Corelight, Endace and Gigamon

Comprehensive visibility across your network for rapid and accurate incident response

Eliminate blind spots. Endace, Gigamon and Corelight deliver more effective threat hunting and incident response for SOC teams with deep, network-wide visibility. The combined solution delivers global insight into network activity, linked with the detailed evidence required to rapidly investigate and resolve incidents anywhere on your network.

Tap and monitor pervasively across your network with Gigamon. Generate actionable real time network data with Corelight. Automatically link log data to 100% accurate, recorded network history from Endace to accelerate incident response and improve security posture.

Deploying EndaceProbe and Corelight sensors together with a Gigamon Visibility Analytics Fabric (VAF) tightly couples log data with recorded network history, allowing analysts to quickly see exactly what occurred on the network. This tight connection between log and packet data enables analysts to investigate threats rapidly and drill down to recorded network history to see the full extent of any threat.

Network Wide Visibility by Gigamon

The Gigamon Visibility and Analytics Fabric (VAF) reduces tool sprawl, lowers cost, and optimizes the delivery of relevant data for tool consumption.

The VAF delivers scalable agility and accuracy to your security architecture. It provides visibility and consumable network traffic to tools, such as Corelight, to inspect and analyze traffic for threats and then tools such as Endace, to record and store the network evidence needed for accurate forensic investigations.

Gigamon VAF delivers traffic capture, deduplication, data-masking, decryption, filtering, flow/metadata creation and traffic slicing - letting you get the right information to the right tools efficiently, and scale as needed.

Network Traffic Analysis by Corelight

Corelight sensors are built on Zeek (formerly known as Bro), the powerful and widely-used, open source network analysis tool. Thousands of organizations use Zeek to generate actionable, real-time network data for their high-performance security teams. Zeek extracts more than 400 fields directly from network traffic in real time. Zeek logs are structured, and interconnected, specifically to support threat hunting and incident resolution.

Corelight Sensors - available in physical, cloud, software, and virtual formats - take the pain out of deploying open-source Zeek. They combine the integrations and capabilities large organizations need with high-end, out-of-band hardware and a specialized version of open source Zeek for excellent performance.

corelight Gigamon®

PRODUCTS

Corelight Sensors

EndaceProbe Analytics Platforms with Application Dock

Gigamon G-TAPs, G-vTAPS, and GigaVUE visibility nodes

BENEFITS

- Full visibility across your entire infrastructure including encrypted threats
- Open, flexible and customisable to keep pace with changing threat landscapes and network growth
- Resolve incidents up to 20x faster with structured network insights and the ability to review network activity from application down to the packet layer for any event.
- Unlock threat hunting capabilities with comprehensive insights.
- Enterprise class deployment and management
- Greater productivity with one click access from security events to related packet evidence for rapid incident response.
- Easily and quickly expand threat coverage by deploying Corelight Virtual Sensors on any EndaceProbe.
- Keep a definitive evidence trail with an accurate record of packets relevant to threats.
- Reduced threat exposure through faster and more conclusive incident response

When Corelight sensors are paired with EndaceProbes, the log data is linked with the recorded network history on EndaceProbes, enabling rapid and conclusive incident response. Corelight Virtual Sensors can also be hosted on any EndaceProbe, giving security teams expanded threat coverage without the need to deploy additional hardware.

Network History Recorded by Endace

EndaceProbe™ Analytics Platforms capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. Application Dock™ extends security and performance monitoring by allowing third party analytics applications – including Corelight Virtual Sensors - to be hosted on the open EndaceProbe platform without rolling out additional hardware.

The EndaceProbe's powerful API lets security and network operations teams integrate network history directly into all their tools.

From within their favorite SIEM or SOAR tools, analysts can click on any linked event or alert generated by Corelight and go directly into EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze

the related, packet-level Network History. This single-click workflow dramatically reduces the time required to investigate and resolve incidents and improves the security posture of the organization.

A Flexible Security Architecture

Gigamon VAF delivers effective visibility into all the far reaches of the network: selecting, filtering, masking and grooming critical traffic for analysis by Corelight and recording by EndaceProbes. This combined architecture allows security teams to easily adapt and change network monitoring as threats evolve and as the network grows. Additional traffic can be selected and steered to tools. New tools can be easily added and commercial, open source or custom software analytics tools can be deployed on-demand.

The architecture also handles the need to decrypt or fingerprint encrypted traffic if required, providing full visibility into threats that may be running over encrypted sessions.

Custom Zeek detection scripts can be deployed to any Corelight Sensor, enabling advanced teams to develop specific monitoring data to complement existing NetFlow, IDS or other network sensor data.

Open source tools or additional Corelight sensors can also be easily deployed onto EndaceProbe providing additional flexibility to adapt monitoring architectures as threats and traffic changes.

