GigaVUE Cloud Suite for AZURE

Network Visibility into Public Cloud

Organizations are migrating to public cloud Infrastructure-as-a Service (IaaS) to take advantage of scale, elasticity and availability.

IaaS cloud providers operate under a Shared Responsibility model — the cloud provider is responsible for security of the cloud infrastructure, whereas the customer is responsible for their data, applications, access and identity management.

GigaVUE Cloud Suite resides in the Azure VNets and aggregates flows from all compute sites, including from Azure virtual TAPs. This suite provides advanced network traffic processing and optimally distributes traffic to the appropriate network monitoring and security tools. This helps ensure effective and comprehensive cloud security.

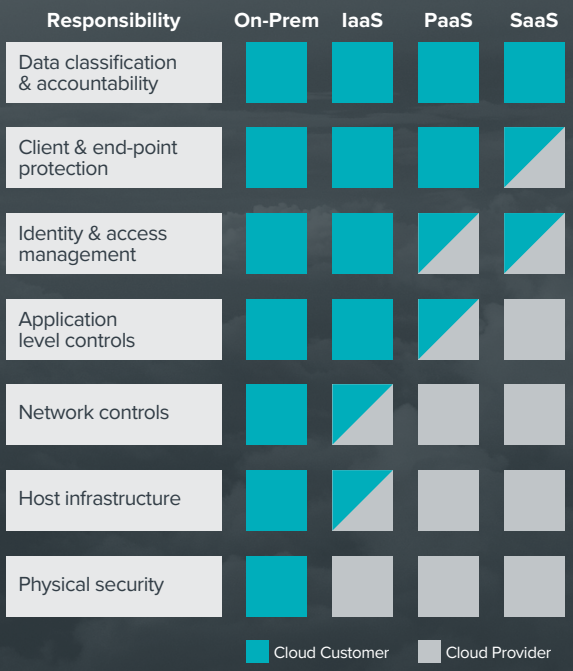

Figure 1: Microsoft's shared responsibilities model for different cloud services

KEY FEATURES

- GigaSMART intelligence – slice, sample and mask packets, header decapsulation and NetFlow/IPFIX generation
- Traffic acquisition with Azure virtual TAPs or with GigaVUE vTAPs with IPsec and pre-filtering
- Publish REST APIs: integrate with third-party systems to dynamically orchestrate new traffic policies
- Centralized orchestration and management with a single pane of glass GUI using GigaVUE-FM

KEY BENEFITS

- Delivery of optimized traffic to the proper security and networking monitoring tools
- 100 percent visibility into your Azure infrastructure
- Reduction in application downtime: there is no need to redesign applications when adding new tools
- Discovery of new workloads, proper traffic direction and adjustment of the visibility tier, all without manual intervention

