network access products including a range of network TAPs and Network Packet Broker devices, supporting the entire wire spectrum from 10/100M copper to 1G/10G/40G/100G.

Key Capabilities

- **Complete Network Visibility** by passing all live wire data
- **Ensure No Dropped Packets** for out-of-band tools
- **Quality standard**, all TAPs are tested with live network data and validated
- **100% failsafe packet capture** – all Network TAPs are tested and validated, and have built-in failsafe and/or heartbeat technology.
- **Reliable traffic aggregation, load balancing, and filtering** – full control over traffic behavior and flexibility for aggregation and regeneration.

Corelight Sensors

Corelight offers a suite of network traffic analysis sensors that use a specialized version of the open-source Zeek Network Security Monitor to ingest network traffic and transform it into rich network logs, extracted files, and security insights. Corelight Sensors are available in both physical (1U) and virtual form factors (VMware), sized to support a range of network throughput speeds at 2 Gbps, 10 Gbps, and 25 Gbps.

Key Capabilities

- **All network traffic logged for security operations** - Corelight Sensors extract over 400 fields of data from network traffic in real time across 35+ protocols from Layer 3 to 7 (HTTP, DNS, SSL, and much, much more.) The logs provide nearly the fidelity of full traffic at less than 1% of the file size. Logs are organized by protocol with fields extracted specifically for SOC / DFIR teams so that they can make fast sense of their network to threat hunt and resolve incidents more efficiently.

- **Actionable traffic insights, Out-of-the-box** - Corelight Sensors come preloaded with the Core Collection, a set of Zeek packages curated and certified by Corelight for performance and stability that provide specific threat detection, data enrichment, and operational insight capabilities, such as identifying port scanning behavior or extracting URLs from email bodies for filtering.

- **Zeek, made easy for the enterprise** - Compared to open-source Zeek sensors, Corelight Sensors take minutes not months to deploy, provide up to 10x peak performance gains, and come packed with additional enterprise functionality and support from the creators and maintainers of Zeek.

corelight

GARLAND TECHNOLOGY
See every bit, byte, and packet™

About Corelight

Corelight delivers the most powerful network visibility solutions for information security professionals, helping them understand network traffic to detect, stop and remediate cyber attacks. Corelight built its first solution incorporating Zeek, the powerful and widely-used open source framework that provides wide-ranging real-time understanding of the traffic on the network. Corelight is based in San Francisco, CA. For more information, visit www.corelight.com or follow @corelight_inc.

Have Questions? sales@garlandtechnology.com | +1 716.242.8500 | garlandtechnology.com

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2010, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information, or learn more about the inventor of the first bypass TAP, visit GarlandTechnology.com or @GarlandTech.