GARLAND TECHNOLOGY
See every bit, byte, and packet®

corelight

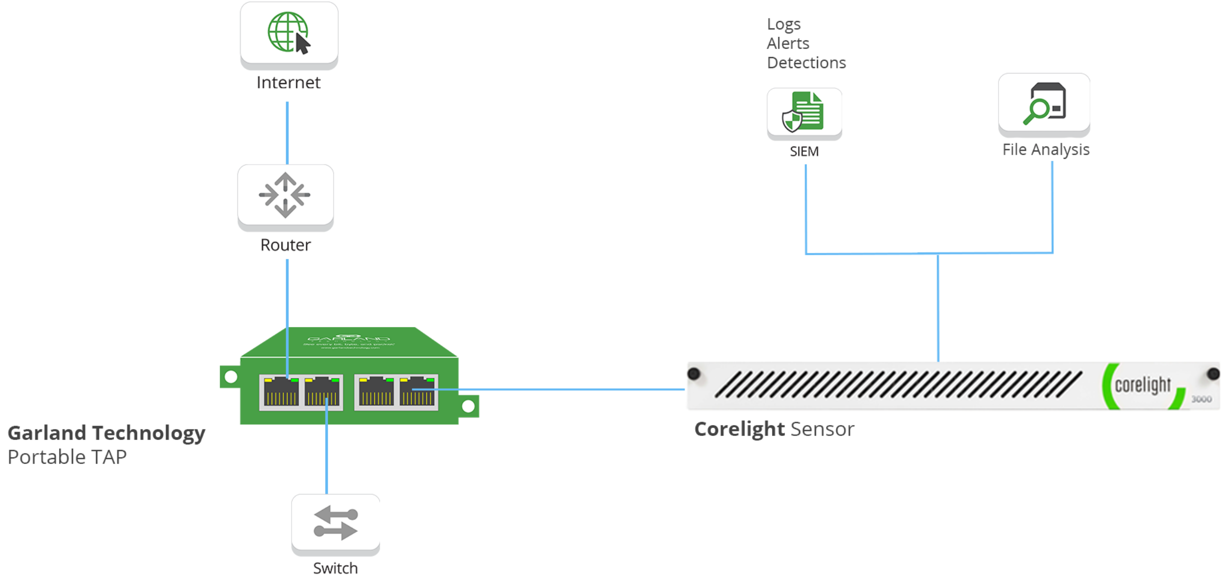
Comprehensive Network Detection and Response At Scale

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

When most cyber-attacks must cross the network, extracting relevant data from network traffic is essential for security operations. Many security teams have limited or no traffic visibility at the perimeter, leaving them blind to attackers who hide and establish malicious C2 server communications, deploy malware, and exfiltrate sensitive data.

Finding a way to reliably and cost-effectively capture and transform traffic into usable security data can be challenging, especially in environments with limited data center space and high throughput traffic. The Corelight and Garland solution takes minutes, not months, to deploy and emit actionable insights. The solution provides 100% visibility of your network for up to 10x peak performance gains and is packed with additional enterprise functionality from the creators and maintainers of Zeek.

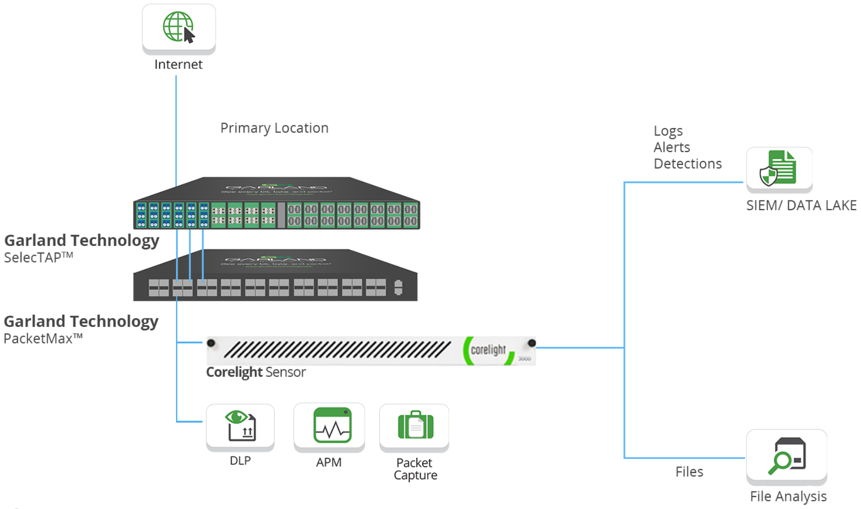
Base Deployment for Network Security and Visibility



