



強化虛擬環境安全性的新利器

如何簡化整體資安架構並提昇資安工具應用效率

資安訊息派送平台 – Security Delivery Platform

Simon Chien 錢旭光
Gigamon 行銷業務總監



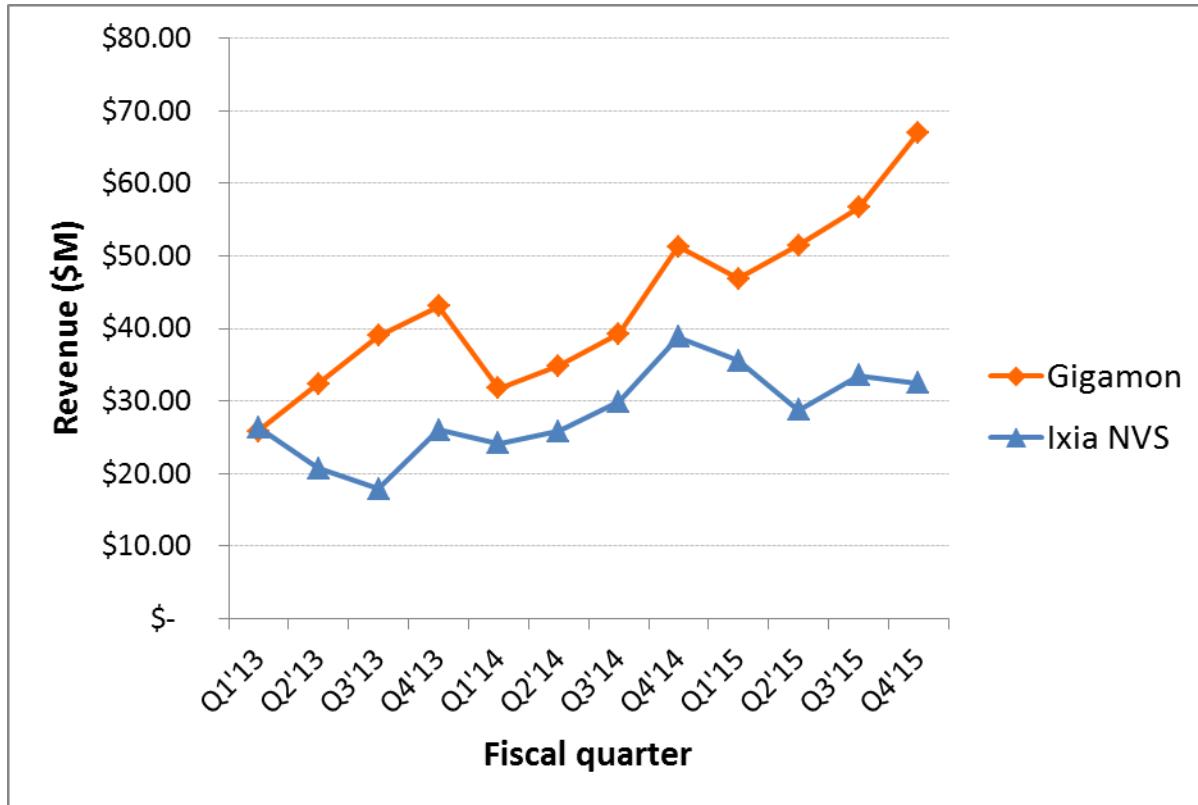
Gigamon Inc. – 美商奇望

The Company. The Team. The Results.



- 成立於 2004 年美國加州，2005 年第一個產品交貨 – 2013年六月在NYSE IPO
- 創造了Data Access Network – 現在稱為 Unified Visibility Fabric 架構
- 多項專利技術 – 31 項專利, 28 項申請中
- 超過 2000 個集團大型客戶使用GigaVUE，分布在 60 多個國家
- 美國開發與生產
- 超過 78 個世界 Fortune 100 公司已採用Gigamon的方案

