Corelight and Endace

Integrated alerts, logs, and network history for rapid and accurate incident response

EndaceProbe Network History integrated with Corelight Sensors provides rich, contextual, network evidence to everyone in the SOC for fast and accurate decisions even with the most challenging threats.

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 over 400 fields directly from network traffic in real time. Zeek logs are structured, and interconnected, specifically to support threat hunting and incident resolution.

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. Customers can deploy instances of Corelight Virtual Sensors onto any EndaceProbe without rolling out additional hardware.

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. All models of Corelight sensor can be integrated with EndaceProbe for rapid and conclusive incident response.

Deploying EndaceProbe and Corelight sensors together tightly couples log data with recorded network history, allowing analysts to quickly see exactly what occurred on the network. This tight connection between logs and packets lets analysts investigate incidents rapidly and drill-down to recorded network history to see the full extent of any threat.

Efficient Investigation and Threat Hunting

The full Network History recorded by EndaceProbes can be integrated into Corelight users' workflows using the Pivot-To Vision™ function of the EndaceProbe API. Pivot-To-Vision lets security analysts pivot from threat logs generated by Corelight directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

Corelight logs are typically ingested by SIEMs - such as Splunk, Elastic, Chronicle, Securonix, Exabeam, and many more - for analysis, alerting and reporting. From those tools, SecOps analysts can drill down from threat indicators to related network packet data in EndaceVision using the IP address and time range of the trigger event, focusing the analyst directly on relevant incident data. EndaceVision lets them dissect, review and extract the relevant traffic from the petabytes of Network History recorded on EndaceProbes deployed on the network. EndaceVision supports analysis to microsecond level detail, with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, providing rapid insights and enabling accurate conclusions.

Being able to get directly to the related packets with a single click lets security analysts quickly establish the root cause of issues as they perform threat hunting in their environment. They can respond quickly to threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of security threats escalating to become more serious breaches.

Rapid Deployment with Application Dock

Deploying next-generation security hardware takes significant planning and effort. New rollouts can often take 6 months or more to acquire and deploy new hardware. This puts security teams at a disadvantage when trying to defend against criminals who can launch attacks at the click of a mouse.

Corelight virtual Sensors can be hosted on the EndaceProbe in Application Dock. Every packet captured and recorded by the EndaceProbe can also be streamed to Corelight Sensors in real time. EndaceProbes are designed to ensure system resources used for capture

corelight

PRODUCTS

Corelight Sensors

EndaceProbe Analytics Platforms with Application Dock

EndaceVision and Investigation Manager

BENEFITS

- 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 insight into network traffic and definitive network evidence.
- Enterprise class deployment, performance and management of Zeek
- Customize detection capabilities by utilizing the flexibility of Zeek.
- Filter out false positives more quickly and confidently.
- 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 without truck rolls or complicated hardware deployments.
- Keep a definitive evidence trail with an accurate record of packets relevant to threats.
- Reduced threat exposure through faster and more definitive incident response

END_fp_end_corelight_1.0_0720

and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when the hosted the Corelight virtual Sensor is processing heavy traffic loads.

Conclusion

Corelight structured logs combined with the Network History recorded by EndaceProbes delivers comprehensive security and deep contextual insight for rapid investigation and response. Integrating the two technologies lets security analysts respond to security threats with much greater speed and accuracy.

