Delivering Network Insights for Rapid Investigation and Response

You can't protect a network if you can't see what's happening on it.

Delivering complete network wire-data visibility - with all its rich, contextual, evidence - to security and network teams, and their tools - is crucial to enabling faster, more accurate decisions and more effective network security. By combining Garland Technology, Endace and Corelight, customers can do this scalably, reliably and cost-effectively even on the largest networks.

Why Network Visibility is Critical and What is Needed

It's impossible for network and security engineers to defend against threats they can't see. Designing your infrastructure to ensure complete visibility is essential to enable these teams to work effectively.

To accurately detect cyber threats and performance issues, network security and monitoring tools need packet-level visibility into traffic across the entire network. If this data is not accurate and complete, tools cannot accurately detect threats or problems.

Packet data is also a critical resource for enabling SecOps and NetOps teams to investigate and remediate security threats and performance problems quickly and effectively. Analysts need to be able to look back in time and drill into historical network traffic to quickly and accurately reconstruct past events. Teams with full access to detailed packet data can conclusively investigate incidents and neutralize threats early in the lifecycle.

To provide their teams with deep network visibility organizations need to be able to:

- Acquire traffic from the network accurately in all the places you need to monitor, and direct it to your security and performance monitoring tools at line rate withour packet loss.
- Analyze traffic, including deep-packet-analysis, to provide rich contextual insight into security threats or performance problems.
- Accurately record days or weeks of packet-level data to provide a resource for teams to analyze and reconstruct historical network activity.

Network-wide Packet Access with Garland Technology

Garland Technology's high-speed network TAPs deliver 100% raw packet data for full network visibility. The TAPs deliver packet-level data to Garland Technology's PacketMAX™ network packet broker, enabling advanced aggregation, filtering, and load-balancing.

The load balanced traffic is delivered to Corelight Sensors, for real-time analysis, and EndaceProbes™, which record and store the data for historical investigation and analysis.

For virtual environments, Garland Technology's Prisms vTAP provides packet mirroring, enabling traffic in private and public cloud environments - including AWS, Google Cloud Platform, and Azure - to be captured.

corelight

GARLAND TECHNOLOGY

PRODUCTS

Garland Technology TAPS and Packet Brokers

Corelight Sensors

EndaceProbe™ Analytics Platforms with Application Dock™
EndaceVision and Investigation Manager

BENEFITS

- 360° visibility with complete packet-level history across physical, virtual, and cloud networks
- Optimize network security and monitoring tool performance
- Resolve incidents up to 20x faster with structured network insights
- Reduce threat exposure through faster and more definitive incident response
- Unlock threat hunting capabilities with comprehensive insight into network traffic and definitive network evidence.
- Filter out false positives more quickly and confidently.
- Keep a definitive evidence trail with an accurate record of packets relevant to threats.

Powerful Network Analytics and Rich Metadata with Corelight

Corelight Sensors replace patchwork visibility with a single source of network truth — so you can know if you've been breached, and if control measures have been evaded. Corelight's complete, coherent, interconnected data gives your team an enduring advantage without disrupting workflows to resolve incidents, perform forensics, and triage alerts.

Corelight is built on the Zeek® network security monitor, the gold standard in forensics. Corelight Sensors extend Zeek's robust capabilities, integrating it with Suricata and making it truly enterprise-grade. Corelight logs are typically ingested by SIEMs - such as Splunk, Elastic, Chronicle, Securonix, Exabeam, and many more - for analysis, alerting and reporting.

Deep Network History with EndaceProbe

EndaceProbes capture and record packet data at line rate from the Garland Technology TAPs and Packet Brokers, providing petabytes of storage capacity sufficient for days, weeks or even months of network history. This packet data is indexed for fast search and data-mining and can be integrated with a wide variety of commercial, open-source or custom security and performance monitoring solutions to provide one-click access from alerts in these tools directly to the related packet data.

The EndaceProbe's built-in hosting environment, Application Dock, can also be used to host Corelight Software Sensors.

END_sb_end_corelight_garland_v1.0_0621

Every packet captured and recorded by the host EndaceProbe can be streamed to Corelight Sensors in real time, and recorded traffic can also be replayed to Corelight Sensors to provide powerful, back-in-time analysis of historical activity.