Gigamon – Visibility 產業的領導者

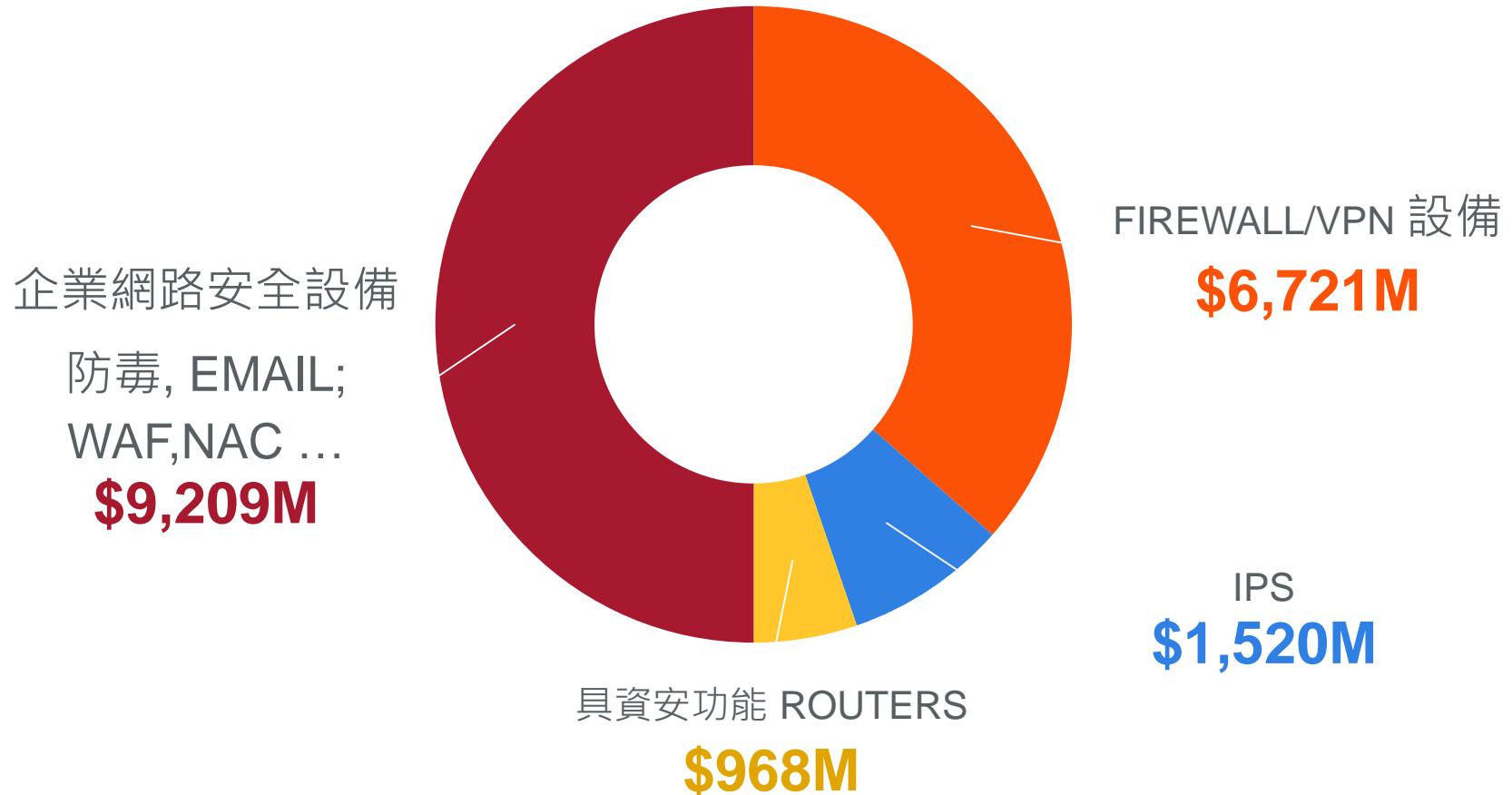


- 較次大市場佔有率廠家成長率高出4倍
 - 37.6% 市佔率 – Gartner 2016/1 報告
- “Gigamon is the market share leader in the NPB market delivering Layer 2 through Layer 7 NPB visibility, filtering and correlation via its GigaSMART platform”**
- Gartner, Jan 2016

資訊安全面對與過往不同的挑戰？

每一年預算達數百億美元的資安設備建置

投資不可謂不多了



Source: Gartner Trends Telecom Forecast (March 2014)

資安問題卻不斷發生 – 規模之大令人震驚



“...美國人事行政局 (OPM) 指出大約有
22.1M 個人資料已被盜用 ... ” + 2015年

“Sony公司CEO, Michael Lynton, 告訴員工, Sony公司嚴密的資安防護網因被黑客駭入而**員工個資及內部資料被竊取的狀況空前嚴重**” * 2014年

“美國第二大健保公司安泰公司, Anthem Inc. , 正式宣佈約有**8千萬**客戶資訊被盜用 ” ++ 2015年

*<http://variety.com/2014/film/news/sony-hack-unparalleled-cyber-security-firm-1201372889/>

+<http://www.opm.gov/news/releases/2015/06/opp-to-notify-employees-of-cybersecurity-incident/>

++<http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/>

今日頭條資安事件 – 第一銀行ATM遭盜領事件

ATM被遠端控制，更顯示駭客已進化，無法使用現有資安防堵方式防禦！



給CIO與CSO組長的提醒



- 當今網路資訊安全的架構趨勢已由**防堵(Prevention)**模式轉化為**偵測與立即反應 (Detection & Response)** 模式
- 此種資安運作模式必須仰賴一套**整合式的資安聯結架構**, 以供各種不同資安設備的佈建與擴充
- **GigaSECURE**是業界首套**資安訊息派送平台 (Security Delivery Platform)** ,此架構將轉化現有資安服務建置的方式 – 使資安設備更有防治效益, 更自動化,更降低成本



