DATA SHEET

# GigaSECURE Cloud for AWS

Intelligent network traffic visibility for AWS

aws partner network

Advanced Technology Partner

Networking Competency

Public Sector Partner

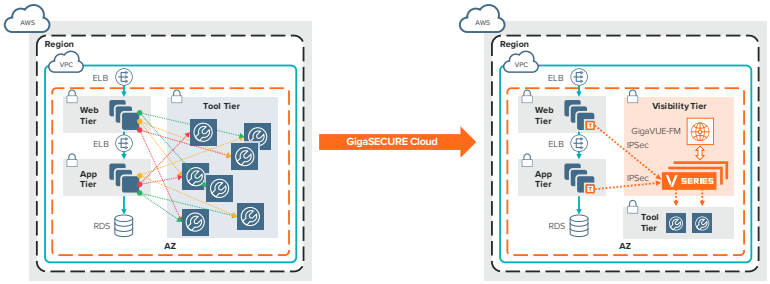
## Highlights

- **Reduce complexity** – One platform for visibility across the entire IT environment: one consistent method to acquire network traffic and apply traffic intelligence before distributing to multiple tools
- **Increase ROI** – Re-use existing security tools across your entire infrastructure
- **Cost savings** – Leverage traffic intelligence to deliver the right traffic to the right tools
- **Ensure SLA** – Tight integration with Amazon EC2 APIs and Amazon CloudWatch to automatically detect instance changes in Amazon Virtual Private Clouds (VPCs)
- **Centralized visibility for security monitoring** – of all Amazon VPCs in an enterprise
- **Gain insight into traffic traversing VPCs** – To effectively deliver summarized, critical data to security and monitoring tools
- **Generate NetFlow for any traffic flow** – within your OpenStack environment

The rapid evolution of Infrastructure-as-a-Service (IaaS) brings instant advantages of economies of scale, elasticity and agility to organizations seeking to modernize their IT infrastructures. Migrating workloads into the public cloud, however, introduces a new set of 'shared' responsibilities and challenges – primarily to manage, secure and understand all of the data now traversing the public cloud.

The obvious challenges of this approach include the inability to access all traffic in support of threat detection/response, application and network performance. Current security and monitoring tools that operate in public clouds often lack complete access to this data-in-motion.

One approach to this challenge is to adopt an agent per tool as an option to provide visibility and address these challenges as shown in the Figure below on the left. Such an approach can quickly overload compute instances, increases application and bandwidth costs and forces an architecture redesign when adding new security and monitoring tools. An efficient and optimal solution is to use GigaSECURE Cloud as shown in the Figure below on the right.

