Public Cloud Network-Traffic Visibility

GigaVUE Cloud Suite for Microsoft Azure Is an Intelligent Network Traffic Visibility Fabric that Acquires, Optimizes and Distributes Selected Traffic to Security and Monitoring Tools

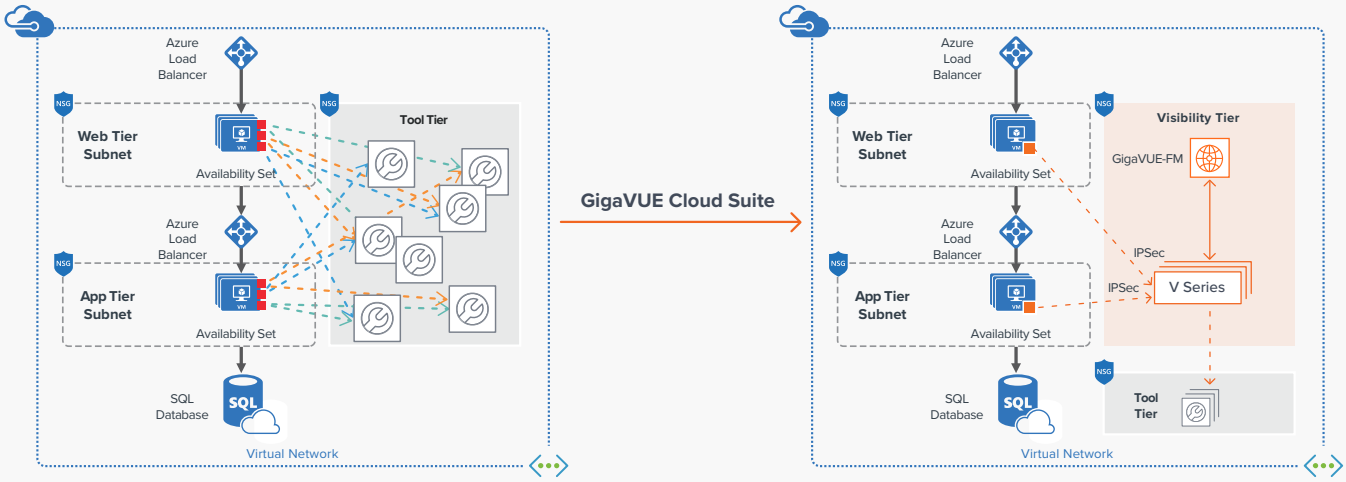

Figure 1. This cloud-native suite is fully integrated and certified within Azure environments. The solution dramatically simplifies and accelerates traffic acquisition and tool deployment.

Key Features and Benefits

- GigaSMART® modules, including packet slicing, masking, decapsulation and NetFlow generation, offload tools from processor-intensive tasks
- Flexible packet acquisition through either agentless Azure VNet virtual network TAPs, or GigaVUE® vTAPs that add IPsec security and pre-filtering
- Automatic Target Selection® and Flow Mapping™ to extract traffic of interest anywhere in the infrastructure being monitored
- GigaVUE-FM for centralized orchestration and management of on-prem or cloud traffic with a single-pane-of-glass interface
- 100 percent visibility into the entire Azure infrastructure
- Auto discovery of new workloads and appropriate routing of that new traffic to augment Gigamon V Series visibility – without any manual action
- Traffic steering, service-chain and load-balancing techniques to simplify traffic distribution among multiple tools and ensure availability
- Comprehensive visibility fabric to acquire and aggregate all traffic and optimally distribute to cloud-based network monitoring and security tools

Initiating new workloads, or migrating existing ones, into the public cloud introduces new challenges. Organizations must manage, secure and understand all the data now traversing this environment to support the needs of security detection and response and application and network performance. Traditionally IT had to install one agent per tool on every compute node and direct that traffic to the tool. This quickly overloaded compute instances, increased bandwidth and forced an architecture redesign when adding new tools.

A better method is to deploy GigaVUE Cloud Suite for Azure. Using GigaVUE Cloud Suite for Azure, security architects can ensure an effective security posture in the cloud, thereby accelerating the onboarding of new Azure applications. NetOps teams can also leverage this solution to troubleshoot degraded user experience, ensure network performance and meet SLAs.

