Gigamon

Flowmon Networks

Joint Solution Brief

Optimize Network Performance and Security with Flow-based Monitoring from Flowmon and Gigamon

The Challenge

The increasing complexity of IT enviroments has led to decreasing visibility into network traffic. And the harder it is for organizations to see what's happening on their networks, the more they struggle to detect anomalies, troubleshoot performance issues, and protect against volumetric DDoS attacks.

Integrated Solution

Organizations no longer need to trade security for performance—or vice versa. With enhanced visibility, they can have it all: fast, reliable, and secure networks. The joint Flowmon and Gigamon solution delivers advanced flow-based (NetFlow/IPFIX) traffic monitoring for complete network visibility and advanced security.

Joint Solution Benefits

- Manage and secure networks through high-performance monitoring and advanced behavior analytics
- Enhance visibility and gain easy access to traffic from physical and virtual networks via the GigaSECURE® Security Delivery Platform
- Generate NetFlow/IPFIX from any traffic flow within the GIgaSECURE platform and share records with Flowmon and any other tool benfiting from the metadata
- Optimize the performance of Flowmon technology at minimal cost with automatic traffic load balancing
- Accelerate processing throughput by aggregating, filtering, and distributing relevant traffic to Flowmon modules

Introduction

Network performance and security are paramount in contributing to the success of any business today. However, with the growing complexity of IT infrastructures has come a growing challenge to streamline troubleshooting of operational and security issues. This is not an ideal situation—especially when considering that even a minor network breach can lead to significant financial loss, reputation damage, or customer churn.

To respond to this challenge and help alleviate complexity, organizations have begun to turn to flow-based (NetFlow/IPFIX) network traffic monitoring. Flow-based monitoring provides detailed information—metadata—on who is communicating with whom, when, for how long, how often, with what protocol, and more. Using this metadata, network administrators can perform real-time monitoring of network utilization and uncover root causes of performance degradation while security engineers are able to detect traffic anomalies and suspicious behavior to help curtail the threat of advanced cyber attacks.

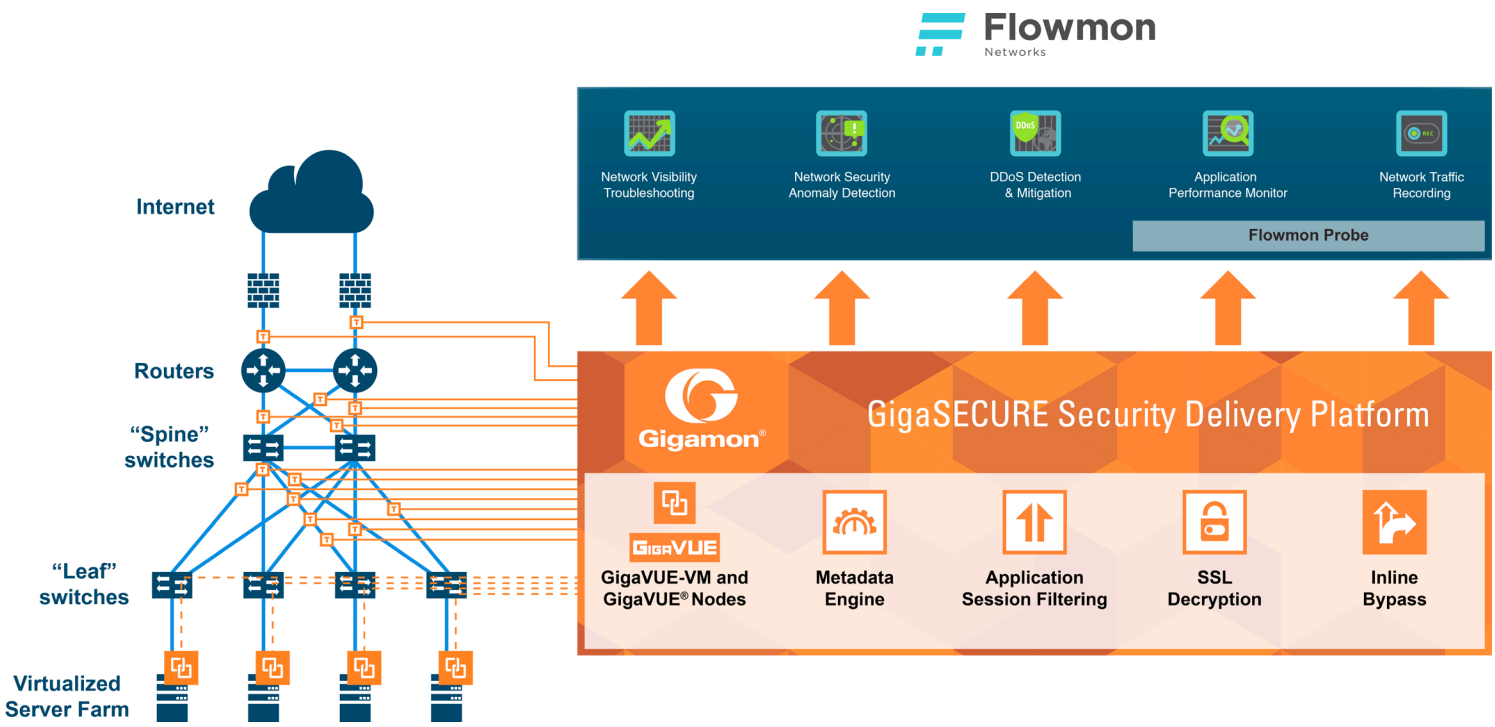
The Gigamon and Flowmon Networks Joint Solution