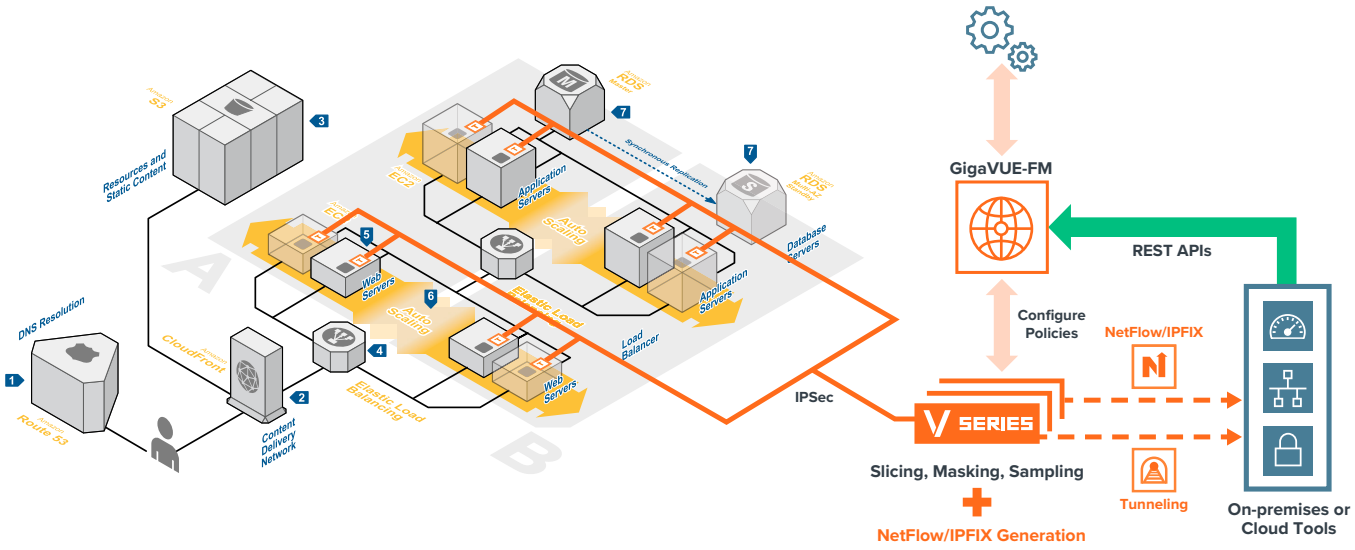



GigaSECURE Cloud is an intelligent network traffic visibility solution that acquires, optimizes, and distributes selected traffic to security and monitoring tools. This enables enterprises to extend their security posture to AWS and reduce the time to detect and mitigate threats to applications, while helping assure compliance.

## Accelerate Application Migration to the Cloud

Using GigaSECURE Cloud, security architects can ensure an effective security posture in the cloud thereby accelerating the on-boarding of applications to AWS.

GigaSECURE Cloud, as shown below, acquires traffic with a single, lightweight agent installed on the workloads, i.e. Amazon EC2 instances. The platform integrates with Amazon EC2 APIs to discover the cloud infrastructure, deploy visibility nodes in the Virtual Private Clouds (VPCs) that collect aggregated traffic from all the agents, and apply advanced traffic intelligence prior to sending selected traffic to security and monitoring tools. The integration then enables GigaSECURE Cloud to remain in sync with all the changes occurring with the environment automatically.




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:** Optimize costs with up to 100% visibility for security without increasing load on compute instances as more security tools are deployed. Acquire traffic once from compute instances and leverage traffic intelligence to optimize data to multiple tools. Specifically, with NetFlow, up to 99% reduction in data to tools can be achieved.[1]
- **Operational efficiency:** One common platform for visibility across the entire IT environment enables consistent insight in AWS, other public cloud platfomrs 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 specific target compute instances to monitor.
  - Flexibility to perform the analysis of traffic anywhere.
  - Automate and orchestrate visibility using open REST APIs.

[1]Based on Gigamon internal testing, November 2017

## GigaSECURE Cloud Components

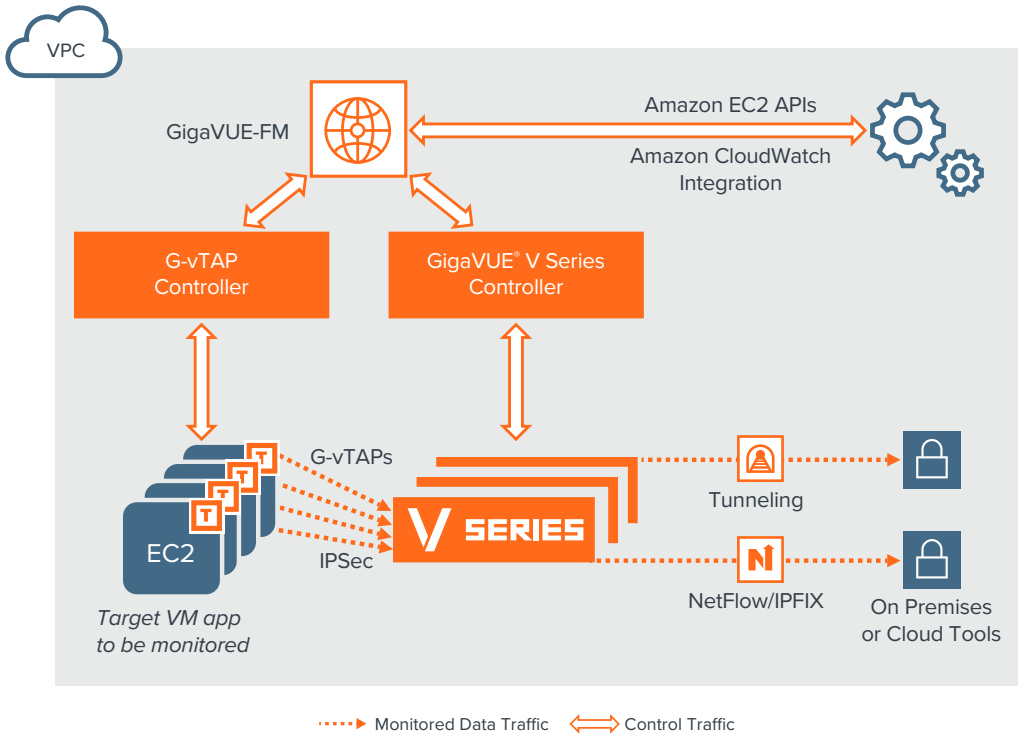
GigaSECURE Cloud comprises of multiple components that enable traffic acquisition, traffic aggregation, intelligence and distribution along with single-pane-of-glass orchestration and management of the solution.

