Power of Public Cloud Network Traffic Visibility

GigaVUE Cloud Suite for AWS is an intelligent network and application traffic visibility fabric that acquires, optimizes, and distributes selected traffic to security and monitoring tools

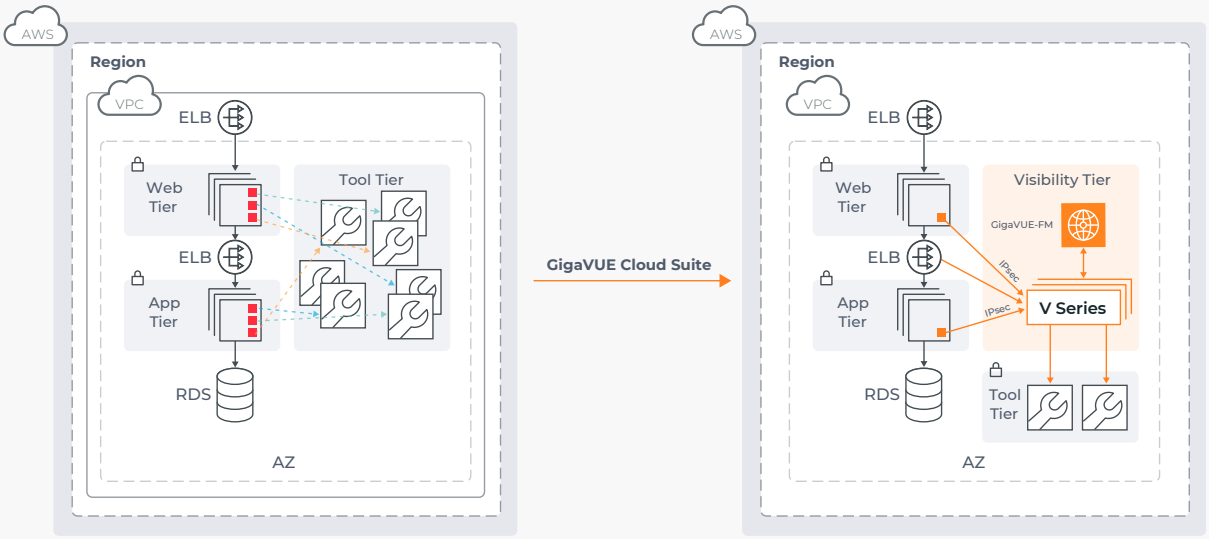

Figure 1. The suite is a cloud native application-aware platform and is fully integrated and certified within AWS environments. The solution dramatically simplifies and accelerates traffic acquisition and tool deployment.

Key Features and Benefits

- GigaSMART® modules to offload tools from processor-intensive tasks including Application Intelligence, packet slicing, adaptive packet filtering, masking, and packet de-duplication
- Flexible packet acquisition through agentless AWS VPC traffic mirroring, or through GigaVUE vTAPs that add IPsec security and prefiltering or tunnel-as-a-source
- 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 AWS CloudWatch, Ansible, and third-party orchestration tools such as Terraform
- Comprehensive visibility into the AWS infrastructure and the workloads present with traffic aggregation and application filtering and distribution to cloud or on-premises tools
- Dynamic discovery of new workloads and appropriate routing of that new traffic to augment 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
- Supports external AWS Network and Gateway Load Balancers with GENEVE protocol to substantially improve visibility node performance with reduced scaling and more deployment flexibility
- High-performance GigaSMART processing with V Series nodes that scale as needed
- Ensure visibility across interconnected VPCs and on-premises tools with AWS transit gateway support

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 security detection/response, workload, and network performance needs. 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. 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 AWS. Gigamon helps organizations gain full workload application visibility into East-West traffic and improve their security posture, while extending current network and application performance monitoring to AWS traffic. Using GigaVUE Cloud Suite for AWS, security architects can ensure an effective security posture in the cloud, thereby accelerating the onboarding of new AWS applications. NetOps teams can also leverage this fabric and advanced L4–7 metadata to troubleshoot degraded user experience, ensure network performance, and meet SLAs.

