

## Solution Brief

# Pervasive Visibility Platform

We live in an era where business and society are embracing lifestyles that are enhanced and enabled through access to networks at home, at work and while on the move. As a result there is a global dependency upon the communication and information that traverses these networks—from social media messages to trading transactions, from medical health records to lectures delivered by video. The challenges of operating and managing networks have fundamentally changed.

### Driving Forces Affecting Network Infrastructure

Virtualization, cloud computing, mobility, and big data are powerful forces that are not only driving opportunities to improve business, but also creating and extenuating significant challenges and opportunities in how organizations manage, analyze, and secure their networks. These include:

- Managing increased network traffic volumes
- Maintaining infrastructure security and compliance
- Addressing the proliferation of connected devices
- Embracing the consumerization of IT
- Adopting cloud-based IT

Even though the environment is evolving, the need to provide an efficient, secure and reliable network remains.

### Need for a Comprehensive Visibility Solution

Organizations are seeking to improve visibility and control of their networks through the collection and analysis of traffic without adversely impacting network performance or reliability. However, the process of capturing and analyzing network traffic is complex. It requires the extraction of the traffic, classification to determine appropriate priority of the traffic, and delivery to the relevant tool or tools that help manage, analyze, and secure the network.

### Legacy Approaches to Traffic Visibility

IT organizations have historically had access to a limited range of approaches to address traffic visibility. Legacy approaches have included: wide-spread proliferation of tools, repurposing Ethernet switches, the use of mirror ports to duplicate traffic, and the division of traffic flows via network TAPs.

However, these approaches fail to address the challenges faced by network owners—offering only limited filtering capabilities and visibility from a single switch, network segment, or TAP. In addition, these approaches are difficult and costly to scale and manage, often requiring change orders or network downtime in order to adapt to events occurring within the evolving network. Given the performance limitations, cost and complexity of legacy approaches, organizations struggle to scale and ensure the performance, reliability, and integrity of their network infrastructure.

### A New Approach to Traffic Visibility is Needed

At Gigamon we realized that delivering the visibility essential to operate, secure and maintain complex networks requires a new approach. With millions of traffic flows, thousands of events and hundreds of changes occurring within the infrastructure on a daily basis, visibility needs to be pervasive, it needs to be intelligent, and it needs to be dynamic. It needs to be able to understand the criticality and priority of traffic and recognize when specific traffic is significant to more than just one management system. It needs to be able to see across the boundary of physical and virtual and into the cloud providing the clarity needed to secure, maintain, and support both physical and virtualized services and applications.

Results of an independent survey of IT managers, conducted by the Enterprise Strategy Group highlight a variety of drivers that both identify the shortcomings of current alternatives and substantiate the need for a new approach (see Figure 1).

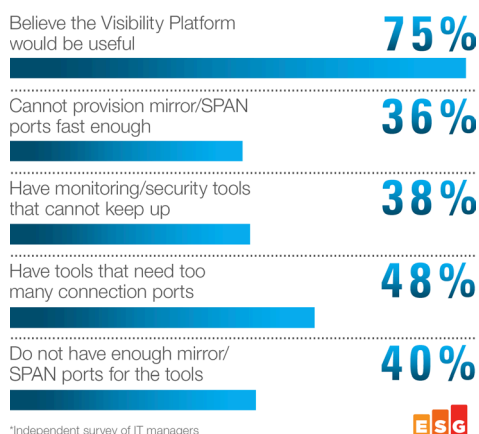


Figure 1: Enterprise Strategy Group Results

### The Gigamon Visibility Platform

The Gigamon® Visibility Platform is an innovative and complete visibility solution to bridge communication networks. For truly pervasive visibility, this must include physical, virtual and emerging SDN/NFV environments.

The Gigamon Visibility Platform is a layered architecture (see Figure 2) that includes the following tiers:

- Visibility Nodes
- Traffic Intelligence
- Orchestration
- Tools and Applications

#### Visibility Nodes Tier

Distributed nodes provide pervasive visibility across physical, virtual, and remote sites, as well as future SDN/NFV production networks. Gigamon provides the industry’s broadest portfolio of visibility nodes. These GigaVUE® visibility nodes include:

- GigaVUE H Series forms the foundation of a distributed fabric. The high-performance visibility nodes are modular and extensible for a range of scale and performance requirements from 1Gb 1RU nodes to larger 2.56Tb chassis-based solutions. The GigaVUE-HC1 node is an ideal choice for space constrained locations, smaller sites, or remote sites where native intelligence from GigaSMART® technology is required.
- The GigaVUE TA Series forms the physical edge of the visibility infrastructure. Optionally, Gigamon’s market-leading software, GigaVUE-OS may also be used on white box hardware to economically extend reach into every rack of a mega data center.

