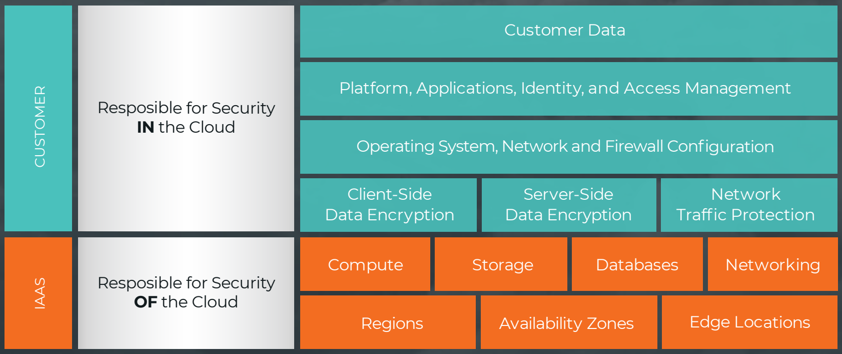
GigaVUE Cloud Suite for Public Cloud

Unparalleled Network and Application Visibility

Organizations are increasingly 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, whereas the IaaS customer is responsible for security in the cloud.

GigaVUE® Cloud Suites resides in the VPCs and VNets and aggregates flows from all compute sites, including from native traffic mirroring nodes. These suites provide advanced high-performance traffic processing such as removing duplicate packets, identifying and filtering applications, generating advanced metadata and optimally distribute and load balance data to the appropriate network monitoring and security tools. This helps ensure effective and comprehensive cloud security.



CUSTOMER

Resposible for Security **IN** the Cloud

Customer Data

Platform, Applications, Identity, and Access Management

Operating System, Network and Firewall Configuration

Client-Side Data Encryption

Server-Side Data Encryption

Network Traffic Protection

IAAS

Resposible for Security **OF** the Cloud

Compute

Storage

Databases

Networking

Regions

Availability Zones

Edge Locations

Figure 1: IaaS Shared Security Model.

KEY FEATURES

- GigaSMART® intelligence – includes packet de-duplication, slicing, masking, and tool load balancing
- Application Intelligence – automatically identify and filter over 3,200 apps and generate 5,000 metadata attributes
- Traffic acquisition with traffic mirroring services or with GigaVUE vTAPs with IPsec and prefiltering
- Transit gateway support
- Integration of GigaVUE-FM with AWS, Azure and third-party cloud management suites to instantiate unlimited virtual nodes
- Centralized orchestration and management with a single-pane-of-glass GUI using GigaVUE-FM

KEY BENEFITS

- Delivery of optimized traffic to offload security and networking monitoring tools
- 100 percent visibility into your multi-cloud infrastructure located workloads
- Ensure visibility across interconnected virtual clouds and regions and on-premises tools
- Simplified and automated deployment of a dynamic visibility fabric with limitless scalability
- Discovery of new workloads, proper traffic direction and adjustment of the visibility tier, all without manual intervention

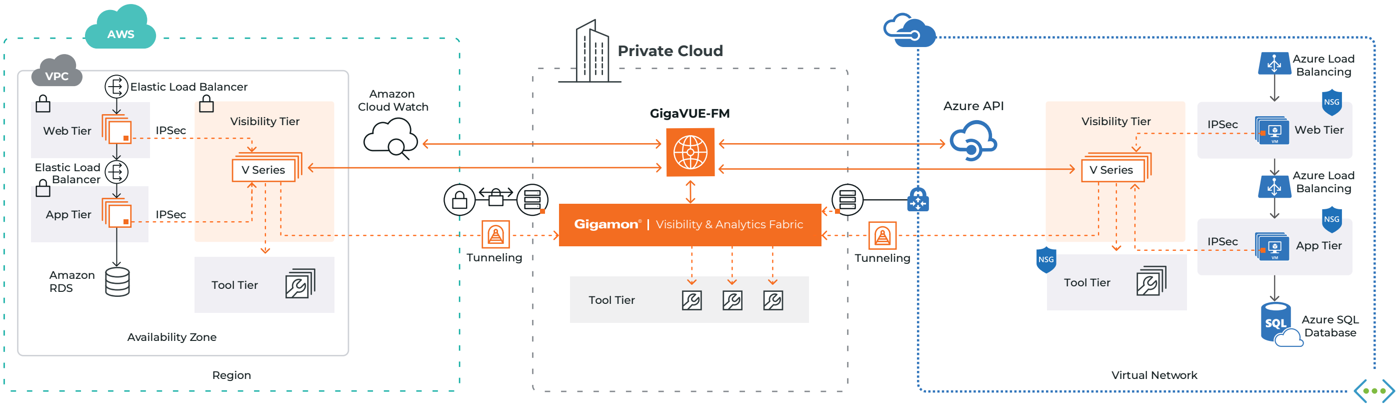


Figure 2: GigaVUE Cloud Suite for Multi-Clouds.