GigaVUE Cloud Suite for AWS, as shown in Figure 2, acquires traffic in three ways: via AWS VPC traffic mirroring instances, external AWS elastic load balancers, or with a lightweight Gigamon G-vTAP agent installed within the VMs housing Amazon EC2 instances. The Gigamon fabric integrates with Amazon EC2 APIs to discover the cloud infrastructure, deploy visibility nodes in VPCs that collect all the aggregated traffic and apply advanced traffic intelligence, including application and session filtering, and apply load balancing algorithms prior to sending selected traffic to security and monitoring tools. Supports AWS transit gateways to ensure visibility across interconnected VPCs and on-premises tools. This integrated solution enables this suite to automatically remain in sync. With this solution, organizations can take advantage of:

- Increased security: Centralized visibility for security monitoring of all Amazon VPCs 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 leverage traffic intelligence to optimize data to any number of tools. Load-balancer support eliminates the AWS mirroring limits and allows unlimited VM traffic to be load balanced and efficiently sent to V Series. Distribution is based on volumes to reduce the V Series scaling needs.
- Offload tools: Apply multiple GigaSMART applications, including application filtering intelligence, packet de-duplication, slicing, advanced packet filtering, masking, and flow mapping to reduce the processing burden on tools.
- Operational efficiency: One common platform for visibility across the entire IT environment; consistent insight into AWS, along with other public cloud platforms and on-premises infrastructure. Acquire network traffic with minimal impact to Amazon EC2 utilization and apply traffic intelligence before distributing to multiple tools for analysis.
- Operational agility:
  - Rapidly detect changes in Amazon VPCs 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.

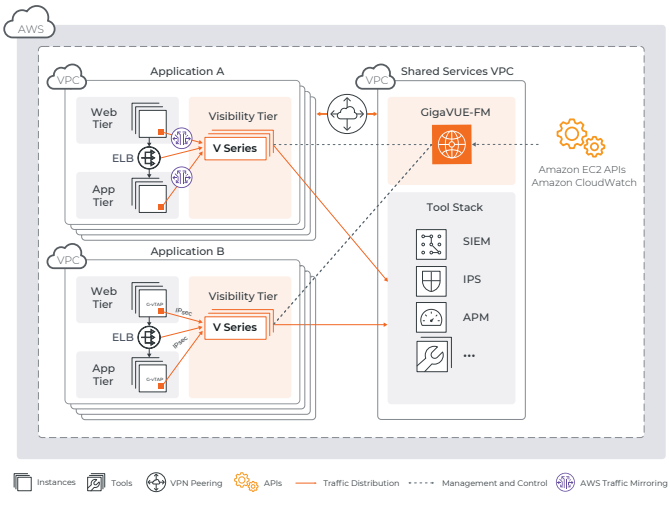

Figure 2. GigaVUE Cloud Suite for AWS supports multiple VPCs and has tight integration with AWS cloud management tools to enable automation. Either AWS's agentless native VPC traffic mirroring, AWS external load balancers, tunnel-as-a-source or Gigamon's GigaVUE lightweight G-vTAPs can collect all traffic streams.

