GigaVUE-FM

Centralized Orchestration and Management of the Gigamon Deep Observability Pipeline with AI Assistance

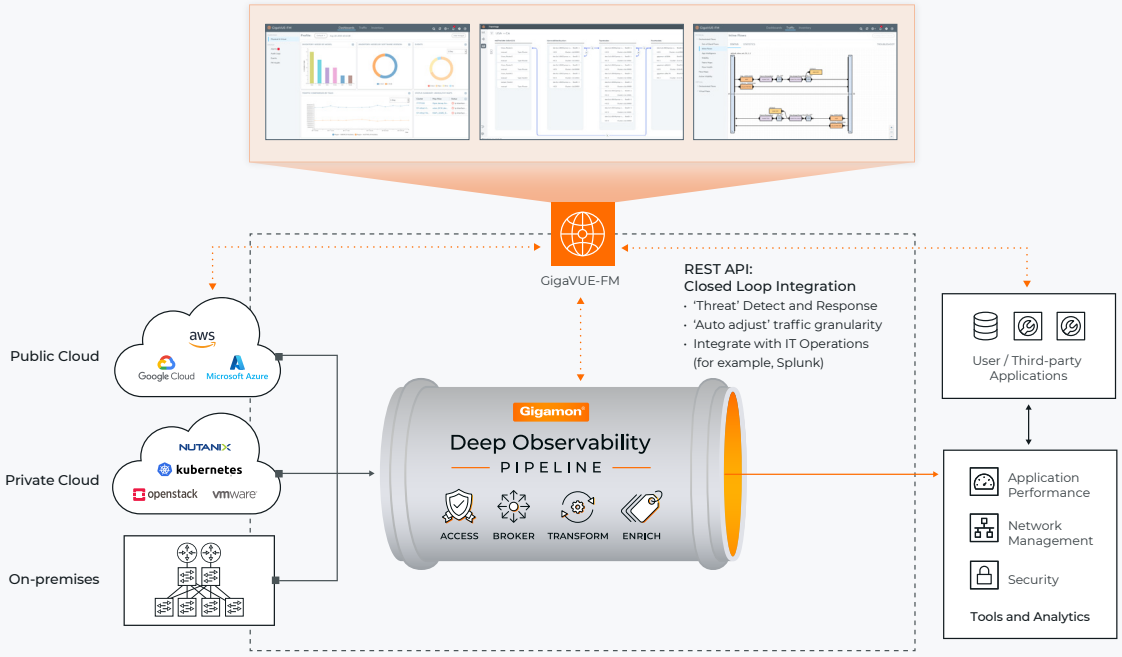
GigaVUE-FM is available both as a physical (shown above) or virtual appliance.

Management - Configuration - Orchestration - Automation - Health - Alarms

Key Benefits

- Centrally manage, monitor, and configure traffic policies for all Gigamon nodes
- Accelerate and simplify onboarding, simplify operations, and troubleshoot faster at scale with assistance from GigaVUE-FM Copilot
- Integrate with public and private cloud platforms
- Reduce the mean time to resolution (MTTR) of traffic hot spots for NetOps, CloudOps, and SecOps teams with auto-discovery of network topology
- Assign rights to specific roles based on the user's job function to lower risk exposure and prevent accidental changes with role-based access control (RBAC)
- Provide business continuity with high availability (HA) for GigaVUE-FM instances
- Expedite and reduce manual effort for Gigamon Deep Observability Pipeline deployments via automation and bulk configuration management using REST APIs and Ansible Automation
- Run GigaVUE-FM natively in AWS and Azure Government Secret and Top Secret regions with secure, custom CA–based TLS to non-public endpoints, so even your most sensitive workloads get consistent visibility and control
- Enable government and defense organizations to standardize on a single deep observability platform across commercial and IL6 environments
- Support importing custom root CAs into the GigaVUE-FM trust store for secure TLS connectivity to isolated, air-gapped AWS and Azure Gov service endpoints, maintaining compliance while eliminating monitoring blind spots

© 2026 Gigamon. All rights reserved.



GigaVUE-FM manages all Gigamon visibility nodes: physical, virtual, and cloud (the Gigamon Deep Observability Pipeline).

