SOLUTION BRIEF

GigaVUE Cloud Suite for AWS

Network Visibility into Public Cloud

aws partner network

Advanced Technology Partner

Networking Competency

Public Sector Partner

Key Features

- GigaSMART intelligence – includes packet slicing, masking, decapsulation and NetFlow generation
- Traffic acquisition with agentless AWS VPC traffic mirroring, or with GigaVUE vTAPs that add IPsec security and pre-filtering
- Automatic Target Selection® and Flow Mapping™
- Centralized orchestration and management with a single pane of glass GUI using GigaVUE-FM

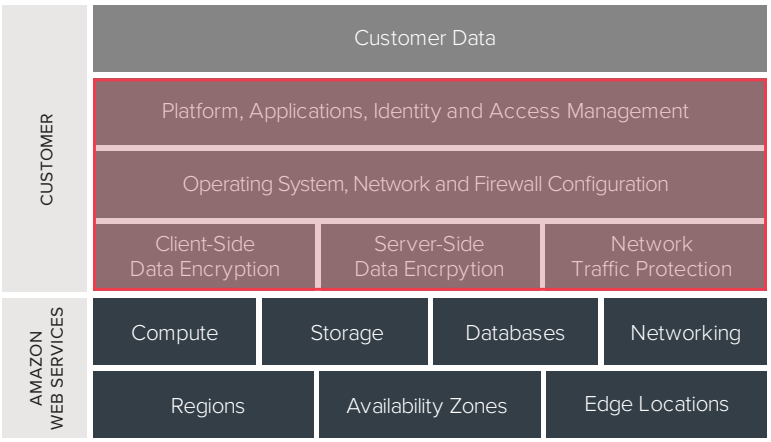
Key Benefits

- Delivery of optimized traffic to the proper security and network monitoring tools
- Up to 99 percent reduction in traffic with NetFlow/IPFIX generation[1]
- 100 percent visibility into your AWS infrastructure
- Significantly lower processing demands on tools by delivering only the appropriate traffic
- Discovery of new workloads, proper direction of their traffic and adjustment of the V Series visibility tier, all without any manual intervention

Organizations are increasingly migrating to public cloud Infrastructure-as-a-Service (IaaS) to take advantage of scale, elasticity and availability. For an effective IaaS strategy, enterprises need to recognize security implications.

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. While Amazon 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 AWS environment is imperative.

GigaVUE Cloud Suite (formerly GigaSECURE Cloud for AWS) resides in the AWS virtual private cloud (VPC) and aggregates flows from all compute sites, including from AWS VPC traffic mirroring nodes. The Cloud Suite provides advanced network traffic processing and optimally distributes this traffic to the appropriate virtual or physical network monitoring and security tools. The result is comprehensive insight from a single pane of glass, simplified operations and reduced TCO.



Amazon Web Services (AWS) Shared Security Model

Key Considerations for IT, Cloud and Security Architects

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

- As part of the shared responsibility model, how do I assure that AWS is being used securely by everyone in the enterprise?
- How do I run more applications on AWS 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 AWS?
- 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 AWS delivers intelligent network traffic visibility for workloads running in AWS and enables increased security, operational efficiency and scale across Virtual Private Clouds (VPCs). With this solution, organizations can:

- Optimize costs with up to 100 percent visibility for security without increasing load on compute instances as more security tools are deployed[1]
- Leverage GigaSMART traffic intelligence to deliver optimized traffic to the right tool, with up to 99 percent reduction in traffic with NetFlow/IPFIX generation[1]

The solution consists of three key components:

- Traffic acquisition using G-vTAP agents
- Traffic aggregation, intelligence and distribution using GigaVUE V Series
- Centralized orchestration and management using GigaVUE-FM