To help businesses take control over their IT infrastructures, Flowmon Networks provides a comprehensive platform for flow-based (NetFlow/IPFIX) network monitoring and security.

Integrated with the GigaSECURE Security Delivery Platform, Flowmon technology provides everything needed for complete network traffic visibility and analysis, including powerful collectors (Flowmon Collectors) that consume and store Gigamon-generated NetFlow/IPFIX metadata, including HTTP response codes and DNS queries, for deeper contextual analysis of network and security events. Additional modules are available for behavior analysis and anomaly detection (Flowmon ADS) and protection against volumetric DDoS attacks (Flowmon DDoS Defender). Dedicated Flowmon Probes, that can be provided access to traffic via GIgaSECURE, move the solution beyond flow technology enabling broad L7 visibility, HTTP/HTTPS application performance monitoring (Flowmon APM) and on-demand full packet capture (Flowmon Traffic Recorder).

Key GigaSECURE Security Delivery Platform features that augment the value of Flowmon technology include:

Easy access to traffic from physical and virtual networks: The GigaSECURE platform manages and delivers all network traffic to Flowmon solutions, efficiently and in the correct format. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to Flowmon as metadata files. This ensures that all traffic is monitored and analyzed together and eliminates blind spots.



Aggregation to minimize tool port use: Where links have low traffic volumes, the GigaSECURE platform can aggregate these together before sending them to the tool in order to minimize the number of ports that need to be used. By tagging the traffic, the Security Delivery Platform ensures that the source of the tagged traffic can be identified.

Filtering: The platform can be configured to send only relevant traffic or sessions to Flowmon modules avoiding unnecessary processing.

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

Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single Flowmon Collector can cope with, the GigaSECURE platform can be used to split the flow across devices, while keeping sessions together.

SSL decryption: Real-time SSL decryption integration increases traffic visibility for Flowmon solutions.

Easier control of asymmetric routing to ensure session information is kept together: Most security devices require all the packets in a session to be inspected by the same device as incomplete sessions risk being blocked. The GigaSECURE Security Delivery Platform provides an intelligent and efficient way to ensure this inspection happens in most architectures.

Learn More

For more information on Flowmon and Gigamon solutions, contact:

Flowmon Networks
www.flowmon.com

Gigamon®
www.gigamon.com

3205-01 09/16

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