Gigamon

FlowTraq

Joint Solution Brief

Catch More Bad Guys with Deeper Visibility Telemetry from FlowTraq and Gigamon

The Challenge

Threats are all around, all the time. Defense cannot begin and end at network borders. To spot and catch the most dangerous bad guys requires deliberate commitment and investment in pervasive visibility and detection.

Integrated Solution

FlowTraq, augmented with the GigaSECURE® Security Delivery Platform, arms cyber hunters with widespread visibility to detect malicious activity, perform quick security analyses, and perform forensic recall of network traffic.

Joint Solution Benefits

- Broad and deep visibility across traffic on both physical and virtual networks enables FlowTraq to hasten anomaly, APT, and data exfiltration detection
- Detect and mitigate distributed denial of service (DDoS) attacks intelligently and quickly
- Enable the cyber hunter by detecting unsual data movement and new services deep inside your network
- Generate unsampled NetFlow/IPFIX from traffic flow while avoiding processing load on routers and switches

Introduction

Cyber hunting is an art that requires a one-two punch. A good cyber hunter will seek to understand bad guys first; shut them down second. The reason: most intelligent, motivated adversaries already assume they are being watched. Shutting them down at the first sign of malicious activity simply tips them off and allows them to change tactics.

Likewise, cyber hunters should also assume that adversaries have gained an extensive foothold throughout the network. In order to quickly map out malicious activity and eliminate threats across the board, they need broad and deep visibility. Together, FlowTraq and Gigamon® not only arm cyber hunters with improved visibility telemetry, but also enable powerful detection, quick security analysis, and forensic recall of network traffic. FlowTraq can detect suspicious behavior from NetFlow data and provide protection by reacting in seconds.