How it works

1. Garland Technology's compact, high-performance network TAP provides 100% wire data.
2. A complete copy of network traffic is delivered to the out-of-band Corelight Sensor,
3. The Corelight Sensor captures and converts traffic for comprehensive protocol logs via the power of the Zeek Network Security Monitor

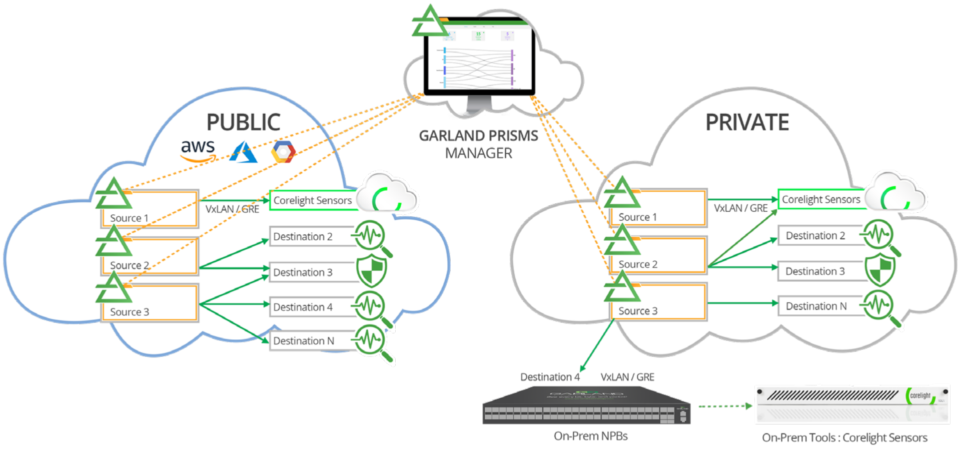
A Scalable Deployment For Growing Network Infrastructures



How it works

1. The scalable design of a multi-network with satellite locations enables easy deployment of Garland Technology network TAPs to provide 100% wire data from the primary and remote locations.
2. Multiple tapped links send the copied traffic to Garland's PacketMAX™ Advanced Aggregator where the data is aggregated, load-balanced, filtered, and distributed.
3. The aggregated traffic is delivered to the Corelight Sensors and other tools in the data center from the primary location.
4. Corelight Sensors transform captured traffic into comprehensive protocol logs for analysis that provides critical security context.

Network Visibility in Hybrid Cloud Environments



How it works

1. Garland Prisms vTAP provides packet mirroring in virtual environments, so corporate traffic in private and public cloud environments including AWS, Google Cloud Platform, and Azure can be captured.
2. The traffic is delivered to the Garland Technology PacketMAXTM network packet broker
3. through VXLAN / GRE tunneling.
4. The cloud traffic is transmitted and streamed to a Corelight Sensor to be transformed into logs, extracted files, and security insights.

Integration Benefits

The Corelight and Garland Technology solution offers a scalable way to capture and efficiently make sense of 100% the network traffic no matter the environment. By dramatically accelerating network security operations with Zeek data, the solution reliably reduces blind spots in the network and the risk of any malicious data on the wire. Whether a lean or robust security team, the easy deployment and infinite features with Zeek data provide a comprehensive solution for security performance.

IT and Sec Ops Team Benefits

- Full visibility across on-premise data centers and private, public (AWS, Azure, Google), or multi-cloud environments.
- Easy access and monitoring of network traffic from physical, virtual, and cloud networks.
- Reduce network downtime, improve reliability, reduce costs, and gain better device utilization by spreading the load data across multiple tools.
- Extract over 400 fields of data from network traffic in real-time across 35+ protocols from Layer 3 to 7 (HTTP, DNS, SSL, ext.)
- 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.
- Preloaded with the Core Collection, a set of Zeek packages curated and certified for performance and stability.
- Provide specific threat detection, data enrichment, and operational insight capabilities, such as identifying port scanning behavior or extracting URLs from email bodies for filtering.

About Corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.
info@corelight.com | 888-547-9497

About Garland Technology

Garland Technology is an industry leader delivering network products and solutions for enterprise, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs) and network packet brokers (NPB), and Cloud visibility solutions enabling data centers to address IT challenges and gain complete network visibility. For help identifying the right NPB solution for projects large and small, or to learn more about the inventor of the first bypass technology, visit GarlandTechnology.com or @GarlandTech.

Learn More
GarlandTechnology.com/Corelight

Let's Talk
+1 716.242.8500
sales@garlandtechnology.com

GARLAND TECHNOLOGY
See every bit, byte, and packet®