

Product Brief

GigaVUE-FM

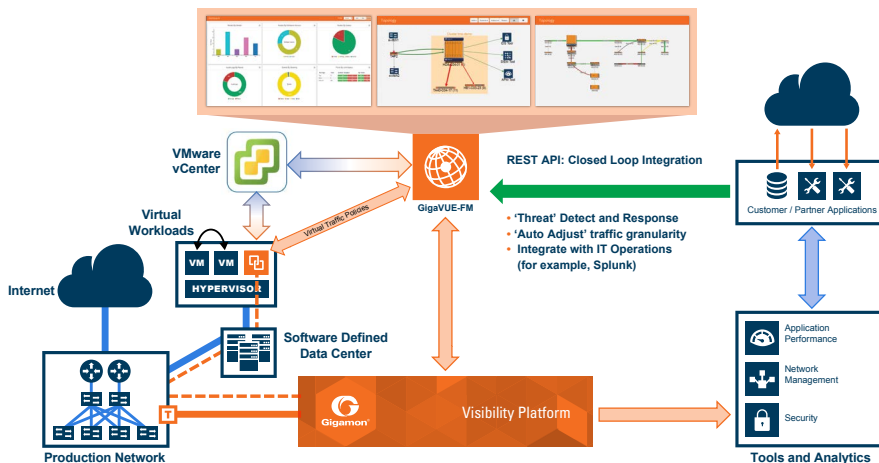


Available as a virtual or hardware appliance

Orchestration and Management of the Gigamon Visibility Platform

The Gigamon Visibility Platform delivers pervasive visibility across enterprise, data center, public cloud, and service provider environments to enable security, network, and application performance analytics and management. GigaVUE-FM delivers a single-pane-of-glass view of all the physical and virtual nodes across the Visibility Platform, while also providing a simple-to-use graphical user interface (GUI) to orchestrate the patented Flow Mapping® traffic policies, visualize network topology connectivity, and to identify visibility hot spots.

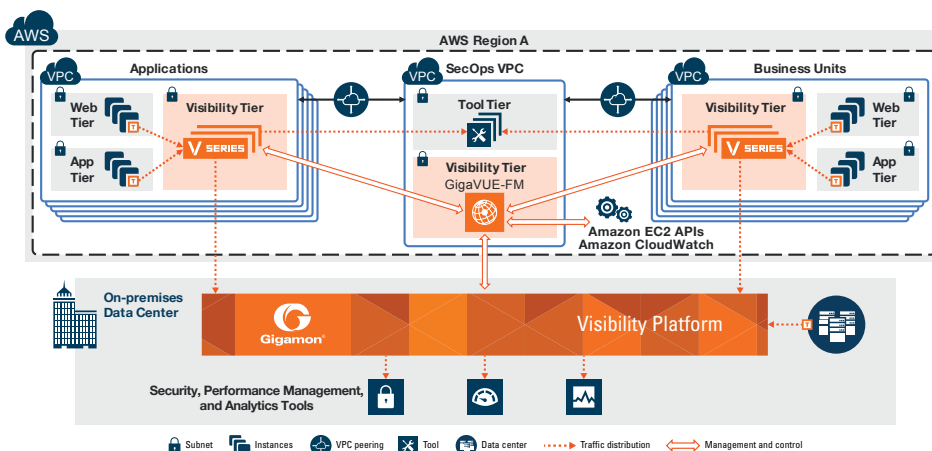
Use case: GigaVUE-FM for on-premises and private cloud visibility



Quick Specs

- ✓ Centralized Orchestration and single-pane-of-glass visualization of the Gigamon Visibility Platform deployed across the enterprise – on-premises, public, private, and hybrid cloud
- ✓ Grouping of Visibility Nodes, by sites, data centers, locations, etc. for hierarchical management and monitoring
- ✓ Auto-discovery and end-to-end topology visualization of the entire visible network
- ✓ Hot spot monitoring and live contextual search for faster MTTR
- ✓ Software-Defined Visibility and automation using REST APIs
- ✓ Automatic Target Selection for elastic and automated visibility for public cloud workloads
- ✓ Available as software-only virtual appliance or turnkey hardware appliance

Use case: GigaVUE-FM for public and hybrid cloud visibility



A single instance of GigaVUE-FM can manage hundreds of physical and virtual visibility nodes across multiple locations, data centers or AWS Virtual Private Clouds (VPCs). With tiered pay-as-you grow licensing, GigaVUE-FM also allows customers to grow their management capabilities proportional to the complexity and reach of their growing production networks.

