

Gigamon 教育單位面臨之挑戰

- 從教育資料中心與私有雲建構 零信任網路開始

Sep 2023

錢旭光

Gigamon台灣分公司

業務總監



Gigamon是Global可視化 方案領導廠商 – 市佔40%

Gigamon deep observability pipeline harnesses network intelligence to amplify the power of security and observability tools.

Gigamon 深度可視性方案利用網路可視化智能來增強安全工具效能與涵蓋完整範圍。

IT can assure security and compliance, speed root-cause analysis and lower operational costs for their hybrid- and multi-cloud infrastructures.

資訊部門可確保其混合雲和多雲基礎架構的安全性和合規性，加快根本原因分析並降低維運成本。

台灣客戶

金融

企業

教育

政府

電信



教育單位面臨的維運與資安挑戰 – Pain point

主任與組長須面對頻寬成長、維運作業與資安防禦的挑戰

- + 教網流量不斷提昇，介接頻寬不敷使用
- + 資安設備如IPS/WAF等工具效能不足流量快速成長
- + ASoC偵測到資安事件要花費多時查找來源與解決回覆
- + 校園網路有問題發生時急迫需找出原因 – 流量動態如何取得？
- + 虛擬主機與私有雲流量無法有效導出 – 能運用既有維運或資安設備？
- + 人力不足與管理人員變動的銜接 – 新工具需耗時學習、人力備援？
- + SILO建置 – 分段式建置管理，造成疊床架屋複雜架構而導致查找問題之困難

The Silo Problem



如何實現快、精、準混合雲系統維運與資安防護而不耗費過多人力？

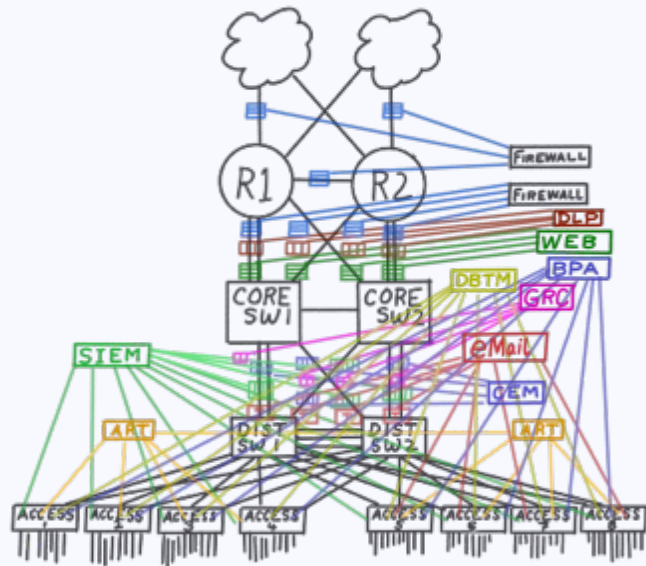


Gigamon Deep Observability pipeline

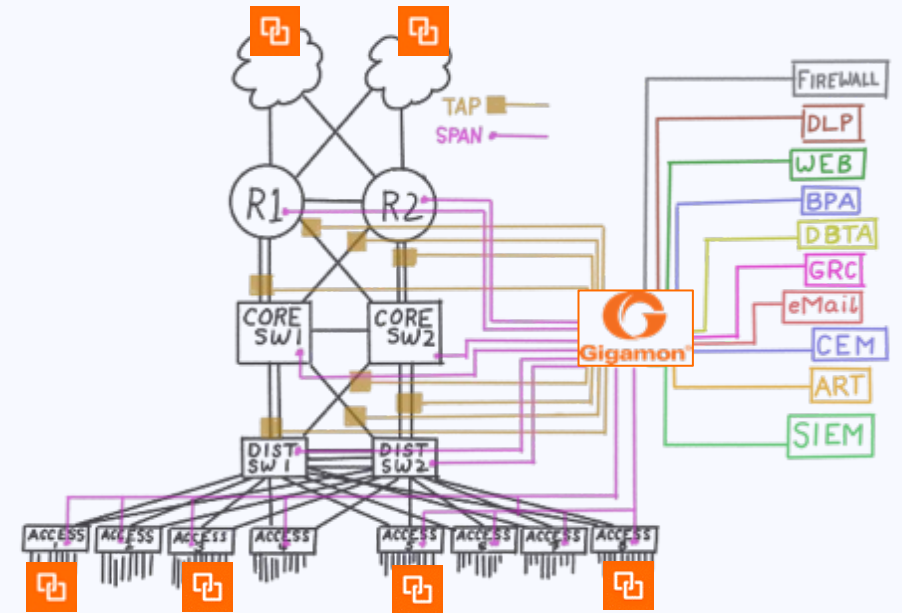
化繁為簡的資安網路整合架構 – Gigamon Deep Observability pipeline目標

