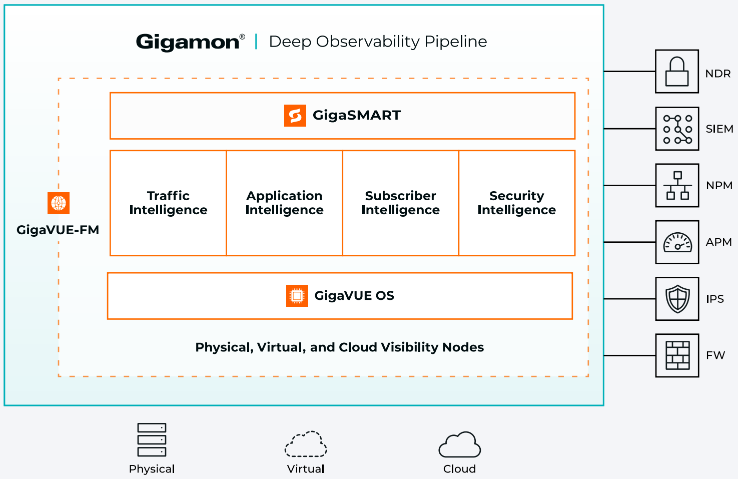
GigaSMART Intelligent Traffic Handling

Gigasmart is a Set of Intelligent Applications That Improve Network Visibility, Performance, and Security



Key Benefits

- Drop duplicate packets and eliminate superfluous header and payload content to improve tool accuracy and efficiency
- Offload NetFlow generation from routers and switches to focus on their core function
- Filter streaming media or any application to optimize tools capacity
- Identify and block rogue or shadow IT applications
- Find and throttle back or stop bandwidth hogs to improve network performance
- Generate contextual metadata to expedite and simplify incident detection and response and expedite troubleshooting and remediation
- Automatically identify, decrypt, and deliver TLS/SSL traffic to multiple tools for inspection, ensuring comprehensive visibility into encrypted traffic
- Precisely control exposure of personal information (SSN, credit card number, etc.) and stay compliant with regulatory requirements such as HIPAA and GDPR
- Leverage key service provider network features to offer superior mobile end-user performance in advanced 5G environments
- Application metadata JSON export over KAFKA, and application metadata export to partner tools
- Easily deploy specific metadata use cases by using pre-defined use case templates
- Create signatures using user-defined signatures to identify and filter unknown applications on your network

© 2024 Gigamon. All rights reserved.

In GigaVUE HC Series hardware appliances, GigaSMART applications run on specialized GigaSMART advanced-processing engines. These engines perform real-time functions on the traffic to enhance network visibility, improve security, and optimize the performance of other tools. One important feature of GigaSMART is TLS decryption, which is crucial for network security and application monitoring tools. While encryption protects data, it can also blind these tools. TLS decryption allows for the inspection of encrypted traffic, enabling effective threat detection and analysis. The GigaSMART advanced processing engines can be accessed from any GigaVUE HC Series node without restrictions based on ports or cards. Additionally, multiple GigaSMART engines can be combined to handle higher traffic loads and optimize for specific applications. GigaSMART plays a vital role in enhancing network intelligence and ensuring the effectiveness of security measures.

In GigaVUE Cloud Suite, GigaSMART applications run on the virtual visibility node (typically GigaVUE V Series), which can be scaled to meet the traffic volume and processing needs. The GigaSMART applications are categorized as follows:

Traffic Intelligence

Adaptive Packet Filtering, Advanced Load Balancing, De-duplication, Header Stripping, Masking, NetFlow Generation, Packet Slicing, Advanced Flow Slicing, Source Port Labeling, and Tunneling

Application Intelligence

Application Visualization, Application Filtering, Application Metadata, NetFlow Generation, and Application Metadata Exporter

Subscriber Intelligence

5G Correlation, GTP Correlation, and Stateful Flow Sampling

Security Intelligence

TLS/SSL Decryption

Top Use Cases

Network Operations

- Eliminate contention for network data due to SPAN port limitations
- Reduce or eliminate network downtime during upgrades
- Avoid data-speed mismatches between the network and tools
- Effectively filter streaming media or any of 3,500+ applications to optimize tool processing
- Access and monitor network data within SDN and private cloud environments
- Access subscriber traffic in the GTP user plane tunnels by correlating and passing the identified subscriber's control and data sessions to the analytics/monitoring probes and/or billing subsystems

Security Operations

- Improve detection of malicious activities by decrypting traffic and enhance network protection against attacks
- Identify sensitive data by decrypting traffic, prevent unauthorized access or exfiltration
- Decrypt traffic to gain insights into user and application behavior and identify suspicious activities
- Provide full context during security incidents by decrypting traffic, aid in root cause identification, and prevention of future occurrences
- Decrypt traffic to improve fraud detection, protect customers from financial loss by identifying stolen data transmission
- Decrypt encrypted traffic to ensure compliance with traffic inspection regulations
- Gain insights into hidden network traffic by decrypting traffic, troubleshoot issues, and improve network performance

© 2024 Gigamon. All rights reserved.

