Whitepaper

Pervasive Visibility Platform – A New Approach to Visibility

Trends

Networks continually change and evolve. Many trends such as virtualization and cloud computing have been ongoing for some time. Although they have matured, their cycles have not completed. So they continue to evolve while newer themes such as Compute Everywhere, Software-defined Networking (SDN), and Risk-based Security take center stage. Each theme drives changes that affect the way we monitor and manage the IT infrastructure.

Compute Everywhere is a form of ubiquitous computing. Although it is driven by the personalization of wearable systems and is intended to distribute compute power wherever it is needed using sensor-based technologies, the fact remains that the majority of the information used will continue to be processed and stored in traditional IT data centers. Expanding data needs drive a significant increase in the volume of data carried across systems. Therefore, data monitoring must extend across systems as well.

The agility of virtualization in the server world has set the stage for similar evolutions in the networking arena. Software-defined Networking (SDN) and Network Functions Virtualization (NFV) are just two examples offering to abstract functions from networking hardware. Such transformational networking changes provide overall cost savings and operational simplicity. But whether the infrastructure is working properly still needs to be verified. Troubleshooting and visibility is still required, only it gets more complex and convoluted. Given the ever-changing complexity of today's infrastructure, it is important that the Visibility Fabric provides visibility into physical, virtual, and remote sites as well as emerging SDN/NFV infrastructure as a single unified fabric with a common management and policy model, rather than as a set of disjointed nodes. Such a unified management model allows rapid visibility into infrastructure blind spots.

Security is another trend that is not going away. Risk-based security allows organizations to apply risk management to the over-arching security concerns faced on a daily basis. The existing trend of using multiple simultaneous security products will continue, but the priorities will change based on the largest risk factors. The key to determining risk factors is robust data analytics, once again requiring visibility into both existing and new information.

Traditional Approach to Network, Security, and Application Performance Monitoring

Traditional approaches to network, application, and security management are breaking down in the face of these changes. With the growing volume of data and the increased mobility of users, devices, and applications, tools are having a harder time providing accurate and timely analysis. This is because tools in the past would directly attach into the production network through TAPs or through mirror/SPAN ports. This leads to several challenges:

- As networks grow, the number and types of network analysis tools also grow. Networks are evolving to encompass islands of topologies, for example remote/branch offices, private/public cloud, and more recently, SDN. The approach of dropping tools directly into these networks significantly increases the number of tools and the cost of the monitoring/management infrastructure as well.
- As network speeds/links are upgraded, for example moving from 1Gb to 10Gb or 10Gb to 40Gb, tools that are directly connected into the network through TAP or SPAN ports are challenged as the tool interfaces do not necessarily keep up with network upgrade cycles. IT departments are now forced down a path of "rip and replace" for their monitoring infrastructure in order to connect tools to the higher speed links, even though they do not need to see all 10Gb or 40Gb of the traffic.
- As the volume of traffic in the network grows, tools directly connected through TAPs or mirror/SPAN ports see growing volumes of traffic on that link, thereby forcing the tools to process increasingly large volumes of data. At some point the tools reach the limit of their processing capability, forcing traffic/data to be dropped and diluting the veracity of their analysis.
- As departments within IT organizations are being held to internal SLAs, these departments are now all contending for control of the TAPs or SPAN ports to connect their tools into. Given the limited number of TAPs or SPAN ports in any given segment of the network, this leads to contention across departments for access to those TAPs or SPAN ports.