GigaVUE-FM is available as both a software-only virtual appliance for VMware ESX, Microsoft Hyper-V, KVM, Amazon Machine Image (AMI) and as a hardware appliance for deployments where customers prefer a turnkey solution for management, or when the reach and scale of the Visibility Platform needs dedicated compute capacity for management.

The GigaVUE-FM software-only option is available at no charge for single physical node management and is also available as trials for customers wishing to try on-premises deployments or in public, private or hybrid cloud environments.

Features & Benefits

- **Centralized Management and Control**—Provides centralized management, monitoring, and configuration of the physical and virtual traffic policies for the Visibility Platform allowing administrators to map and direct network traffic to the security and monitoring tools for analytics.
- **Public, Private, and Hybrid Cloud Visibility**—Integration with Amazon EC2, CloudWatch, VMware ESX/NSX and OpenStack APIs to orchestrate the deployment and configuration of the Gigamon Visibility Solution for Public (V Series nodes) and Private Clouds (GigaVUE-VM), including automated visibility for elastic workloads in AWS and VMware NSX powered Software-Defined Data Centers (SDDC).
- **Auto Discovery of Network Topology**—Automatic discovery and topology visualization of the attached networks using Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) analysis from the sourced traffic. Using the Visibility Platform, NetOps and SecOps teams can trace back the production network interfaces that are detected to be at fault—this helps to drastically cut down on the mean time to resolution (MTTR).
- **End-to-end Topology Visualization with Traffic Overlays**—End-to-end visualization of edge-to-core connectivity between the Visibility Nodes, import and display connected production network switches, and pre-defined security and monitoring tools; overlay traffic policies from the ingress network port to the egress tool port.
- **Group-based Visibility**—Create hierarchical grouping of Visibility Nodes per site or location or data centers to allow for granular control and management.
- **Network-wide Reporting**—Summarize and customize dashboards for inventory, node/cluster status, events, audit trail, and Top-N/Bottom-N port/map usage with options to export and schedule HTML/PDF reports for offline viewing.
- **Advanced Monitoring with Faster MTTR**—Pro-actively monitor and troubleshoot hot spots in your visibility network:
 - Top-N, Bottom-N network/tool port and map usage widgets in the dashboard
 - Identify unhealthy traffic policies based on network and port operational status
 - Historical trend analysis (1 hour, 1 day, 1 week, 1 month) for port and traffic policies
 - Live contextual search to quickly troubleshoot hot spots (ports, traffic policies, VMs, IPs, MACs, etc.)
- **FabricVUE™ Traffic Analyzer**—Provides network-centric visualization of network traffic, allowing IT administrators to use GigaVUE-FM as a first-level dashboard to identify Top-N conversations, applications, end points, and protocols. Uses NetFlow/IPFIX records from GigaVUE® Visibility Nodes to collect and analyze network traffic:
 - That is being filtered out of the monitoring appliances
 - To identify any hot spots on new traffic that needs to be forwarded to the monitoring appliances
- **Programmable APIs for Software-Defined Visibility**—RESTful APIs that can be used by the traffic monitoring or IT operations management tools to discover the Visibility Nodes for inventory and status collection.
- **Gigamon Visibility App for Splunk**—Enables integration of the Visibility Platform inventory, health, port, and traffic insight into Splunk Enterprise. This application, available at no charge from the Splunk App Store (splunkbase), uses REST APIs to periodically collect information from GigaVUE-FM and display the data within the Splunk dashboards.

Use Cases

- Centralized Operations Center looking to configure, direct, and control traffic from any network (public, private, hybrid cloud, on-premises data centers or service provider networks) to the security or monitoring tools for analysis
- Network security team that is chartered with detecting, reacting, and responding to emerging threats based on packet- or flow-based traffic analysis
- SecOps and NetOps teams tasked to monitor and troubleshoot traffic hot spots with the help of the Gigamon Visibility Platform