Endace and Gigamon

Deep observability from Endace and Gigamon delivers the insights you need to defend against the toughest security threats.

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.

Gigamon + Endace

Gigamon provides organizations with complete East-West visibility across their entire infrastructure and complements the full packet capture provided by the EndaceProbe™ Analytics Platform.

Customers can use the Gigamon Deep Observability Pipeline to access, broker, and filter important traffic to EndaceProbes which continuously record weeks or months of full-packet data to solve cybersecurity, network and application issues.

By deploying Gigamon and Endace products together, customers can

- Record an accurate, packet-level record of all network activity.
- 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

EndaceProbes 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™, the EndaceProbe's built-in hosting environment.

Customers can extend their security monitoring capability by deploying security tools on demand, wherever EndaceProbes are deployed. Hosted tools 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 continuous, full-packet capture and recording provided 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.

Gigamon®

PRODUCTS

Gigamon Deep Observability Pipeline

EndaceProbe Analytics Platform with Application Dock

BENEFITS

- Remediate any incident leveraging weeks or months of full-packet capture at your fingertips.
- SSL decryption for full visibility of threats hiding inside encrypted traffic.
- Maximize visibility into far reaches of physical, virtual, cloud and containers 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

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.

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 EndaceProbes 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 40 Gbps and 100 Gbps links. The distributed fabric is centrally managed using the EndaceCMS™ Central Management Server which reduces both OPEX and CAPEX costs.

END_fp_end_gigamon_1.3_0123

The Gigamon Deep Observability Pipeline gives you the ability to monitor any segment of your infrastructure, 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.

GigaVUE load balancing is used to combine EndaceProbes for increased throughput, hosting capacity and storage depth, without compromising the ability for EndaceProbes to capture and record network traffic with 100% accuracy.

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.

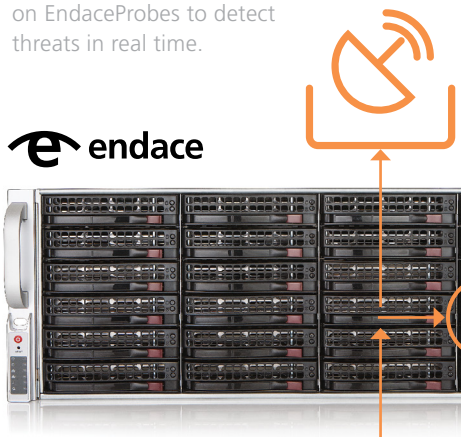
Deploying Gigamon to decrypt traffic in real time allows un-encrypted traffic to be recorded by EndaceProbes, and streamed to security tools running in Application Dock. Strong crypto algorithms such as Perfect Forward Secrecy (PFS), Diffie-Hellman and its variants, Elliptic Curve ciphers are no longer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

Conclusion

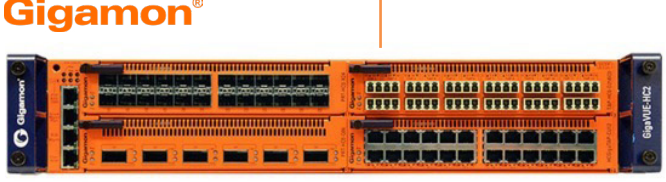
The Gigamon Deep Observability Pipeline and EndaceProbe Analytics Platforms provide a robust and flexible foundation for your network security infrastructure. Improved security posture, greater agility and enhanced security tool ROI is achieved. State of the art security tools can be fully utilized, 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 Deployment and Workflow

Host third-party security monitoring tools directly on EndaceProbes to detect threats in real time.

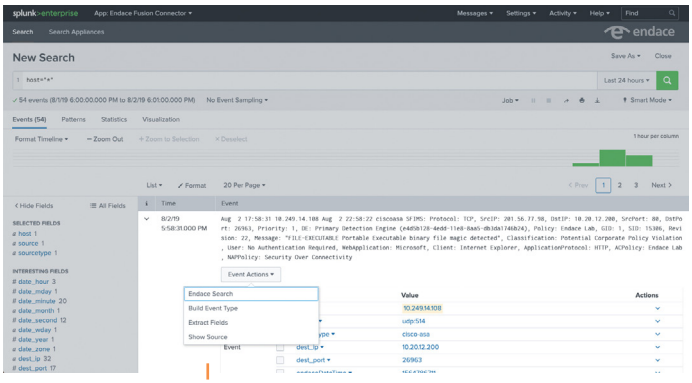


EndaceProbe continuously records weeks or months of full packet data

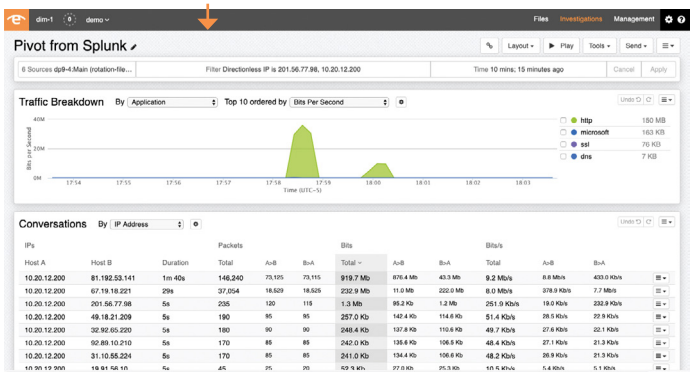


GigaVUE HC Series directs decrypted traffic to EndaceProbe

Pivot from alerts in security tool dashboards, or from SIEM tools such as Splunk, directly to the related packet data on EndaceProbes.



Pivot from Splunk alerts to packet investigations in EndaceVision



Analyze recorded traffic in EndaceVision. View decoded packet data directly in hosted Wireshark™ on the EndaceProbe or download pcaps for local analysis and/or archival.

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

For further information, email: info@endace.com