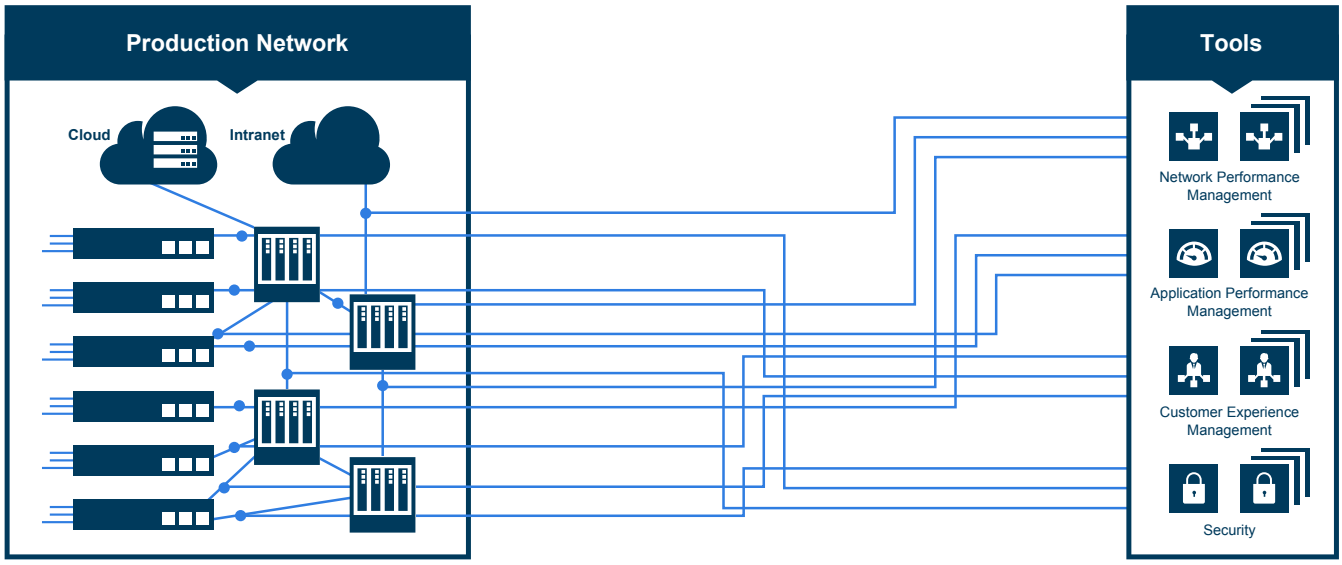

Figure 1: An example of a network with tool proliferation

The Visibility Platform

Gigamon has pioneered the Visibility Platform. This platform sits between the production network and monitoring or management tools. It acts as a pervasive, centralized fabric that delivers relevant data from various networks under an administrative domain (including any campus networks, branch/remote office networks, private cloud, or SDN islands that an enterprise or service provider may have) to a centralized set of tools that are connected to the Visibility Platform.

In the process of delivering data from the production network to the tools, the Visibility Platform fulfills a variety of functions, such as filtering and replication, to ensure that only relevant data gets delivered. Traffic delivered to each tool is individually tuned within the fabric, independent of the traffic profile of other tools, in order to optimize the functioning of each tool. In other words, non-relevant traffic can be filtered out from the set of traffic delivered to that tool without affecting the traffic delivered to other tools. This can be done independently for each tool. The Visibility Platform takes care of replicating, filtering, and forwarding traffic based on each individual tool's traffic profile.