Gigamon方案達到Zero Trust Network全網無盲區的實現

原有架構複雜 → 有許多盲區、工具增生成本
高、不具動態調整彈性

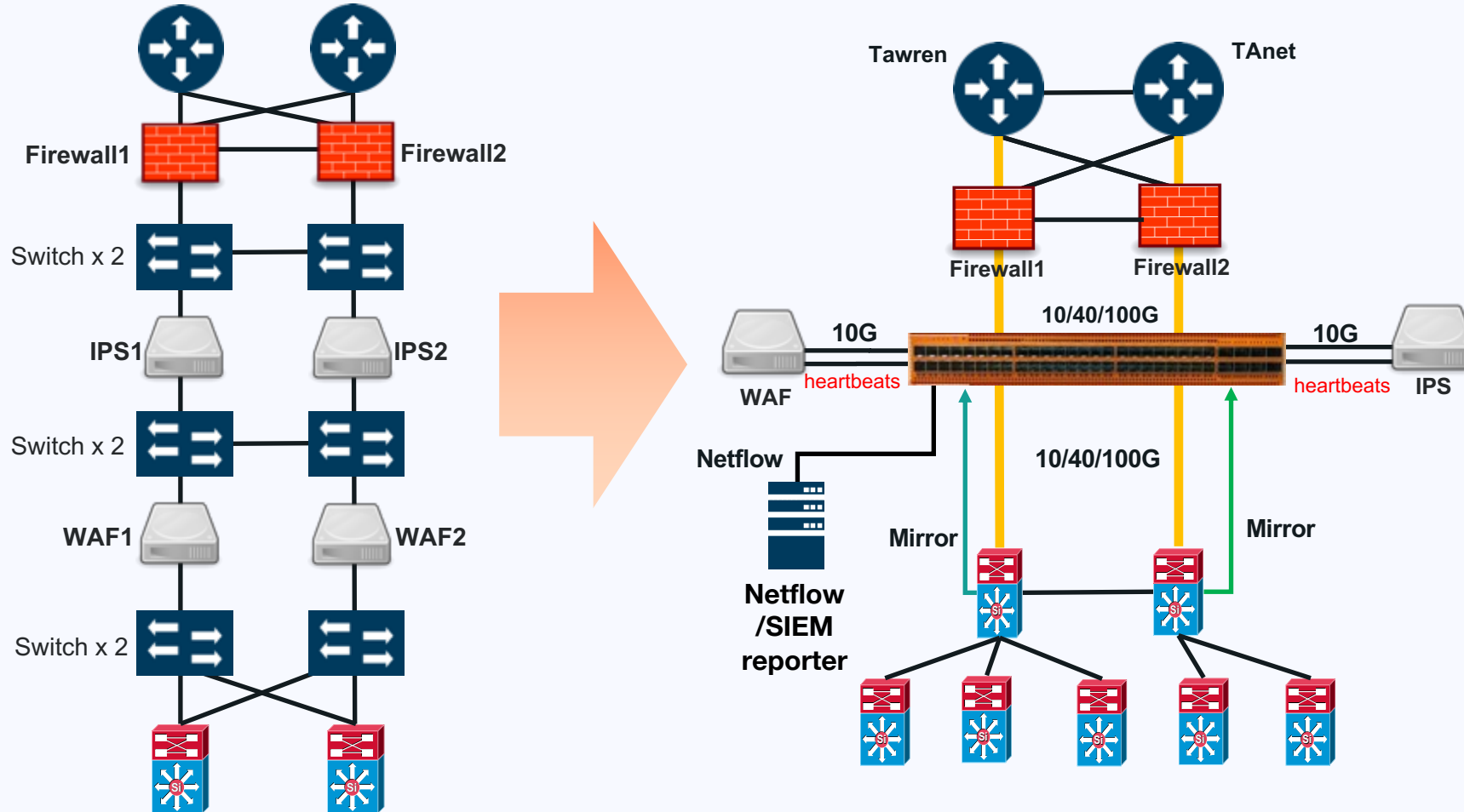


Gigamon方案目標 → 全網可視無盲區、過濾雜
訊降低成本、簡化架構提昇彈性



教育單位應用一 – In-Line Bypass 提供WAF/IPS 流量篩選與彈性Bypass效果

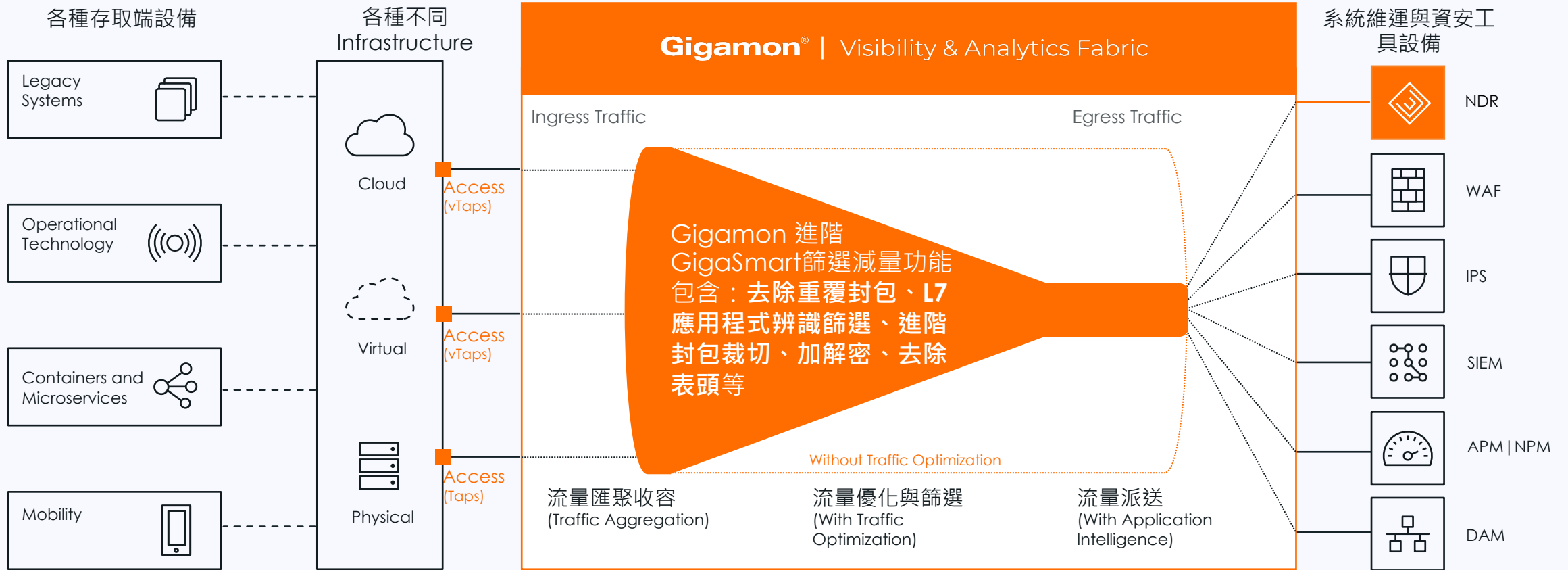
可降低資安設備容量並產生Netflow或Metadata給SIEM分析



- + Gigamon多種選擇 – TA25、HC1、HC3
- + TA25具備 10/25/40/100G介面可執行工具inline bypass
- + HC1具備10/40G介面可執行工具inline bypass與 Netflow/Metadata輸出
- + HC3具備10/40/100G 實體Bypass 介面與 Netflow/Metadata輸出