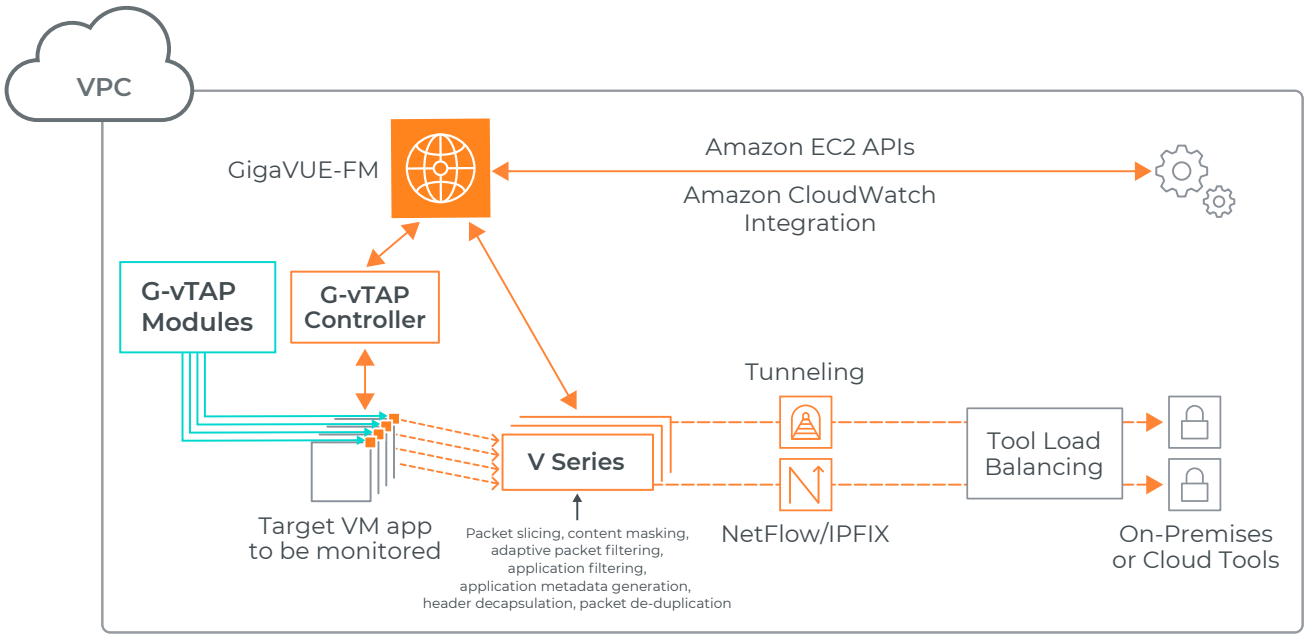

Figure 3. GigaVUE Cloud Suite for AWS is composed of four components: G-vTAP, V Series, G-vTAP Controller, and Fabric Manager (FM).

GigaVUE Cloud Suite for AWS

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 Amazon EC2 instance to mirror production traffic and send this traffic via IPsec to GigaVUE V Series nodes. IP addresses on a denial list can be optionally prefiltered out. They can be deployed using GigaVUE-FM or via third-party orchestration tools such as Terraform and self-register with FM.

GigaVUE V Series – Visibility nodes in AWS aggregate and select traffic of interest, then optimize and distribute acquired traffic to multiple tools located in any VPC. V Series is based on a common architecture for multiple on-premises and cloud environments; supports multiple GigaSMART applications, including application filtering intelligence, application metadata generation, packet de-duplication, adaptive packet filtering, packet slicing, masking, flow mapping, and tool load balancing. Includes DPDK for high-performance packet processing. They can be deployed using GigaVUE-FM or via third-party orchestration tools such as Terraform and self-register with FM.

GigaVUE-FM – Provides centralized orchestration and management across the entire enterprise including on-premises, AWS, and private clouds (OpenStack, VMware, and Nutanix). The traffic policies for both G-vTAP Module and V Series 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 FM does not reside in the same location, such as where it is on-premises or a separate VPC or even different cloud vendor, GigaVUE V Series Proxy can optionally be 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, then it is not required. They can be deployed using GigaVUE-FM or via third-party orchestration tools such as Terraform and self-register with FM.

Key Features and Benefits

G-vTAP Module

Lightweight agent deployed on an EC2. Mirrors traffic and sends via IPsec to GigaVUE V Series.

Minimize Agent Overload

- Requires just one agent per Amazon EC2 instance vs. needing to deploy one per security tool. This approach lowers impact on EC2 CPU utilization.

Reduce Application Downtime

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

Scale What's Being Monitored

- As EC2 instances scale out due to demand, the agent automatically scales appropriately. This is achieved with the integration between GigaVUE FM, Amazon EC2 APIs, and Amazon CloudWatch.

