DATA SHEET

GigaSECURE Cloud for Microsoft Azure

Intelligent network traffic visibility for Microsoft Azure

Microsoft Azure Certified

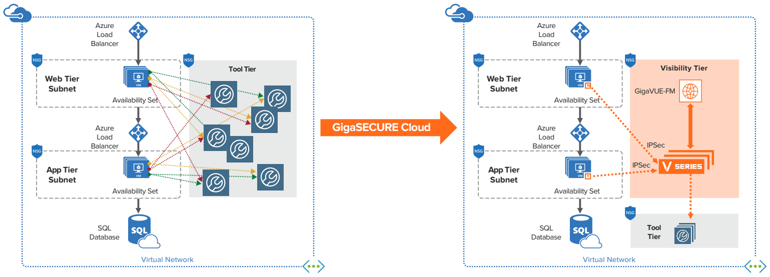
Highlights

- **Reduce complexity** – One platform for across 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 entire infrastructure
- **Cost savings** – Leverage traffic intelligence to deliver the right traffic to the right tools
- **Ensure SLA** – Tight integration with Azure APIs to automatically detect instance changes in Virtual Networks (VNets)
- **Centralized visibility for security monitoring** – Of all Azure VNets in an enterprise
- **Gain insight into traffic traversing VNets** – To effectively deliver summarized, critical data to security and monitoring tools
- **Generate NetFlow for any traffic flow** – Within your Azure 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 its 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 a one agent for each tool approach to visibility 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.

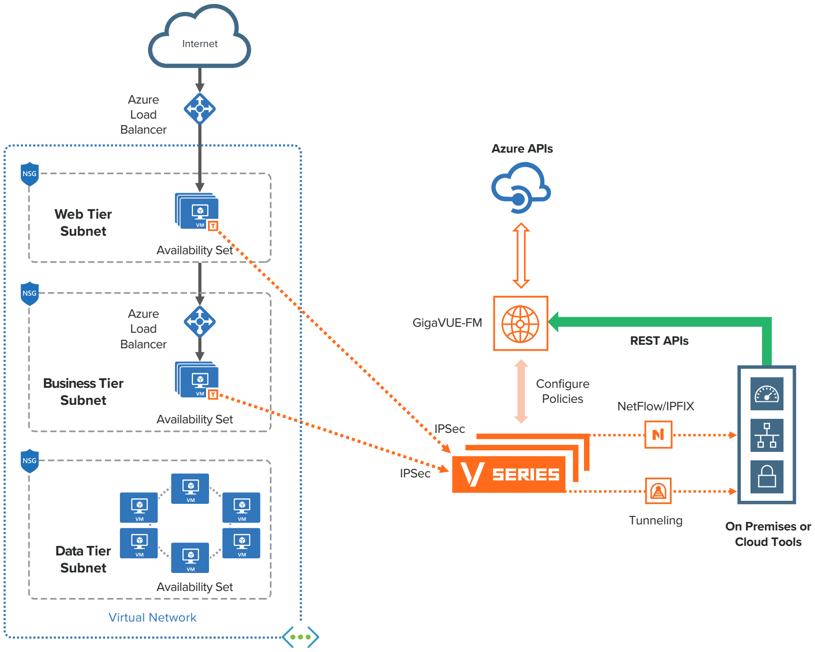


GigaSECURE Cloud is an intelligent network traffic visibility solution that acquires, optimizes and distributes selected traffic to security and monitoring tools. This enables enterprises to extend their security posture to Azure and accelerate the time to detect and mitigate threats to applications,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

Accelerate Application Migration to the Cloud

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

GigaSECURE Cloud, as shown below, acquires traffic with a single, lightweight agent installed on the workloads, i.e. Azure Virtual Machines. The platform integrates with Azure APIs to discover the cloud infrastructure, deploy visibility nodes in the Virtual Networks (VNets) 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 within the environment automatically.



With this solution, organizations can take advantage of:

- **Increased security:** Centralized visibility for security monitoring of all Azure VNets 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:** A common platform across the entire IT environment enables consistent insight into network traffic in Azure, and other cloud environments, as in on-premises infrastructure. Acquire network traffic with minimal impact to Azure VM utilization and apply traffic intelligence before distributing to multiple tools for analysis.
- **Operational agility:**
  - – Rapidly detect changes in Azure VNets being monitored.
  - – Automatic Target Selection: A patented method to 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

© 2019 Gigamon. All rights reserved.