- GigaVUE-VM forms the virtual edge of the visibility infrastructure and extends visibility within virtual networks and monitors traffic between virtual machines. This will be particularly important in future cloud and NFV environments where critical components of the network infrastructure may be virtualized—maintaining accurate visibility in such a disaggregated environment is paramount.
- In addition to the GigaVUE visibility nodes, TAPs provide non-intrusive access to (physical) traffic at various network interface speeds—1Gb (Copper or Fiber), 10Gb, 40Gb (including Cisco 40Gb BiDi) and 100Gb. TAPs could be active, passive or embedded and are offered for a variety of cable types and in a variety of split ratios.

Together, the visibility nodes provide traffic aggregation, filtering, replication, and intelligent packet and flow manipulation optimized for the tools that manage, analyze and secure the network. Dynamic changes can be made easily without impacting the production network so IT organizations can be agile and responsive to threats, events or anomalies on the network.

#### Traffic Intelligence Tier

The visibility nodes offer two distinct set of services, traffic control powered by GigaVUE-OS and Traffic Intelligence powered by GigaSMART:

- Gigamon’s patented Flow Mapping® technology identifies and directs incoming traffic flows of interest to single or multiple tools based on user-defined rules implemented from a centralized management system. Flow Mapping allows multi-tenant access and segregation of monitored traffic and policies by providing advanced role-based management.

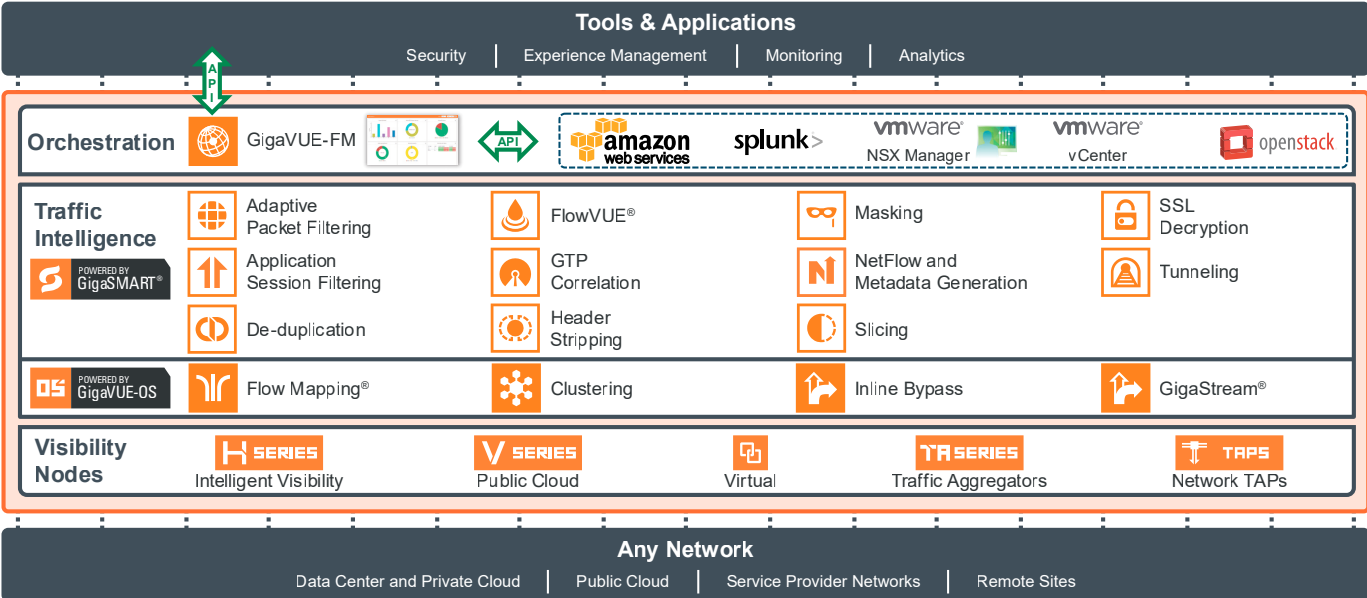


Figure 2: The Gigamon Visibility Platform

- Clustering allows multiple GigaVUE nodes to be managed as a single logical entity. Traffic can enter one node and be directed out a different node as a single “logical chassis”. An important attribute of clustering is the ability to extend GigaSMART traffic intelligence to anywhere in the cluster.
- Inline bypass bridges the performance gap between the network and critical security tools that need to be placed inline (e.g. Intrusion Protection Systems, Advanced Threat Protection security tools etc.). By applying intelligence such as application-aware bypass, traffic can be selectively distributed to such inline security tools. The bypass functions can either be logical or physical.