Key Considerations for IT, Cloud, and Security Architects

While IaaS vendors ensure protection from the physical datacenter 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 cloud 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:

- As part of the shared responsibility model, how do I assure that the cloud is being used securely by everyone in the enterprise?
- How do I run more applications while meeting the needs for applying compliance and security controls?
- What methods can be used to realize a fully automated environment that dynamically adjusts for workload relocations?
- Can the necessary traffic processing performance levels with proper scalability be assured in the cloud?
- As applications are moved from on-premises to the cloud, can the same traffic processing be applied, including application identification and filtering, payload masking, packet de-duplication, app-aware metadata generation and tool load balancing?
- Are there effective methods to reduce the cost of backhauling traffic when the tools monitoring traffic in the cloud are on-premises versus part of a tool tier in the cloud?
- How is granular VM and container visibility achieved while minimizing agent sprawl and simultaneously sending traffic to multiple tools?
- Which orchestration tools (in addition to the cloud vendor) are supported by the visibility and analytics fabric vendor? Terraform, Ansible, Chef, Puppet?

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 Suites deliver automated intelligent network and application traffic visibility for dynamic workloads running in multiple clouds including AWS, Azure, GCP and Oracle and enables increased security, operational efficiency, and high-performance processing across these environments. Organizations can optimize costs with up to 100 percent visibility for security without increasing load on compute instances as more security tools are deployed.

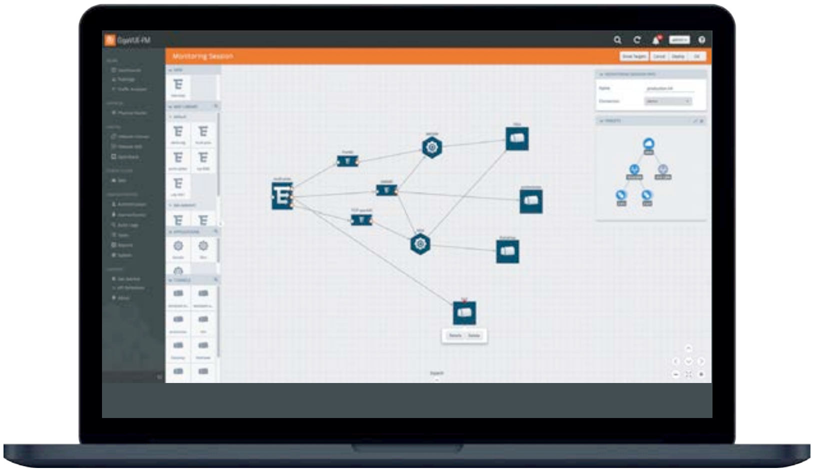


Figure 3: Centralized management, automation, and straightforward process with IaaS vendor orchestration suites and Gigamon Fabric Manager.

GigaVUE G-vTAPs

For traffic acquisition, lightweight 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, intelligent high-performance packet processing, 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 VPCs
- Flow Mapping®: Selection of L2–4 traffic
- GigaSMART intelligence: Packet de-duplication, slicing, sample, and masking combined with load balancing to optimize traffic sent to tools, reducing tool overload
- Fully interoperable with native traffic mirroring
- Application Filtering Intelligence: Automatically identify and filter out thousands of applications in real-time and direct their traffic to the appropriate tools
- Application Metadata Intelligence: Generate over 5000 metadata attributes across applications and protocols to enhance security and monitoring tool effectiveness.

GigaVUE-FM (Fabric Manager)

Centralized orchestration and management are done by GigaVUE-FM. Tight coupling with Ansible, AWS CloudWatch, Azure Network Watcher and third-party orchestration suites, including Terraform, Ansible, Chef, and Puppet, automatically instantiates, configures, and monitors G-vTAP and V Series instances and supports dynamic workload migrations.

- Detect compute instance changes in the virtual clouds and automatically adjust the visibility tier, through pre-built integration with the orchestrator's APIs
- Publish REST APIs: Integrate with a broad range of orchestrators and tools to dynamically adjust traffic received or to orchestrate new traffic policies
- Auto-discover and visualize end-to-end network topology, including virtual cloud workloads, by using an intuitive drag-and-drop user interface
- Eliminate manual processes and errors by automatically identifying each new workload and its associated traffic mirroring via ATS, and then configuring the traffic mirroring to direct traffic to the V Series Nodes
- Deep integration with multiple orchestration tools automatically instantiate the G-vTAP Modules and Controllers, as well as the V Series and their optional proxies.

Conclusion

Whether your organization is already using IaaS public cloud providers or considering a future migration, GigaVUE Cloud Suite solutions provide intelligent network traffic visibility for workloads running in the cloud. Integration with multiple cloud orchestrator APIs automatically deploys a visibility tier in all virtual clouds, whether based on VPCs, VNets, or VCNs, collects aggregated traffic and applies advanced packet processing prior to sending selected traffic to existing security tools. With GigaVUE, organizations can obtain consistent insight into their infrastructure across multi-cloud and their on-premises environment.

Gigamon®

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