

# GigaVUE-VM for VMware



## Quick Specs

- Automated traffic visibility for VMware-powered SDDC
- Optimized traffic delivery from the virtual infrastructure through the production network
- Automated migration of monitoring policies
- Hotspot detection of virtual monitoring policies

## Active Visibility for Virtual Workloads

With exponential growth in virtualized traffic within the data center, a primary challenge for the centralized monitoring infrastructure is to access this virtual traffic for application, network and security analysis. GigaVUE-VM for VMware provides an intelligent filtering technology that allows virtual machine (VM) traffic flows of interest to be selected, forwarded, and delivered to the monitoring infrastructure centrally attached to the Gigamon Visibility Platform, thereby eliminating any traffic blind spots in the enterprise private clouds or service provider NFV deployments.

Gigamon is the only vendor to provide traffic visibility solutions for virtual workloads in VMware-powered SDDC (ESXi and NSX) and powered multi-tenant clouds.

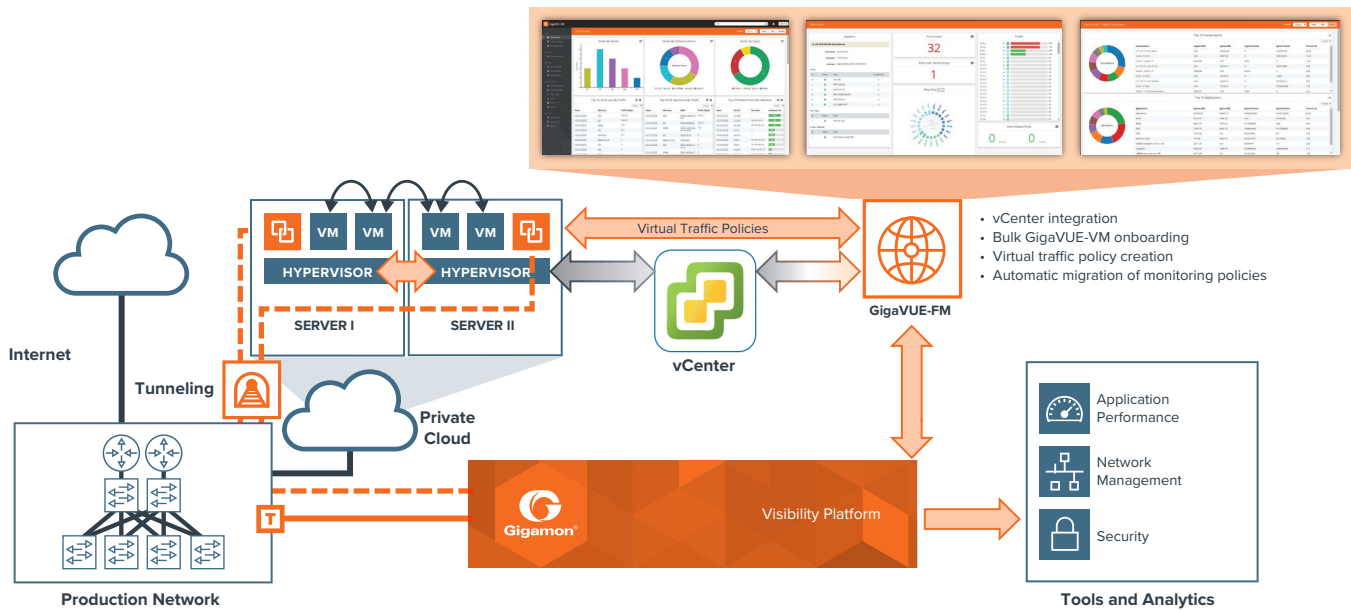
## Features & Benefits

- **Visibility into Virtual Traffic**—Intelligently select, filter, and forward tenant virtual traffic to the monitoring and tool infrastructure, extending the reach and leveraging existing tools to monitor virtual network infrastructure
- **Multi-Hypervisor Support**—Supports the most popular private cloud hypervisors, VMware ESXi and VMware NSX
- **Automated Visibility for VMware NSX**—Use VMware NSX Dynamic Service Insertion to associate visibility policies with security groups, thereby providing continuous and automated traffic visibility for applications as they scale up
- **Centralized Management**—Manage and monitor the physical and virtual visibility nodes using GigaVUE-FM while also configuring the traffic policies to access, select, transform, and deliver the traffic to the tools
- **Integration with the Gigamon Visibility Platform**—Seamless end-to-end visibility across physical and virtual network infrastructure. Optimize monitoring infrastructure by enabling aggregation, replication, and sharing of traffic streams across multiple monitoring tools and IT teams. Additional intelligence gained from Flow Mapping® and GigaSMART® technologies can be applied on the virtual traffic before forwarding the tools
