Joint Solution Brief

Improve Network Analysis and Security with Real-Time Relevant Data Retrieval from Napatech and Gigamon

The Challenge

In a time of data overload, relevance is everything. Without it, network monitoring and analysis applications cannot reach their full potential to improve performance, compliance, or security.

Integrated Solution

Integrated with GigaSECURE®, Gigamon Security Delivery Platform, the Napatech Pandion solution not only provides packet capture with nanosecond precision timestamping, but it allows for relevant data retrieval on demand and in real time.

Key Benefits

- Enhanced visibility and easy access to traffic from physical, virtual, and public cloud networks via GigaSECURE
- SSL decryption from GigaSECURE to avoid unnecessary processing by the Napatech Pandion solution while helping to ensure visibility into encrypted sessions
- Aggregation, filtering, and distribution of relevant traffic to Pandion accelerates processing throughput

Introduction

Network analysis is only as good as the data it's based upon. For example, when analyzing network congestion, breaches, or performance compliance, it is not only crucial to know what happened, but also when it happened in order to correlate events recorded by several devices. In other words, it's about relevance and the ability to retrieve specific data to satisfy specific needs.

And the solution for relevant data retrieval? Napatech Pandion. A fully scalable network recorder, Pandion was designed to capture all network traffic in real time, at line rate, without packet drops, and with nanosecond-precision timestamping. As necessary and on demand, it indexes and stores all relevant data for reliable behavior analyses, faster discovery and containment of threats, and complete forensic investigation of incidents and breaches.

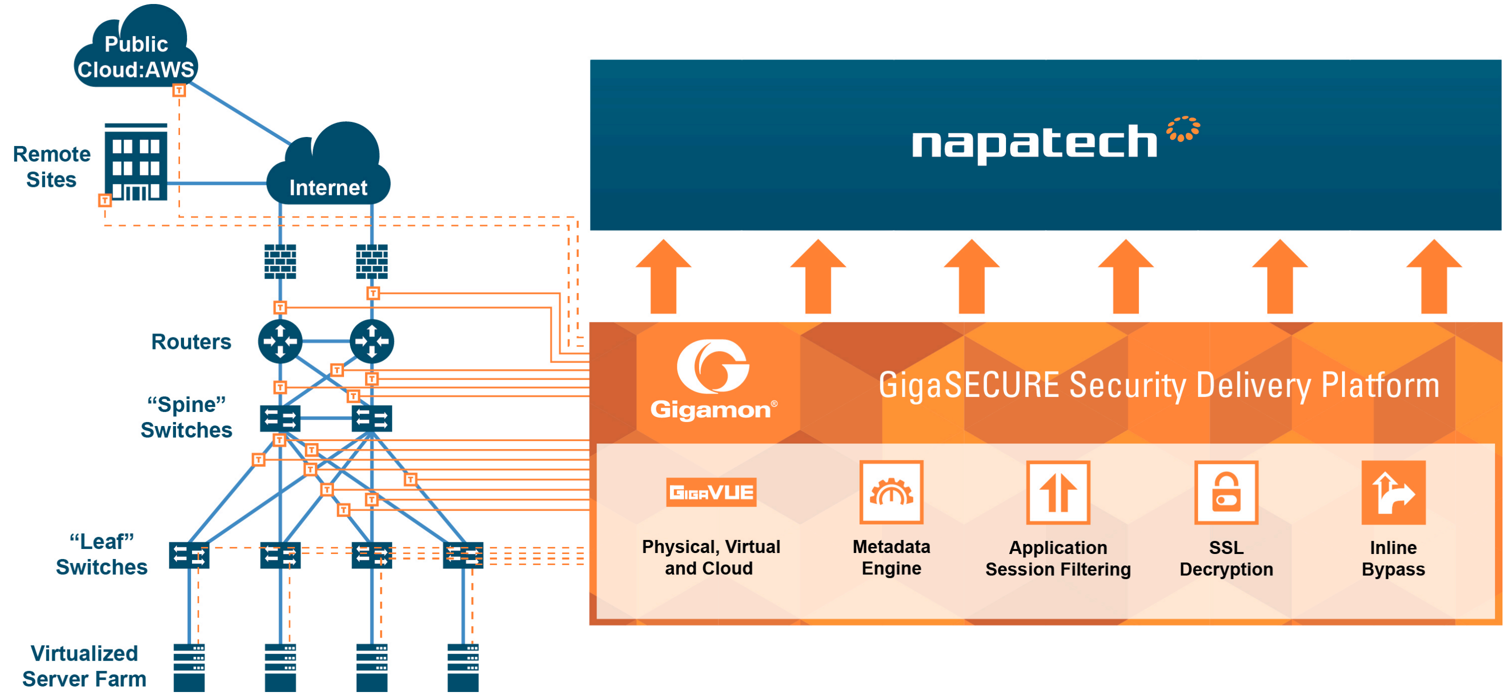
The Gigamon and Napatech Joint Solution

Napatech Pandion transports critical data with the lowest possible delay so that network monitoring and security systems can visualize all transactions in real time. Pandion correlates data from different parts of networks so organizations can deploy the right defense measures as and where needed. For example, they can retrieve historical data to determine the cause of a breach and help begin the recovery process. Or, should a security event require a full forensic investigation, the solution can send a full copy of the data with sustained throughput up to 40 Gbps.

Integrated with GigaSECURE®, Pandion helps shine a light on every relevant data detail. This way, security tools can focus on their core competencies at stopping attacks, protecting against data leaks, and providing complete and accurate records of everything that has happened on a network.

Key Gigamon® solution features that augment the value of Napatech technology deployments include:

Easy access to traffic from physical, virtual, and public cloud networks: The GigaSECURE Security Delivery Platform manages and delivers all network traffic to the Napatech Pandion solution, efficiently and in the correct format. To monitor east-west data center traffic and public cloud workloads, Gigamon taps virtual traffic and incorporates it into GigaSECURE for delivery to Pandion on the physical network. This eliminates blind spots and helps ensure that all traffic is monitored and analyzed together.



SSL decryption: Real-time SSL decryption integration increases traffic visibility for the Pandion solution.

Aggregation to minimize tool port use: GigaSECURE can aggregate links with low traffic volumes before sending them to Pandion to minimize the number of ports required. And by tagging the traffic, GigaSECURE helps ensure that the traffic source can be identified.

Deduplication: 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 on Pandion, Gigamon offers a highly effective deduplication engine that removes duplicates.

Traffic filtering: GigaSECURE sends specific traffic or sessions (e.g., HTTP, HTTPs, email) to Pandion devices so they do not become overloaded with irrelevant traffic that would only be dropped at a later point.

Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single tool can handle, GigaSECURE can split the flow across multiple tools while helping to ensure sessions are kept together and tool numbers can be incrementally grown by adding new devices to those already connected.

Masking for security: GigaSECURE is able to mask any sensitive data (e.g., credit card numbers in e-commerce and patient identification in healthcare) within packets before sending them to Pandion where operators or other unintended recipients may see them.

Learn More

For more information on the Napatech and Gigamon solutions, contact:

napatech
www.napatech.com

Gigamon®
www.gigamon.com