DATA SHEET

GigaSECURE Cloud for OpenStack

Intelligent network traffic visibility for OpenStack

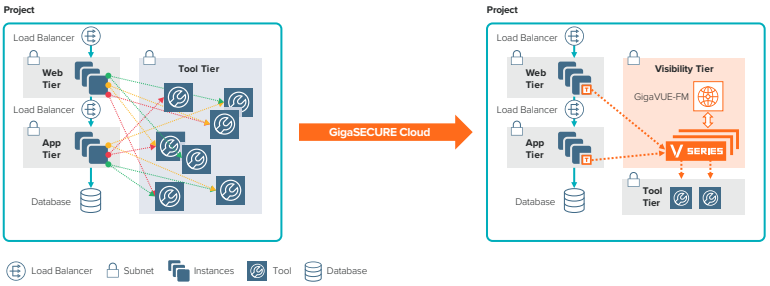
Highlights

- **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 OpenStack APIs to automatically detect instance changes
- **Centralized visibility for security monitoring** – of all projects in an enterprise
- **Gain insight into traffic traversing projects** – to effectively deliver summarized, critical data to security and monitoring tools

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.

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

One approach to this challenge is to adopt as shown in the Figure below on the left. Such an approach overloads 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.

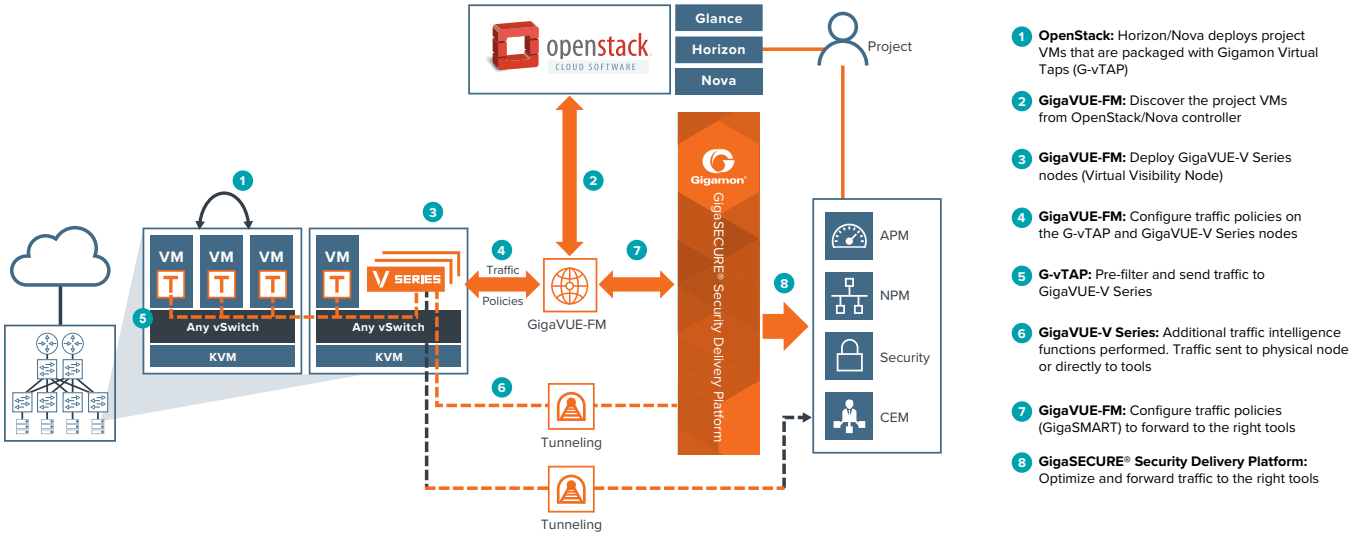


GigaSECURE Cloud is an intelligent network traffic visibility solution that acquires, optimizes, and distributes selected traffic to security and monitoring tools. This enables enterprises to extend their security posture to OpenStack and accelerate the time to detect and mitigate threats to applications,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

GigaSECURE Cloud, as shown below, acquires traffic with a single, lightweight agent installed on the workloads, i.e. OpenStack instances. The platform integrates with OpenStack APIs to discover the cloud infrastructure, deploy visibility nodes in the projects that collect aggregated traffic from all the agents, and apply advanced traffic intelligence prior to sending selected traffic to security and monitoring tools.