How it Works

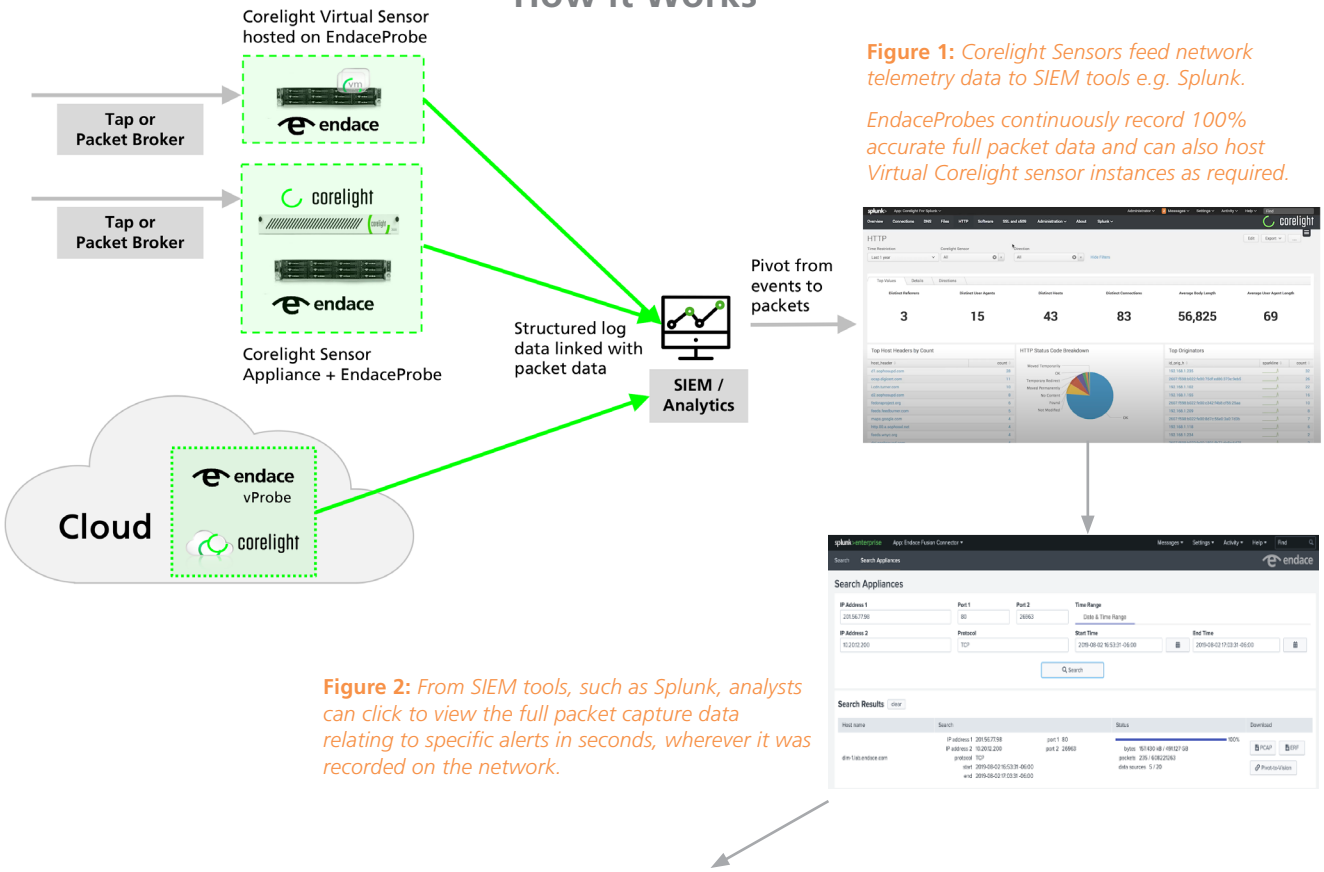

Figure 1: *Corelight Sensors feed network telemetry data to SIEM tools e.g. Splunk.*

EndaceProbes continuously record 100% accurate full packet data and can also host Virtual Corelight sensor instances as required.

Figure 2: *From SIEM tools, such as Splunk, analysts can click to view the full packet capture data relating to specific alerts in seconds, wherever it was recorded on the network.*

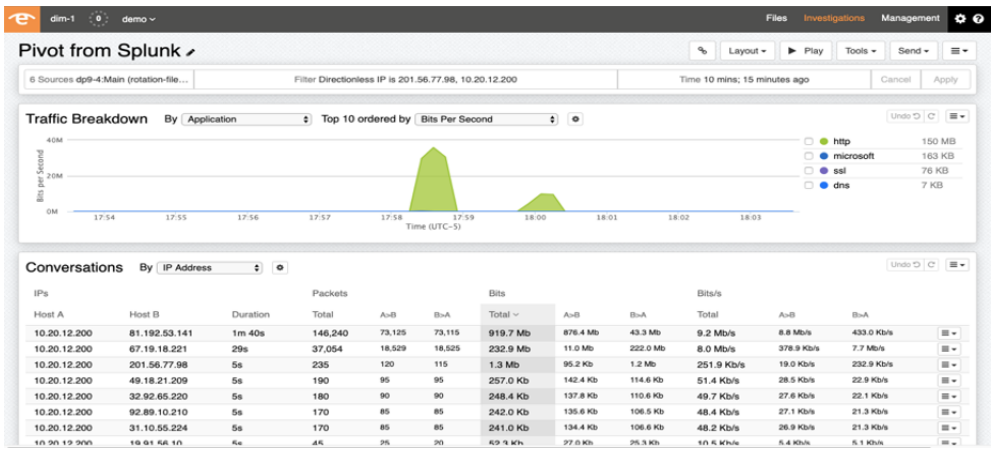

Figure 3: *Once traffic-of-interest has been analyzed in EndaceVision, full packet data can be saved as a pcap for local analysis, or opened in Wireshark directly on the EndaceProbe without the need to download pcaps..*

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

For further information, email: info@endace.com