

Setting General Trap Questions for Competitors

Question	The Gigamon Response
Are you able to ensure network availability while switching security tools between passive detection and and active prevention modes?	<ul style="list-style-type: none"> Gigamon provides one complete solution: the Gigamon® Visibility and Analytics Fabric. A multi-function platform enabling both active (i.e. inline or prevention) and passive (i.e. out-of-band or detection) technologies.
What do you expect to pay for maximum port count and capacity?	<ul style="list-style-type: none"> Gigamon GigaVUE — HC and TA series are very competitively priced for maximum port count and capacity.
Would you like to easily and reliably detect & filter on specific applications, especially when applications use different or variable	<ul style="list-style-type: none"> Gigamon's Application Intelligence supports 3200+ applications, out of the box, without relying on L4 port numbers
Would you like to Tap, Aggregate, Filter, Balance, and Optimize traffic all in one box?	<ul style="list-style-type: none"> GigaVUE-HC Series products provide this all in a single box

Responding to General Competitor Claims

Competitor Claim:

Our CLI and GUI are easier to use than Gigamon's

The Gigamon Response

- ▶ Our single pane of fabric management with GigaVUE-FM is easy to use and covers all products (physical, virtual and cloud).
- ▶ Our CLI is Cisco-like (based on Cisco IOS) and common across all products.
- ▶ Most competitors require multiple UIs to manage their multiple components.
- ▶ We also provide a REST XML API, Python SDK, and Ansible for automation, integration, and orchestration

Proof Points

- ▶ Demonstrate GigaVUE-FM and ask how they manage all of their physical and virtual visibility products.
- ▶ Suggest them to look at the competition's multiple UIs and components that lead to management complexity.
- ▶ Ensure they are comparing GUI to GUI, CLI to CLI, **not** GUI to CLI

Competitor Claim:

External Test results show, compared to Gigamon, our products:

- ▶ Always guarantee full performance
- ▶ No performance change at minimum packet size
- ▶ No performance change after enabling all functions













The Gigamon Response

- ▶ This limitation only applies to slicing, static masking, and deduplication. Only FPGA-based implementations may not have an issue with these. However, deduplication can still be an issue for FPGA designs.
- ▶ For all competitors, this limitation will apply to application filtering, metadata generation, SSL/TLS decryption, GTP & SIP/RTP correlation, or any other stateful or DPI-based feature.
- ▶ This is a typical Ixia claim based on a 5-year old Tolly report, using biased test methodology









Proof Points

- ▶ Request a live traffic PoC and Gigamon will be happy to prove these points.
- ▶ Engage Spirent to help with an unbiased test methodology.
- ▶ Manage the bandwidth scaling and should not present an issue, even for deduplication.

Why customers choose Gigamon over Non-NPB Decryption Devices

Customer Req	Gigamon	Other NPBs	Why it is important
Comprehensive application filters	 Yes	 Few support this, and those that do are not very extensive	New apps come along and internal bespoke apps are developed. Filtering on application level is important for optimizing tool effectiveness
Integrated virtual and physical traffic access and brokering	 Yes	 Some that have a virtual solution treat it separately to physical solution	Single pane of management whether virtual or physical, with orchestration integration
Inline bypass and OOB monitoring using same boxes	 Yes	 Many need a different box for inline versus passive OOB brokering	Single NPB solution for both Security and Network operations
Integrated SSL/TLS decryption	 Yes	 Very few support this, relying on external 3rd party appliances	Easy configuration, and different types of passive OOB and active inline security and monitoring tools can see encrypted or decrypted flows, or both, as required
High reliability of Hardware	 Yes	 Many do not have a good reputation of reliability	Can trust to put product into operation and it will continue to operate correctly
Excellent service	 Yes	 Smaller vendors don't have true global support, Others don't have good record	Feel confident that support knows the products, issues will get resolved in a timely manner (no matter where), and being treated with importance

Why customers choose Gigamon over Non-NPB Decryption Devices

Customer Req	Gigamon	Standalone Decryptors	Why it is important
Unified Management	 Yes	 Require separate management	Different, uncoordinated user interfaces for configuring and managing causes headaches and needs extra training
Simultaneous active inline and passive OOB traffic forwarding	 Yes	 Don't have required packet brokering features	Both active and passive security and monitoring tools require decrypted visibility, so need more than one appliance or need a separate NPB anyhow
Forwarding of both encrypted and decrypted flows	 Yes	 Don't have required packet brokering features	NPM tools require actual encrypted flows whereas APM and Security tools require decrypted flows, so need a separate NPB anyhow
Minimize the transmission of Clear Text across wires between boxes	 Yes	 Every external Decryptor instance requires external cabling	Minimizes physical security risk within datacenter