With this solution, organizations can take advantage of:

- **Increased security:** Centralized visibility for security monitoring of all projects 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 OpenStack. Acquire network traffic with minimal impact to instance utilization and apply traffic intelligence before distributing to multiple tools for analysis.
- **Operational agility:**
  - Rapidly detect changes in projects 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

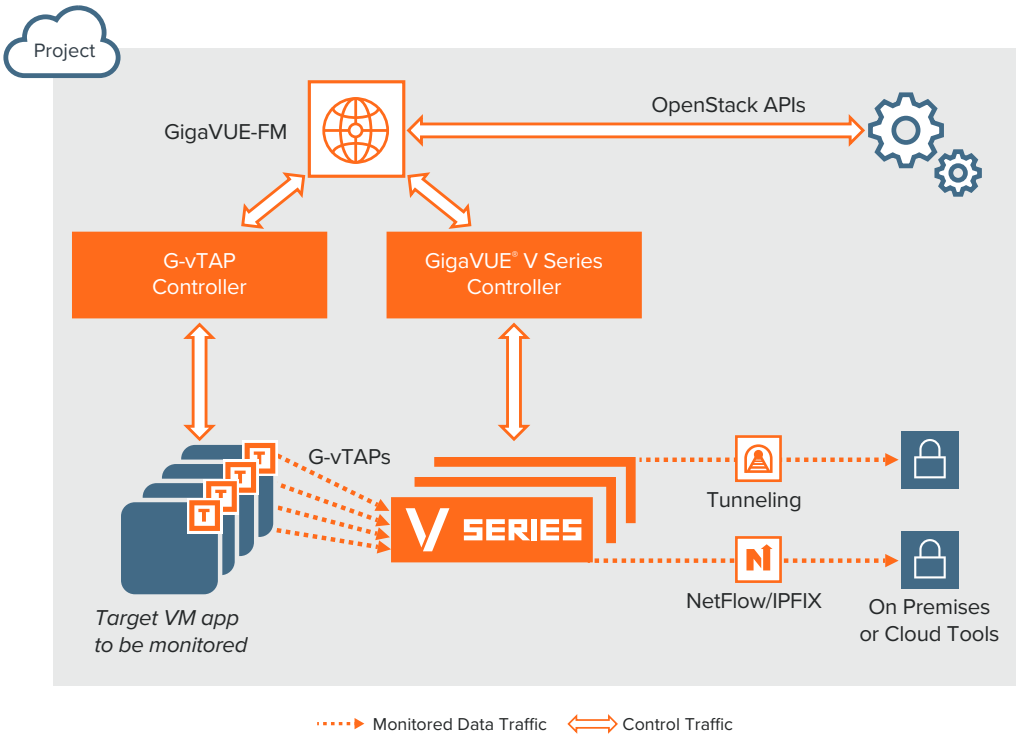
GigaSECURE Cloud comprises of multiple components that enable traffic acquisition, traffic aggregation, intelligence and distribution along with single-pane-of-glass orchestration and management of the solution.