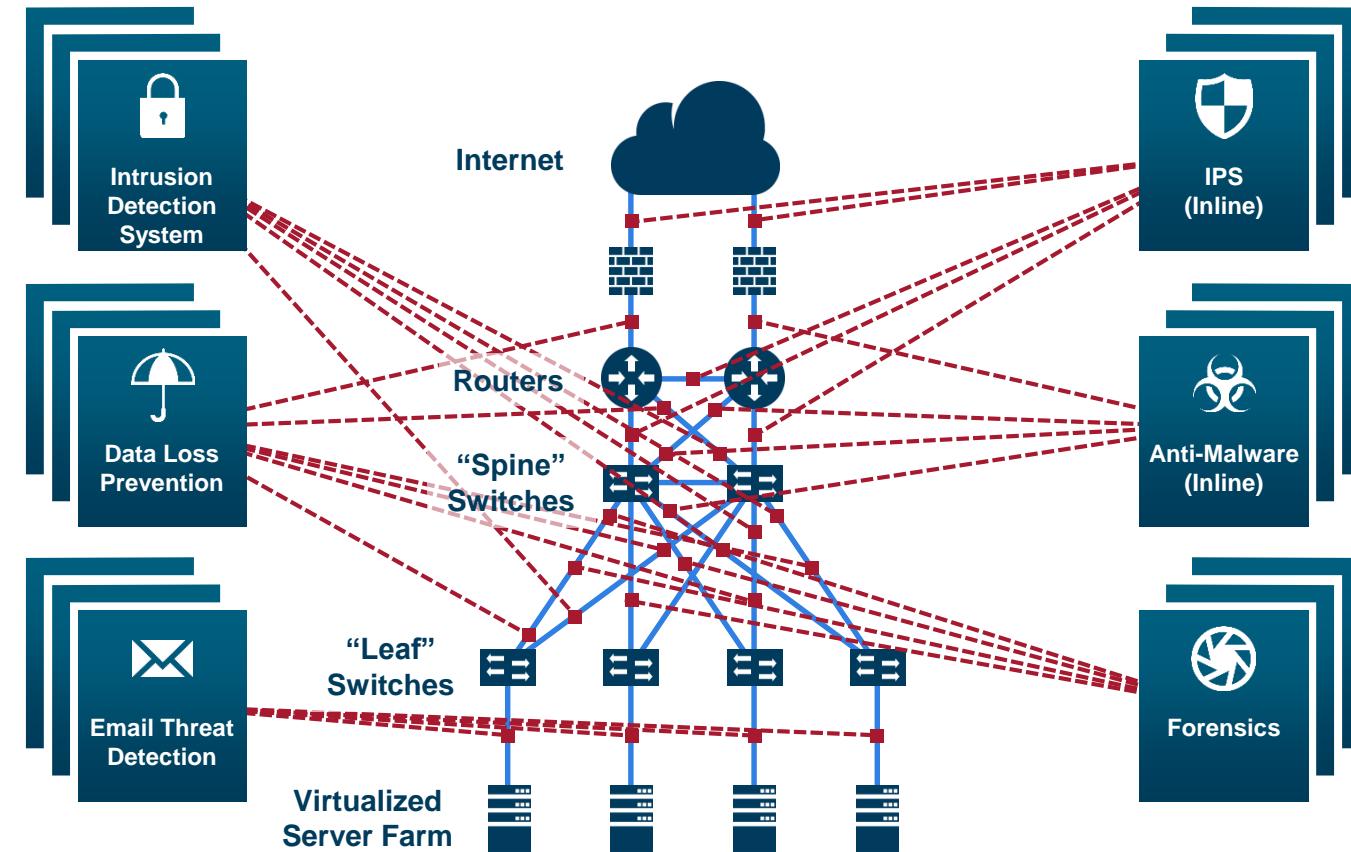
Introducing GigaSECURE®

業界第一套資安訊息派送平台

SECURITY DELIVERY PLATFORM

如何鎖定資安威脅：現有的資安佈建面臨巨大挑戰

視別訊務有地點或時間的限制

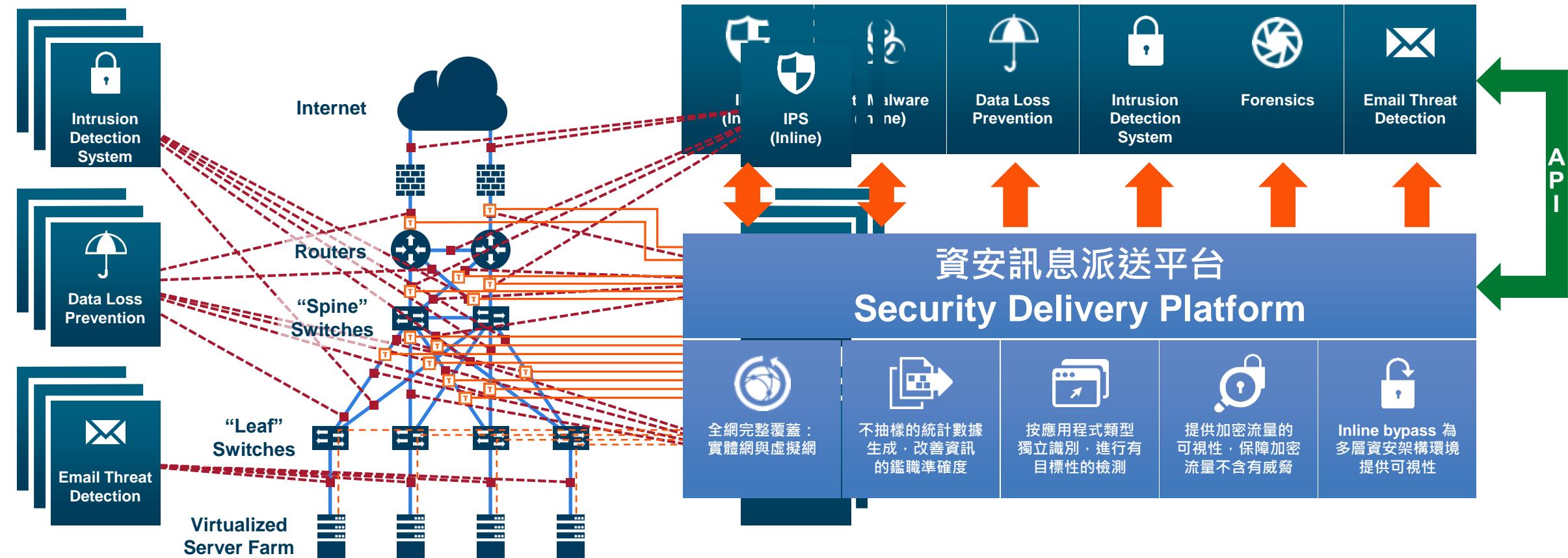


資安防禦的挑戰：

- 整體網路盲點太多無法全面視別
- 為達資安效能要求導致成本極高
- 資安設備爭奪訊務流量的取得
- 訊務流量無法保持一致性
- 加密封包無法快速解密
- 導致太多假警報 false positives