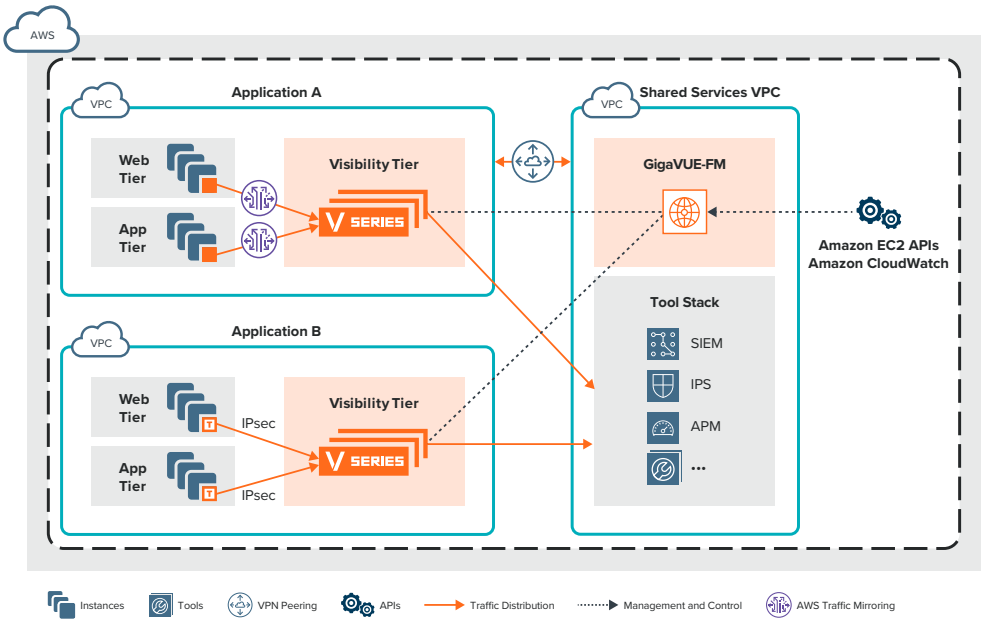


Figure 1: GigaVUE Cloud Suite for AWS

[1]Based on Gigamon internal analysis, November 2017

G-vTAPs

For traffic acquisition, light weight G-vTAPs are deployed within EC2 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 above).

Key benefits include:

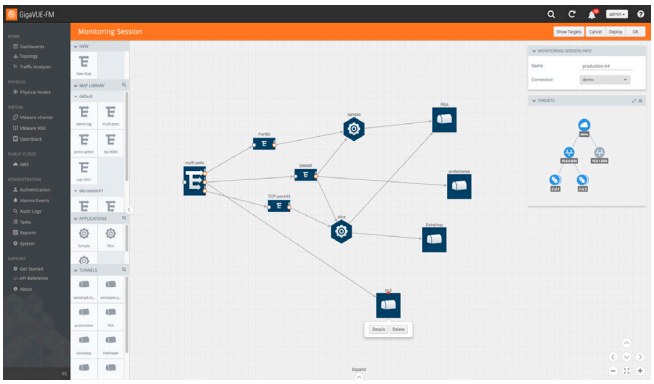
- Automatic Target Selection (ATS): Automatically extract traffic of interest from any workload with an agent deployed without explicitly specifying target VPCs
- Flow Mapping®: Selection of Layer 2 to 4 traffic
- NetFlow/IPFIX generation: Create flow records from network traffic to determine IP source and destination
- Header Transformation: Modify content in the header (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 AWS VPC traffic mirroring traffic acquisition methods

GigaVUE-FM

Centralized orchestration and management are done by GigaVUE-FM. This single pane of glass creates policies for workloads within AWS.

Key benefits include:

- Detect EC2 changes in a VPC and automatically adjust the visibility tier, through pre-built integration with AWS 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 VPC 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 VSeries Nodes.

Conclusion

Whether your organization is already using AWS or considering a future migration, GigaVUE Cloud Suite for AWS provides intelligent network traffic visibility for workloads running in the cloud. Integration with AWS APIs automatically deploys a visibility tier in all VPCs, 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 AWS and their on-premises environment.

For more information on GigaVUE Cloud Suite for AWS: Please read the data sheet. Learn more at www.gigamon.com/aws.

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