**G-vTAP Agent** – The G-vTAP agent is a lightweight agent deployed in an Amazon EC2 instance. The agent mirrors traffic from the production instance and sends the mirrored traffic via IPSec to GigaVUE V Series nodes.

**GigaVUE V Series** – The GigaVUE V Series are visibility nodes in AWS that aggregate, select traffic of interest, optimize and distribute acquired traffic to multiple tools located anywhere.

**GigaVUE-FM** – The GigaVUE-FM provides centralized orchestration and management across the entire enterprise including on-premise, AWS, Microsoft Azure, and private clouds (OpenStack and VMware). The traffic policies can be configured using a simple drag-and-drop user interface.

**G-vTAP Controller and GigaVUE V Series Controller** – To support flexible deployment models such as hybrid deployments and multi-VPC deployments at scale, Gigamon CloudVUE leverages a controller-based architecture to proxy the command-and-control APIs while preserving existing Network Address Translation (NAT) or IP addressing schemes. The G-vTAP Controller is used to proxy commands from GigaVUE-FM to the G-vTAP agents. The GigaVUE V Series Controller is used to proxy commands from GigaVUE-FM to the GigaVUE V Series nodes.



## Features and Benefits

| Solution Component | Key Features and Benefits |
|---|---|
| **G-vTAP Agent**<br>Lightweight agent deployed on a EC2. Mirrors traffic and sends via IPSec to GigaVUE V Series in visibility tier. | **Minimize Agent Overload**<br>• Deploy one agent per Amazon EC2 instance vs. having to deploy one per security tool. This approach lowers impact on EC2 CPU utilization. |
| | **Reduce Application Downtime**<br>• Avoids need to redesign infrastructure to add new tool agents as applications scale out in AWS or as more operational tools are added. |
| | **Scalability**<br>• As EC2 instances scale out due to demand, the agent automatically scales due to the integration between GigaVUE-FM, Amazon EC2 APIs and Amazon CloudWatch. |
| | **Minimize Production Changes**<br>• Option to use either the production Elastic Network Interface (ENI) or a separate ENI to mirror the workload traffic. The separate ENI option allows customers to preserve application traffic policies. |
| | **Reduce Costs**<br>• Pass or Drop rules to filter traffic of interest prior to sending it via IPSec to the GigaVUE V Series to reduce application and data egress costs. |
| **GigaVUE V Series**<br>Visibility nodes that aggregate, select, optimize, and distribute traffic. | **Traffic Aggregation**<br>• Acquire and aggregate traffic from multiple EC2 instances. The traffic is acquired from the EC2 instances using IPSec and via GRE or VXLAN tunnels. |
| | **Traffic Intelligence: Select, Optimize and Distribute**<br>• Flow Mapping®: Select Layer 2-Layer 4 traffic of interest with a variety of policies and forward of 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.<br>• 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, causes of congestion, etc.<br>• 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.<br>• 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.<br>• Distribute optimized traffic to multiple tools anywhere. |
| | **Service Chaining**<br>• Service chain multiple traffic intelligence operations dynamically based on tool needs. |
| | **Elastic Scale and Performance**<br>• Automatic Target Selection: Automatically extract traffic of interest anywhere in the infrastructure being monitored.<br>• Automatically scales based on varying number of EC2s without lowering performance of visibility node. |

