Solution Brief

Software-Defined Visibility

Challenges with Static Visibility

A comprehensive security and monitoring architecture requires a variety of tools, including NGFW, IPS, IDS, Forensics, DLP, Application Performance, Network Performance and other inline or out-of-band appliances. Still, all these protection systems are only as effective as the network traffic they see. In fact, the breadth of visibility to network traffic directly impacts the effectiveness of any security architecture.

For pervasive visibility and security, the network traffic should be acquired from as many of the devices and applications present in the data center and span physical, virtual and SDN/NFV environments, as well as private and public clouds.

But pervasive reach and static visibility alone are not sufficient to address the most salient of the current challenges:

- Emergence of new blind spots and threat vectors require dynamic changes to be in the visibility infrastructure in order to first detect and then eliminate those blind spots.
- Key Performance Indicators (KPIs) and Key Capacity Indicators (KCIs) are always being adjusted and fine tuned for optimal monitoring.

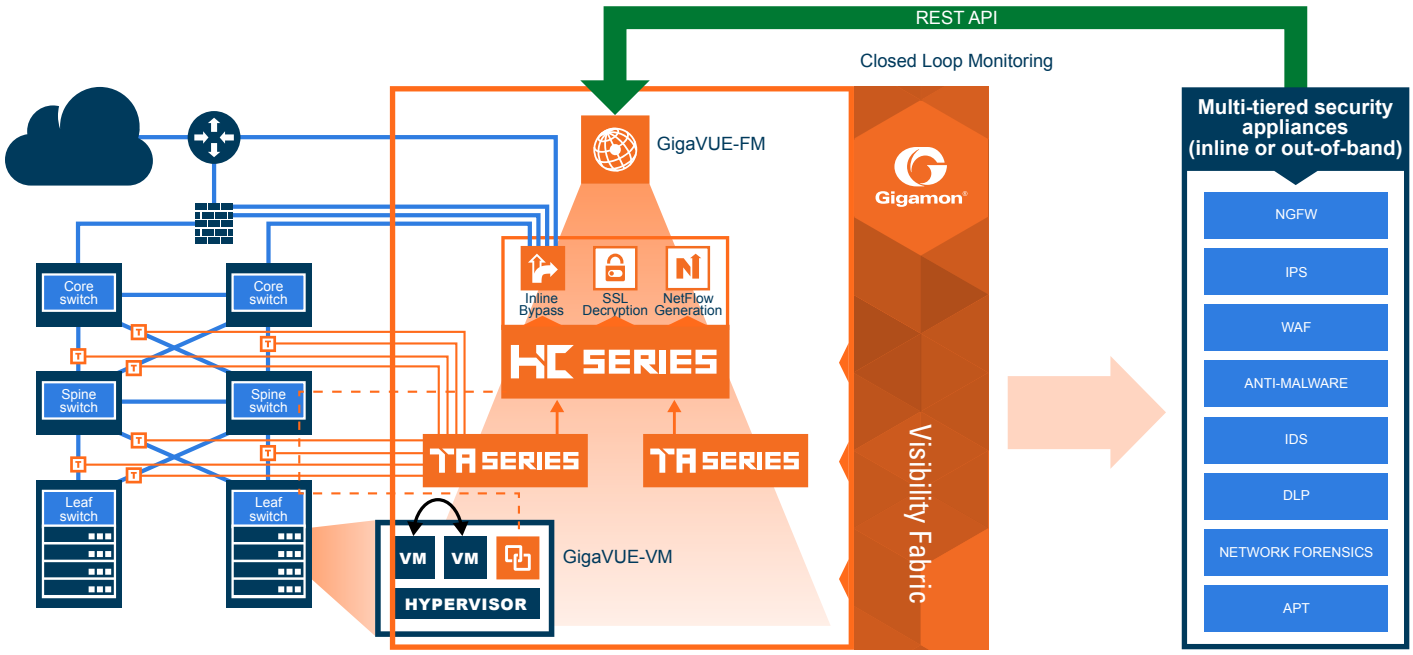
SecOps and NetOps administrators need a framework for increased automation so that the visibility infrastructure can respond dynamically to events or situations that diminish network access. These capabilities are the building blocks for modern IT.

Gigamon Solution—Software-Defined Visibility

To understand what Software-Defined Visibility (SDV) is, begin with the following questions:

- What if the applications and other operational tools that receive traffic from a Visibility Fabric™ also had a way to respond dynamically to events they detect without waiting for administrative intervention?
- What if the security application that detected a threat pattern had the capability to auto-adjust traffic to react and respond to the threat?
- What is the best way to implement visibility with automation?

For a CISO or stakeholder in IT operations, the response to the first two questions is likely, "That would be great!" The third question, however, might give pause.



A well-understood, general, and powerful approach is to integrate a Web-services framework based on RESTful Application Programming Interfaces (APIs) directly into the Visibility Fabric itself. This approach allows any device on the network to interact directly with the Visibility Fabric on an as-needed basis. APIs exposed through a centralized policy controller provide the ability for external systems to interact with the Visibility Fabric in a programmatic fashion. These open RESTful APIs support programmability in the Visibility Fabric itself to ensure visibility that is pervasive, dynamic, active, and therefore very agile as well. We refer to this highly programmable and easy-to-automate framework as Software-Defined Visibility (SDV), a new paradigm for network security and IT operations management.

Software-Defined Visibility is to a visibility infrastructure what Software-Defined Networking (SDN) is to a network infrastructure. SDV combines the pervasive reach of visibility with an automation framework.

In an SDN infrastructure, network switches and routers form the physical network or the Layer 2-3 data plane. Virtual networks are abstracted from the underlying data plane using encapsulations such as VXLAN, MPLS, NVGRE etc. to allow multi-tenancy on a common infrastructure. The SDN controller supports the control and management planes that in turn provide control of the virtual and physical networks.

Key Use Cases

- Active Visibility for Operational Intelligence – IT Operations Management (ITOM) integration
- Threat Pattern detection and response – Send traffic to another tool or initiate on-demand packet capture
- Automatic adjustment of "monitor mode" and "traffic flows" for inline security tools
- Private cloud and virtual data center monitoring

Key Benefits

- SecOps and NetOps administrators can now augment production network KPIs and KCIs with Visibility Fabric analytics using the Gigamon Visibility App for Splunk
- Security and monitoring tools can program the GigaSECURE® Security Delivery Platform to react-and-respond to new threat or traffic patterns. For example:
  - Filter or drop streaming traffic from packet capture tools using GigaSMART® Application Session Filtering (ASF)
  - Decrypt SSL traffic if a certain threshold is crossed using GigaSMART SSL Decryption

3173-01 09/15

Gigamon®

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