- **Support for Packet Slicing**—Further reduce IO resources by removing irrelevant information with packet slicing before sending to the tool, and optimize long-term storage of data by capturing only the data of interest
- **Tunneling Support**—Leverage the production network to tunnel (support standards based L2GRE encapsulation) and forward the filtered virtual traffic from the hypervisor to the GigaVUE platforms

- **Optimized Traffic Delivery**—Tunneled traffic can be marked with DSCP values for per hop behavior to get preferential treatment on the production network. If changing MTU size in the network is an issue, fragmentation can be enabled to transport the packets using standard MTU sizes. These packets will then be re-assembled at the visibility nodes before further analysis
- **Support for vMotion and Live Migration**—Ensure the integrity of visibility and monitoring policies in a dynamic infrastructure, have realtime adjustment of monitoring and security posture to virtual network changes, and the ability to respond to disasters/failures without losing NOC insight and control
- **Hotspot monitoring**—Pro-actively monitor and troubleshoot GigaVUE-VM nodes by elevating Top-N and Bottom-N virtual traffic policies to the centralized dashboards

## VMware ESX Integration

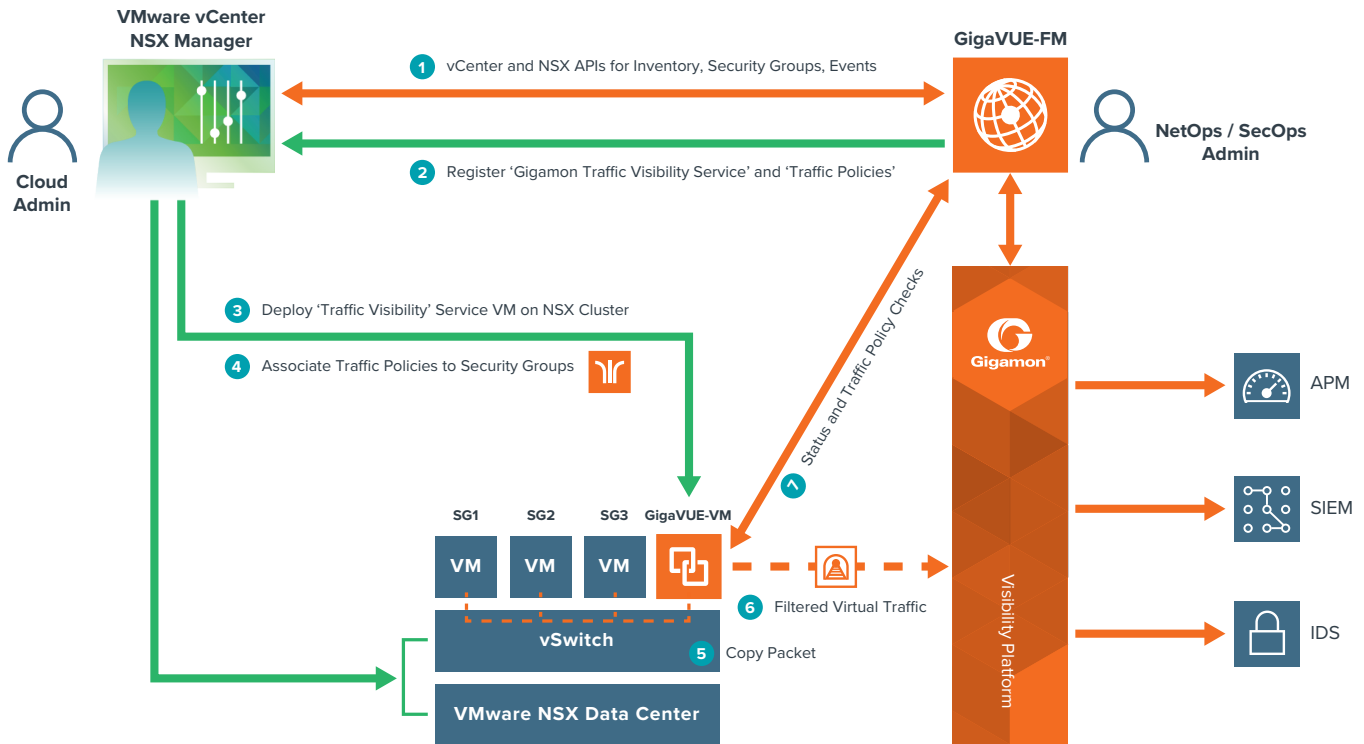
- A vSphere guest VM, the light footprint GigaVUE-VM visibility node is installed without the need for special software, kernel modules, or changes to the hypervisor
- GigaVUE-FM (Fabric Manager), Gigamon's centralized management application, tightly integrates with VMware vCenter and to facilitate simplified bulk onboarding of the GigaVUE-VM visibility nodes and configuration of the VM level traffic monitoring policies
- Leveraging vCenter APIs, GigaVUE-FM can track vMotion events across Distributed Resource Scheduler (DRS) and high-availability (HA) cluster environments, enabling visibility policies to be tied to the monitored VMs and migrate with the VMs as they move across physical hosts; this automation provides Active Visibility into an agile and dynamic SDDC
- GigaVUE-VM is auto-pinned to a host, so DRS doesn't impact continuous traffic visibility
- In addition to ESXi hypervisor, GigaVUE-VM also extends traffic visibility to the VMs deployed on the VMware NSX-V network hypervisor, a network virtualization platform that delivers the operational model of a hypervisor for the network