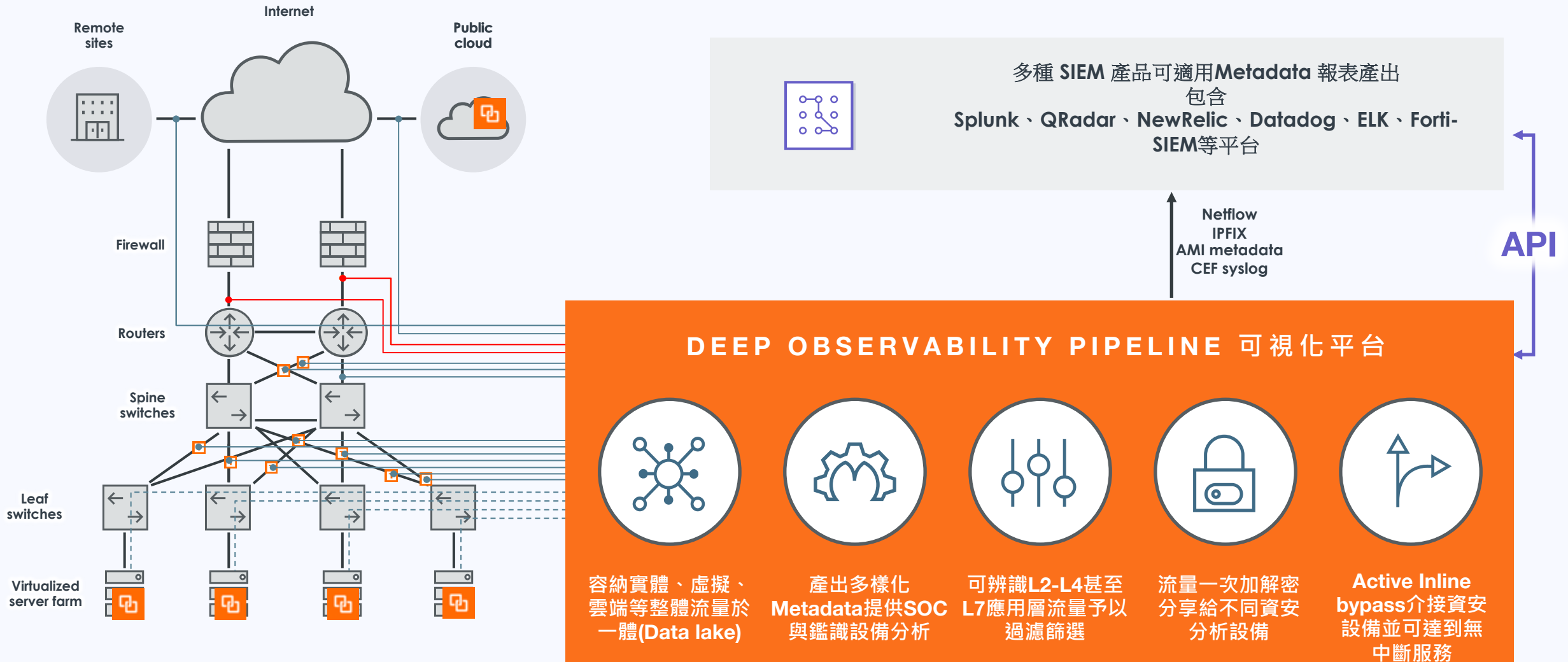
經由Gigamon進階GigaSmart功能去除雜訊後減少工具處理容量

提昇工具設備效率、降低工具投資成本、擴大資安防禦面向



*A TOOL is defined as a hardware and/or software device that ingests network traffic or data for the purpose of network and application performance monitoring analysis, security analysis and threat mitigation, monitoring customer experience, recording, or troubleshooting