是該將主動權由攻擊者手上移轉至防禦者的時候了

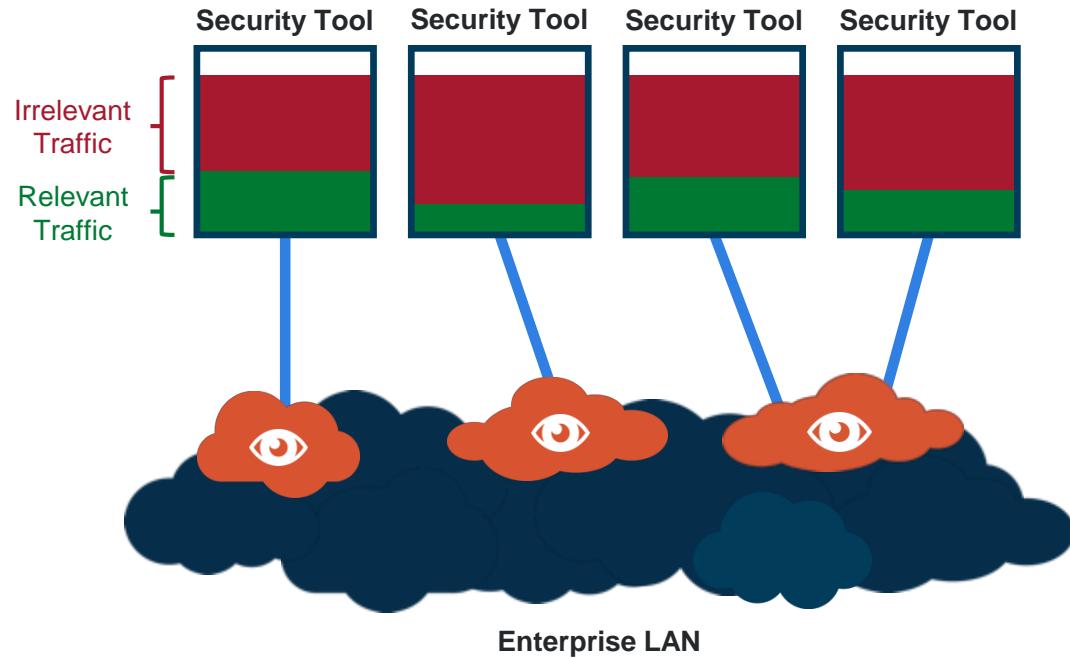
網路可視性Visibility的革命: 資安訊息派送平台



Security Delivery Platform: 創造高效益資安系統的基礎平台

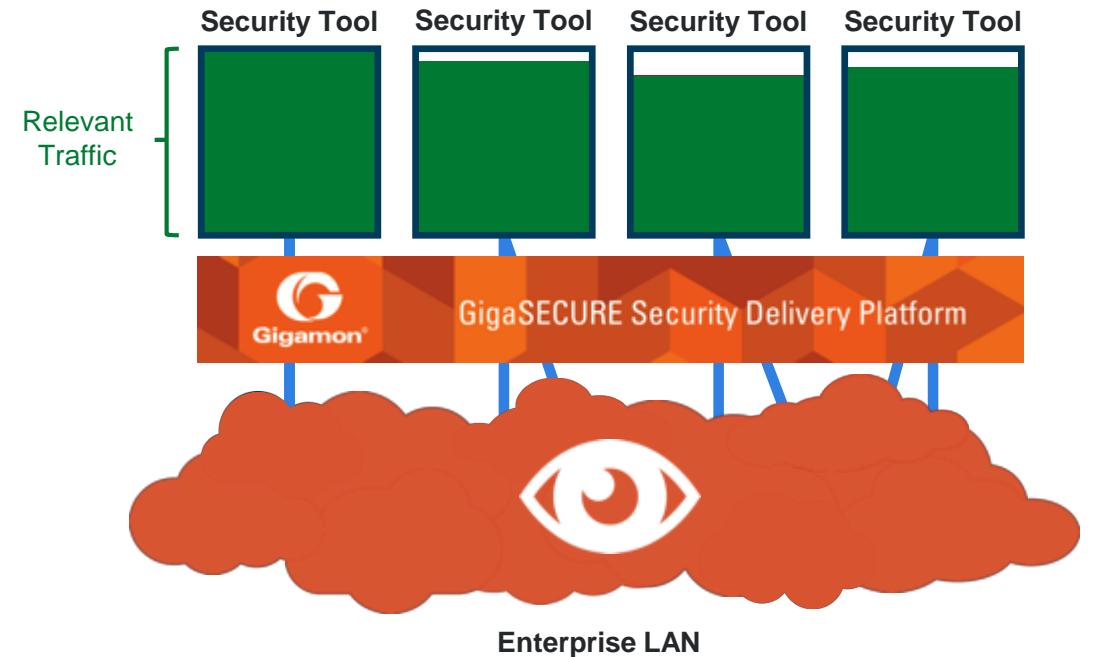
GigaSECURE® 的優勢

Legacy Approach Without Gigamon



- 只見局部網路點之訊務
- 無法控制要取得哪種訊務
- 資訊設備的效能無法善用

With Gigamon Security Delivery Platform

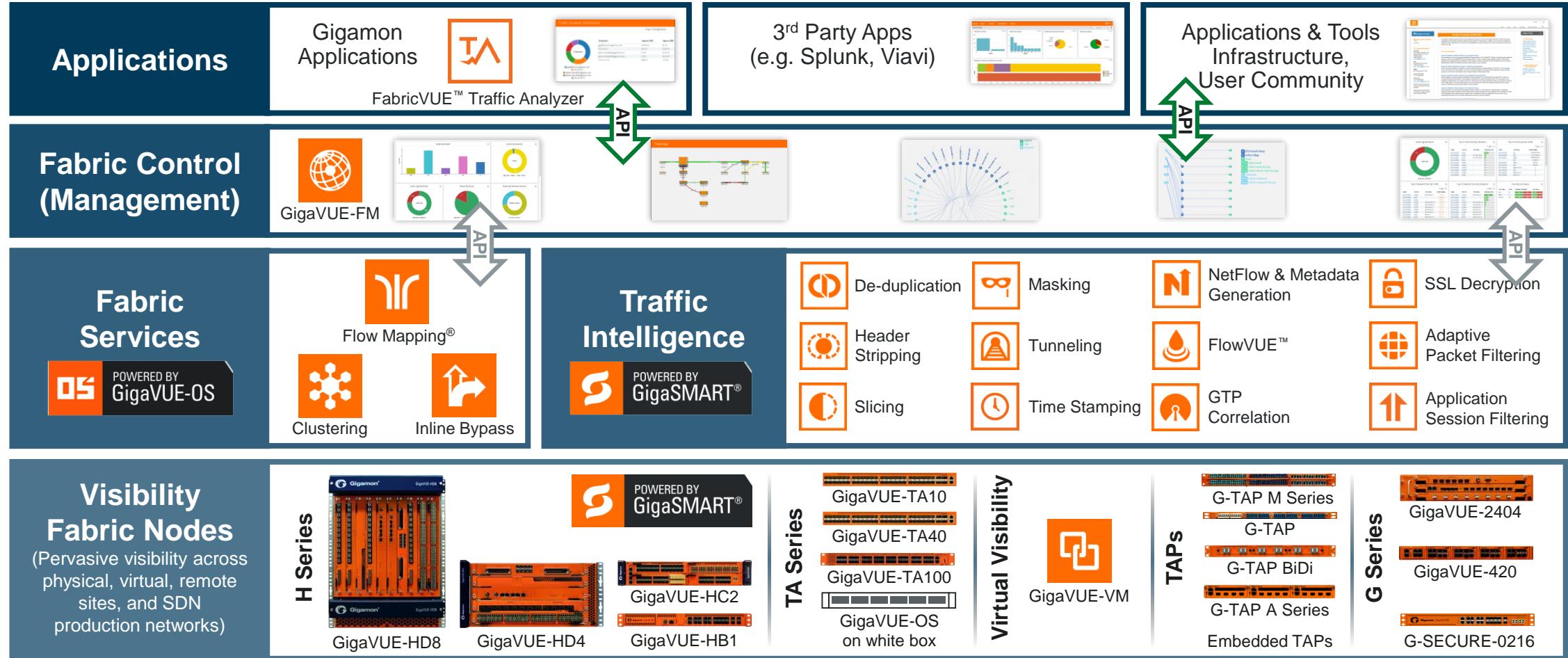