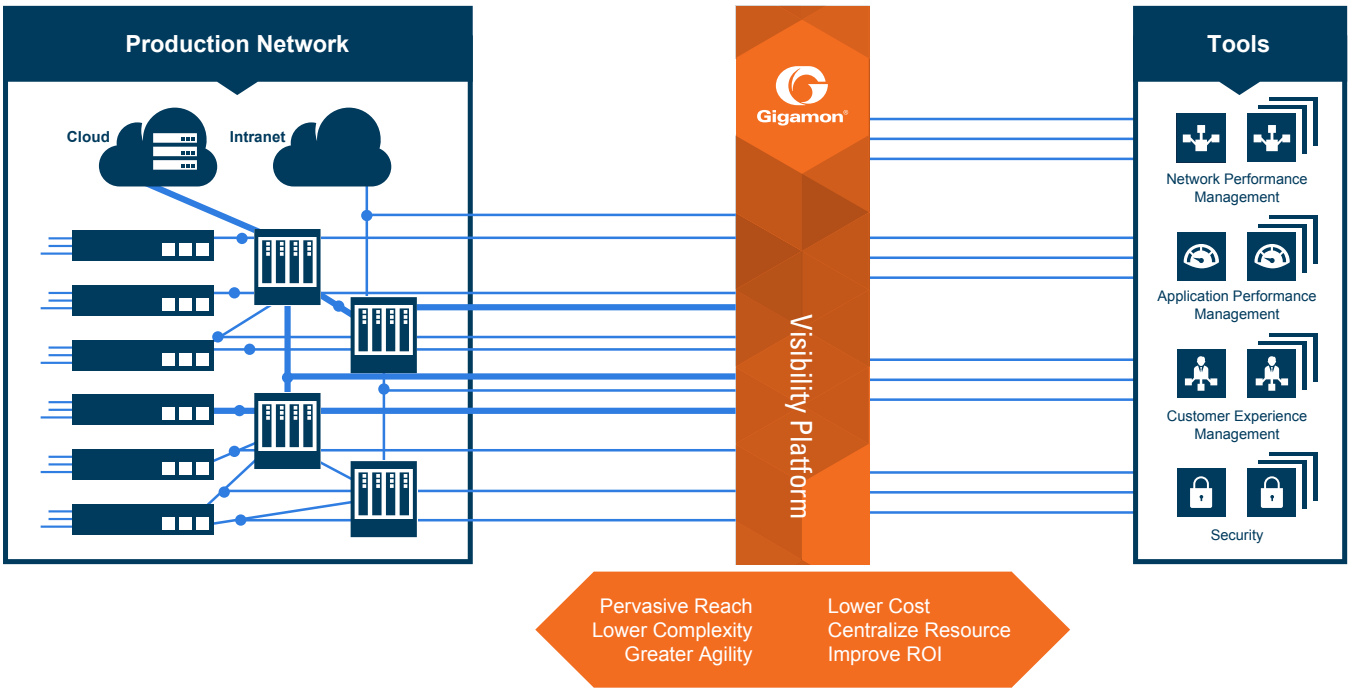

Figure 2: A simplified example of a network with the Gigamon Visibility Platform deployed

In addition to filtering, aggregation, and replication, the Visibility Platform adds traffic intelligent to make the tools more efficient and keep traffic flowing. Examples of intelligence would include de-duplication capabilities to minimize traffic processing, header stripping to deliver normalized traffic for analysis, or NetFlow and metadata generation to offload this function from the network itself.

Gigamon Visibility Platform

Visibility is key to any type of security, monitoring, or analysis solution. Advanced networks can be quite complex, so achieving pervasive visibility into network traffic requires a basic structure or architecture to meet the needs of modern data centers. The Gigamon Visibility Platform is based upon a flexible, yet robust model that scales to meet any need of even the most demanding IT infrastructures. The Gigamon Visibility Platform consists of the following four tiers:

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

Visibility Nodes Tier

At the base layer are a distributed set of nodes that provide pervasive visibility across physical, virtual and even future SDN/NFV production networks. These nodes form the foundation for the fabric and can be located in both data centers as well as remote locations. Components include basic TAP infrastructures as well as high-performance GigaVUE® fabric nodes to combine traffic flow processing with extended intelligent capabilities. GigaVUE nodes in this tier are available in a variety of form factors:

- The GigaVUE TA Series forms the physical edge of the visibility infrastructure, providing aggregation of traffic prior to processing by other nodes
- Optionally, GigaVUE-OS, Gigamon's market-leading software, may 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, extending visibility within virtual networks and monitoring traffic between virtual machines. This will be particularly important for NFV environments in the future where critical components of the network infrastructure will get virtualized and maintaining accurate visibility into disaggregated environments is paramount
- The GigaVUE H Series provide high-performance capabilities combined with GigaSMART® technology to meet the needs of wide-ranging performance and port densities. The GigaVUE H Series includes configurations from the 1RU GigaVUE-HC1, designed for smaller or remote sites, to the high-end 14RU GigaVUE-HD8 chassis with throughput capabilities up to 2.56Tb

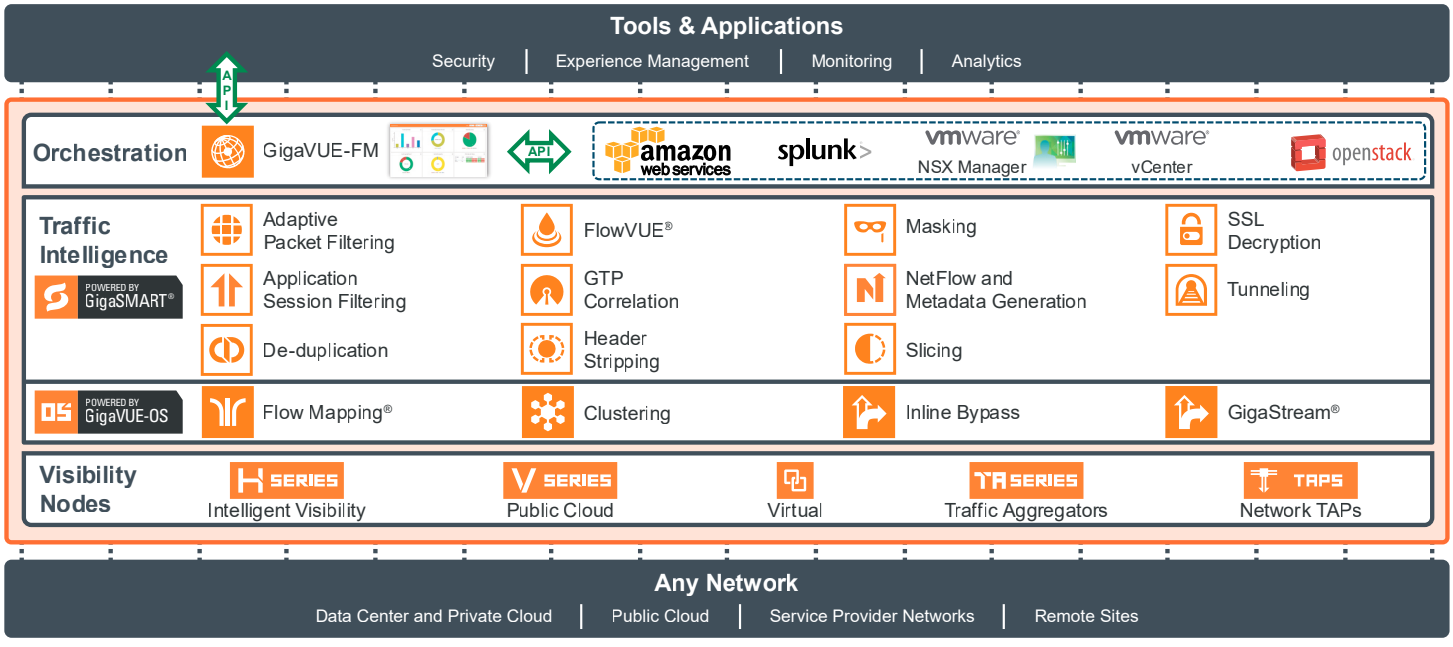

Figure 3: The Gigamon Visibility Platform

Traffic Intelligence Tier

The physical and virtual nodes in the Visibility Platform nodes tier only exist to perform certain visibility services. So the second tier of the model is services based. These fall into two categories: basic platform services and traffic intelligence.