Traffic Intelligence is powered by GigaSMART technology. GigaSMART provides stateful and packet-level optimization and normalization functions that run as software applications on high-performance compute engines in the visibility nodes. GigaSMART applications span a variety of functions and include:

- **Packet Slicing/Masking:** Slice/mask confidential information in a packet before sending it to a monitoring tool
- **Header Stripping:** Remove extraneous headers to deliver normalized IP packets to monitoring tools—this is especially useful when adopting network virtualization or SDN
- **Adaptive Packet Filtering:** Filter across advanced encapsulation headers including VXLAN, VN-Tag, GTP, MPLS, etc., and inner (encapsulated) Layer 3/Layer 4 packet contents; useful for delivering tenant-specific traffic to monitoring tools
- **Application Session Filtering:** Builds upon Adaptive Packet Filtering by extracting entire application sessions of interest; allows filtering based on signatures or patterns that can appear across any part of the payload
- **De-duplication:** Remove duplicate instances of the same packet to avoid unnecessary traffic processing by tools
- **GTP (GPRS Tunneling Protocol) Correlation:** Correlate traffic between user and data planes in 3G and 4G/LTE mobile networks
- **SSL/TLS Decryption:** Decrypt SSL/TLS traffic to offload inline and out-of-band security tools from the processor-intensive decryption function
- **NetFlow and Metadata Generation:** Generate un-sampled NetFlow/IPFIX/metadata records along with additional context-aware extensions like URLs, HTTP Response Codes from traffic fed to the Visibility Platform; this provides a high-fidelity view of the traffic in the production network
- **FlowVUE®:** Provides subscriber-based IP sampling that enables existing tools to connect to high-speed traffic pipes by providing a representative view of traffic for diagnostic coverage and many more; in addition, this GigaSMART application also allows whitelisting of subscribers of interest to extract traffic from premium subscribers for SLA management or attachment of specific services

Other applications are also available.

### Orchestration Tier

GigaVUE-FM (Fabric Manager) provides centralized management and a common policy framework for the Visibility Platform. GigaVUE-FM delivers a single-pane-of-glass view of all the physical and virtual nodes across the Visibility Platform, while also providing an easy-to-use wizard-based approach for provisioning patented Flow Mapping and GigaSMART traffic policies.

In addition to centralized management and control, GigaVUE-FM also features end-to-end topology visualization including network auto discovery using CDP/LLDP inspection, platform-wide reporting, summarized and customizable dashboards, backup and restore functions, and enhanced monitoring capabilities to proactively monitor and troubleshoot hot spots in the Visibility Platform. GigaVUE-FM provides a set of RESTful APIs to integrate with third-party applications and tools to enable dynamic changes in the platform.

### Tools and Applications Tier

This tier interfaces with GigaVUE-FM Fabric Manager through open RESTful APIs. These APIs allow third-party development of applications integration with SDN controllers, and integration with other specialized IT applications and tools infrastructure. FabricVUE™ Traffic Analyzer, an add-on licensable application, provides centralized visualization of traffic monitored by the Visibility Platform. This application can be used as a first level dashboard to identify traffic patterns that need to be filtered for further analysis by the security and monitoring infrastructure.

The Gigamon Visibility App for Splunk uses these open RESTful APIs to extend the health and analytics of the Visibility Platform for the IT Operations Management (ITOM) user. This app augments intelligence collected from the production network to help SecOps and NetOps teams to trigger first-level troubleshooting within the ITOM realm. To enable user community adoption of the RESTful APIs, the Gigamon customer portal acts as a central hub for sample cookbooks and scripts for customers to consume and exchange ideas and use cases. GigaVUE-FM also features pre-integration with VMware vCenter APIs to track vMotion events across virtualized infrastructure. This integration allows continuous visibility without administrator intervention.

Together, this framework allows an extensible environment for visibility into infrastructure blind spots and maximizes performance of the tool infrastructure.

A pervasive visibility platform can address the security and monitoring challenges facing today's IT organizations by helping to:

- **Extend Visibility:** Bridge islands of physical, virtual, and eventually SDN/NFV worlds with end-to-end visibility for tools across enterprise, data center, cloud, and service provider infrastructure. This unified management model allows rapid visibility into infrastructure blind spots by providing a common platform for IT operations management tools such as security, APM, NPM, and others.

- **Respond Dynamically:** Grow the security and monitoring infrastructure dynamically without impacting production traffic. This architecture also provides an open environment through RESTful APIs that address react and respond scenarios to real-time events that occur within the network through automation and orchestration.
- **Improve ROI:** Control traffic to avoid oversubscription, extend the life of existing tools and ensure that the tools used to manage, analyze and secure the network receive the critical information they require to realize their full potential.
- **Reduce Costs:** Centralize tools into a Unified Tool Rail to reduce CAPEX; simplify management to reduce OPEX with a flexible policy engine that enables parallel monitoring policies to serve multiple departments simultaneously.
- **Enable Scale:** Invest in a solution that can grow to address future needs as your network grows from 1Gb to 10Gb, 40Gb, or 100Gb, and evolves from physical to virtual to SDN and NFV environments.

To find out how the Gigamon Visibility Platform can help you, visit us at: [www.gigamon.com](http://www.gigamon.com)