Use Cases

- Centralized operations centers looking to configure, direct, and control traffic from any network (public, private, hybrid cloud, on-premises data centers, or central offices) to security and monitoring tools for analysis
- Reduce configuration errors and simplify deployments with less training and more real-time guidance using GigaVUE-FM Copilot
- Network security teams tasked with detecting, reacting, and responding to emerging threats based on packet- or flow-based traffic analysis
- Using the Gigamon Deep Observability Pipeline to monitor and troubleshoot traffic hot spots
- Operations teams aiming to reduce cost and improve efficiency through automation

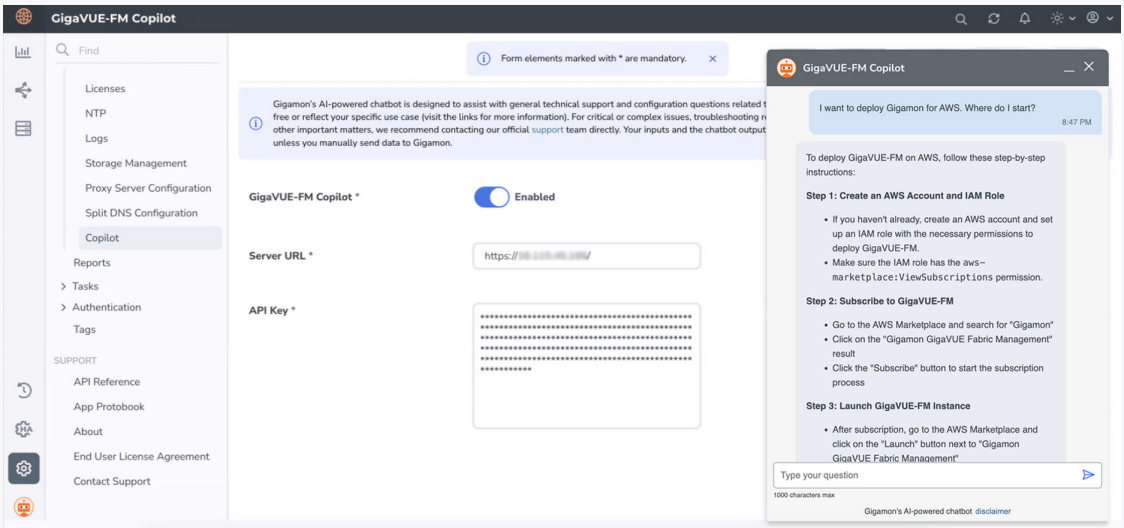
Introduction

GigaVUE-FM provides centralized orchestration and a single-pane-of-glass view of all physical, virtual, and cloud-based nodes in the Gigamon Deep Observability Pipeline. Its intuitive GUI makes it easy to manage the entire Gigamon footprint across your hybrid cloud. The Gigamon Deep Observability Pipeline delivers network-derived telemetry—packets, flows, and metadata—to the right security, performance, and observability tools. This empowers organizations to eliminate blind spots, optimize network traffic, and lower cost and complexity.

AI Assistance

GigaVUE-FM Copilot is an optional AI-powered assistant that simplifies operations, accelerates onboarding, and helps teams realize the full value of their Gigamon deployment more quickly. Integrated directly into GigaVUE-FM, Copilot uses natural language interaction to guide users through tasks,

© 2026 Gigamon. All rights reserved.



GigaVUE-FM Copilot ccelerates and simplifies onboarding, operations, and troubleshooting.

troubleshoot issues, assist with configurations and deliver contextual insights in real time. By reducing operational complexity and providing expert guidance when it's needed most, Copilot enhances operational efficiency and boosts confidence in securing and managing hybrid cloud infrastructure.

Built for scale

A single instance of GigaVUE-FM can manage up to 1,000 Gigamon physical visibility nodes across multiple locations, data centers, public and private clouds, and up to 3,000 in high-availability cluster arrangements. GigaVUE-FM helps protect against failure and lets you scale seamlessly as the size and complexity of your networks grow.

GigaVUE-FM is available as a software-only virtual appliance for AWS AMI, KVM/OpenStack, Microsoft Azure/Hyper-V, Google Cloud Images, Nutanix AHV, and VMware NSX/ESXi. It is also available as a hardware appliance for deployments where turnkey solutions are preferred. The GigaVUE-FM software-only option is available at no charge for cloud-only visibility and/or when managing a single physical device only.

GigaVUE-FM now supports AWS and Azure Government Secret and Top Secret regions, including custom CA–based TLS to non-public endpoints. Agencies can extend the same deep observability, centralized control, and compliance posture from commercial clouds into IL6 workloads—without redesigning their visibility architecture.