- ✓ 全面性的訊務視別能力
- ✓ 精密篩選訊務供不同資安設備
- ✓ 大幅提昇資安設備效能

Gigamon適用於各種不同資安, 分析設備應用



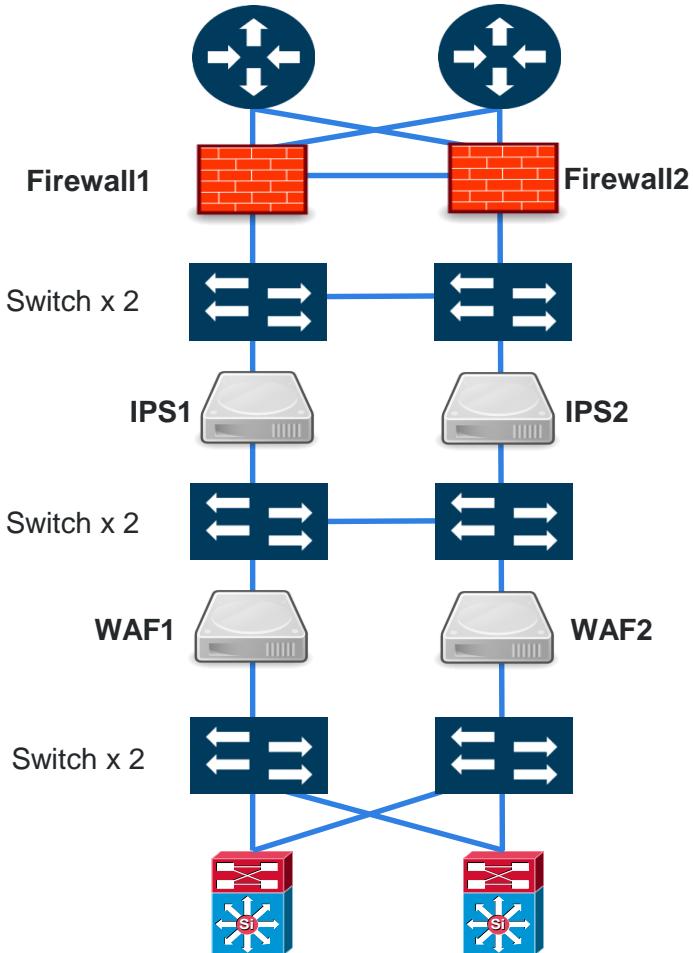
Gigamon全範圍可視化方案 - Visibility Fabric™



資安訊息派送平台應用範例

應用一：In-Line Bypass 增進資安運作效能與彈性

現有資安與網路的棘手問題



Active-Standby
浪費一台工具

資安設備必須與網路
頻寬同速率

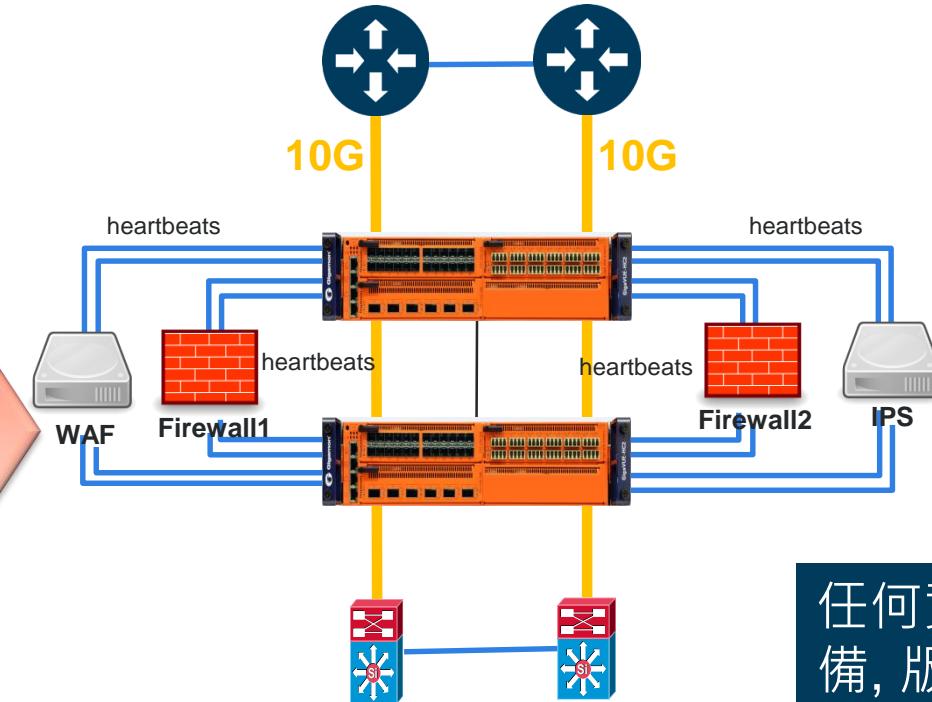
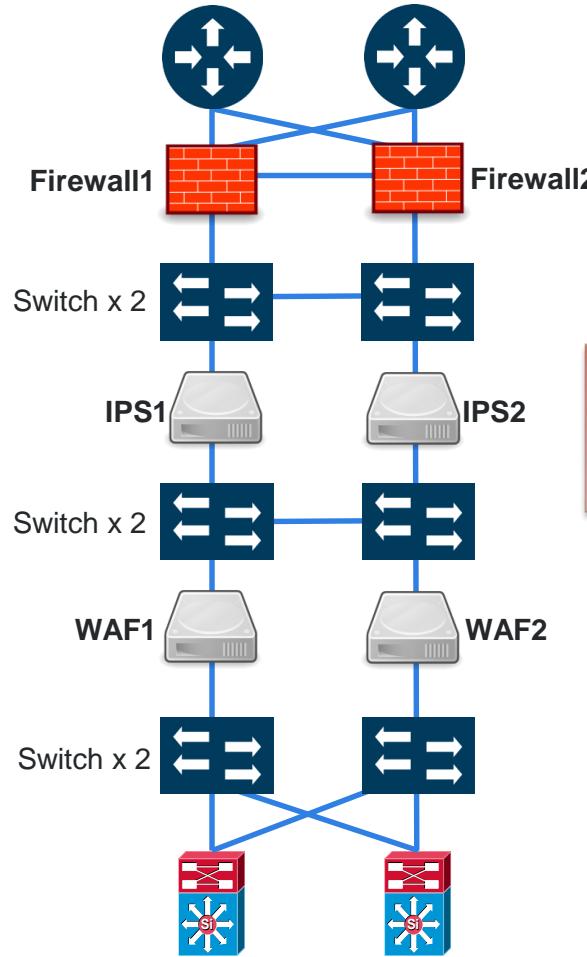
任一資安設備問題導致整個
網路運作受到影響