GigaSECURE Cloud Components

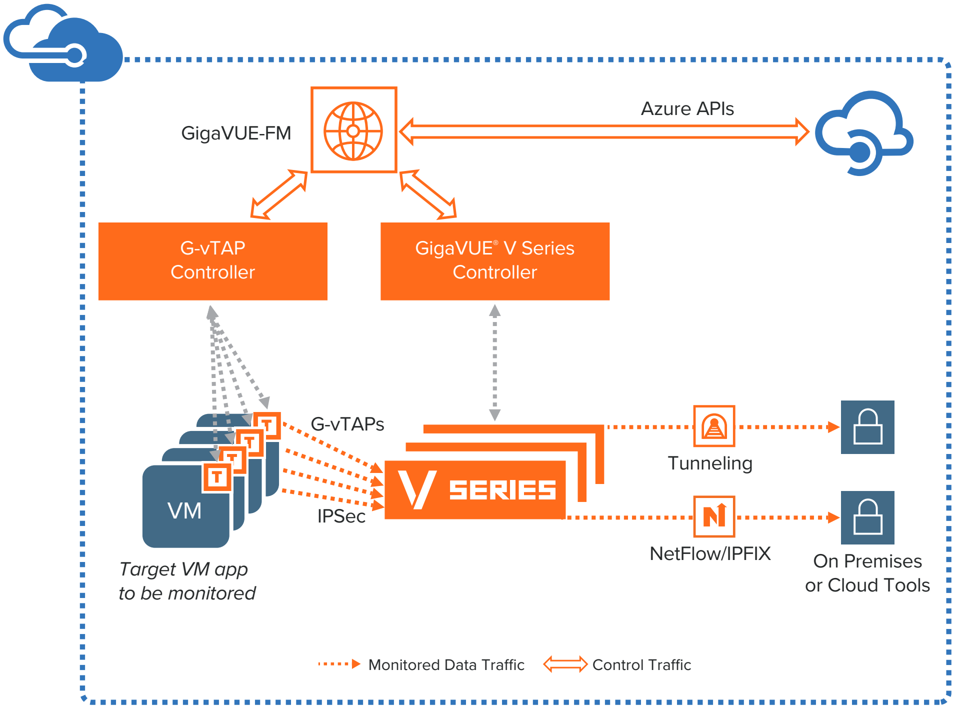
GigaSECURE Cloud is comprised of multiple components that enable traffic acquisition, traffic aggregation, intelligence and distribution along with single-pane-of-glass orchestration and management of the solution.

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

GigaVUE V Series – The GigaVUE V Series are visibility nodes in an Azure VNet 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 Azure, AWS and public clouds (e.g. 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-VNet 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.



© 2019 Gigamon. All rights reserved.

Features and Benefits

Solution Component	Key Features and Benefits
G-vTAP Agent Lightweight agent deployed on a VM. Mirrors traffic and sends via IPSec to GigaVUE V Series in visibility tier.	Minimize Agent Overload • Deploy one agent per Azure VM vs. having to deploy one per security tool. This approach lowers impact on VM CPU utilization.
	Reduce Application Downtime • Avoids need to redesign infrastructure to add new tool agents as applications scale out in Azure or as more operational tools are added.
	Scalability • As VMs scale out due to demand, the agent automatically scales due to the integration between GigaVUE-FM and Azure APIs.
	Minimize Production Changes • Option to use either the production Network Interface (NIC) or a separate NIC to mirror the workload traffic. The separate NIC option allows customers to preserve application traffic policies.
	Reduce Costs • 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 Visibility nodes that aggregate, select, optimize, and distribute traffic.	Traffic Aggregation • Acquire and aggregate traffic from multiple VMs. The traffic is acquired from the VMs using VXLAN tunnels.
	Traffic Intelligence: Select, Optimize and Distribute • 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. • 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 or maintain compliance. • 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 VMs 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 of the platform 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 Azure APIs to detect VM changes in the Azure VNet 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 VM instances.

Minimum Requirements for the GigaSECURE Cloud Components

Table 1: Recommended Minimum Compute Specifications

Solution Component	Minimum VM Type	Description
G-vTAP Agent	Standard_B1ms	Linux: Available as an RPM or Debian package. Windows: Available for Windows Server 2008/2012/2016
G-vTAP Controller	Standard_B1ms	Command-and-Control component for the G-vTAP agents
GigaVUE V Series Node	Standard_D2s_v3	Supports throughput up to 1000 Mbps. NIC 1: Data IP (mirrored traffic from G-vTAP) NIC 2: Tunnel IP (traffic to tools or on prem GigaVUE H/W) NIC 2: Management IP (commands from the controller)
GigaVUE V Series Controller	Standard_B1ms	Command-and-Control component for the V Series Nodes
GigaVUE-FM	Standard_D4s_v3	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.

© 2019 Gigamon. All rights reserved.

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 Azure Marketplace and Azure Government (US). Table 2 below lists the SKUs for procurement.

Table 2: Part Numbers for the Solution

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

- Azure Marketplace Metered – GigaSECURE Cloud can be purchased as a subscription from the Azure marketplace for 100 virtual tap points on an hourly basis. In this option, Azure 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, a NIC in an VM. A single VM could have multiple NICs that can be tapped. For example, if an application uses ten VMs with two NICs each, then the total Virtual TAP Points are 20.
- Try-and-Buy: Launch the BYOL offering in Azure 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 the BYOL model, GigaVUE-FM notifies the customer of the 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-AZU-100 or GFM-AZU-1000 at no additional charge.

Support and Services

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

© 2019 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.