- Basic fabric services are powered by the GigaVUE-OS. Gigamon's patented Flow Mapping® technology directs incoming traffic flows of interest to one or multiple tools, based on user-defined rules implemented from a centralized management system. Gigamon's patented Flow Mapping technology allows multi-tenant access and segregation of monitored traffic and policies through advanced role-based management. Clustering is also available, bringing multiple nodes together to work as a single system by using processing capabilities across the node. Finally, inline bypass protects traffic for inline tools (such as Intrusion Protection Systems [IPS]). If traffic begins to show signs of impact, physical or logical bypass can properly divert the traffic to keep it flowing smoothly.
- Traffic intelligence is powered by GigaSMART technology. GigaSMART provides both 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 more than a dozen different functions including:
  - **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.

Orchestration Tier

As a visibility platform grows, it is important to have a unified, end-to-end management infrastructure. GigaVUE-FM (Fabric Manager) provides centralized provisioning and control across the Visibility Platform. Single-pane-of-glass views depict both physical and virtual deployments using an easy-to-use wizard to configure 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, fabric-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. The GigaVUE-FM provides a set of RESTful APIs to integrate with third-party applications and tools to enable dynamic changes in the Visibility 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 fabric-centric visualization of traffic monitored by the Visibility Platform. This application can be used as 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 Fabric 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.

Benefits of the Visibility Platform Approach

The Visibility Platform fundamentally changes the way traffic is delivered to tools. By consolidating and connecting tools into the Visibility Platform instead of connecting them directly into the production network, several benefits are realized:

- **Less disruption to the production network**—The Visibility Platform enables a "wire once" model where the Visibility Platform is set up once to TAP or SPAN at various relevant points from the production network. Any tools that need to be enabled can be conveniently added to the Visibility Platform with no disruption to the production network. Traffic patterns to the tools can be changed and tools can be upgraded, taken down, or modified without any impact to the production network.
- **Better tool accuracy and utilization**—By delivering only relevant data as well as reducing the amount of processing through offload operations performed in the Visibility Platform, tools are better able to keep up with traffic flow and with fewer packet drops. This leads to more accurate analysis as well as better utilization of the tools.
- **Lower TCO (and therefore better ROI)**—By centralizing the tools and delivering only relevant data, the number of tools and probes deployed can be significantly reduced. Furthermore, as the network infrastructure is upgraded, the monitoring and tool infrastructure no longer has to go through a "rip and replace" cycle. The tools continue to connect into the Visibility Platform and the platform can be tuned to manage the data streams to the tools. Finally, as the Visibility Platform optimizes data stream delivery, the load on the tools is reduced, resulting in more efficient utilization, extending their longevity as well as reducing their total number. All of these factors as a whole reduce the total cost of ownership for the monitoring and management infrastructure.

Summary

The Visibility Platform provides a new and complete approach to the monitoring and management of IT infrastructure. By centralizing tools and connecting them into the Visibility Platform, significant cost savings and operational efficiencies can be realized. The Gigamon Visibility Platform provides pervasive visibility across campus, branch, virtualized and, ultimately, SDN islands. It consists of four key tiers—Visibility Nodes, Traffic Intelligence, Orchestration, and Tools and Applications, which combined provide a scalable, flexible, and centralized Visibility Platform solution.