GigaVUE Cloud Suite for Azure, as shown in Figure 2, acquires traffic in two ways: Either via Azure VNet virtual network TAPs or via a lightweight Gigamon G-vTAP agent installed within the VMs housing Azure compute instances. The Gigamon Visibility and Analytics Fabric integrates with Azure compute APIs to discover the cloud infrastructure, deploy visibility nodes in VNets that collect all the aggregated traffic and apply advanced traffic intelligence prior to sending selected traffic to security and monitoring tools. This integrated solution enables this suite to automatically remain in sync. With this solution, you can take advantage of:

- Increased security: Centralized visibility for security monitoring of all Azure VNets in an enterprise. Security operations and incident response teams can use network visibility to rapidly detect and respond to threats, vulnerabilities and compliance violations across the enterprise.
- Reduced data costs: Up to 100 percent traffic visibility without increasing load on compute instances, even as new security tools are deployed. Acquire traffic once from compute instances, and then leverage traffic intelligence to optimize data to any number of tools. Specifically, with NetFlow you can reduce data to tools by up to 99 percent.
- Operational efficiency: One common platform for visibility across the entire IT environment; consistent insight into Azure and on-premises infrastructure.
  Acquire network traffic with minimal impact to Azure compute utilization and apply traffic intelligence before distributing to multiple tools for analysis.
- Operational agility:
  – Rapidly detect changes in Azure VNets being monitored.
  – Automatic Target Selection: Automatically extract network traffic of interest anywhere in the infrastructure being monitored, without having to specify the target compute instances to monitor.
  – Ability to automate and orchestrate traffic visibility using open REST APIs.

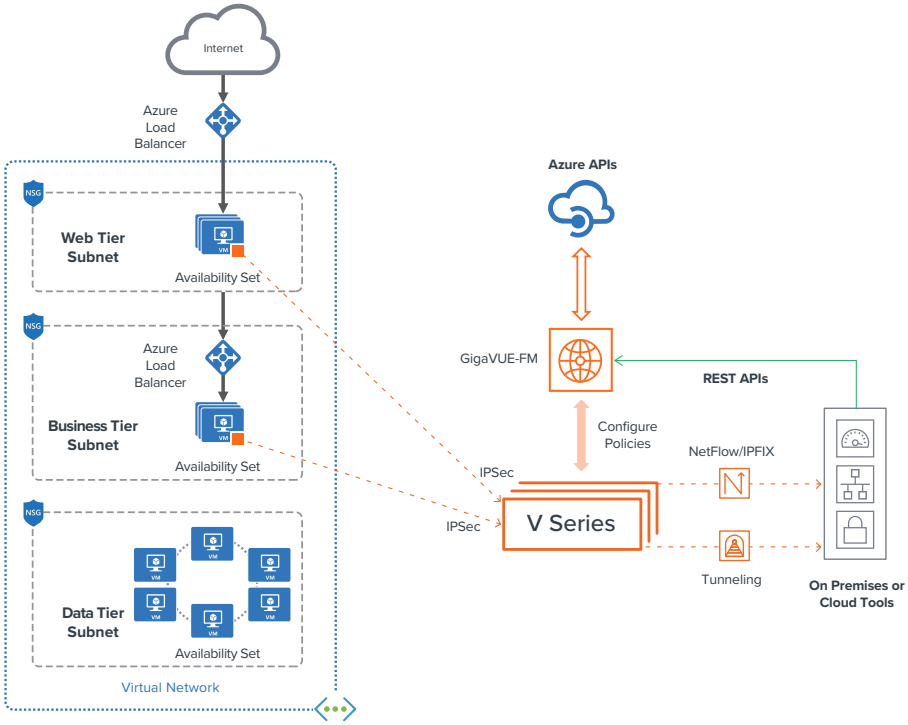

Figure 2. GigaVUE Cloud Suite for Azure supports multiple VNets and has tight integration with Azure cloud management tools to enable automation. Either Azure's agentless native VNet virtual network TAPs or Gigamon GigaVUE lightweight G-vTAPs can collect all traffic streams.