© 2026 Gigamon. All rights reserved.

Table 1. Key Features and Benefits

Centralized Management	Centralizes management, monitoring, and configuration of physical and virtual traffic policies for all Gigamon nodes. Administrators can better map and direct network traffic to security, network, and application-performance monitoring tools.
GigaVUE-FM Copilot	Embedded AI assistant in GigaVUE-FM simplifies configuration and management. It provides AI-powered search across documentation for faster troubleshooting and self-service. Install on AWS via the marketplace, or on your own VM with an OVA file from the VUE community.
High Availability	GigaVUE-FM provides high availability in a group of three, ensuring no loss of management or view across the Gigamon Deep Observability Pipeline if an active FM goes offline
Tool View	Facilitates tool capacity planning by: • Ensuring the tool is optimally utilized • Empowering users to select the best tool to route network traffic based on resource availability • Tracking tool storage capacity and data wraparound time
Visibility Policy Workflows	Simplifies visibility policy configuration for: • Inline security tools, including traffic forwarding and bypass • Visibility into encrypted traffic with inline SSL/TLS decryption • Application-aware filtering and metadata • Flow Mapping across hundreds of nodes in one or more clusters
Traffic Policy	Provides a unified, intent-based way to describe how traffic is filtered, processed, and delivered to monitoring and security tools. Consolidates multiple maps and per-node configurations into a single policy, cutting change time and reducing misconfigurations for hardware deployments.
Fabric Health Analytics	Advanced dashboards for monitoring the health of the Gigamon Deep Observability Pipeline and identifying hot spots
Alarm Management	Reduces mean time to resolution (MTTR) by providing root cause of a fault in the fabric. Provides accurate node health information and granular alarm views for easier troubleshooting and serviceability.
Integrated PCAP on IP interfaces	Extend packet capture beyond physical ports to IP interfaces, allowing operators to trigger ingress, egress, or bidirectional captures directly from the GigaVUE-FM IP Interface page. Speeds troubleshooting of control-plane and management-plane issues without requiring CLI access
Network-wide Reporting	Provides summarization and customization of dashboards for inventory, node/cluster status, events, and audit trail with options to export and schedule HTML/PDF reports for offline viewing
Customer Deployed Assets (CDA) Reporting	Produces on-demand and scheduled reports of all deployed Gigamon hardware and software by SKU, version, and location. Simplifies true-ups, renewals, and compliance attestations by giving operations, finance, and audit teams a single, authoritative source of asset truth.
Visibility Fabric Topology	Displays physical deployment and interconnectivity, grouping nodes based on user-defined tags to match the physical data center and for hierarchical management and monitoring
Spine Source Map Mode	Add a global mode (SEPARATE/COMBINE) that controls whether GigaVUE-FM creates one cluster-level spine-source map per spine or a single combined map across all spines. Improves scalability and correctness for large multi-spine fabrics by aligning fabric maps with actual traffic paths.
License Management	Manages GigaSMART® application licenses for the Gigamon Deep Observability Pipeline and floating licenses between duplicate HC Series nodes

© 2026 Gigamon. All rights reserved.

Task Scheduling	Automates future and periodic actions including: • Scheduling of firmware version updates to one or many visibility nodes • Scheduling of visibility node configuration backups that allow you to restore a good baseline if inadvertent changes are applied • Back up and restoration of the GigaVUE-FM configuration database to allow for GigaVUE-FM appliance replacement or restoration to a well-known configuration
Programmable Integration Interfaces	Includes REST XML API, Ansible – Automation SDK which facilitates operations teams to: • Automate bulk fabric configurations, reducing the overall time for fabric deployments • Integrate inventory, health, port, and traffic insights of the Gigamon Deep Observability Pipeline into Splunk Enterprise for correlation and analysis • Integrate with cloud and virtual infrastructure managers like Amazon CloudWatch, Microsoft Azure Resource Manager, Google Cloud Operations Suite, OpenStack Horizon, and VMware ESXi/NSX-T • Empower traffic monitoring or IT operation management tools to discover deep observability pipeline nodes for inventory and status collection
IL6-Ready Cloud Integration (AWS and Azure)	Extend GigaVUE-FM integration to AWS and Azure Government Secret and Top Secret regions, including support for custom root CA imports and secure TLS to isolated endpoints. Enables government and defense organizations to standardize on a single deep observability platform across both commercial and IL6 environments.
Role-Based Access Control (RBAC)	Allows users to be assigned specific roles based on their function to increase security and prevent unauthorized changes. Create, read, update, and delete operations at granular levels using tags.
Single Sign-On (SSO)	Simplifies secure single sign-on access including, HA deployments, to enterprises by integrating with identity and access management (IAM) vendors such as Okta
Automatic Certificate Management Environment (ACME)	Automates updating of authentication certificates from an enterprise's certificate management and repository systems
Certifications	FIPS 140-3 Inside #4912