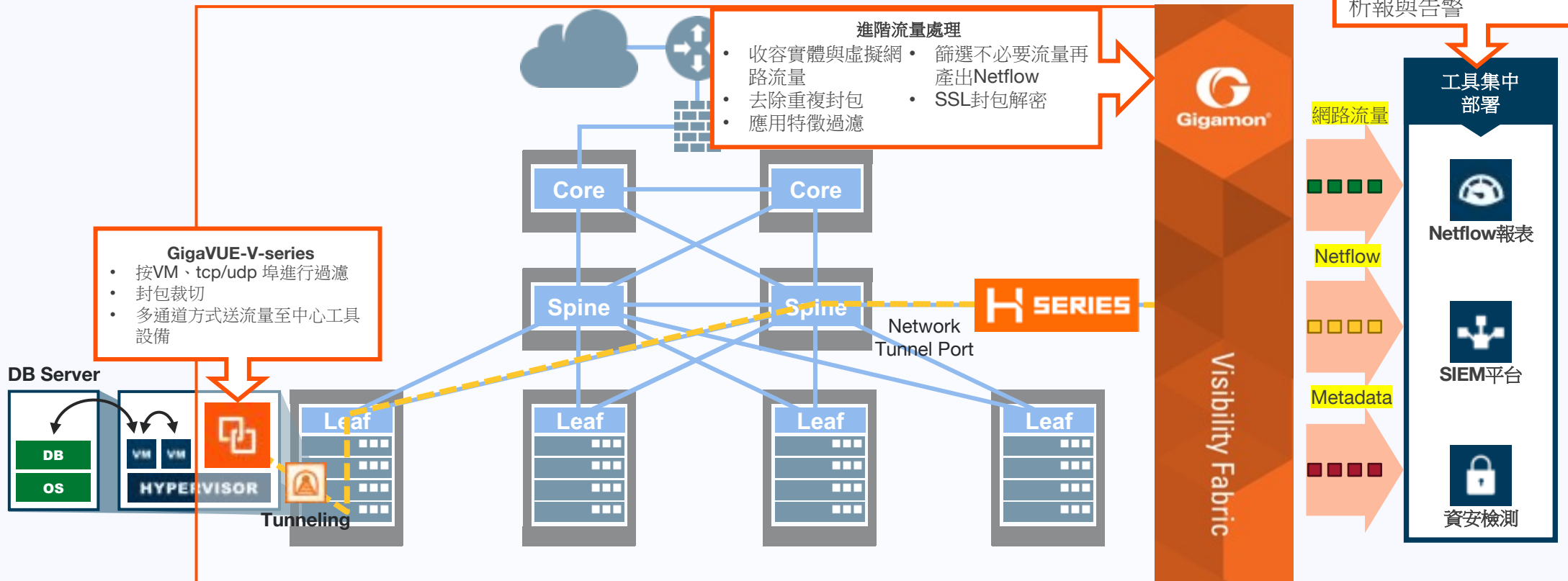
教育單位應用二 – 多種Metadata輸出供SIEM平台產出多種用途報表



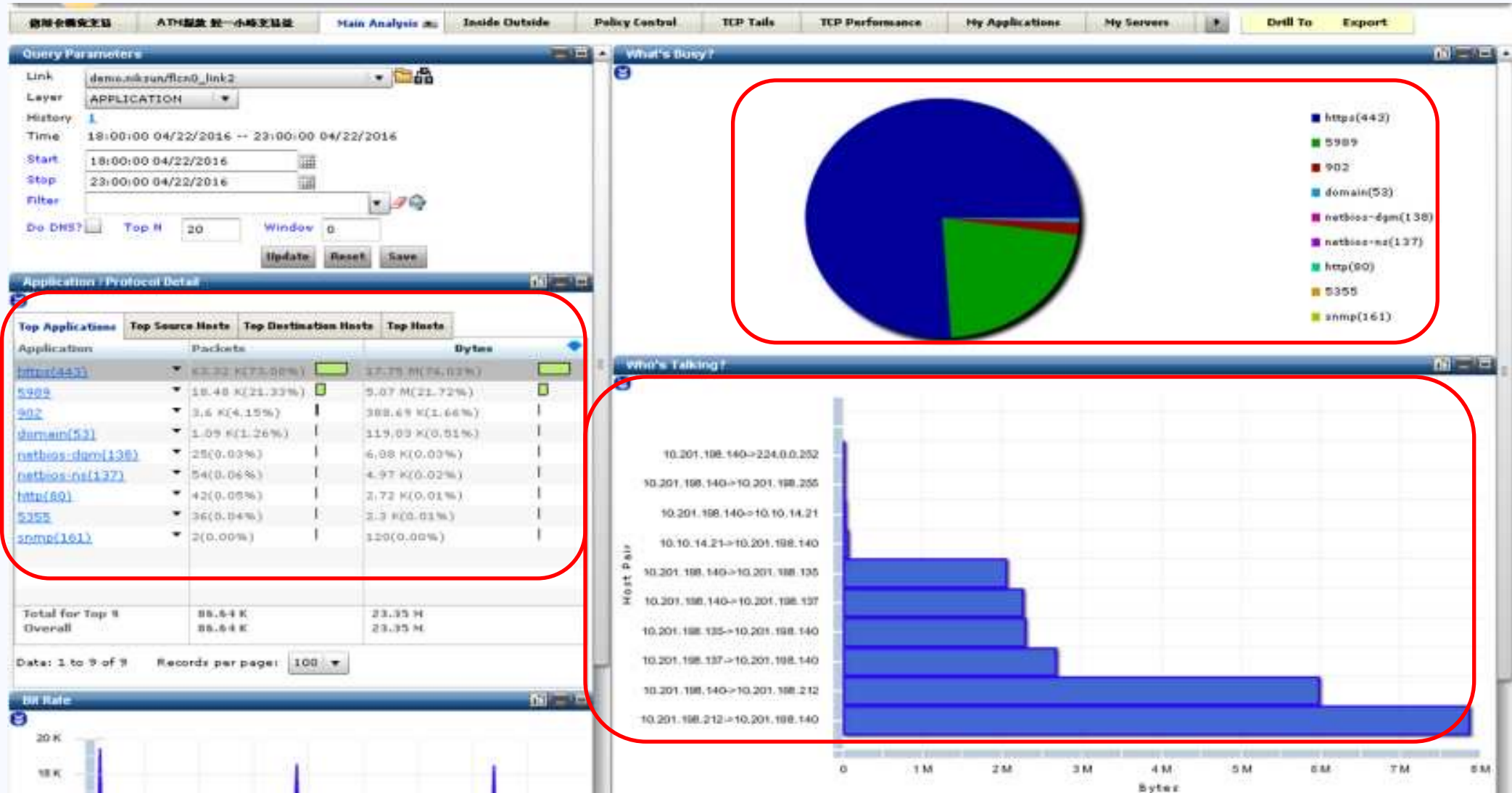
教育單位應用三 – Vmware/Container環境流量可視性：Gigamon V-series

非侵入式虛擬主機東西向流量收集、篩選後可輸出減量之網路流量亦可再產出NETFLOW與METADATA

全校園流量包含虛擬主機
流量篩選後可產出
Netflow與Metadata做分
析報與告警



經由V-series輸出流量或Netflow製作VM/Container分析報表



Fabric Manager統一管理平台管理地端資料中心、混合雲佈署

管理者無需在不同平台學習不同管理操作



The image displays the GigaVUE-FM ITD interface, which is a unified management platform for physical and virtual environments. The interface is divided into several sections:

- Physical & Virtual:** Shows audit logs for a 'Default' profile over a '1 Day' period.
- Monitoring Session:** A central dashboard showing a network topology with nodes like 'HTTP', 'SSH', and 'ICMP' connected to a central 'GigaVUE' node.
- Monitoring Session Info:** A detailed view of a monitoring session, including the name, monitoring domain, connection type, and pre-filtering options.
- Targets:** A section showing the targets of the monitoring session, including a tree view of the network topology and a legend for 'Transformed Link' (Pass/Drop).