Complete Network Visibility, Rapid Investigation and Response and Powerful Threat Hunting

Combining Garland Technology TAPs and Packet Brokers, Corelight Sensors and EndaceProbes delivers a complete network visibility solution. It enables packet data to be accurately captured, analyzed and recorded from everywhere on the network, ensuring that security and network teams - and the tools they use - have complete visibility into activity across the network in real-time and a reliable record of past activity for historical analysis and investigation.

Investigation and response workflows are streamlined through the integration of Corelight's rich, enhanced log file data with the packet history recorded by EndaceProbes.

Analysts can pivot from logs generated by Corelight - or from the SIEM or SOAR tools that these logs are ingested by - directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History in detail.

EndaceProbes provide rapid search and data-mining, allowing packets-of-interest to be located in, and extracted from, petabytes of distributed storage in seconds, dramatically accelerating the investigation process.

Agile Deployment and Flexible Infrastructure that Evolves with your Needs

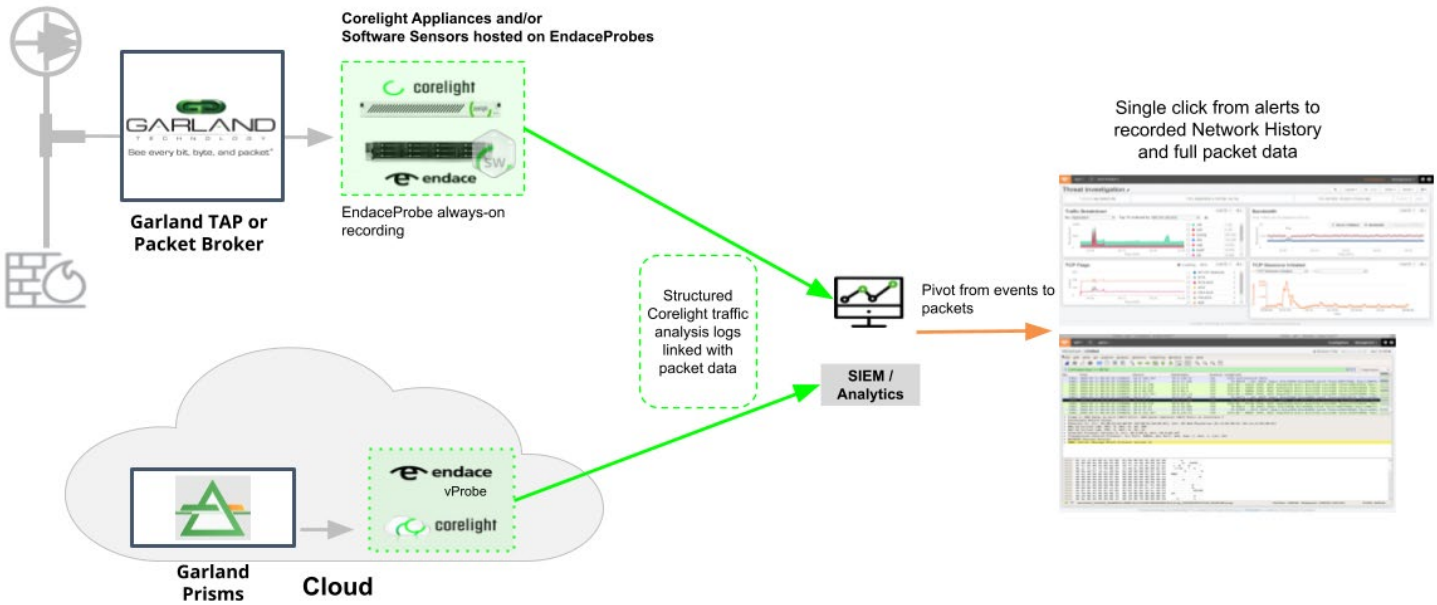
Deploying next-generation security hardware takes significant planning and effort. New rollouts can often take 6 months or more. This puts security teams at a disadvantage when trying to defend against criminals who can launch attacks at the click of a mouse. The ability to quickly reconfigure your visibility and monitoring infrastructure to adapt to changing needs without having to make major infrastructural changes is crucial.

Conclusion

Combining Garland Technology, Corelight and Endace delivers the true network visibility that SecOps and NetOps teams need to protect the network efficiently and effectively.

It also gives organizations the flexibility and agility they need to continually evolve to meet new threats, scale as network speeds and loads increase, and improve the return on the investment in security and performance monitoring tools that they already have.

How it Works



For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com