GigaVUE Operating System

The proven and extensible operating system for Gigamon visibility nodes

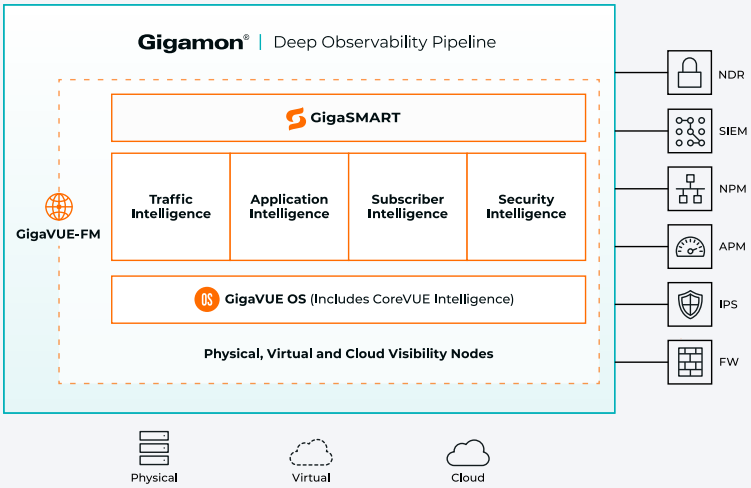

Figure 1. GigaVUE-OS is the underlying software that drives all physical GigaVUE® appliances.

Key Benefits

- Rich network visibility, management and data-delivery services
- Select traffic of interest through user-defined map rules
- Combines multiple devices to be managed as one logical node
- Load shares across multiple tool instances of the same type
- Replicates traffic across multiple tools
- Enables network traffic visibility into cloud and remote sites for cloud-based or on-premises tools
- Makes security and performance monitoring tools more effective

As a key element within the Gigamon Deep Observability Pipeline, the GigaVUE-OS software provides the basis for the GigaVUE HC Series and GigaVUE TA Series products to perform aggregation, replication, filtering, tunneling, header stripping, forwarding and traffic distribution at scale. These network packet brokers are ideal choices to enhance your security and performance monitoring solutions. GigaVUE-OS is also used on G-TAP A Series 2 for management through SSH CLI and/or GUI and/or API with GigaVUE-FM.

GigaVUE-OS enables the Gigamon Deep Observability Pipeline to provide traffic intelligence across 32 clustered nodes, greater network traffic visibility into data-in-motion, minimized traffic overloads, and more effective options for deploying both inline and out-of-band security and performance monitoring tools.

The Solution: GigaVUE HC Series and GigaVUE TA Series

The foundational GigaVUE-OS service provides the ability to select traffic flows of interest using our patented Flow Mapping® mechanism.

Flow Mapping takes line-rate traffic at 100Mb, 1Gb, 10Gb, 25Gb, 40Gb, 100Gb, or 400Gb from various sources — such as visibility nodes, network taps, virtual taps, and mirror/SPAN ports across physical, virtual, and cloud networks — and sends it through a set of user-defined map rules to tools that secure, monitor, and analyze your network infrastructure. You can optimize tools by sending only traffic of interest and dropping all irrelevant traffic.

GigaStream load sharing distributes network traffic to multiple monitoring tools, allowing you to group multiple tool ports into a logical bundle that can scale as your monitoring needs grow. It provides tools with complete traffic flows, maintaining the integrity of sessions, providing full visibility for security and application monitoring. Tool weighting and session sampling further optimize tool performance while tool failover provides high availability.

MPLS and VxLAN protocol header-stripping allows monitoring and security tools that don't understand these network-encapsulation protocols to see into the encapsulated packets or remove the need for them to remove these protocols themselves, thereby making the tools more effective and efficient.

L2GRE and VXLAN tunnel initiation, encapsulation, termination, and de-encapsulation provides network traffic visibility into cloud and remote sites for cloud-supported or on-premises tools.