The interface also features a sidebar with navigation options for various cloud providers and services, including AWS, Azure, OpenStack, Kubernetes, and AnyCloud. The bottom right corner of the interface shows a table with columns for Cluster ID, Host Name, Port ID, Port Alias, and Traf..., and a message stating 'No Records Found'.



Gigamon portfolio

All Managed by GigaVUE-FM Fabric Manager

All Managed by GigaVUE-FM

GigaVUE Cloud Suite



G-vTAP Container / Module



GigaVUE V Series

Virtual/Private and Public Cloud

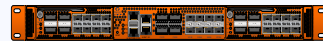
Access, Aggregate, Filter, Optimize, Balance, Transform

- ▶ G-vTAP Module: Tapping agent for network data access in public and private cloud
- ▶ G-vTAP Container: Tapping agent for network data access in containerized clouds
- ▶ GigaVUE V Series: Virtual appliance for Public and Private clouds
 - ▶ Integration with orchestration systems for automated visibility

GigaVUE HC Series



GigaVUE-HC3



GigaVUE-HC1P



GigaVUE-HC1

Intelligent Visibility Nodes

Access, Aggregate, Filter, Optimize, Balance, Transform

- ▶ HC1: 10M/100M, 1G, 10G
- ▶ HC1P: 10M/100M, 1G, 10G
- ▶ HC3: 10G, 25G, 40G, 100G
- ▶ Full spectrum of traffic / application / subscriber / security intelligence
- ▶ Inline bypass; physical and logical
 - ▶ Cluster multiple nodes for additional scale

GigaVUE TA Series



GigaVUE-TA400



GigaVUE-TA200



GigaVUE-TA25

Traffic Aggregators

Aggregate, Filter, Balance

- ▶ Traffic aggregators for 1G, 10G, 25G, 40G, 100G, 400G
- ▶ Commodity appliances for simple brokering use cases
 - ▶ Inline bypass; logical
- ▶ Cluster with GigaVUE HC Series for traffic / subscriber / application / security intelligence

Network TAPs



G-TAP M Series



G-TAP A Series

Embedded TAPs

see GigaVUE HC Series

Physical Taps

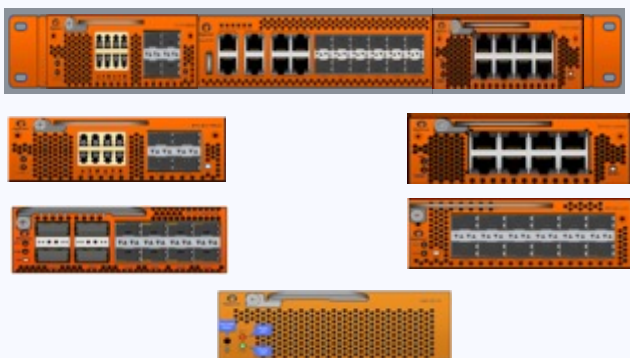
Access

- ▶ High-density powered active and unpowered passive TAPs
- ▶ Non-intrusive physical access to network traffic
- ▶ 1 Gbps to 400 Gbps fiber (incl. 40/100 Gbps BiDi)
 - ▶ 10/100/1000 Mbps copper
- ▶ 10G copper (SFP+ only)

Gigamon HC 系列與TA25 – 提供教育折扣

All Managed by GigaVUE-FM

10G/40G bypass – 1U



GigaVUE-HC1

- 10 / 100 / 1000Mb Copper
 - 1 / 10Gb / 40Gb Fiber
- 可具備Netflow或Metadata輸出

40G/100G bypass – 1U



TA25

- 100 / 1000Mb Copper
 - 1 / 10G/ 25Gb Fiber
 - 40Gb/100G Fiber

40G/100G 實體bypass – 3U



GigaVUE-HC3

- 10G/40G/25G/100G介面
 - 40Gb Fiber
- 40G/100Gb 實體Fiber Inline bypass
 - 可具備Netflow或Metadata輸出

Q & A

Sep 2023