*GigaVUE-VM integrated with the Gigamon Visibility Platform*

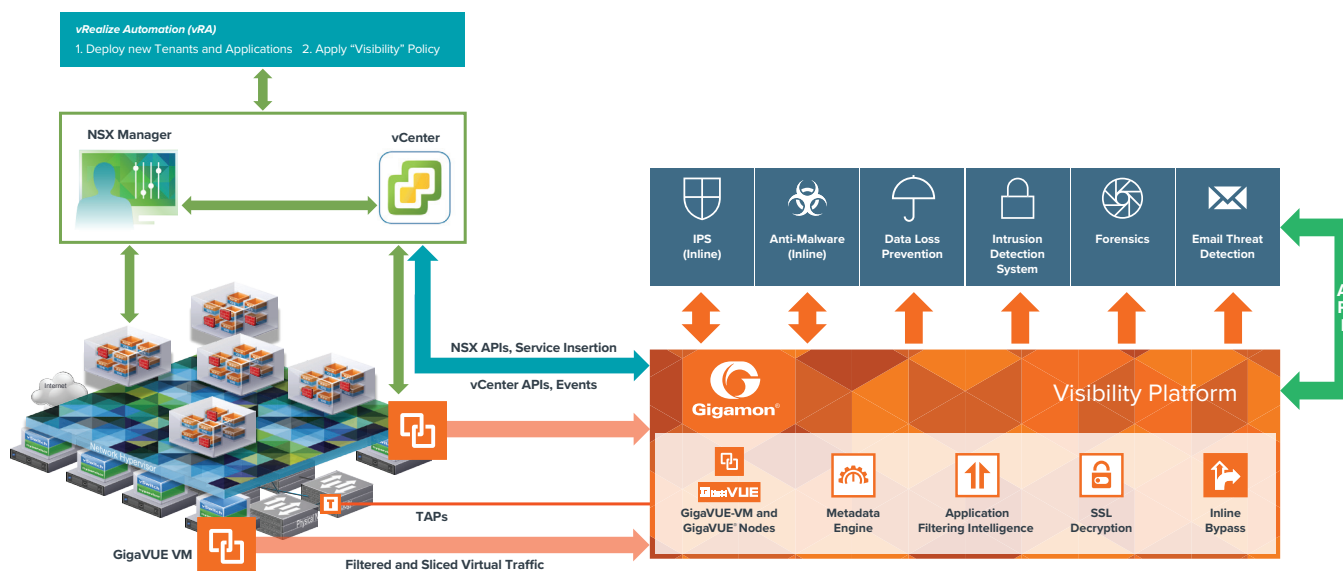
## VMware NSX Integration

- Automate traffic visibility for securing the micro-segmented SDDC
- Enable SecOps and NetOps teams to automate the selection, filtering and forwarding of the ever growing east-west virtual traffic for security and monitoring analytics
- Leverage the power of the NSX network virtualization platform and distributed service insertion framework for automated deployment of virtual components in the Gigamon Visibility Platform while also enabling dynamic provisioning of visibility traffic policies within customers' software defined data centers
- Insert a Visibility Service using the Gigamon platform's virtual visibility component, GigaVUE-VM
- Define security or traffic policies that select, filter and forward the tenant's virtual traffic to security and monitoring tools for analysis
- Can auto-update this service and the traffic policies as new tenants come onboard or existing tenant's security groups scale dynamically