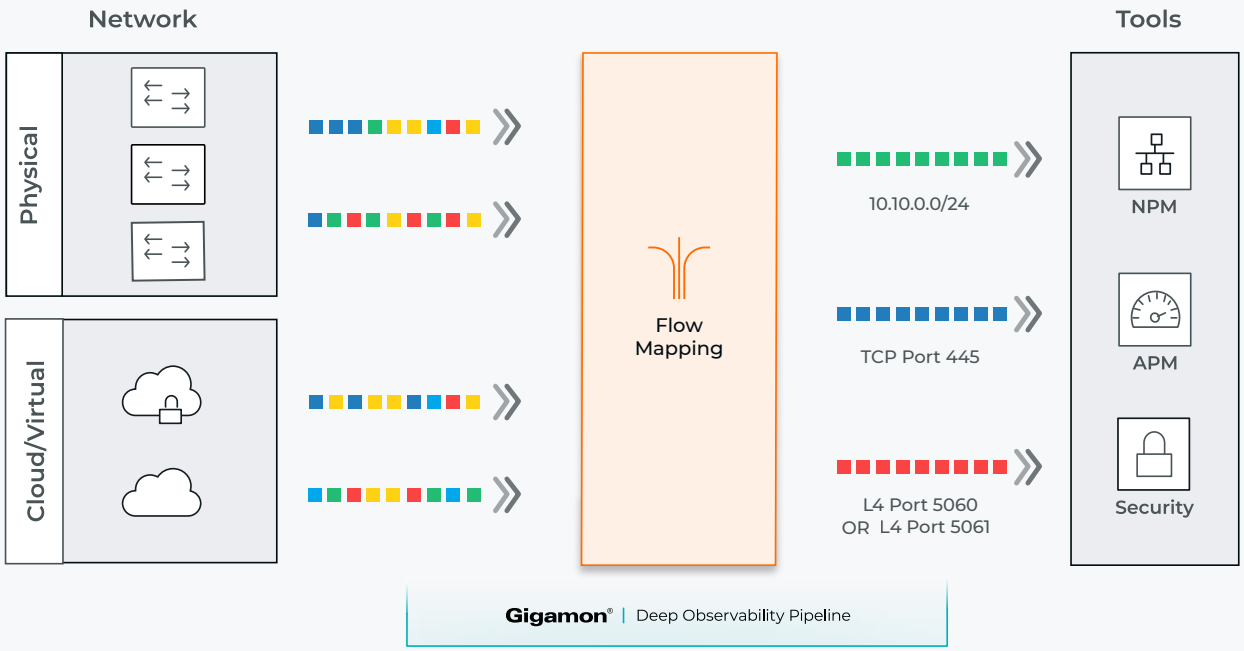

Figure 2. Flow Mapping — a key GigaVUE-OS feature.

Clustering lets you manage multiple heterogeneous nodes with different underlying hardware capabilities running GigaVUE-OS as a single logical unit. This unique service allows advanced capabilities in GigaSMART® modules to be accessed anywhere within the logical unit even if, for example, traffic arrives on a unit in the cluster that does not have hardware resources natively within it.

In addition to Gigamon hardware, GigaVUE-OS is also available on select whitebox hardware. This lets you extend the rich visibility services GigaVUE-OS offers into whitebox deployments.

GigaVUE-OS supports multiple management methods, including GigaVUE-FM, web interface, SNMP, and command line interface (CLI). GigaVUE-FM also offers a REST XML API.

Top Use Cases

Network Operations

- Replicate and/or distribute traffic across multiple network, security, and monitoring tools based on a programmable rules engine.
- Combine core capabilities in GigaVUE-OS with GigaSMART traffic intelligence to maximize tools performance and ROI.

Security Operations

- Create a deep observability pipeline that greatly expedites deployment of inline, out-of-band, and flow-based tools across the network.
- Improve overall network performance and uptime during upgrades.

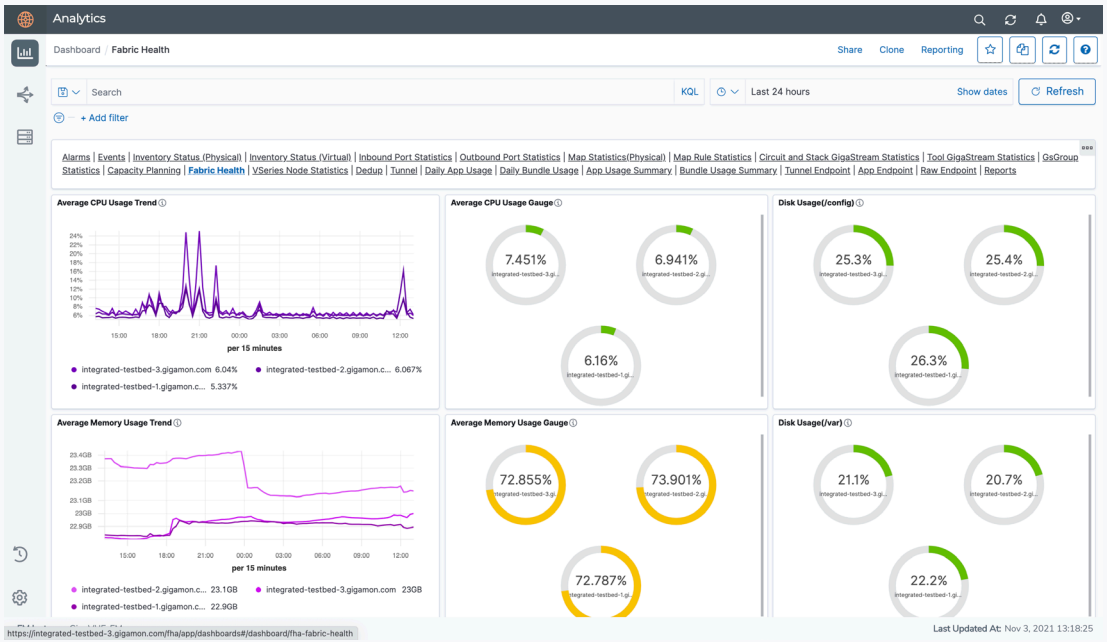

Figure 3. Fabric Health Analytics visualized via GigVUE-FM.