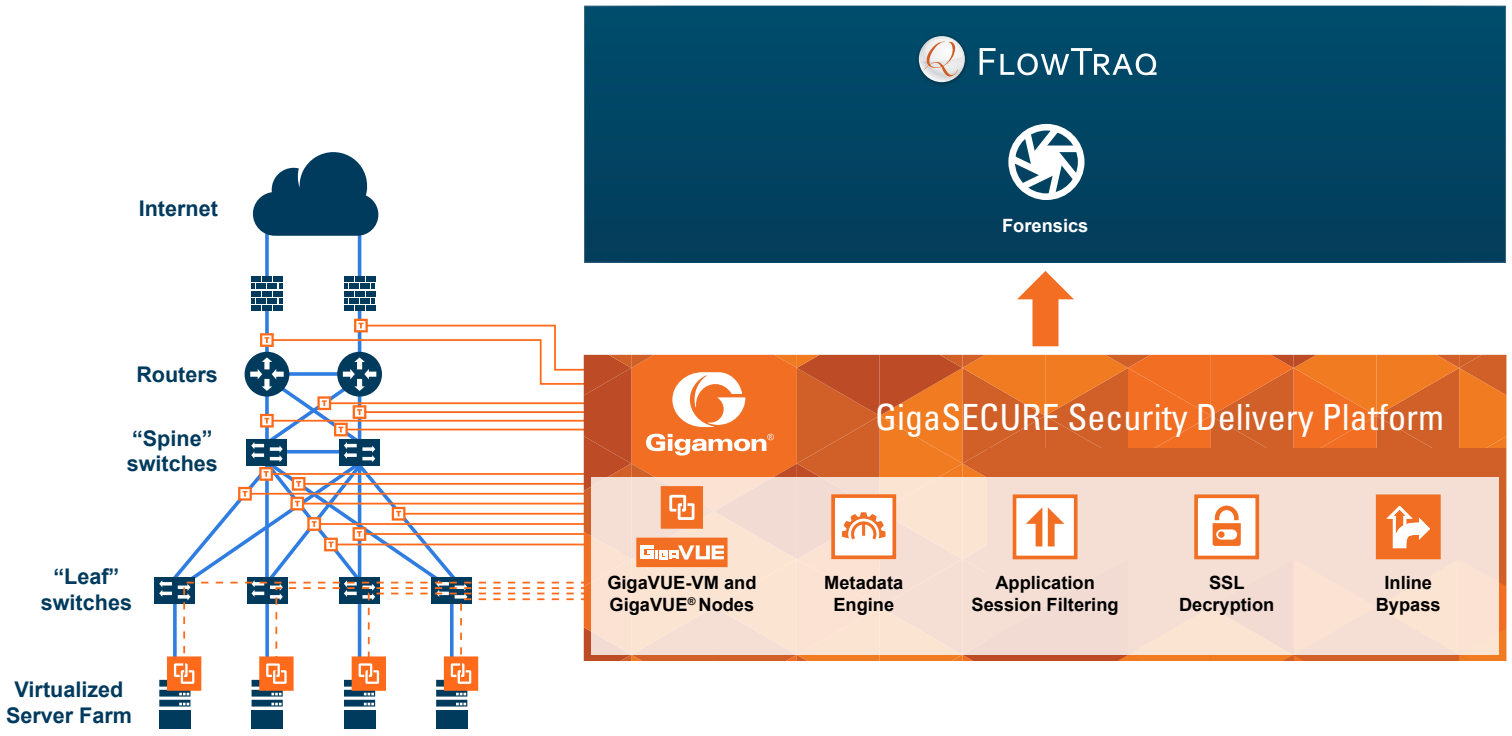
The Gigamon and FlowTraq Joint Solution

The most dangerous bad guys are the ones who are hardest to find—and already inside your network. They have the time, skill, and wherewithall to remain hidden as they move laterally across other systems and subnets. That is, unless cyber hunters arm themselves with wide and deep network visibility.

Designed to detect and alert on suspicious activity in big networks, FlowTraq leverages the GigaSECURE Security Delivery Platform for increased visibility into what is happening throughout networks in order to:

- Detect and alert on suspicious activity such as hacker movement
- Catch unknown attacks, botnet control channels, and new viruses
- Detect and mitigate DDoS attacks in seconds
- Detect and address unwanted data theft or leakage
- Perform valid traffic audits to investigate past connections.

Available for on-premise and cloud deployments, FlowTraq's network monitoring, analysis, and forensics tools are particularly suited to handle the high-traffic volumes of today's large and growing networks. Specifically, FlowTraq analyzes network traffic flow records, maintaining a high-fidelity record of flow-based network traffic and delivering visibility through a flexible, browser-based dashboard view. The solution's powerful Network Behavioral Intelligence engine learns and understands the changing patterns of behavior in networks and can send an alert when a system, mobile device, or server begins to behave outside normally-expected patterns. FlowTraq can detect a DDoS attack from the NetFlow data in seconds, react to the DDoS by sending an alert, and protect by triggering DDoS scrubbing, null route injection, or other defensive actions.



As networks grow, the GigaSECURE platform also helps FlowTraq facilitate cyber hunting even further by offering network visibility management. This way, security analysts can focus less time on administration and more time on finding botnets, backdoors, and other varieties of espionage or system sabotage. Key GigaSECURE features for FlowTraq deployments include:

- **Easy Access to traffic from physical and virtual networks:** The GigaSECURE platform enables traffic from across the network to be managed and delivered to FlowTraq efficiently and in the correct format. Also, east-west data center traffic is growing increasingly fast. Gigamon is able to tap virtual traffic and incorporate it into the GigaSECURE Security Delivery Platform for delivery to FlowTraq on the physical network—allowing traffic to be monitored and analyzed together, minimizing blind spots and increasing the likelihood of spotting suspicious behavior.
- **Filtering traffic to only send relevant traffic:** There's no point in loading FlowTraq with traffic it will only drop after identifying. The GigaSECURE platform can be configured to only send relevant traffic—or relevant sessions—to the FlowTraq solution.
- **Aggregation to minimize number of tool ports used:** Where links have low traffic volumes, the GigaSECURE platform can aggregate these together before sending them to FlowTraq in order to minimize the number of ports that need to be used. By tagging the traffic, the Security Delivery Platform allows the source of traffic to be identified.
- **NetFlow Generation and SSL Decryption:** If desired, processing intensive tasks can be offloaded from FlowTraq by using the GigaSECURE functionality for generating unsampled, enhanced metadata in NetFlow or IPFIX format from selected traffic streams. FlowTraq can detect suspicious behavior from NetFlow data and provide protection by reacting in seconds. Similarly, the Security Delivery Platform can be used to decrypt SSL encrypted traffic before sending to the FlowTraq solution.

Networks that only collect telemetry (such as Netflow and sFlow) at border points will be blindsided once adversaries are inside. Together, FlowTraq and the GigaSECURE Security Platform enhance network visibility so that the bad guys can be found and removed.

Learn More

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

FLOWTRAQ
www.flowtraq.com

Gigamon®
www.gigamon.com

3198-01 06/16

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