Joint Solution Brief

Pervasive Visibility from Gigamon and LogRhythm Facilitates Rapid Threat Detection and Response

The Challenge

Too much traffic compromises a security operator's ability to see and analyze the complete network and accurately detect anomalous behavior.

Integrated Solution

Together, Gigamon and LogRhythm deliver the visibility and insight necessary to accelerate detection and response to emergent threats across an organization's holistic attack surface.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic from physical, virtual and cloud networks with the GigaSECURE Security Delivery Platform.
- Automatic traffic load balancing helps optimize the performance of LogRhythm.
- Aggregation, filtering and distribution of relevant traffic to LogRhythm accelerates processing throughput.
- Ability to generate NetFlow from any traffic flow and decrypt SSL traffic to avoid unnecessary processing.
- Masking of sensitive data according to industry regulations before sending to LogRhythm.

Introduction

No matter what prevention technology organizations deploy, persistent hackers will find a way in. That's why today's security efforts must focus on finding and neutralizing malicious activity — faster, more effectively and before significant damage can be done. To do this, organizations must be able to see and patrol their complete network.

Understanding the power and necessity of visibility, Gigamon and LogRhythm have integrated their solutions – the Gigamon GigaSECURE® Security Delivery Platform and the LogRhythm Threat Lifecycle Management Platform with Network Monitor – to provide organizations with a comprehensive view of network traffic. This view supports rapid detection of and response to threats, including custom malware, nation state espionage, routine network misuse and many other types of anomalous behavior.

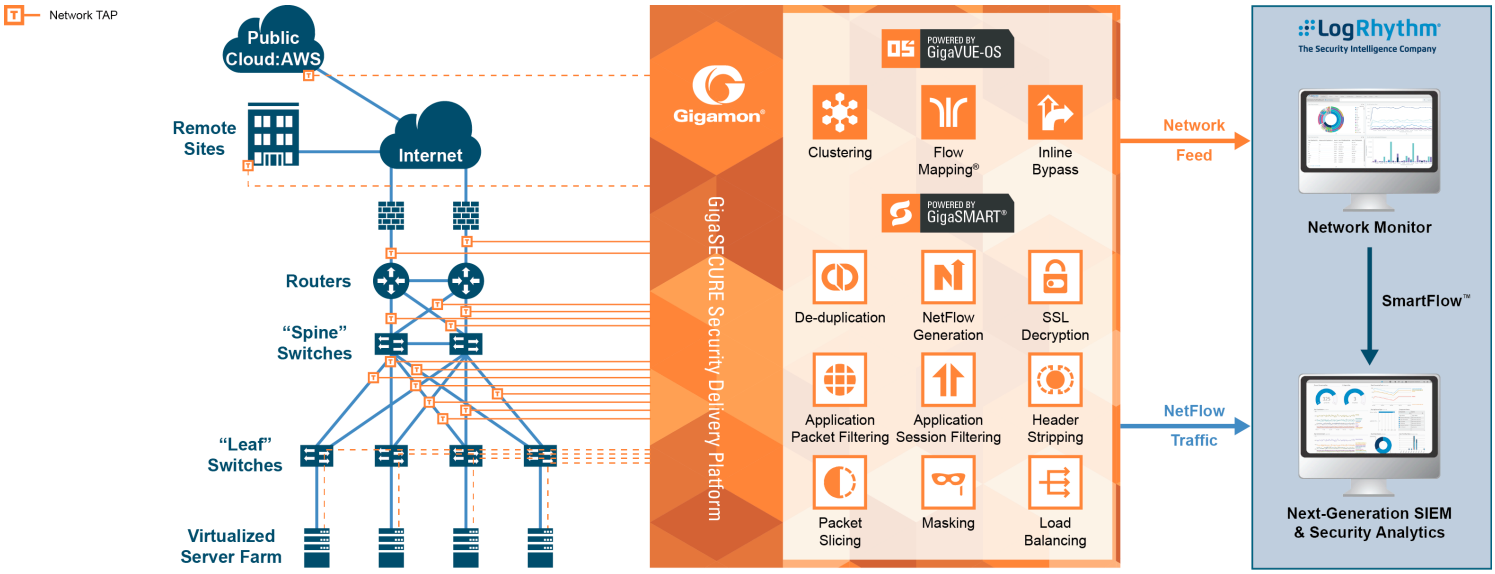
The Gigamon and LogRhythm Joint Solution