Minimize Production Changes

- Option to use either the production Elastic Network Interface (ENI) or a separate ENI 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 EC2 instances. The traffic is acquired from the EC2 instances using IPsec and via GRE or VXLAN tunnels and support prefiltering. Alternatively, traffic may be acquired from AWS VPC traffic mirroring instances or from AWS Network Load Balancers or from AWS Gateway Load Balancers that utilize GENEVE (V Series supports decapsulation of this protocol). Tunnel-as-a-source methods including traffic from Nokia and Ericsson virtual TAPs is also supported.

Traffic Intelligence: Select, Optimize, and Distribute

- Application Intelligence: Automatically identify over 3,200 applications in real time and selectively drop or send as appropriate to specific tool(s) to improve their efficiency and effectiveness. Provide contextual insights by leveraging over 5,000 application-aware metadata attributes that empower SIEMs and NPMD and APM tools to solve security and network performance issues.
- Flow Mapping®: Select Layer 2-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, instance tags, etc. Advanced policies using overlapping rules and nested conditions can be specified.
- Other GigaSMART traffic intelligence functions: Optimize selected traffic by applying applications to remove duplicated packets, slice out superfluous content, sample packet flows, and mask confidential information to reduce tool overload and maintain compliance.
- Adaptive Packet Filtering: Filter any header or payload content, such as specific encapsulation protocols, URLs, or basic app identifications, by searching for patterns based on strings and offsets or PCRE Regular Expressions.
- 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 EC2s, without lowering performance of visibility node.
- Processes at multi-Gbps rates per instance leveraging DPDK technology

GigaVUE-FM Centralized management and orchestration.	Centralized Orchestration and Management • Centralized orchestration and single-pane-of-glass visualization across entire infrastructure – public, private, and hybrid. • Configures all policies on the visibility fabric components and manages their self-registration process in conjunction with the orchestration tool used. • Traffic policies are defined using simple drag-and-drop user interface. • Monitors heartbeat communications from all fabric elements to help ensure availability. • Software-Defined Networking constructs are used to configure traffic policies. Automation • Tight integration with Amazon APIs detects EC2 changes in the Amazon VPC 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 to orchestrate new traffic policies. • When deployed with AWS load balancer, GigaVUE-FM automatically scales V Series based on traffic levels, not the number of target VM count. Topology View • Auto-discovery and end-to-end topology visualization of visibility tier and EC2 instances.

Minimum Requirements for GigaVUE Cloud Suite for AWS

Table 1: Recommended Minimum Compute Specifications

SOLUTION COMPONENT	MINIMUM EC2 INSTANCE 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	T2 Micro	Command-and-Control component for the G-vTAP agents
GigaVUE V Series Node	T3A.X Large	Requires minimum of two ENIs ENI 1: Management ENI 2: Traffic acquisition and distribution ENI 3+: Optional additional data acquisition and distribution
GigaVUE V Series Proxy Optional	T2 micro	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
GigaVUE-FM	M4 xlarge 40GB root disk 40GB data disk	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 AWS, with all the solution components, can be consumed using the following:

- AWS Marketplace Metered – GigaVUE Cloud Suite for AWS can be purchased as a subscription from the AWS marketplace and pricing is based on daily total volumes of traffic processed. In this option, AWS 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, Controllers, 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, App Metadata Intelligence, App 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, App Metadata Intelligence, App 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, App Metadata Intelligence, App 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, App Metadata Intelligence, App Filter Intelligence. Min Term is 12 months. Includes bundled Elite Support.

Note:

- Utilizes a true-forward method when usage exceeds 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 5.11 and above.

Support and Services

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

aws partner network

Advanced Technology Partner

Networking Competency

Public Sector Partner

Learn More

For more information on GigaVUE Cloud Suite for AWS, visit this website. Read the Solution Brief and request a demo.

Gigamon®

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