Key Features and Benefits

Traffic Intelligence

Feature/Application	Benefit
De-duplication Remove duplicate packets based on user-definable packet comparison criteria and duplicate detection window	• Offload de-duplication function from tools, increasing their capacity • Enable forensics tools to store more data
Source Port Labeling Add labels to packets indicating the ingress port	Identify the source of the packet for traffic brokering flexibility
Header Stripping/Protocol De-encapsulation Remove heavy tagging and encapsulation protocol headers (e.g., multiple VLANs, VN-tag, MPLS, GRE, GTP) including custom protocols	Allow any and all tools to more effectively monitor the network traffic of any type
Advanced Load Balancing • Distribute traffic among multiple ports based on a variety of options: hashing, bandwidth, cumulative traffic, packetrate, connections, and round robin • Balance packets based on L2–L4 criteria inside heavy tagging and encapsulation (e.g., multiple VLANs, VN-tag, MPLS, GRE, GTP)	• Assign custom traffic percentages or weights for distribution to tools • Ensure desirable balancing for all traffic types
Adaptive Packet Filtering Filter packets based on L2–L4 rules inside heavy tagging and encapsulation (e.g., multiple VLANs, VN-tag, MPLS, GRE, GTP)	• Enhance visibility into tunneled application flows • Maintain regulatory compliance by obscuring sensitive data • Optimize monitoring tools by selectively trimming traffic flow
Packet Slicing Remove all packet payload starting from L2, L3, or L4 header reference	• Allow tools to operate more effectively by forwarding less traffic volume and more packets • Maintain regulatory compliance by removing sensitive and private data
Advanced Flow Slicing Forward initial number of packets in each flow, then drop or slice the rest of the flow's packets	Reduce amount of traffic to forward and thereby improve efficiency and effectiveness of tools without impacting visibility
Data Masking Dynamically identify and overwrite specific packet content	Maintain regulatory compliance by obfuscating sensitive and private data without removing the packet payload

© 2024 Gigamon. All rights reserved.

Traffic Intelligence cont'd

Feature/Application	Benefit
Advanced Tunneling • Terminate remote spanning tunnels (Custom, ERSPAN, GMIP, L2GRE, TCP, VXLAN) • Initiate tunnels to IP destinations (GMIP, L2GRE, VXLAN) • Fragment and reassemble jumbo frames in accordance with network MTU limits	• Monitor remote and virtualized traffic with multiple on-premises tools • Monitoring of physical network traffic by virtualized or cloud-based tools • Forward traffic between remote Gigamon virtual and physical appliances • Reliable and intact delivery over IP networks
NetFlow Generation (for Traffic Intelligence) • Monitor IPv4/v6 traffic using L2-L4 standard information elements • Monitor DNS, TLS/SSL, and HTTP traffic using Gigamon extended IPFIX private elements • Export flow data in the following formats: NetFlow (v5 and v9), IPFIX, and CEF records • Supported only on Gen2 GigaSMART modules for on-prem	• Send reliable, full-traffic (vs. sampled) network flow data to tools, such as forensics for analysis • Offload NetFlow generation from the routers and switches to improve their core performance • Export flow data to up to 6 collectors or analytic tools

Application Intelligence

Feature/Application	Benefit
Application Visualization • Identify and display traffic metrics for over 4,000 applications • Define custom applications	• Improve troubleshooting and capacity planning of your network and monitoring infrastructure • Categorize applications into web, social media, email, etc. • Dynamically detect and obtain the latest updated application signature database
Application Filtering Intelligence • Filter traffic based on over 4,000 standard and custom applications	• Forward traffic for only those applications of interest, or drop only those that are not of interest • Extract and treat each application, or family of applications, uniquely based on threat potential and each tool's needs • Bring application awareness to your SOC and NOC, helping teams make better decisions faster
Application Metadata Intelligence • Forward contextual data for Layers 2 to 7 in IPFIX or CEF formats • Provide close to 6,000 metadata elements across applications	• Automatically generate protocol and application attributes that are otherwise not attainable • Improve performance, security, and customer experience with additional visibility • Dynamically detect and obtain the latest updated AMI attribute database • Send to up to 5 collectors

© 2024 Gigamon. All rights reserved.