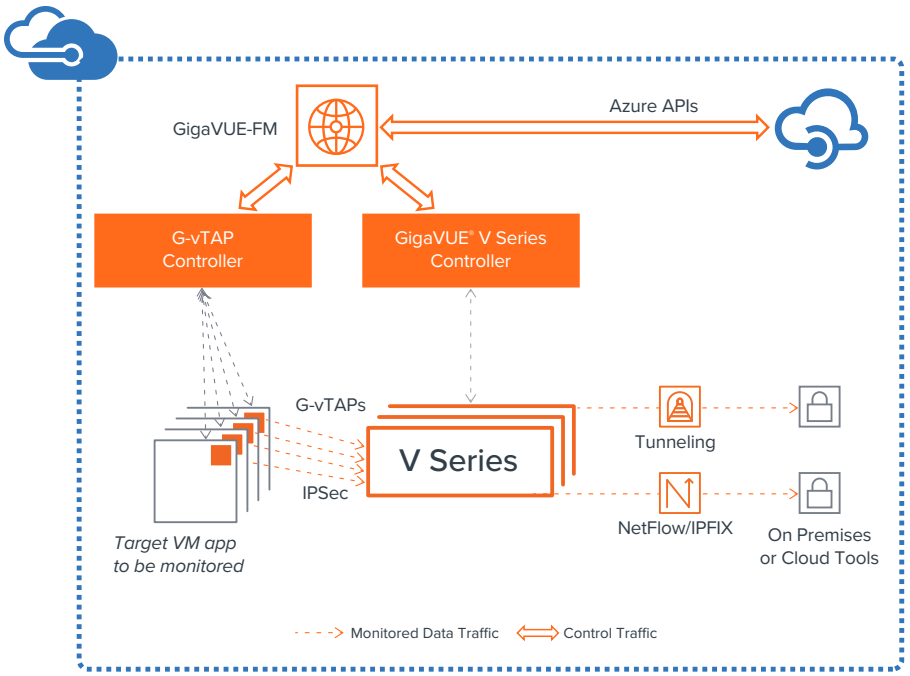

Figure 3. GigaVUE Cloud Suite for Azure is composed of four components: G-vTAP, V Series, Fabric Manager (FM) and Controllers

GigaVUE Cloud Suite for Azure

The suite comprises multiple elements that enable traffic acquisition, aggregation, intelligence and distribution, along with centralized single-pane-of-glass orchestration and management.

G-vTAP Agent – Lightweight agent deployed in an Azure compute instance to mirror production traffic and send this traffic via IPSec to GigaVUE V Series nodes. Black- or white-listed IP addresses can be optionally pre-filtered out. These agents support a high 'fan-out' to send traffic to up to 25 V Series.

GigaVUE V Series – Visibility nodes in Azure aggregate and select traffic of interest, then optimize and distribute acquired traffic to multiple tools located in any VNet.

GigaVUE-FM – Provides centralized orchestration and management across the entire enterprise including on-premise, Azure and private clouds (OpenStack, VMware and Nutanix). The traffic policies are configured using a simple drag-and-drop user interface.

G-vTAP Controller and GigaVUE V Series Controller – For hybrid and multi-VNet deployments GigaVUE uses a controller-based design to proxy the command-and-control APIs while preserving existing IP addressing schemes or Network Address Translation (NAT). G-vTAP Controller proxies commands from GigaVUE-FM to the G-vTAPs. GigaVUE V Series Controller is used to proxy commands from GigaVUE-FM to the GigaVUE V Series nodes. See figure 3.

Key Features and Benefits

G-vTAP Agent

Lightweight agent deployed on compute nodes. Mirrors traffic and sends via IPSec to GigaVUE V Series.

Minimize Agent Overload

Requires just one agent per Azure compute instance vs. needing to deploy one per security tool. This approach lowers impact on CPU utilization.

Reduce Application Downtime

Avoid the need to redesign infrastructure to add new tool agents as applications scale out in Azure or as more operational tools are added.

Scale What's Being Monitored

As compute instances scale out due to demand, the agent automatically scales appropriately. This is achieved with the integration between GigaVUE-FM, Azure compute APIs and Azure cloud management.

Minimize Production Changes

Option to use either the production network interfaces or a separate NIC to mirror the workload traffic. The separate ENI option allows IT to preserve application traffic policies.

Reduce Costs

Pass or drop rules to filter traffic of interest prior to sending it to the GigaVUE V Series. This reduces application and data egress costs.

GigaVUE V Series

Visibility nodes that aggregate, select, optimize and distribute traffic.

Traffic Aggregation

Acquire and aggregate traffic from multiple VMs. The traffic is acquired from the VMs using IPSec and via GRE or VXLAN tunnels and support pre-filtering. Alternatively, traffic may be acquired from Azure VPS virtual network TAPs.

Traffic Intelligence: Select, Optimize and Distribute

- Flow Mapping®: Select Layer 2–4 traffic of interest with a variety of policies and forward to specific tools. Criteria can include IP addresses/subnets, TCP/UDP ports, protocols and instance tags. Advanced policies using overlapping rules and nested conditions can be specified.
- GigaSMART NetFlow and IPFIX generation: Generate flow records from any type of network traffic to determine IP source and destination of traffic, class of service and causes of congestion.
- Header Transformation: Modify key content in the packet header to ensure security and segregation of sensitive information. This capability also enables support for overlapping subnets and protecting privacy of sensitive information in regulated environments.
- Other GigaSMART traffic intelligence functions: Optimize selected traffic by applying GigaSMART traffic intelligence to slice, sample and mask packets to reduce tool overload or maintain compliance.
- Distribute optimized traffic to multiple tools anywhere.