Corelight logs are typically ingested by SIEMs such as Splunk, Elastic, Chronicle, Securonix, Exabeam, and many more, for analysis, alerting and reporting. The EndaceProbe's RestFul API enables full integration with SIEM, SOAR and other tools that require access to full packet data for incident response.

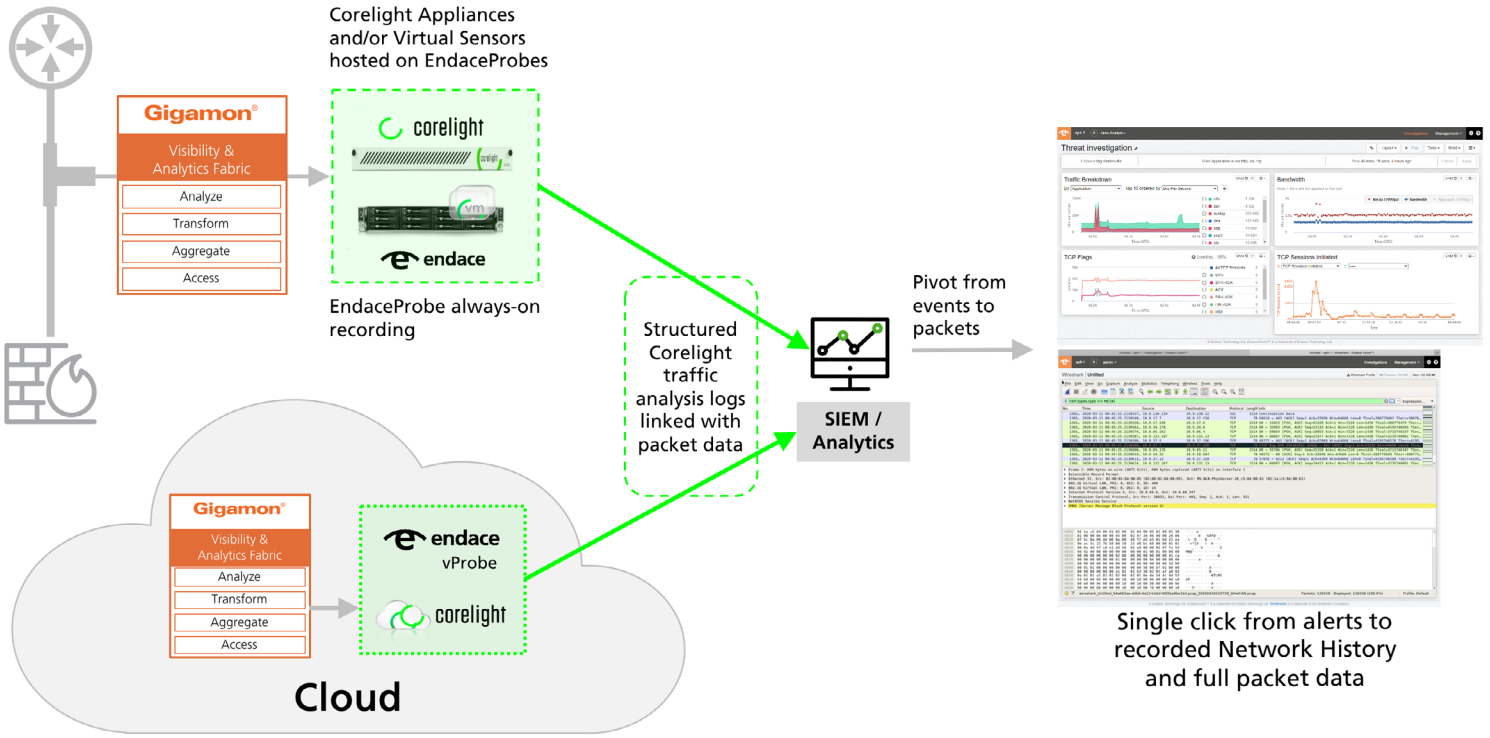
From those tools, SecOps analysts can drill-down, in context, to tamper proof, full packet data in EndaceVision.

Conclusion

Combining Gigamon, Corelight and Endace delivers much greater visibility into attack activity, more effective threat detection and definitive evidence. It enables SecOps teams to combat increasingly numerous and sophisticated attacks.

Integrating the three technologies enables security teams to be more agile and efficient. Hosting Corelight Sensors on EndaceProbes provides the flexibility to rapidly deploy sensors anywhere EndaceProbes are deployed. Teams can analyze traffic across the entire network, investigate threats and alerts faster, and accurately determine the impact of events so they can respond quickly and appropriately.

How it Works



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

For further information, email: info@endace.com