任何資安設備的變動，如新加/移除設
備，版本升級，必導致網路運作停頓

新增設備測試時，必須以實際運作的流量做測試，
導致測試時網路運作受到斷續續續的影響

應用一：In-Line Bypass 增進資安運作效能與彈性

解決了資安與網路組的棘手問題



簡化資安連結架構

雙資安設備可同時運作, 提昇檢測容量

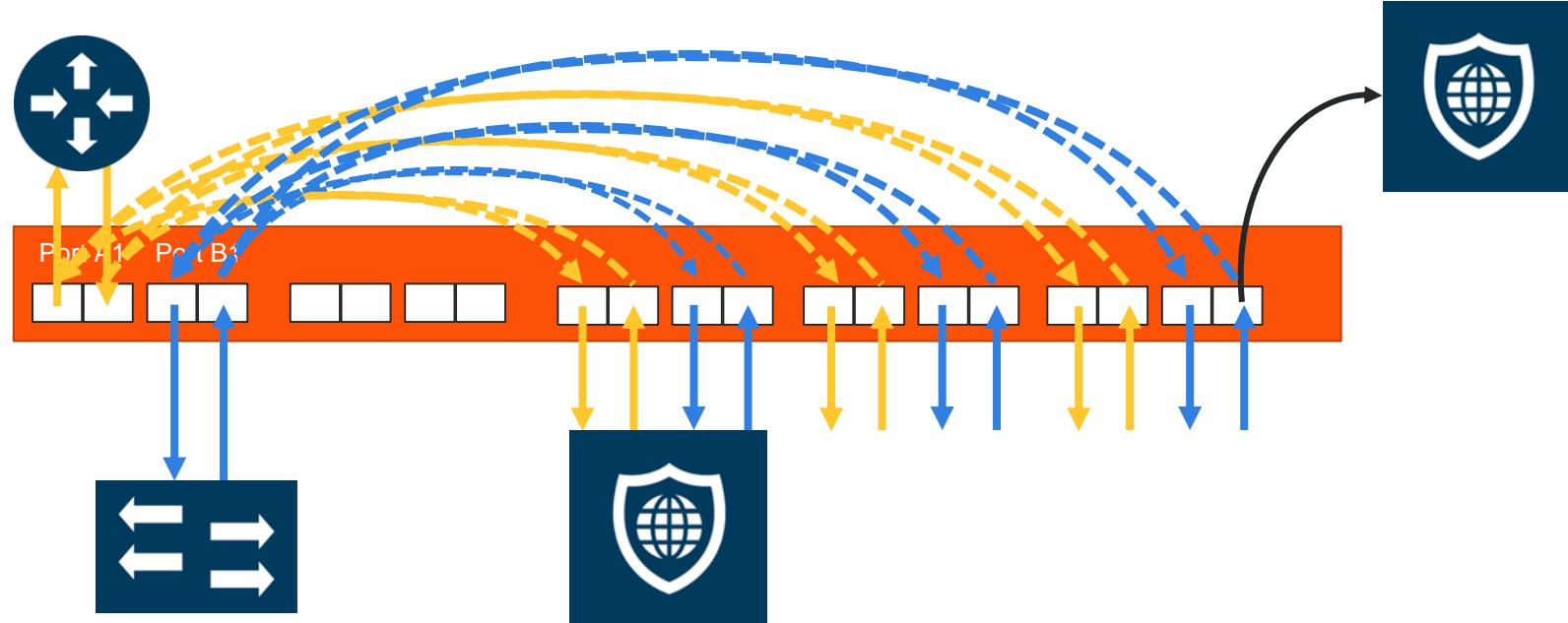
資安效能依網路實際流量配置而非網路頻寬而定

任何資安設備的變動, 如新加/移除設備, 版本升級, 並不影響網路運作

整合串接 Inline, 旁接 Out-of-Band, Flow-based 設備於 GigaSECURE® 平台一體架構

應用一：In-Line Bypass 增進資安運作效能與彈性

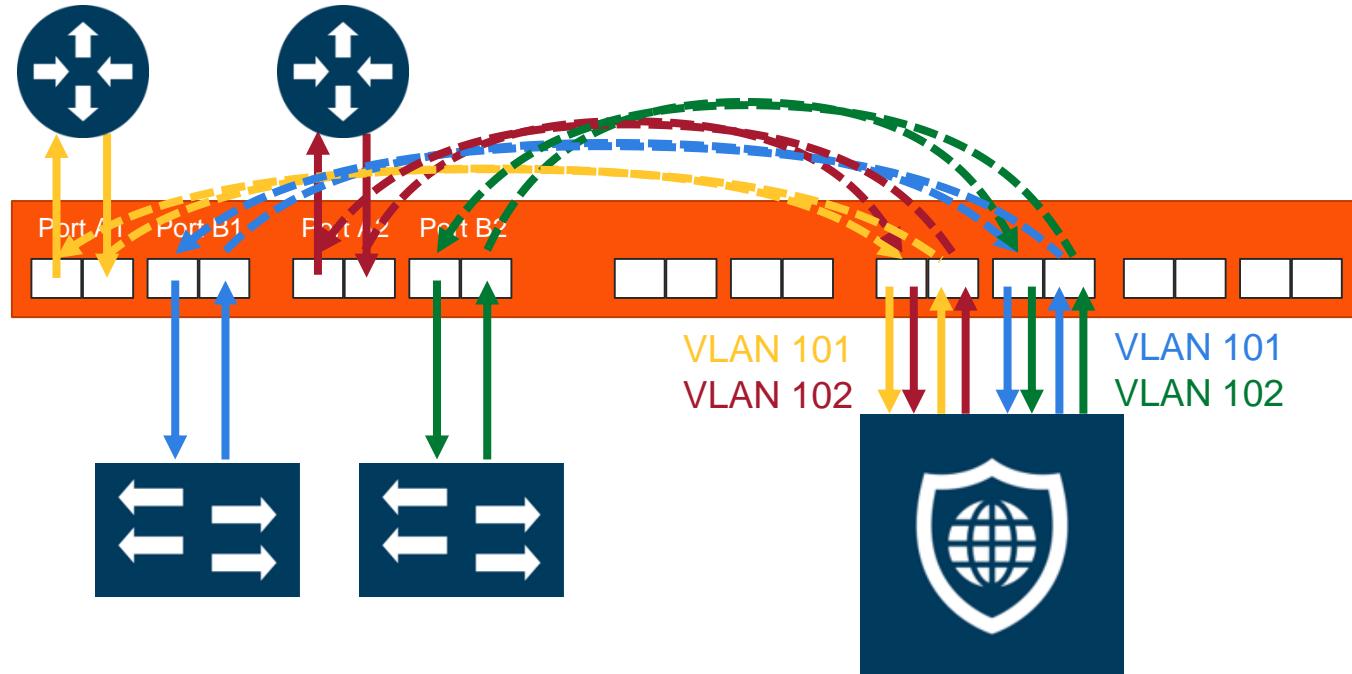
一對一、一對多



- 把流量均衡分配到幾台設備上，擴大資安管理的規模
- 同時可加入頻外(out-of-band)分析工具，擴大資安管理的能力

應用一：In-Line Bypass 增進資安運作效能與彈性

多對一、多對多



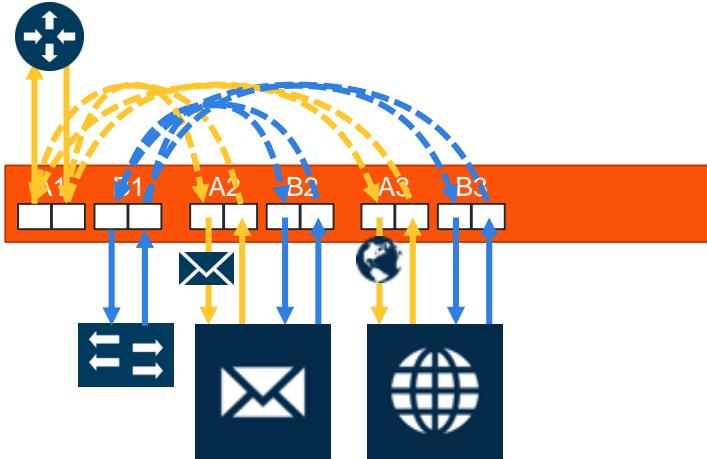
- 合併多條線路的流量 (最多可以36條線路)，轉發去同一台 inline 資安分析設備上
- VLAN標籤用來區分回路 (回到真正線路前會自動去掉)

