Detect Anomalies and Threats, Facilitate Rapid Response with Gigamon and LogRhythm

Overview

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

LogRhythm helps busy and lean security operations teams save the day. There is a lot riding on the shoulders of security professionals including the reputation and success of their company, the safety of customers and employees across the globe, and the security of critical resources. Understanding the power and necessity of visibility, Gigamon and LogRhythm have integrated their solutions to provide organizations with a comprehensive view of network traffic.

This joint solution enables rapid detection of and response to threats, including custom malware, nation state espionage, routine network misuse and many other types of anomalous behavior.

The Challenge

An overload of irrelevant traffic compromises a security team's ability to detect and respond to anomalous behaviors in their infrastructure.

Integrated Solution

Together, Gigamon and LogRhythm deliver the visibility and insight necessary to accelerate detection and response to emerging 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 Gigamon Deep Observability Pipeline.
- 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 private/sensitive data to meet industry regulations before sending to LogRhythm.

The Gigamon Deep Observability Pipeline manages and delivers network intelligence to Log Rhythm providing teams with:

Easy access to traffic from physical, virtual, and cloud networks: The Gigamon Deep Observability Pipeline accesses East-West, North-South traffic from public cloud, virtual, and physical data center deployments for further brokering and processing. This ensures delivery of all traffic to LogRhythm for combined monitoring and analysis without blind spots.

Aggregation: The Gigamon Deep Observability Pipeline aggregates traffic from multiple network links before sending it to one or more tools and tool instances. This handles asymmetric routing and link aggregation groups, maximizes tool utilization, and ensures operational effectiveness of tools. Tagging the traffic also ensures the source of traffic is identifiable.

Packet de-duplication: Complete 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. The Gigamon Deep Observability Pipeline has a de-duplication engine that removes duplicates before they consume bandwidth.

Filtering and forwarding relevant traffic: The Gigamon Deep Observability Pipeline can be configured to forward only relevant traffic or sessions to the LogRhythm and other tools.

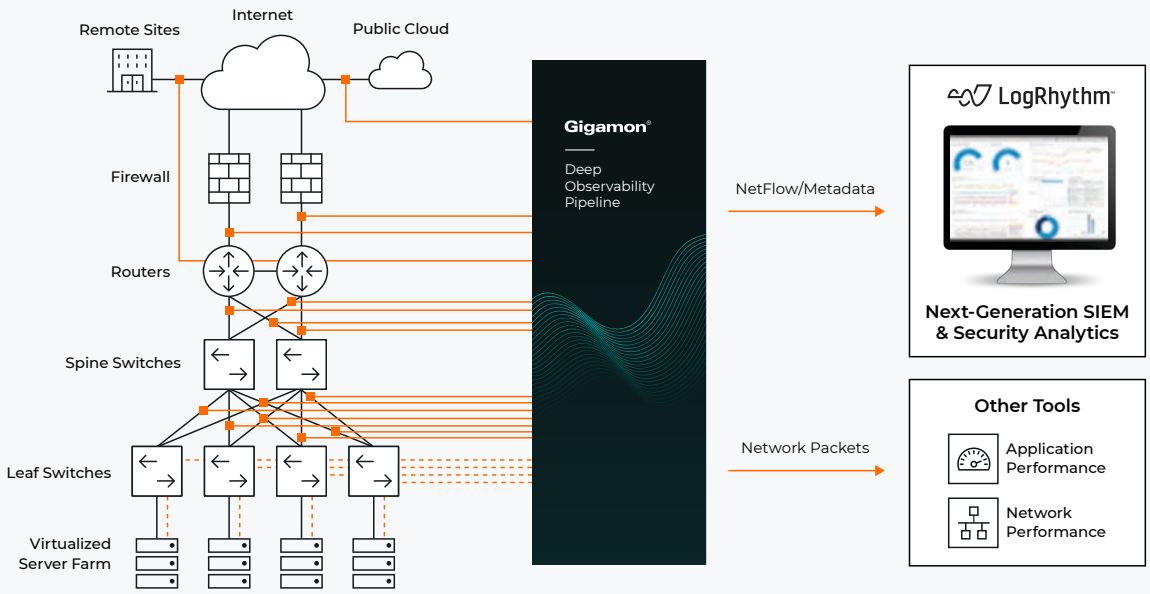

Figure 1. The Gigamon Deep Observability Pipeline and LogRhythm Combined Solution.

Load-balancing to spread traffic across multiple devices: For significant traffic volumes, the Gigamon Deep Observability Pipeline can spread the flows across multiple tool instances and NetFlow/Application metadata generation engines to match the processing capacities.

SSL/TLS decryption: Real-time decryption of TLS flows by the Gigamon Deep Observability Pipeline increases traffic visibility for the LogRhythm SIEM, broadening the scope for analysis and inspection for malicious activity.

Masking for compliance: The Gigamon Deep Observability Pipeline can mask private or 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 unauthorized recipients may see them.

Flow and metadata generation: The Gigamon Deep Observability Pipeline generates and sends unsampled L2-L4 NetFlow records in NetFlow or IPFIX formats and/or L3-L7 application metadata in IPFIX, CEF, or JSON formats for any traffic flow to tools such as the LogRhythm SIEM. Generated metadata can be selected from over 7,000 attributes across over 3,000 applications – for example, HTTP response codes and DNS queries – to provide highly detailed contextual analysis when looking at network events.

The Gigamon and LogRhythm Joint Solution

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

The Gigamon Deep Observability Pipeline aggregates a variety of links of any speed or media type, and then:

- De-duplicate packets to help maximize tool efficiency.
- Apply L2-L7 filtering to focus in on only relevant traffic for tools to analyze, with DPI detection of over 3,000 pre-defined applications.
- Mask personal or sensitive data, such as credit cards and user identifiers, for compliance.
- Decrypt flows encrypted using SSL, including TLS 1.3
- Transform packets and flows into L2-L4 NetFlow and/or L3-L7 rich metadata, with over 7,000 attributes to select from.
- Feed this network and application data to LogRhythm

And for other packet ingesting tools, the Gigamon Deep Observability Pipeline can also:

- Slice off superfluous data from packets, or slice off packets from flows, to help maximize efficiency.
- Balance the load across multiple instances of each tool.

In turn, the LogRhythm provides:

- Customizable deep-packet analytics for real-time detection of network-born threats and anomalies
- Search-based forensics and selective full-packet capture
- Log management
- Multidimensional behavioral analytics
- Security orchestration and automation

Together, the Gigamon Deep Observability Pipeline and LogRhythm solution provides network and endpoint monitoring that delivers a complete solution for end-to-end threat lifecycle management.

Figure 2. LogRhythm SIEM Analysis of Network and Application Metadata from the Gigamon Deep Observability Pipeline.

LogRhythm is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an everchanging threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Together, we are ready to defend.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

For more information on Gigamon and LogRhythm please visit gigamon.com | logrhythm.com

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

06.23_02