Public Cloud Network-Traffic Visibility

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

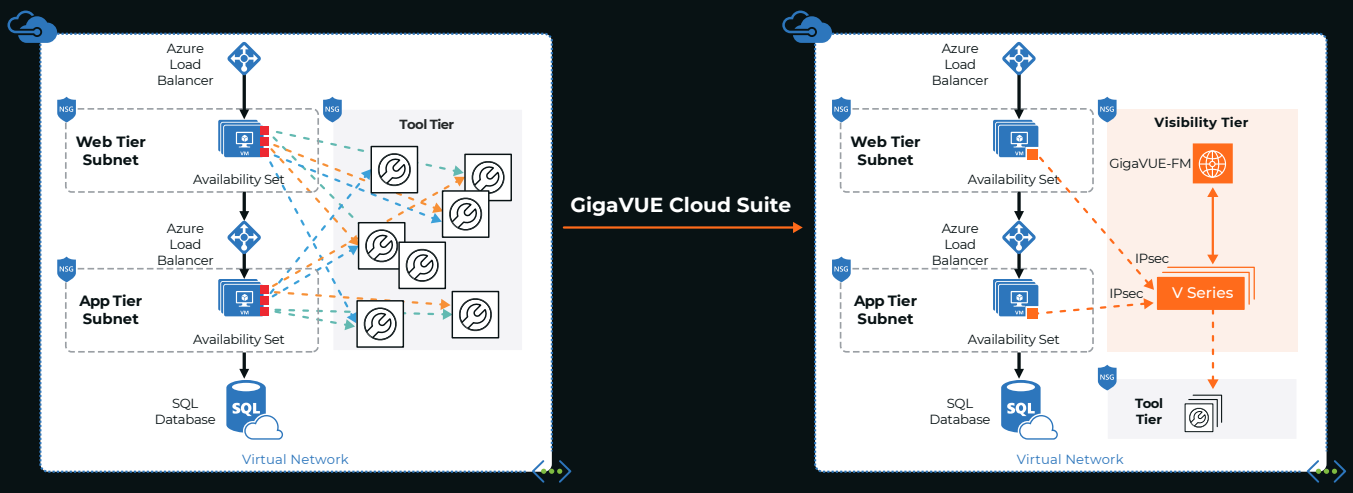

Figure 1. This cloud-native suite is fully integrated, application aware, and certified within Azure environments. The solution dramatically simplifies and accelerates traffic acquisition and tool deployment.

Key Features and Benefits

- GigaSMART® modules, including Application Intelligence, Packet Slicing, Masking, and Decapsulation offload tools from processor-intensive tasks
- Flexible packet acquisition through GigaVUE® vTAPs that add IPsec security and pre-filtering or tunnel-as-a-source methods
- 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-premises or cloud traffic with a single-pane-of-glass interface
- Simplified and automated deployment of a dynamic visibility fabric through tight integration with Azure Network Watcher, Ansible, and third-party orchestration tools such as Terraform
- Comprehensive visibility into the entire Azure infrastructure, the workloads present, and all VMs of interest
- Identify over 3,500 applications present, selectively filter as appropriate, and generate 5,000 metadata attributes to provide contextual insights
- Dynamic 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 tool 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
- High-performance GigaSMART processing with V Series nodes that scale as needed

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, including visualizing and filtering applications, to support the needs of security detection and response as well as workload and network performance. They also need not just NetFlow metadata but application-aware attributes to further understand how the network and apps are behaving. Traditionally IT had to install one agent per tool on every compute node and direct that traffic to the tool to gain full workload VM visibility into East-West traffic. This quickly overloaded compute instances, increased bandwidth, and forced an architecture redesign when adding new tools. Cloud deployments have been blind to apps running on the network and metadata generation has been nearly impossible.

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 and advanced Layer 4 through Layer 7 metadata 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 a lightweight Gigamon G-vTAP agent installed within the VMs housing Azure compute instances or through tunnel-as-a-source. 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, including application and session filtering. Then it applies load-balancing algorithms and sends 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

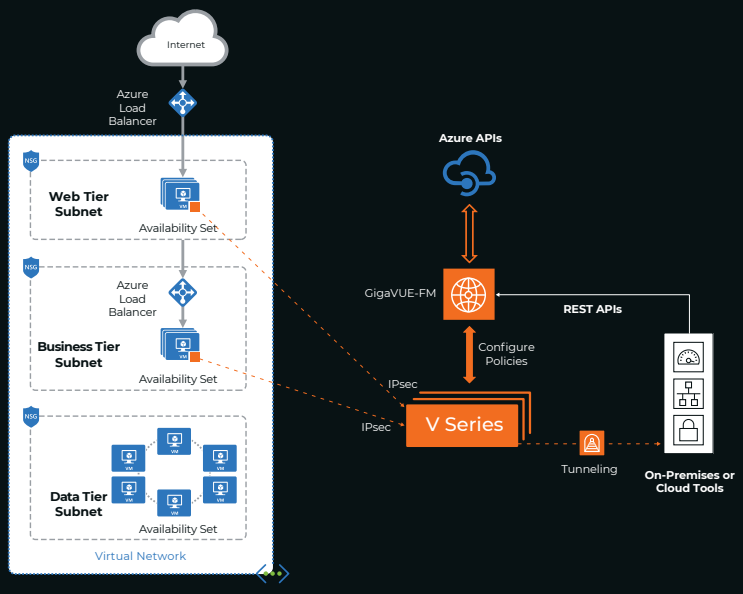

Figure 2. GigaVUE Cloud Suite for Azure supports multiple VNets and has tight integration with Azure cloud management tools, including Resource Manager, to enable automation. Gigamon GigaVUE lightweight G-vTAPs can collect all traffic streams.

