Joint Solution Brief

Accurate Packet Capture for Quick, Conclusive Investigation of Network Performance and Security Issues with Gigamon and Endace

The Challenge

Due to the transient nature of network activity – once packets traverse a network, only traces of their activity remain – network and security analysts can struggle to investigate performance and security issues in a timely and definitive manner.

Integrated Solution

Combined with the Gigamon GigaSECURE® Security Platform, the EndaceProbe™ Network Analytics Platform records an accurate history of network activity, giving analysts the definitive, packet-level evidence they need to quickly and conclusively investigate and respond to performance and security issues.

Joint Solution Benefits

- Efficiently and accurately record every packet on any segment of your network, from physical, virtual or cloud environments.
- Aggregation, de-duplication, load balancing and advanced filtering of traffic ensures only relevant data is captured.
- See inside encrypted traffic and record it on your EndaceProbe.
- Rapidly and accurately investigate incidents using workflow integration with leading security and performance tools.
- Rely on nanosecond precise timestamped packet history to show exactly what happened and when it happened.
- Use Playback™ to analyze recorded traffic using virtual tools running in Application Dock on EndaceProbes, removing the need to ship large sensitive packet capture files around the network for analysis.

Introduction

Incident investigation can be a slow, challenging and an inconclusive process – especially as network speeds and loads continue to grow. Analysts must hunt for clues in system and application logs, authentication records and metadata to find the evidence they need to diagnose and respond to security threats, data breaches and network or application performance issues.

A complete, detailed and accurately time-stamped source of packet data gives analysts the definitive evidence they need to quickly identify and respond to security or performance issues. Other evidence sources, such as NetFlow records for example, simply do not deliver the detail necessary to reconstruct events with certainty in order to understand how to remediate the issue.

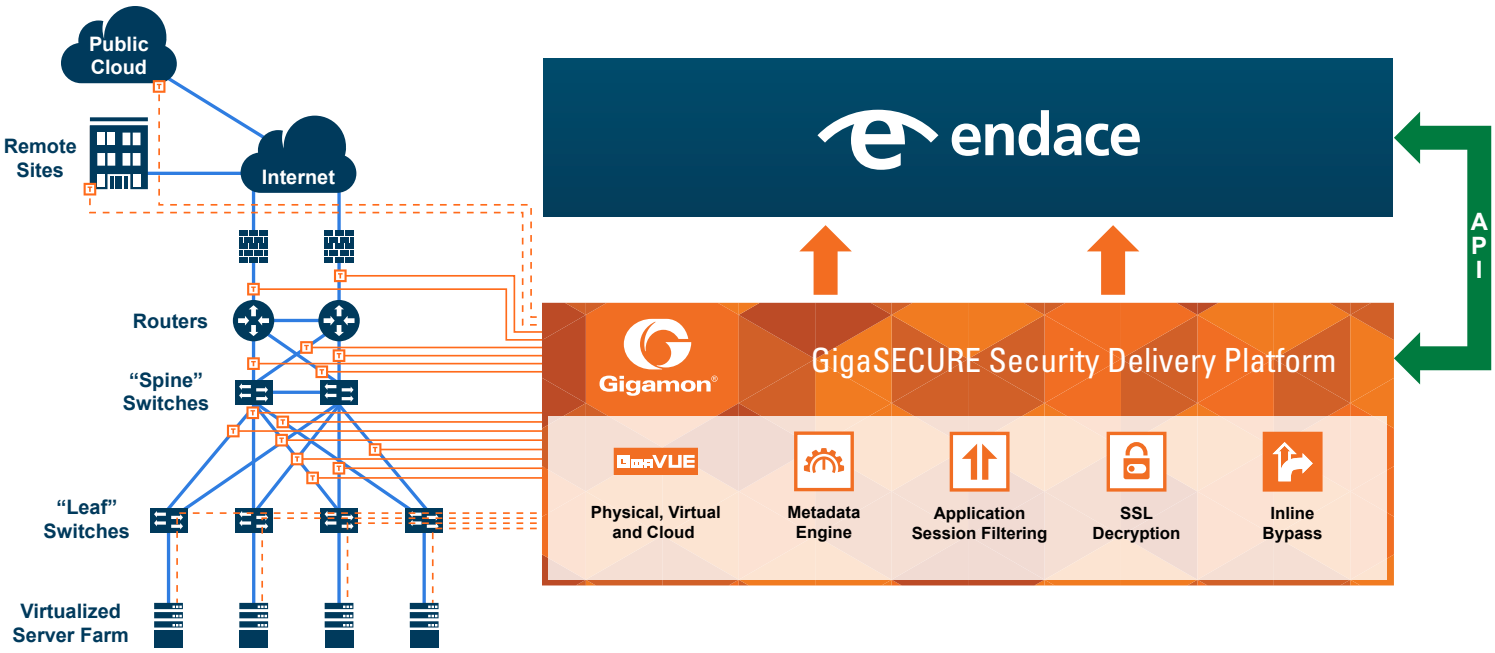
The Gigamon and Endace Joint Solution

EndaceProbes can capture, index and store a highly-accurate, packet-level history of network activity – in real-world conditions without dropping packets – to support cybersecurity investigations, security breach analysis and network or application troubleshooting.

The GigaSECURE Security Delivery Platform can be used together with EndaceProbes to provide pervasive visibility across the entire infrastructure, providing security teams with broad and consistent visibility into network activity. The result is a more effective network security infrastructure with a vastly improved return-on-investment (ROI).

Multiple EndaceProbes can be connected to form a centrally managed, centrally searchable, network-wide packet capture and analytics fabric – the EndaceFabric. With a rich API, and built-in hosting for analytics applications in Application Dock™, they integrate easily with third-party security, network monitoring and application performance monitoring applications to facilitate rapid access to historical traffic for analysis. Hosted applications can access live traffic at full line rate and provide the flexibility to deploy your tools of choice quickly, on-demand, to monitor any network - without truck rolls or hardware installs.

EndaceProbes apply nanosecond-accurate time stamps to captured packets, allowing for precise reconstruction of even ultra-short-lived network events. Integration with a wide variety of security and performance monitoring tools means analysts can click on alerts in those tools and jump straight to the related packet-level history to see what's happened, streamlining and automating issue investigation.



Key features of the GigaSECURE® Security Delivery Platform and EndaceProbes include:

Easy access to traffic from physical, virtual and cloud networks: The GigaSECURE Security Delivery Platform manages and delivers all network traffic – including east-west data center traffic and private and public cloud workloads – to EndaceProbes and EndaceFabrics efficiently, and in the correct format, to eliminate blind spots and help ensure visibility of all traffic.

SSL decryption: Real-time SSL decryption increases traffic visibility for EndaceProbes and EndaceFabrics, broadening the scope for analysis and inspection of malicious activity.

De-duplication: Pervasive visibility requires tapping or copying traffic from multiple points in the network which, in turn, means tools may see the same packet more than once. To avoid unnecessary packet-processing overhead, the GigaSECURE Security Delivery Platform removes duplicates and helps balance monitoring coverage.

Filtering relevant traffic: The GigaSECURE Security Delivery Platform can be configured to send only relevant traffic or sessions to EndaceProbes to help ensure that traffic of interest is recorded and analyzed.

Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single tool can handle, the GigaSECURE Security Delivery Platform can split the flow across multiple tools while helping to ensure sessions are kept together. This feature also facilitates incremental tool growth rather than rip-and-replace upgrades by allowing new devices to be added to those already connected.

Learn More

For more information on Endace and Gigamon solutions, contact:

endace
www.endace.com

Gigamon®
www.gigamon.com

3264-01 04/18