### Features and Benefits continued

| Solution Component | Key Features and Benefits |
|---|---|
| **GigaVUE-FM**<br>Centralized management and orchestration. | **Centralized Orchestration and Management**<br>• Centralized orchestration and single-pane-of-glass visualization across entire infrastructure – public, private and hybrid.<br>• Traffic policies are defined using simple drag-and-drop user interface.<br>• Uses Software-Defined Networking constructs to configure traffic policies. |
| | **Automation**<br>• Tight integration with Amazon APIs to detect EC2 changes in the Amazon VPC and automatically adjust the visibility tier.<br>• 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**<br>• Auto discovery and end-to-end topology visualization of visibility tier and EC2 instances. |

## Minimum Requirements for GigaSECURE Cloud Components

### Table 1: Recommended Minimum Compute Specifications

| Solution Component | Minimum EC2 Instance Type | Description |
|---|---|---|
| **G-vTAP Agent** | t2.medium (single or multiple ENI support) | Linux: Available as an RPM or Debian package.<br>Windows: Available for Windows Server 2008/2012/2016 |
| **G-vTAP Controller** | t2.micro | Command-and-Control component for the G-vTAP agents |
| **GigaVUE V Series Node** | c4.large (2 ENIs) | c4.large supports throughput up to 500 Mbps<br><br>ENI 1: Data IP (mirrored traffic from G-vTAP)<br>ENI 2: Tunnel IP (traffic to tools or on prem GigaVUE H/W)<br>ENI 2: Management IP (commands from the controller) |
| **GigaVUE V Series Controller** | t2.micro | Command-and-Control component for the V Series Nodes |
| **GigaVUE-FM** | m4.xlarge<br><br>40GB root disk<br><br>40GB data disk | GigaVUE-FM needs to be able to access both the controller instances for relaying the commands<br><br>GigaVUE-FM automatically spins up additional V Series nodes based on a pre-defined configuration in the user interface<br><br>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 V Series nodes will be auto-launched by GigaVUE-FM.

## Ordering Information, Renewals

GigaSECURE Cloud, with all the solution components, can be consumed using the following options:

- Bring Your Own License (BYOL) – GigaSECURE Cloud can be purchased as a subscription from AWS Marketplace and AWS GovCloud (US). Table 2 below lists the SKUs for procurement.

**Table 2: Part Numbers for the Solution**

| Part Number | Description |
|---|---|
| GFM-AWS-100 | Monthly Term license for traffic visibility up to 100 virtual TAP points in AWS. Min Term is 12 months and includes Elite support |
| GFM-AWS-1000 | Monthly Term license for traffic visibility up to 1,000 virtual TAP Points in AWS. Min Term is 12 months and includes Elite support |

- AWS Marketplace Metered – GigaSECURE Cloud can be purchased as a subscription from the AWS marketplace for 100 virtual tap points on an hourly or annual basis. In this option, AWS meters and charges the usage of the solution. Customers can register with Gigamon to obtain 24x7 Elite Support for no additional charge.

Note:

- Virtual TAP Point: Any end point from which traffic can be mirrored using the G-vTAP agent, for example, an ENI in an EC2 instance. A single Amazon Machine Image (AMI) could have multiple ENIs that can be tapped. For example, if an application uses ten EC2 instances with two ENIs each, then the total Virtual TAP Points are 20.
- Try-and-Buy: Launch the BYOL offering in AWS Marketplace for a 10 G-vTAP agent, 30-day trial of our solution. Refer to the ordering section to purchase additional term-based subscription.
- 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-AWS-100 or GFM-AWS-1000 at no additional charge.

## 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



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