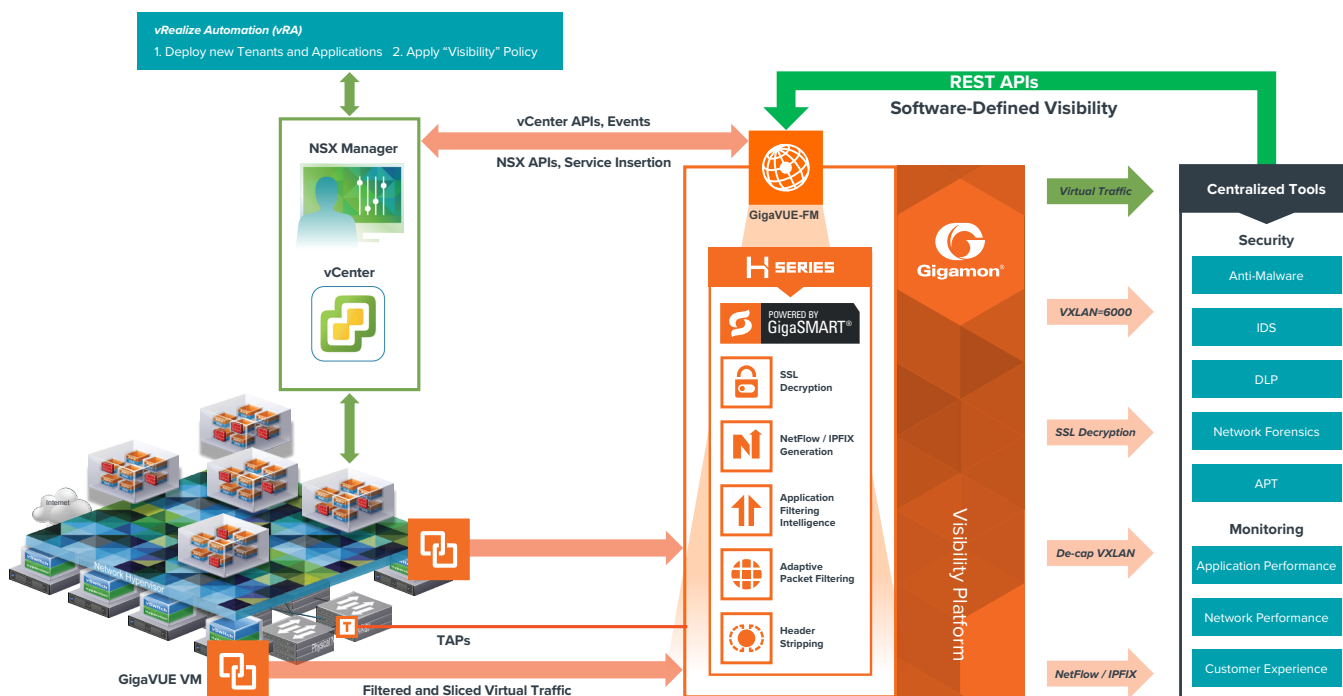


GigaVUE-VM on VMware NSX integrated with Gigamon Visibility Platform

## Use Cases with VMware NSX



Secure the SDDC with Gigamon Visibility Platform – Dynamic Service Insertion of GigaVUE-VM



Tenant level Traffic Visibility for Monitoring – Dynamic Service Insertion of GigaVUE-VM

## Use Cases

- Private clouds that want to provide SLA monitoring of the virtual workload traffic
- Data centers where virtual workload traffic needs to be analyzed along with the physical network traffic by a centralized monitoring tool infrastructure
- IT organizations that are concerned about threats or malware embedded in the SSL/TLS traffic within the virtual infrastructure
- Software defined data centers that are evaluating emerging network virtualization and SDN technologies
- Enterprises providing hosting services for multiple customers or internal groups
- Service providers adopting the Network Functions Virtualization (NFV) architecture to virtualize their physical network functions like SBC, EPC, IMS, etc.