Application Intelligence cont'd

Feature/Application	Benefit
Application Metadata Exporter (AMX) • Be able to export metadata as JSON and JSON over KAFKA to tools • Supports Open Cybersecurity Schema Framework (OCSF) for metadata export to Amazon Security Lake • Supported only on V Series for private and public cloud environments	• Supports out of the box integration with cloud-native tools such as Dynatrace, New Relic, Datadog, Sumo Logic, MS Sentinel, etc. • Reliably and securely export metadata to the partner tools • OCSF export format allows easy ingestion of application metadata into data lakes such as Amazon Security Lake and use AI/ML tools to proactively monitor, troubleshoot, and resolve network and security issues in the environment
NetFlow Generation (for Application Intelligence) • Monitor IPv4/v6 traffic using L2-L4 standard information elements • Export flow data in the following formats: NetFlow (v5 and v9), IPFIX and CEF records • Supported on Gen2 and Gen3 GigaSMART modules for on-prem and V Series for private and public cloud environments	• Send reliable, full-traffic (vs. sampled) network flow data to tools, such as forensics for analysis • Offload NetFlow Generation from the routers and switches to improve their core performance • Export flow data to up to 5 collectors/analytic tools

Subscriber Intelligence

Feature/Application	Benefit
5G Correlation Support 5G standalone and 4G/5G converged core networks with the correlation of control plane and user plane sessions	• Provides granular "subscriber awareness" visibility into 5G and 4G infrastructures to improve efficiency and effectiveness of network monitoring, and broadens security coverage • Significantly reduces network loading using targeted filtering or sampling and load balances resultant traffic
GTP Correlation Coherently filtering and/or balancing, keeping control, and user plane sessions together	• Ensure each monitoring tool gets to see all mobile core sessions associated with a user or domain
Stateful Flow Sampling (FlowVUE®) Stateful user-session sampling based on IP address, and when combined with GTP Correlation can sample based on subscriber ID (IMSI/SUPI), user device ID (IMEI/PEI), RAN ID (ECGI/NCGI), and/or Network Slice ID (NSSAI), including allocation of separate samples for each tool port or tool port group from a common pool of correlated control and user plane data	• Achieve meaningful network monitoring without monitoring every user's or domain's sessions • Selectively reduce traffic bound to monitoring and analytic tools

© 2024 Gigamon. All rights reserved.

Security Intelligence

Feature/Application	Benefit
TLS/SSL Decryption • Supports the latest TLS protocols and cipher suites, including TLS 1.3 • Inline and out-of-band deployment options • Selective decryption • Scalable • Automatically identifies and decrypts SSL traffic and delivers it to multiple tools for inspection • Collects, aggregates, and distributes relevant data to the right security tools • Identify, classify, extract, and take appropriate actions on irrelevant applications such as Netflix and Facebook to improve tool utilization and efficiency	• Ensures that the product can decrypt traffic that is encrypted with the latest encryption methods • Allows organizations to deploy the product in a way that best meets their needs • Allows organizations to decrypt only the traffic that they need to inspect, which can save resources • Saves time and resources by eliminating the need for manual decryption. It also allows security teams to inspect all traffic, regardless of whether it is encrypted • This metadata can be used to identify malicious traffic and to quickly understand the context of an incident. It can also be used to automate incident response workflows • This ensures that security tools have the data they need to detect and respond to threats. It also helps to prevent data silos and to improve collaboration between security teams • This frees up security tools to focus on more important threats. It also helps to improve tool utilization and efficiency • This ensures that the product is always up-to-date with the latest threats. It also minimizes downtime and reduces the risk of security gaps

© 2024 Gigamon. All rights reserved.

GigaSMART Engine Platforms[1]

Product	Description
GigaSMART for GigaVUE Cloud Suite	• Runs within GigaVUE V Series • 6 vCPUs for each instance of V Series running TLS/SSL Decryption • Can run multiple instances for higher throughout
GigaVUE-HCT	Gen3 GigaSMART front module: • Processing up to 80Gbps1 • Includes slicing, masking, source port labeling, tunnel de-encapsulation
GigaSMART for GigaVUE-HC1	Integrated Gen2 GigaSMART: • Processing up to 20Gbs[1] • Does not include any GigaSMART features by default Gen3 GigaSMART front module: • Processing up to 80Gbps[1] • Includes slicing, masking, source port labeling, tunnel de-encapsulation
GigaSMART for GigaVUE-HC1-Plus	Integrated Gen3 GigaSMART: • Processing up to 200Gbps • Includes slicing, masking, source port labeling, and tunnel de-encapsulation Gen3 GigaSMART front modules: • Processing up to 80Gbps[1] Includes slicing, masking, source port labeling, tunnel de-encapsulation Up to 3 GigaSMART modules (2 front and 1 built-in) can be populated per GigaVUE-HC1-Plus to provide scalable performance up to 360Gbps[1]
GigaSMART for GigaVUE-HC3	GigaSMART front modules, two options, each with two engines: Gen3: • Processing up to 200Gbps[1] Includes slicing, masking, source port labeling, and GigaVUE tunnel de-encapsulation Up to 4 GigaSMART modules can be populated per GigaVUE-HC3 to provide scalable performance up to 1.6Tbps[1]

[1] Performance reflects processor speed and not bandwidth, which is dependent upon packet size, packet rate, and specific GigaSMART applications applied.

GigaSMART software is available under a variety of licensing models, including perpetual licensing, as well as the more predictable and budget-friendly subscription and term licensing. For more information, contact your sales representative, your reseller, or contact us at gigamon.com/contact-sales.

© 2024 Gigamon. All rights reserved.

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 harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

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

© 2019-2024 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.