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.
- Offload tools: Apply multiple GigaSMART applications, including Application Filtering Intelligence, Packet De-duplication, Slicing, Masking, and Flow Mapping to reduce the processing burden on tools.
- Operational efficiency: Use one common platform for visibility across the entire IT environment, with 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
- Improved performance and scalability: Packets can be processed at multi-Gbps rates with the integrated DPDK support, and the number of visibility nodes can be expanded to whatever levels required at no extra charge

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 Module – Lightweight agent deployed in an Azure compute instance to mirror production traffic and send this traffic via IPsec to GigaVUE V Series nodes. Allow and deny IP addresses can be optionally pre-filtered out. They can be deployed using GigaVUE-FM or via third-party orchestration tools such as Terraform and self-register with GigaVUE-FM.

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. V Series is based on a common architecture for multiple on-premises and cloud environments and supports multiple GigaSMART applications, including De-duplication, Packet Slicing, Masking, Flow Mapping, and Load Balancing. Includes DPDK for high-performance packet processing. These can be deployed using GigaVUE-FM or via third-party orchestration tools such as Terraform and self-register with GigaVUE-FM.

GigaVUE-FM – Provides centralized orchestration and management across the entire enterprise, including on-premises, Azure, AWS, 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 Proxy – For hybrid and multi-VPC 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 is required, and proxies commands from GigaVUE-FM to the G-vTAP Modules (see Figure 3). For those scenarios where GigaVUE-FM does not reside in the same location, such as when it is on-premises, on a separate VPC, or even on a different cloud vendor, GigaVUE V Series Proxy is used to proxy commands from GigaVUE-FM to the GigaVUE V Series nodes. (If FM is deployed in the same location as the V Series, this it is not required). They can be deployed using GigaVUE-FM or via third-party orchestration tools such as Terraform and self-register with GigaVUE-FM.

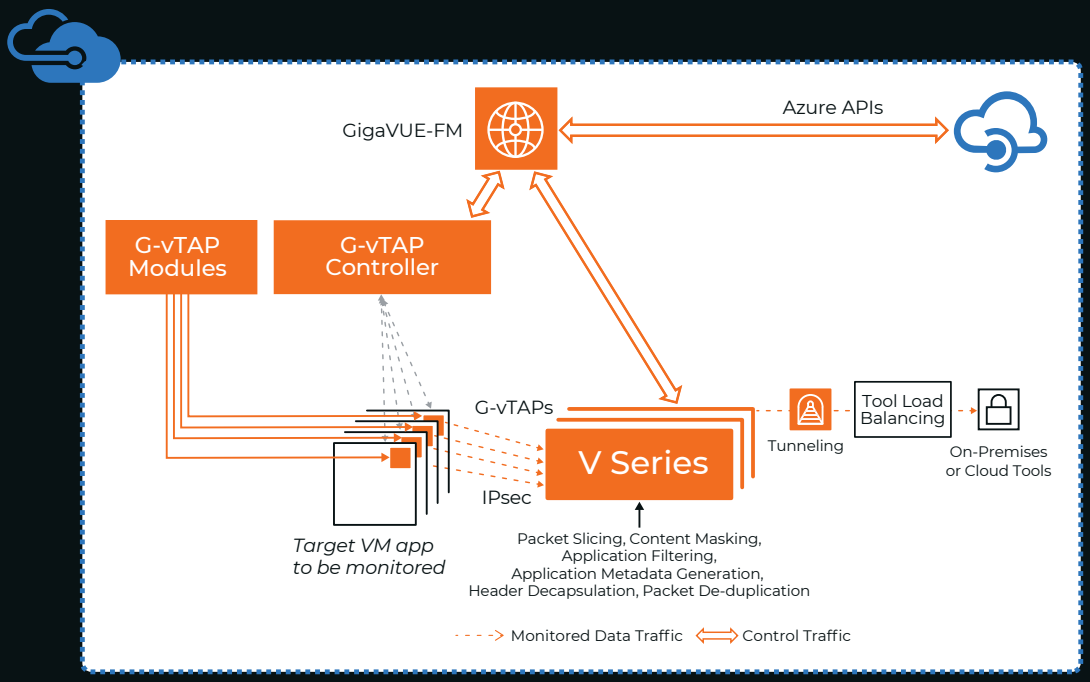

Figure 3. GigaVUE Cloud Suite for Azure is composed of three components: G-vTAP, V Series, and GigaVUE-FM Fabric Manager.