Table 2. Hypervisor Requirements for Software Edition

Requirements	Support up to 50 Devices	Support up to 500 Devices	Support up to 1,000 Devices	Support up to 3,000 Devices (FM-HA Mode)
Memory	16GB	32GB	128GB	128GB
Virtual CPU (vCPU)	2	4	12	12
Virtual Storage for OS	40GB	40GB	40GB	40GB
Virtual Network Interface	1	1	1	1
Number of FM nodes	1	1	1	3

- Devices include HC Series and/or TA Series nodes
- Requirements are tested and verified based on VMware ESXi 6.7.0. Microsoft Hyper-V (Windows Server 2008 R2 SP1 and later, 2012 R2 and later) and KVM are supported, but scaling is not verified
- CPU Min. Speed 2.3GHz

© 2026 Gigamon. All rights reserved.

Table 3. Hardware Appliance Product Specifications*

Feature	Description
Rack mounting	• One rack unit (1RU) • Tool-less mounting in 4-post racks with square or unthreaded round holes • Tooled mounting in 4-post threaded hole racks • Cable management arm
Dimensions	• Height: 1.68 in. (42.8 mm) • Width: 18.97 in. (482.4 mm) • Depth: 29.85 in. (748.8 mm)
Weight	15.9 kg (35 lbs)
Operating system	GigaVUE-FM OS (Gigamon appliance-hardened Linux)
Processor	Dual Intel Xeon 2.0GHz, 20C/40T
Memory	256GB RAM (expandable up to 384GB RAM)
Storage	• OS: 1 x 480GB SSD SATA drive • Data: 2 x 2.4TB HDD (RAID1, 2TB usable)
Management	• IPMI 2.0 compliant • 2 x 100/1000M Base-T LAN
Power supply	• Dual, hot-plug, redundant power supply (1+1) • 800W (Platinum) AC (100–240V, 50/60Hz, 9.2A-4.7A)
Heat dissipation	3000 BTU/hr
Temperature	• Operating: 10° C to 35° C (50° F to 95° F) • Storage: -40° C to 65° C (-40° F to 149° F)
Maximum altitude	• Operating: 3,048 m (10,000 ft) • Storage: 12,000 m (39,370 ft)
Connectors	Back • 2 x 10/100/1000Mbps LOM • 2 x 10/25Gbs SFP28 • 2 x 100Gbps QSFP56 • 1 x iDRAC9 Ethernet port • 1 x USB 3.0, 1 x USB 2.0 • 1 x DB15 VGA Front • 1 x USB 2.0 (disabled in BIOS) • 1 x iDRAC Direct (Micro-AB USB) • 1 x DB15 VGA

* Applicable to GigaVUE-FM Hardware Appliance SKU GFM-HW2-FM001-HW

© 2026 Gigamon. All rights reserved.

Table 4. Scalability

Configuration	Basic (ESXi-VM)	Medium (ESXi-VM)	Large (ESXi-VM)	Extra Large (FM Hardware Appliance)
CPU Specification				
CPU count (minimum)	2	4	12	32
CPU Min speed (per CPU)	2.30GHz	2.3GHz	2.3GHz	2.10GHz
Memory Specification				
Memory Size	16 GB	32GB	128GB	128GB
Appliance Scalability				
Number of HC Series/TA Series nodes (Up to)	50	500	1,000	1,000
Disk Specification (Standalone)				
OS disk size	40GB	40GB	40GB	40GB
Config disk size – 15 Days data	80GB	620GB	1100GB	1100GB
Config disk size – 35 Days data	160GB	1240GB	2200GB	2200GB
Config disk size – Daily Index 35 days + 120 Days Rollup	200GB	1600GB	2500GB	2500GB
Disk Specification (FM High Availability Mode – For Each FM)				
OS disk size	40GB	40GB	40GB	40GB
Config disk size – 15 Days data	80GB	620GB	1600GB	1100GB
Config disk size – 35 Days data	160GB	1240GB	3000GB	3000GB
Config disk size – Daily index 35 Days data (+ Data rollup for 120 Days)	200GB	1600GB	4300GB	4300GB
Appliance Scalability				
Number of HC Series/TA Series Nodes (Up to)	50	500	3,000	3,000