應用一：In-Line Bypass 增進資安運作效能與彈性

Application-Aware Bypass, Serial Inline Tools

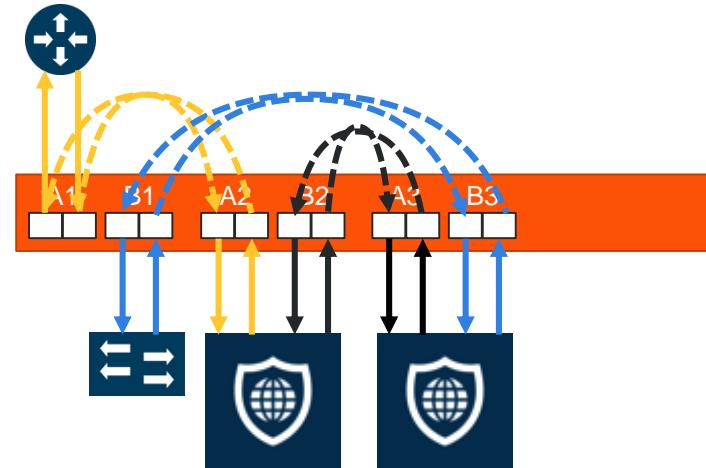


Application Aware Bypass



- 依不同應用程式種類需要去篩選訊務流量至不同資安設備
- Inline訊務流量可以啟用**Flow Mapping**功能
- 對不同資安設備可建立專屬L2-L4篩選政策
- 對不需監的訊務流量直接Bypass
- 可提昇網路與應用程式效能

Serial Inline Tools



- 可同時送串聯訊務流量到多個資安設備介面
- 可以**Bypass** 有問題的資安設備而不會導致網路中斷
 - 串聯設備一台斷線導致全部流量中斷
- 可任意增加/移除或昇級資安設備而不影響網路運作

應用二

全網NetFlow / IPFIX Generation



應用二：全網NetFlow / IPFIX Generation

資安訊息派送平台產生不同需要的NETFLOW METADATA內容



Flow Metadata

- 1:1式NetFlow/IPFIX的輸出，可增進“慢速攻擊”的偵測
- 可依不同資安設備設定不同篩選條件的NetFlow記錄
- 可以Offload資料傳輸交換器產生NetFlow/IPFIX的負擔