Key Features and Benefits

G-vTAP Module

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 versus 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 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

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 via GRE or VXLAN tunnels and support pre-filtering. Alternatively, traffic may be acquired from tunnel-as-a-source methods.

Traffic Intelligence: Select, Optimize, and Distribute

- Application Intelligence: Automatically identify over 3,500 applications in real time and selectively drop or send as appropriate to specific tools to improve their efficiency and effectiveness. Provide contextual insights by leveraging over 5,000 application-aware metadata attributes that empower observability, SIEMs, NPMD, and APM tools to solve security and network performance issues.
- Flow Mapping: Select Layer 2 through Layer 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.
- Other GigaSMART traffic intelligence functions: Optimize selected traffic by applying GigaSMART traffic intelligence to eliminate duplicated packets, slice out superfluous content, sample packet flows, and mask confidential information within payloads to reduce tool overload or maintain compliance.
- Distribute optimized traffic to multiple tools anywhere.
- Supports 5-tuple load balancing to tools to improve tool deployment efficiency and obviate the need for discrete load balancers.

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
- Processes at multi-Gbps rates per instance leveraging DPDK technology

GigaVUE-FM Centralized management and orchestration.	Centralized Orchestration and Management · Configures all policies on the visibility fabric components and manages their self-registration process in conjunction with the orchestration tool used · Centralized orchestration and single-pane-of-glass visualization across the entire infrastructure — public, private, and hybrid · Monitors heartbeat communications from all fabric elements to help ensure availability · 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 · Integration with third-party orchestration tools that optionally instantiate all visibility fabric components: G-vTAP Modules and their controller and V Series nodes and their proxy (if needed) · Open REST APIs published by GigaVUE-FM can be consumed by tools to dynamically adjust traffic received or 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 Module	Any	· Linux: Available as an RPM or Debian package · Windows: Available for Windows Server 2008/2012/2016/2019
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-premises GigaVUE H/W) · NIC 2: Management IP (commands from the controller)
GigaVUE V Series Proxy (Optional)	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 controller instances for relaying the commands · GigaVUE-FM automatically spins up additional V Series nodes based on a predefined 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

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

- Azure Marketplace Metered — GigaVUE Cloud Suite for Azure can be purchased as a subscription from the Azure Marketplace. Pricing is based on daily total volumes of traffic processed. In this option, Azure meters and charges for the usage of the solution, with four tiers of traffic processed per day. If usage exceeds the selected tier by an amount over a specified percentage, the customer will be automatically moved into a higher tier. Customers receive an unlimited number of G-vTAP Modules, proxies, and V Series instances at no additional charges. Traffic throughput rates do not affect charges, only total volumes consumed.

Table 2: Part numbers for the solution

PART NUMBER	DESCRIPTION
VBL-50T-BN-CORE	Volume license with up to 50 TB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-250T-BN-CORE	Volume license with up to 250 TB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-2500T-BN-CORE	Volume license with up to 2.5 PB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-25KT-BN-CORE	Volume license with up to 25 PB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-50T-BN-NV	Volume license with up to 50 TB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-250T-BN-NV	Volume license with up to 250 TB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-2500T-BN-NV	Volume license with up to 2.5 PB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-25KT-BN-NV	Volume license with up to 25 PB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support
VBL-50T-BN-SVP	Monthly term license for SecureVUE Plus software up to 50TB per day in V Series for cloud and virtual environments. Capabilities included: SecureVUE for V Series, Application Metadata Intelligence, Application Filter Intelligence. Minimum term is 12 months. Includes bundled Elite Support.
VBL-250T-BN-SVP	Monthly term license for SecureVUE Plus software up to 250TB per day in V Series for cloud and virtual environments. Capabilities included: SecureVUE for V Series, Application Metadata Intelligence, Application Filter Intelligence. Minimum term is 12 months. Includes bundled Elite Support.
VBL-2500T-BN-SVP	Monthly term license for SecureVUE Plus software up to 2.5 PB per day in V Series for cloud and virtual environments. Capabilities included: SecureVUE for V Series, Application Metadata Intelligence, Application Filter Intelligence. Minimum term is 12 months. Includes bundled Elite Support.
VBL-25KT-BN-SVP	Monthly term license for SecureVUE Plus software up to 25 PB per day in V Series for cloud and virtual environments. Capabilities included: SecureVUE for V Series, Applciation Metadata Intelligence, Application Filter Intelligence. Minimum term is 12 months. Includes bundled Elite Support.

Notes

- Virtual TAP point: Any endpoint from which traffic can be mirrored using the G-vTAP Module, such as a NIC in an VM. A single VM could have multiple NICs that can be tapped. For example, if an application uses 10 VMs with 2 NICs each, then the total virtual TAP points are 20.
- Utilizes a true-forward method when usage exceeds the contracted limit. The 95th percentile usage in the prior three months needs to be less than the contracted limit, or the next tier pricing is applied.
- Licensing: Licenses are activated from GigaVUE-FM.
- Requires the GigaVUE operating system 5.13 and above.

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 gigamon.com/support-and-services/overview-and-benefits.

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 | gigamon.com

03.22_06