Combined, the Gigamon and LogRhythm solutions deliver the insight necessary to detect, prioritize and neutralize damaging cyber threats that have either penetrated the network perimeter or originated from within.

The GigaSECURE Security Delivery Platform aggregates a variety of links of any speed or media type, applies Layer 2-7 filtering on that traffic and delivers only relevant traffic to LogRhythm tools for analysis. The GigaSECURE Security Delivery Platform can also:

- De-dupe packets or slice off superfluous data to help maximize efficiency.
- Mask sensitive data such as credit cards for compliance.
- Include and exclude packets based on payload information – like URL, VoIP caller number or other data contained inside packets – for precise monitoring and analysis.

In turn, the LogRhythm Network Monitor delivers a rich set of searchable Layer 7 metadata – including identification of more than 3,000 applications – and provides customizable deep-packet analytics for real-time detection of network-born threats and anomalies, search-based forensics and selective full-packet capture. Moreover, the highly scalable LogRhythm Threat Lifecycle Management Platform combines next-generation SIEM, log management, multidimensional behavioral analytics as well as security orchestration and automation with network and endpoint monitoring to deliver a complete solution for end-to-end threat lifecycle management.



Key GigaSECURE Security Delivery Platform features that enhance the value of LogRhythm technology deployments include:

Easy access to traffic from physical, virtual and cloud networks: The GigaSECURE Security Delivery Platform manages and delivers all network traffic – in the correct format – to the LogRhythm Threat Lifecycle Management Platform and LogRhythm Network Monitor. Gigamon taps virtual traffic to monitor east-west traffic as well as traffic for private and public cloud deployments and incorporates this traffic into the GigaSECURE Security Delivery Platform. This ensures delivery of all traffic to LogRhythm solutions on the physical network for combined monitoring and analysis, thus eliminating blind spots.

Aggregation to minimize tool port use: Where links have low traffic volumes, the GigaSECURE Security Delivery Platform can aggregate these together before sending them to LogRhythm solutions to minimize the number of ports needed. By tagging the traffic, the GigaSECURE Security Delivery Platform can also identify the traffic source.

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 overheard on LogRhythm devices, the GigaSECURE Security Delivery Platform has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

Filtering and send relevant traffic: The GigaSECURE Security Delivery Platform can be configured to send only relevant traffic or sessions to the LogRhythm solutions to help ensure that they analyze just the traffic that presents a security risk.

Load balancing to spread traffic across multiple devices: When traffic flows are larger, the GigaSECURE Security Delivery Platform can split the flow across multiple LogRhythm instances.

SSL decryption: Real-time SSL decryption increases traffic visibility for the LogRhythm Threat Lifecycle Management Platform, broadening the scope for analysis and inspection of malicious activity.

Masking for compliance: The GigaSECURE Security Delivery Platform can masks sensitive data – for example, credit card numbers in e-commerce data and patient identification in healthcare data – within packets before sending them to other tools where operators or other unintended recipients may see them.

Metadata generation: The GigaSECURE Security Delivery Platform generates and sends unsampled NetFlow records for any traffic flow to the LogRhythm solutions. It also sends extended metadata records – for example, HTTP response codes and DNS queries – to provide highly detailed contextual analysis when looking at network events.

Learn More

For more information on LogRhythm and Gigamon solutions, contact

LogRhythm
www.logrhythm.com

Gigamon®
www.gigamon.com

3138-02 07/17