Service Chaining

Service chain multiple traffic intelligence operations dynamically, based on tool needs.

Elastic Scale and Performance

- Automatic Target Selection: Automatically extract traffic of interest anywhere in the infrastructure being monitored.
- Automatically scale based on varying number of computes without lowering the performance of the visibility node.

GigaVUE-FM Centralized management and orchestration.	Centralized Orchestration and Management • Centralized orchestration and single-pane-of-glass visualization across the entire infrastructure — public, private and hybrid • Traffic policies are defined using a simple drag-and-drop user interface • Software defined networking constructs to configure traffic policies Automation • Tight integration with Azure APIs detects compute changes in the Azure VNet and automatically adjusts the visibility tier • Open REST APIs published by GigaVUE-FM can be consumed by tools to dynamically adjust traffic received or to orchestrate new traffic policies Topology View Auto-discovery and end-to-end topology visualization of visibility tier and compute instances.

Minimum Requirements for GigaVUE Cloud Suite for Azure

Table 1: Recommended minimum compute specifications

SOLUTION COMPONENT	MINIMUM VM TYPE	DESCRIPTION
G-vTAP Agent	Standard_B1ms	• Linux: Available as an RPM or Debian package. • Windows: Available for Windows Server 2008/2012/2016
G-vTAP Controller	Standard_B1ms	Command-and-control component for the G-vTAP agents
GigaVUE V Series Node	Standard_D2s_v3	• NIC 1: Data IP (mirrored traffic from G-vTAP) • NIC 2: Tunnel IP (traffic to tools or on prem GigaVUE H/W) • NIC 2: Management IP (commands from the controller)
GigaVUE V Series Controller	Standard_B1ms	Command-and-control component for the V Series Nodes
GigaVUE-FM	Standard_D4s_v3	• GigaVUE-FM needs to be able to access both the controller instances for relaying the commands • GigaVUE-FM automatically spins up additional V Series nodes based on a pre-defined configuration in the user interface • For on-premises GigaVUE-FM requirements and ordering information, please refer to the GigaVUE-FM data sheet

Based on the number of virtual TAP points, GigaVUE Series nodes will be auto-launched by GigaVUE-FM.

Ordering Information, Renewals

GigaVUE Cloud Suite for Azure, with all the solution components, can be consumed using the following options:

- Bring Your Own License (BYOL) — GigaVUE Cloud Suit for Azure can be purchased as a subscription from Azure Marketplace and Azure GovCloud U.S. Table 2 lists the SKUs for procurement.

Table 2: Part numbers for the solution

PART NUMBER	DESCRIPTION
GFM-AZU-100	Monthly term license for traffic visibility up to 100 virtual TAP points in Azure. Minimum term is 12 months and includes Elite support.
GFM-AZU-1000	Monthly term license for traffic visibility up to 100 virtual TAP points in Azure. Minimum term is 12 months and includes Elite support.

- Azure Marketplace Metered — GigaVUE Cloud Suite for Azure can be purchased as a subscription from the Azure Marketplace for 100 virtual TAP points on an hourly basis. In this option, Azure meters and charges the usage of the solution. Customers can register with Gigamon to obtain 24x7 Elite Support for no additional charge.

Notes

- Virtual TAP pointt: Any end point from which traffic can be mirrored using the G-vTAP agent such as a NIC in an VM. A single VM could have multiple NICs that can be tapped. For example, if an application uses ten VMs with two NICs each, then the total virtual TAP points are 20.
- Try-and-buy: Launch the BYOL offering in Azure Marketplace for a ten G-vTAP agent, 30-day trial of our solution. Refer to the ordering section to purchase additional term-based subscriptions.
- Licensing: Licenses are activated from GigaVUE-FM.
- Renewal: For BYOL model, GigaVUE-FM notifies the customer of term license expiration with advance notice of 30 days. Contact Gigamon for renewals.
- For a limited time immediately following introduction, Gigamon may offer GigaSMART NetFlow and IPFIX generation functionality with the purchase of GFM-Azure-100 or GFM-Azure-1000 at no additional charge.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding our Limited Warranty and Product Support and Software Maintenance Programs, visit www.gigamon.com/support-and-services/overview-and-benefits.

Microsoft Azure Certified

Learn More

For more information on GigaVUE Cloud Suite for Azure, visit this website. Read the solution brief and requesting a demo.

Gigamon®

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