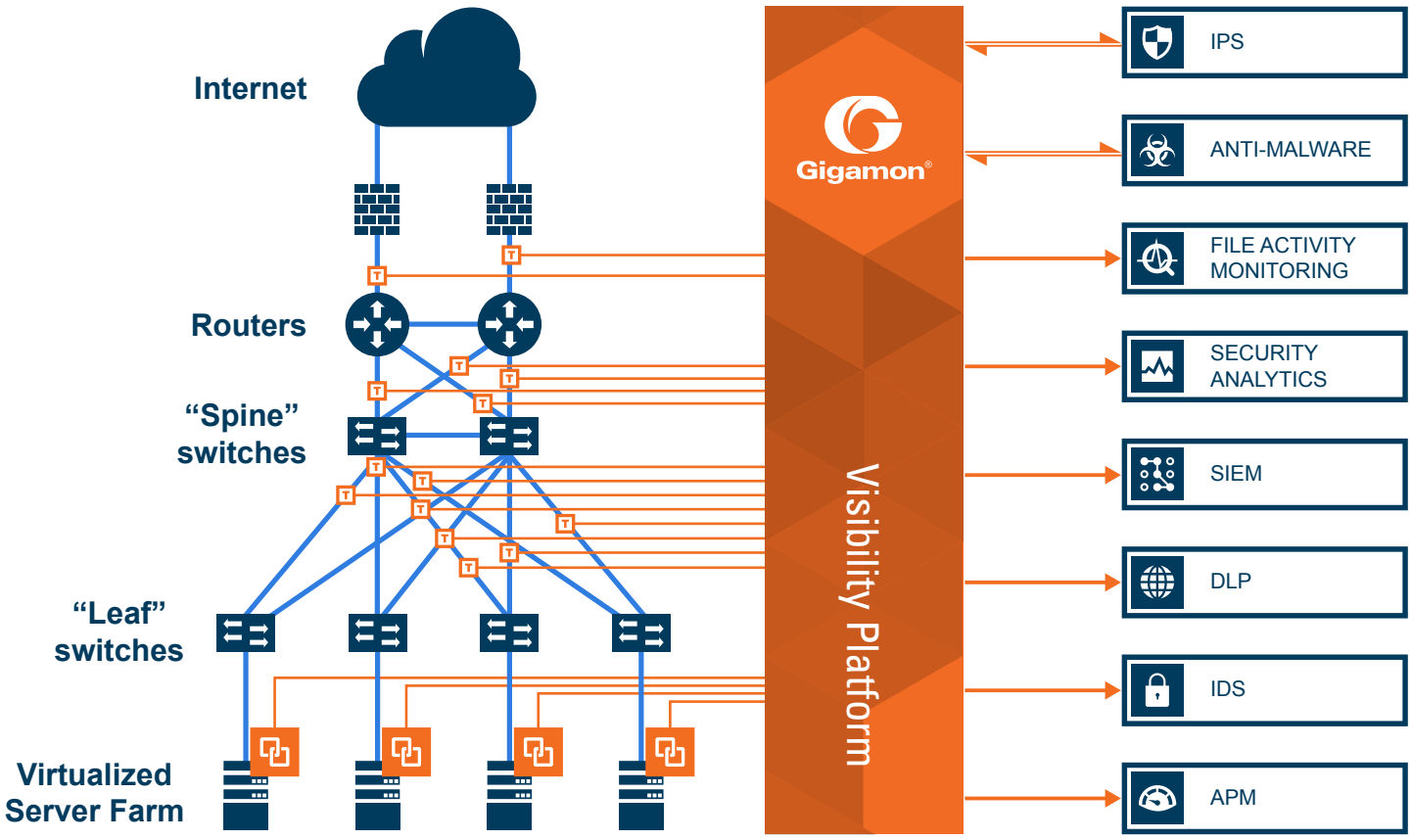

Figure 4: A Visibility Platform deployment in a modern data center deployment

Using the Visibility Platform model, Gigamon solutions span across complex infrastructures providing pervasive visibility. The example shown in Figure 4 includes newer leaf/spine deployments with both virtual and physical traffic links.

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Platform™ and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network, and application performance management solutions in enterprise, government, and service provider networks operate more efficiently. As data volumes and network speeds grow and threats become more sophisticated, tools are increasingly overburdened. One hundred percent visibility is imperative. Gigamon is installed in more than three-quarters of the Fortune 100, more than half of the Fortune 500, and seven of the 10 largest service providers. For more information visit **www.gigamon.com**

3072-13 03/17

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