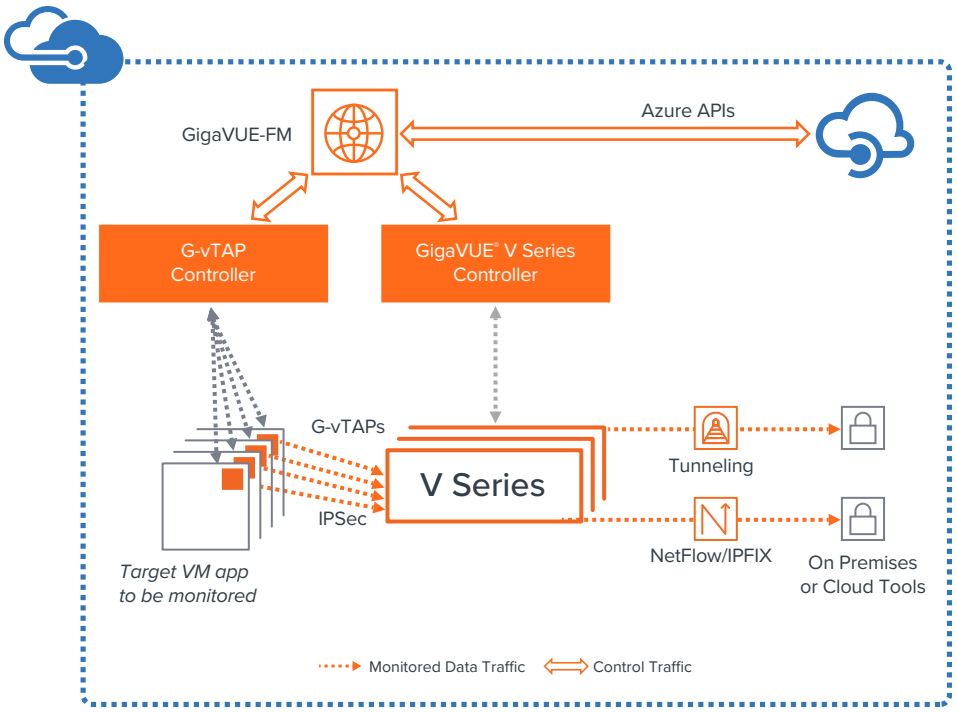

Figure 2: GigaVUE Cloud Suite for Azure

Key Considerations for IT, Cloud and Security Architects

While Azure ensures protection from the physical data center up to the hypervisor, security and compliance of data and applications rests on IT teams, who must ensure that workloads are deployed securely and perform as required. To automatically and proactively identify and remediate security and performance limitations, accurate visibility into the Azure environment is imperative.

IT, cloud and security architects are responsible for addressing the following questions before they can successfully deploy applications in a public cloud, like Azure.

- As part of the shared responsibility model, how do I assure that Azure is being used securely by everyone in the enterprise?
- How do I run more applications on Azure while meeting the needs for applying compliance and security controls?
- If zero-day security vulnerabilities are exploited in software that is yet to be patched, what mechanisms do I have in place to detect them?
- How do I detect and respond to security or network anomalies while deploying applications on Azure?
- Are there efficient ways to consolidate network traffic flows to security and monitoring tools? Are there effective methods to reduce the cost of backhauling traffic when the tools monitoring traffic in the cloud are on-premises vs. part of a tool tier is in the cloud?

Not addressing these considerations slows down the migration of applications to the cloud, and leaves the organization vulnerable to potential security breaches, with potential impact to reputation and brand.

THE SOLUTION

Gigamon CloudVUE Cloud Suite for Azure delivers intelligent network traffic visibility for workloads running in Azure and enables increased security, operational efficiency and scale across VNets. Organizations can optimize costs with up to 100 percent visibility for security without increasing load on compute instances as more security tools are deployed.

Figure 3: Centralized management, automation and straightforward process with Azure and Gigamon Fabric Manager

GigaVUE G-vTAPs

For traffic acquisition, light weight G-vTAPs are deployed within compute instances that mirror traffic to the V Series. Key benefits include:

- Single, lightweight instance minimizes impact on compute nodes
- Reduction in application downtime — there is no need to redesign applications when adding new tools
- Agent filters traffic of interest prior to sending it via IPSec to the GigaVUE V Series to reduce application and data egress costs

GigaVUE V Series Nodes

Traffic aggregation, intelligence and distribution occurs within the GigaVUE V Series nodes, which are deployed within the visibility tier (see figure 2). Key benefits include:

- Automatic Target Selection (ATS): Automatically extract traffic from any workload with an agent deployed without explicitly specifying VNets
- Flow Mapping®: Selection of L2-4 traffic
- NetFlow/IPFIX generation: Create flow records from network traffic to determine IP source and destination
- Header Transformation: Modify header content (L2-L4) to ensure security and segregation of sensitive information
- GigaSMART intelligence: Slice, sample and mask packets to optimize traffic sent to tools, reducing tool overload
- Fully interoperable with native Azure virtual TAPs

GigaVUE-Fabric Manager (FM)

Centralized orchestration and management are done by GigaVUE-FM. This single pane of glass creates policies for workloads within Azure. Key benefits include:

- Detect compute node changes in a VNet and automatically adjust the visibility tier, through pre-built integration with Azure APIs
- Publish REST APIs: Integrate with third-party systems and tools to dynamically adjust traffic received or to orchestrate new traffic policies
- Auto-discover and visualize end-to-end network topology, including VNet workloads by using an intuitive drag-and-drop user interface
- Eliminate manual processes and errors by automatically identifying each new workload and their associated traffic mirroring via ATS, and then configuring the traffic mirroring to direct traffic to the V Series Nodes

Conclusion

Whether your organization is already using Azure or considering a future migration, GigaVUE Cloud Suite for Azure provides intelligent network traffic visibility for workloads running in the cloud. Integration with Azure APIs automatically deploys a visibility tier in all VNets, collects aggregated traffic and applies advanced intelligence prior to sending selected traffic to existing security tools. With GigaVUE, organizations can obtain consistent insight into their infrastructure across Azure and their on-premises environment.

For more information on GigaVUE Cloud Suite for Azure, please read the data sheet. Learn more at www.gigamon.com/azure.

Gigamon®

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

02.20_02