Endace and Gigamon

As the foundation of your security tool suite, EndaceProbe and GigaSECURE provide efficient and rapid threat detection, containment and response.

Security teams are increasingly challenged by an evolving threat landscape, budget and operational constraints that hinder agility, and escalating impacts to companies that are breached.

The combination of Gigamon and Endace as the foundation of your network security architecture, improves security posture and gives organisations greater agility, improved threat coverage and enhanced ROI.

GigaSECURE Meets Endace

GigaSECURE is a next generation network packet broker platform that's purpose built for security.

It's designed from the ground up to:

- Enable security tools to keep up with increasing network speed
- Gain insight into network traffic including encrypted traffic
- Optimize and deliver relevant data for tool consumption
- Reduce tool sprawl and lower costs

EndaceProbe™ Analytics Platforms capture, index and store network traffic with 100% accuracy while simultaneously hosting a wide variety of network security and performance monitoring applications in Application Dock™, EndaceProbe's built-in hosting environment.

Customers can extend their security monitoring capability by deploying security tools on demand, wherever EndaceProbes are deployed. Hosted instances can analyze recorded traffic in real time at full line-rate or analyze recorded Network History for back-in-time investigation.

Accelerating Security Investigations

The Network History recorded by EndaceProbes can be integrated with leading security tools and SIEMs using the Pivot-to-Vision™ function of the EndaceProbe API.

Pivot-to-Vision lets security analysts pivot from threat alerts directly to EndaceVision™ (the EndaceProbe's built-in investigation tool) to analyze the related, packet-level Network History. Using the IP address and time range of the trigger event, Pivot-to-Vision focuses the analyst directly on pre-filtered incident data.

EndaceVision lets analysts dissect, review and extract the relevant traffic from the terabytes of Network History recorded on the network. It enables analysis to get to microsecond level, with views filtered by Application, IP, Protocol, Top Talkers and other parameters, for rapid insights and accurate conclusions.

PRODUCTS

GigaSECURE Security Delivery Platform

EndaceProbe Analytics Platform with Application Dock

BENEFITS

- SSL decryption for full visibility of threats hiding inside encrypted traffic.
- Maximize visibility into far reaches of physical, virtual and cloud networks to eliminate blind spots.
- Agile defense, deploy analytics on demand anywhere an EndaceProbe is deployed.
- Easy packet-deduplication, filtering and traffic load-balancing.
- Access a definitive evidence trail with an accurate record of all relevant packets.
- Reduce threat exposure through improved analyst productivity and faster incident investigation.
- Bridge the gap between NetOps and SecOps by giving both teams the ability to rapidly make critical decisions using a shared source of definitive Network History

Being able to get directly to the related packets with a single click lets security analysts rapidly establish the root cause of issues. They can respond quickly, which dramatically reduces time-to-resolution for critical incidents and minimizes the risk of security threats becoming serious breaches.

Scaled Monitoring Across the Far Reaches of Your Network

As your network and business grows, so should your monitoring capability. EndaceFabric enables multiple EndaceProbe™ Analytics Platforms to be connected into a centrally searchable network-wide fabric. This provides visibility into, and accurate recording of, network traffic across an entire network– including visibility into high-speed 40Gbps and 100Gbps links. The distributed fabric is centrally managed using the EndaceCMS Central Management Server™ which provides low OPEX and CAPEX.

GigaSECURE provides flexibility to monitor any segment of your network, and adjust monitoring points dynamically in response to threats or changes in your network. This allows the EndaceProbe Analytics Platform to be applied to critical parts of your network, and for resources to be moved to hot spots as and when new threats emerge.

GigaSECURE load balancing is used to combine EndaceProbes for increased throughput, hosting capacity and storage depth, without compromising its 100% accurate packet capture.

Detect Threats Inside Encrypted Traffic

SSL Decryption is critical to securing today's enterprise networks due to the significant growth in applications and services using encrypted traffic. In recent years, SSL has evolved to the Transport Layer Security (TLS) standard.

Malware increasingly uses SSL/TLS sessions to hide, confident that security tools will neither inspect nor block its traffic. The very technology that makes the Internet secure can become a significant threat vector.

Deploying GigaSECURE to decrypt in real time allows un-encrypted traffic to be captured by EndaceProbe, and streamed to security tools running in Application Dock. Strong crypto algorithms such as Perfect Forward Secrecy (PFS), Diffie-Hellman and its variants, Elliptic Curve ciphers are no longer a barrier to robust security.

Conclusion

GigaSECURE and EndaceProbe Analytics Platform provide a robust and flexible foundation for your network security infrastructure. Improved security posture, greater agility and enhanced Security tool ROI is achieved. State of the art security tools can be fully utilized, new capabilities can be rolled out quickly without CAPEX cycles or truck rolls, and threats can be detected and remediated quickly and with absolute confidence.

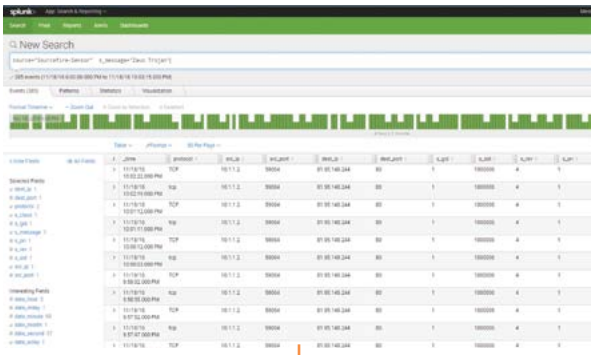
Example

BLUVECTOR

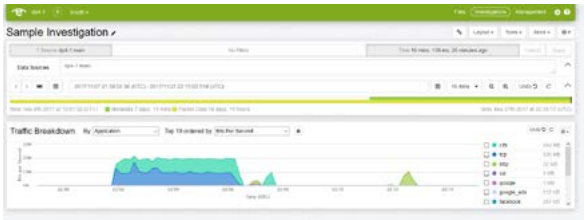
Hosted BluVector Cortex sensor accesses traffic in real time from EndaceProbe

Cortex sends threat alerts to Splunk

splunk>



Pivot from Splunk alert to packet investigation in EndaceVision



endace

Gigamon

GigaSecure directs traffic to EndaceProbe

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

For further information, email: info@endace.com