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

GigaVUE V Series – The GigaVUE V Series are visibility nodes in OpenStack 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 OpenStack, VMware, and public clouds (e.g. Microsoft Azure and Amazon AWS). 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-project deployments at scale, GigaSECURE Cloud 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 Lightweight agent deployed on an instance. Mirrors traffic and sends to GigaVUE V Series in visibility tier.	**Minimize Agent Overload** • Deploy one agent per OpenStack instance vs. one per security tool. This approach lowers impact on instance CPU utilization.
	Reduce Application Downtime • Avoids need to redesign infrastructure to add new tool agents as applications scale out in OpenStack or as more operational tools are added.
	Scalability • As instances scale out due to demand, the agent automatically scales due to the integration between GigaVUE-FM and OpenStack APIs.
	Minimize Production Changes • Option to use either the production Virtual NetworK Interface Card (vNIC) or a separate vNIC to mirror the workload traffic. The separate vNIC option allows customers 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 to reduce 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 OpenStack instances. The traffic is acquired from the instances using GRE or VXLAN tunnels.
	Traffic Intelligence: Select, Optimize and Distribute • Flow Mapping®: Select Layer 2-Layer 4 traffic of interest with a variety of policies. Criteria can include IP addresses/subnets, TCP/UDP ports, protocols, instance tags etc. Advanced policies using overlapping rules and nested conditions can be specified. • 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. • 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. • Other GigaSMART® traffic intelligence functions: Optimize selected traffic by applying GigaSMART® traffic intelligence to slice, sample, and mask packets to reduce tool overload. • Distribute optimized traffic to multiple tools anywhere.
	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 scales based on varying number of instances without lowering performance of visibility node.

Features and Benefits continued

Solution Component	Key Features and Benefits
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. • Traffic policies are defined using simple drag-and-drop user interface. • Uses Software-Defined Networking constructs to configure traffic policies.
	Automation • Tight integration with OpenStack APIs to detect instance changes in the OpenStack project and automatically adjust the visibility tier. • 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 • Auto discovery and end-to-end topology visualization of visibility tier and OpenStack instances.

Minimum Requirements for the GigaSECURE Cloud Components

Table 1: Recommended Minimum Compute Specifications

Solution Component	Minimum EC2 Instance Type	Description
G-vTAP Agent	2 vCPU, 4GB Mem (single or multiple vNIC support)	Linux: Available as an RPM or Debian package. Windows: Available for Windows Server 2008/2012/2016
G-vTAP Controller	1 vCPU, 1GB Mem	Command-and-Control component for the G-vTAP agents
GigaVUE V Series Node	2 vCPU, 8GB Mem (2 vNICs)	vNIC 1: Data IP (mirrored traffic from G-vTAP) vNIC 2: Tunnel IP (traffic to tools or on prem GigaVUE H/W) vNIC 2: Management IP (commands from the controller)
GigaVUE V Series Controller	t2.micro	Command-and-Control component for the V Series Nodes
GigaVUE-FM	4 vCPU,16GB Mem 40GB root 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 V Series nodes will be auto-launched by GigaVUE-FM.

Ordering Information, Renewals

GigaSECURE Cloud can be purchased as a subscription from Gigamon. Table 2 below lists the SKUs for procurement.

Table 2: Part Numbers for the Solution

Part Number	Description
GFM-VTAP-100	Virtual monitoring in OpenStack deployments for up to 100 virtual TAP points. A 'virtual TAP point' is any end point that can be monitored, for example, a vNIC in an OpenStack instance.
GFM-VTAP-250	Virtual monitoring in OpenStack deployments for up to 250 virtual TAP points. A 'virtual TAP point' is any end point that can be monitored, for example, a vNIC in an OpenStack instance.
GFM-VTAP-1000	Virtual monitoring in OpenStack deployments for up to 1000 virtual TAP points. A 'virtual TAP point' is any end point that can be monitored, for example, a vNIC in an OpenStack instance.

Note:

- A single OpenStack Virtual Machine Image (OVMI) could have multiple vNICs that can be tapped. For example, if an application uses ten OpenStack instances with two vNICs each, then the total Virtual TAP Points are 20.
- Licensing: Licenses are activated from GigaVUE-FM.
- Renewal: 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-VTAP-100, GFM-VTAP-250 or GFM-VTAP-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