

72% of SecOps teams cannot scale their network infrastructure to meet the needs of increased data volume

67% cite network blind spots as a major obstacle to data protection

Key Benefits

Network Operations

- Optimize traffic delivered to monitoring tools
- Decrease network downtime

Security Operations

- Reduce hardware and software costs
- Increase security tool efficiency
- Expose threats hidden within encrypted traffic

Manage Your Network Traffic with Advanced Intelligence

GigaSMART® is a comprehensive set of technologies that extend the intelligence and value of the Gigamon Visibility Platform by enhancing the monitoring of your network infrastructure and improving security tool performance. A range of applications are available to optimize the traffic sent from your network to the tools you rely upon to monitor, manage and secure the network. GigaSMART's advanced processing engine can be accessed anywhere within the Gigamon Visibility Platform without port- or card-based restrictions. GigaSMART engines can be combined to manage higher traffic loads and optimized for specific applications. Applications can be combined or service chained so traffic benefits from multiple functions that can be achieved at once, such as generating NetFlow and other network metadata or decrypting SSL/TLS traffic after packet duplicates have been removed, or stripping VLAN headers before load balancing the traffic and sending it out to the appropriate tools.

Network monitoring tools can perform more efficiently by eliminating unwanted content with the de-duplication and packet slicing features. Masking allows network security teams to hide confidential information like passwords, financial accounts or medical data, helping companies to meet SOX, HIPAA and PCI compliance regulations. Enhanced packet distribution features available with Adaptive Packet Filtering or load balancing enable enhanced visibility into packet contents and, when combined with header stripping, allow tools to operate more effectively by removing unwanted protocol headers.

With GTP correlation, service providers can more reliably filter and forward specified subscriber sessions (both GTP-c and GTP-u) to monitoring and analytic tools. The Gigamon FlowVUE® application offers a sampling paradigm for active subscriber's device IPs (UE IPs) across GTP-u tunnels.

Top Use Cases

For Network Operations:	For Security Operations:
<ul style="list-style-type: none">• Eliminate contention for network data due to SPAN port limitations• Reduce network downtime during upgrades• Avoid data speed mismatches between the network and tools• Effectively filter streaming media and network applications to optimize tool processing• Access and monitor network data within SDN and private cloud environments	<ul style="list-style-type: none">• Automatically identify and decrypt SSL traffic and deliver to multiple tools for inspection• Generate metadata to expedite and simplify incident identification and response• Identify, filter and forward traffic corresponding to critical application sessions

Source: "Hide and Seek: Cybersecurity and the Cloud," by Vanson Bourne (May 2017).

GigaSMART technology is available on the GigaVUE® H Series visibility nodes. GigaSMART applications can be applied to any network or tool port on the chassis or the entire cluster, allowing maximum flexibility in configuration and provisioning.

For More Information

To learn more about GigaSMART and its capabilities, please visit the [GigaSMART web page](#).