Managing and Securing the Network through Full Visibility: Flowmon & Gigamon Joint Solution

Challenge

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.

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.

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.

Flowmon technology provides everything needed for complete network traffic visibility and analysis, including powerful **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. Dedicated **Flowmon Probes**, that can be provided access to traffic via **GigaSECURE**, move the solution beyond flow technology enabling broad L7 visibility. Additional modules are available to extend the solution and provide users with more functions and analytical capabilities:

- **Flowmon ADS** (Anomaly Detection System): Network and user behavior analysis for automatic detection of operational issues and security incidents like insider threats, external cyber attacks, indicators of compromise, and other anomalies.
- **Flowmon DDoS Defender**: Artificial intelligence for protection against volumetric DDoS attacks with capabilities to redirect the detected attack to scrubbing centers for the mitigation or mitigate the attack itself using various modern techniques.
- **Flowmon APM** (Application Performance Monitoring): Network-based application performance monitoring for all HTTP/HTTPS and database applications provides overview of user experience and SLA compliance.

- **Flowmon Traffic Recorder**: On-demand packet capturing enables IT operators with full trace of network traffic for forensic analysis of operation and security issues.

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. This ensures that all traffic is monitored and analyzed together and eliminates blind spots.
- **Traffic statistics generation:** Having easy access to the all network traffic and generating statistics in NetFlow or IPFIX format, Gigamon provides all the necessary data for the Flowmon solution to analyze and optimize network performance and detect operational and security issues.
- **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.

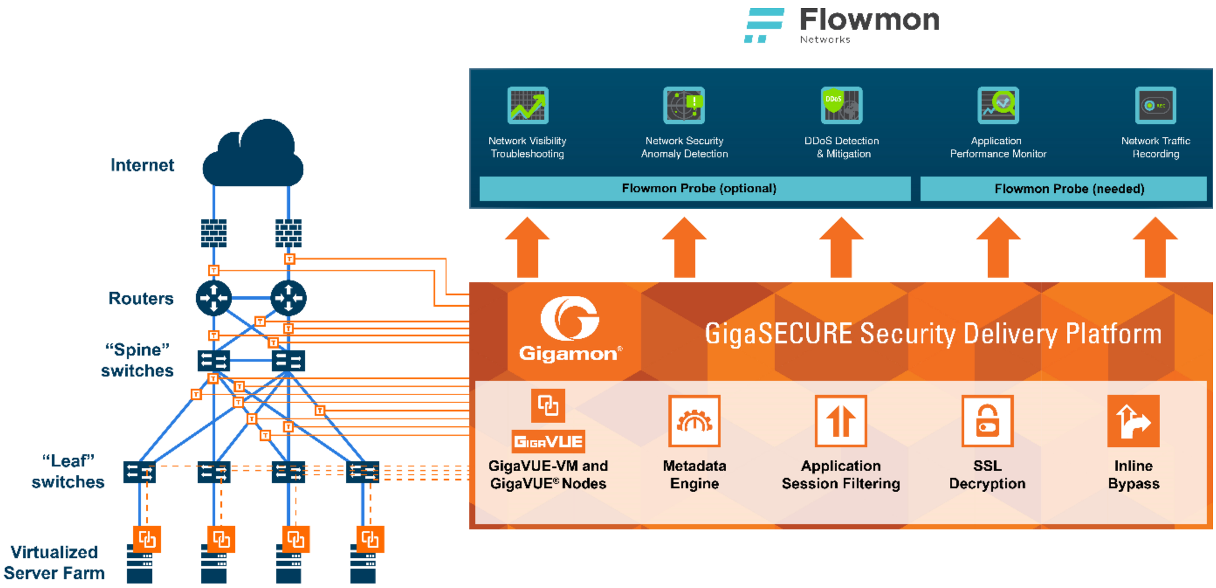
Flowmon
Networks
Network Visibility Troubleshooting
Network Security Anomaly Detection
DDoS Detection & Mitigation
Application Performance Monitor
Network Traffic Recording
Flowmon Probe (optional)
Flowmon Probe (needed)
Internet
Routers
"Spine" switches
"Leaf" switches
Virtualized Server Farm
Gigamon
GigaSECURE Security Delivery Platform
GigaVUE
GigaVUE-VM and GigaVUE® Nodes
Metadata Engine
Application Session Filtering
SSL Decryption
Inline Bypass

Figure 1: Joint solution architecture.

Joint Solution Benefits

- Manage and secure networks through high-performance monitoring and advanced behavior analytics using Flowmon technology.
- 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 benefiting 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.

For more information

For more information, please contact your Gigamon or Flowmon Networks partner.

Gigamon
3300 Olcott Street
Santa Clara
CA 95054 USA
www.gigamon.com

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno
Czech Republic
www.flowmon.com