Note: When deploying FM in ESX use “reservation” option and allocate fixed resource for CPU and memory.
For TLS/SSL advanced dashboards, minimum GigaVUE-FM requirements are Medium (ESXi-VM) or higher.

© 2026 Gigamon. All rights reserved.

Table 5. Compliance and Scalability

Type	Description
Table 5A. Compliance*	
Safety	IEC 60950-1 IT equipment; EN 60950-1 IT equipment
Emissions	FCC Part 15, Class A; EN55022/CISPR-22 Class A; CISPR 24; GOST Russia; CE Mark EN 5502 Class A; Industry Canada ICES-003 Class A; EN 55024; KCC Korea; CCC China
Environmental	RoHS Directive 2011/65/EU; Global ENERGY STAR 3.0; REACH Directive; CECP China
Table 5B. Scalability	
Physical Instance	Up to 1,000 nodes with a single instance and up to 3,000 in a cluster.
Virtual Instance	Up to 1,000 G-vTAP agents with 100 GigaVUE V series nodes.

* Applicable to GigaVUE-FM Hardware

Table 6. GigaVUE-FM Copilot Requirement

In order to run the GigaVUE-FM Copilot AI function, a separate VM is required, in addition to the host that runs GigaVUE-FM. This separate VM can be a VMware instance or AWS instance, and has the following requirements:

VMware ESXi Hardware Requirements
The following table describes the hardware requirements on VMware ESXi to run GigaVUE-FM Copilot.

VMware Hypervisor	vSphere ESXi: v8.xx and above. Refer to Supported Hypervisors for VMware for more detailed information.
CPU	Minimum 4 vCPUs
RAM	At least 16GB
Disk Space	At least 204GB shared (FC, iSCSI, NFS, or FCoE) or locally attached storage (PATA, SATA, SCSI)
Nertwork	At least one 1Gb NIC

AWS Instance Requirements
GigaVUE-FM Copilot can run on EC2 Instance Type m5.xlarge.

© 2026 Gigamon. All rights reserved.

Open Ports Access Requirements
The following table describes the open ports access requirements.

Protocol	Port Number	Service	Source IP Address	Purpose
TCP	22	SSH	Administrator Subnet	Allows CLI access to user-initiated management and diagnostics.
TCP	443	HTTPS	Administrator Subnet	Allows GigaVUE-FM GUI access the GigaVUE-FM Copilot. The chat with Copilot from GigaVUE-FM GUI directly reaches the GigaVUE-FM Copilot.
TCP	443	HTTPS	GigaVUE-FM	Allows GigaVUE-FM to reach GigaVUE-FM Copilot for configuration and health check.
TCP	443	HTTPS	GigaVUE-FM	Copilot LLM Service Providers (Amazon Bedrock): https://docs.aws.amazon.com/general/late st/gr/bedrock.html Allows GigaVUE-FM Copilot to Amazon Bedrock for LLM access
TCP	443	HTTPS	GigaVUE-FM	Copilot Azure: • login.microsoftonline.com • scp1adls1.blob.core.windows.net Export the AI Usage Telemetry Data

Additional Connectivity Requirements
GigaVUE-FM Copilot requires outbound access to AWS Bedrock and Azure Blob Storage. Actual URLs are region-specific and can be found in technical documentation.

Support and Services

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

About Gigamon

Gigamon® delivers an AI-powered Deep Observability Pipeline that provides network-derived telemetry to cloud, security, and observability tools. With AI-driven insights across packets, flows, and application metadata, organizations gain complete visibility into all data in motion to detect threats concealed in encrypted and lateral traffic, resolve network and application performance issues, and validate compliance while reducing operational cost and complexity. Gigamon is trusted by 4,000+ organizations, including 83 of the Fortune 100 and hundreds of public sector agencies and educational institutions. Learn more at gigamon.com.

Gigamon®

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

© 2019-2026 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at 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.