GigaVUE-OS powers the core and edge visibility nodes in the Gigamon Deep Observability Pipeline. Implemented in the most demanding Fortune 100, government agency, and large service-provider environments, GigaVUE-OS provides the reliability required to help ensure acurate and reliable visibility into physical infrastructure.

Key Features and Benefits

System	Modular and portable Linux-based OS Rich network visibility, management, and data-delivery services
	Port configurability: • Full flexibility in selecting ports as ingress, intermediate, interconnect, or egress functions • Unidirectional and bi-directional ports • Tunneling ports, ingress and egress • Enable agile response to changes in monitoring infrastructure and monitoring needs • Facilitate passive out-of-band and active inline monitoring via the same node • Allow virtualized traffic to be accessed, or backhauled between locations, over an IP network
	Local and remote management using: • Command line interface (CLI) • SSH • XML API (HTTP/HTTPS)* • GigaVUE-FM (HTTP/HTTPS) • SNMP (v1, v2, v3) • Syslog • Easy to manage via GigaVUE-FM GUI or via CLI • Easy integration with applications using CLI or RESTful API* • Manage and orchestrate traffic across an entire cluster of nodes from a single login
	User access: • Role-based access control (RBAC) – Multi-tenant user access – Flexible user/role defined privileges, screen views, and access – Port sharing and locking – Map sharing across users • AAA security with local and remote authentication (LDAP, RADIUS, TACACS+) • Automatic Certificate Management Environment (ACME) • Adhere to corporate IT security and authentication policies • Automates updating of authentication certificates from an enterprise's certificate management and repository systems

* In conjunction with GigaVUE-FM

Core Intelligence	**Flow Mapping®, including:** • Aggregation and replication – Selective any-to-any port mapping • Filtering – Layer 2 to 7 rules – Customizable bitmask filters – Ingress and egress pass and drop filtering • Load sharing – Layers 2 to 4 hashing criteria – Session continuity even during tool failover – Tool weighting – Packet Sampling • Access traffic from any link to any tool, even for different link rates • Optimize tools by only forwarding traffic of interest or dropping traffic not of interest
	Clustering and Fabric Maps • Enable resilient traffic forwarding • Manage up to 32 nodes in a cluster as a single logical node • Enact end-to-end Flow Mapping, across clusters, scaling to hundreds of nodes with fabric maps orchestrated through GigaVUE-FM
	Tunneling: L2GRE & VXLAN • Termination/decapsualtion – Receive traffic from remote sites or virtual nodes in private and public cloud – Apply additional filtering and processing before sending to centralized tools • Initiation/origination/encapsulation – Share traffic across physical data centers or remote sites – Forward traffic to viritualized or cloud-based tools
	Protocol header stripping (MPLS, VLAN, VXLAN) Remove network headers that can interfere with tools' ability to effectively analyize traffic
	Source port tagging with VLAN tags Improve tool analysis and troubleshooting by tagging source of traffic Identify traffic using map- and rule-based tagging for more efficient analysis and troubleshooting
	IP and MAC address modification • Obscure original IP and/or MAC information to meet privacy needs while retaining ability to distinguish traffic sources. • Allow certain tool types to ingest traffic that meets specific IP and MAC address requirements.
	Device and link discovery with ARP and LLDP Identify and correlate traffic sources within the network for easier management and troubleshooting

Core Intelligence cont'd	**Inline Bypass:** • Inline network protection for 100M up to 400G for both copper and fiber network links • Remove points of network failure due to malfunctioning inline tools • Protect multiple network segments • Easily configure simple and complex tool chains • Select which traffic goes to which tools, in which order, and which traffic gets bypassed. • Distribute traffic across multiple tools of the same type for increased scalability and failover • Customizable heartbeat packets for positive (through-path) and negative (block) tests • Provide full visibility for each inline security tool type (for example, IPS, WAF) • Easily deploy security in layers solutions, for both active and passive scenarios • Seamlessly migrate tools from passive out-of-band monitoring to active inline mode
Compliance	• FIPS 140-2 Level 1, Common Criteria, DoDIN APL • USGv6r1 • NIAP Common Criteria

Support and Services

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

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

For more information about the Gigamon Platform or to contact your local representative, please visit gigamon.com.

Gigamon®

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

02.25_08