SIEM and NetFlow Forensics Integration

- 經由全流量Flow的視別可達成全域性(End-to-End)的資安防禦
- 對於利用資料傳遞通訊流程的攻擊方式特別有效地偵測
- 與市面領先之SIEM廠家或NetFlow統計鑑識設備商均有結合運作範例



Advanced Information Elements

- 可以選用輸出URL訊息至所產生的客製化格式中如
- 至多可以同時輸出6個不同NetFlow v5/v9 and IPFIX的接收/分析設備
- 可結合LLDP/CDP 定位資料傳輸來源介面

應用二：全網NetFlow / IPFIX Generation

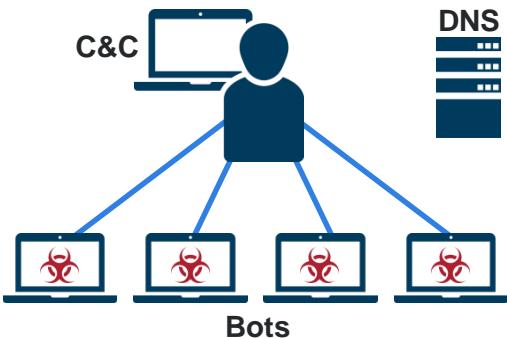
HTTP Response Codes

1XX: Informational
2XX: Success
3XX: Redirection
4XX: Client Error
5XX: Server Error



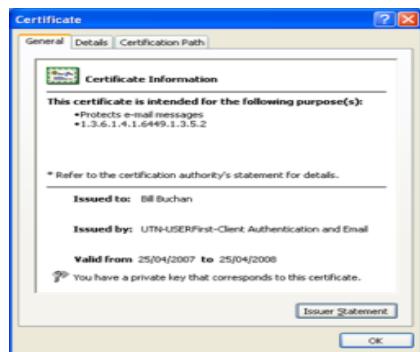
經由HTTP行為可發現DDOS攻擊以及內部網站主機
被入侵情形

DNS Discovery*



DNS transactions 可發現
惡意程式利用C&C控制內
部端點情形

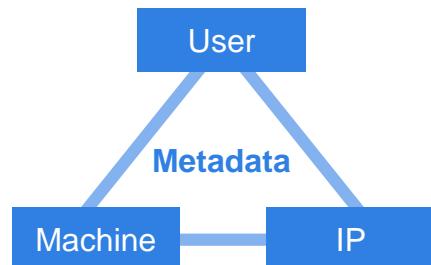
HTTPS Certificate Anomalies*



分析 HTTPS certificates 可
發現異常憑証使用

* Planned

Mapping User, Hostname & IP Address*

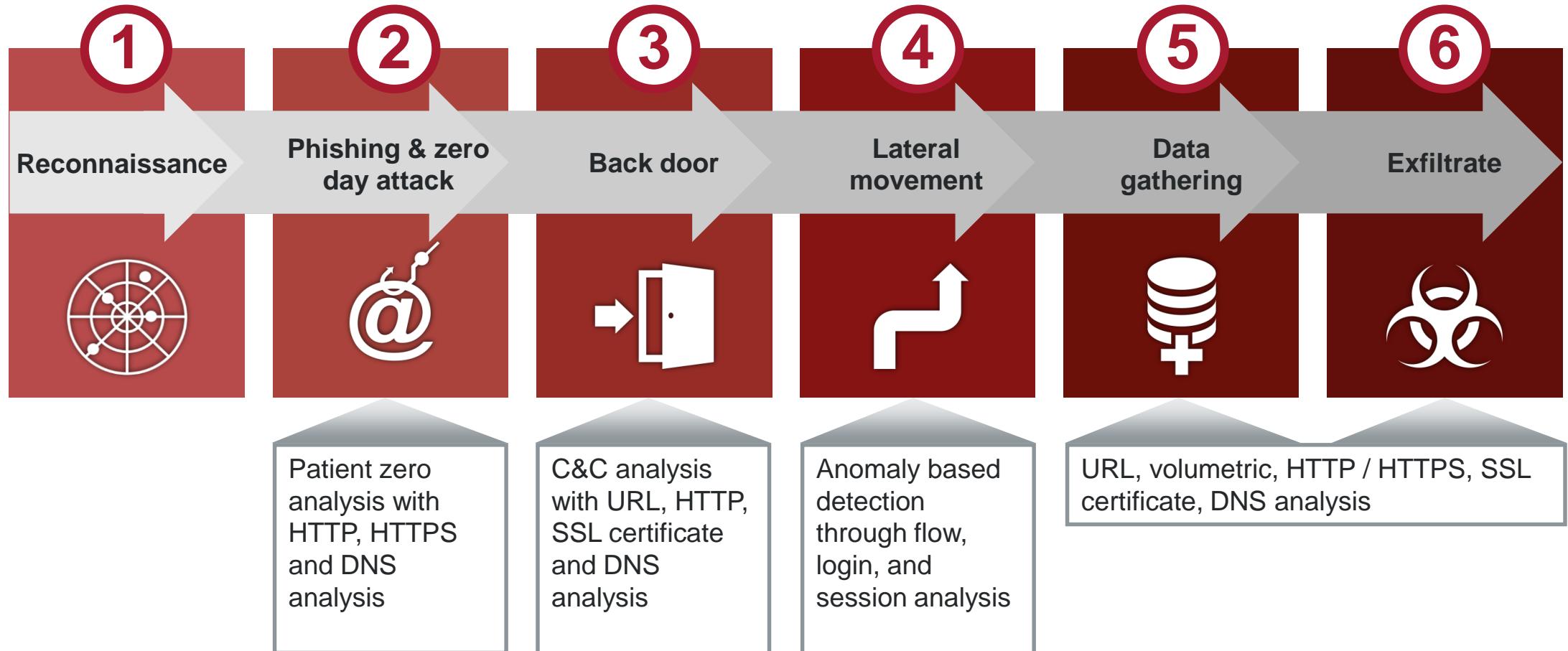


關聯Kerberos 認証與
DHCP記錄以鎖定端點名
稱, IP (hostname and IP)
與其傳輸流向

Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and subject to change.

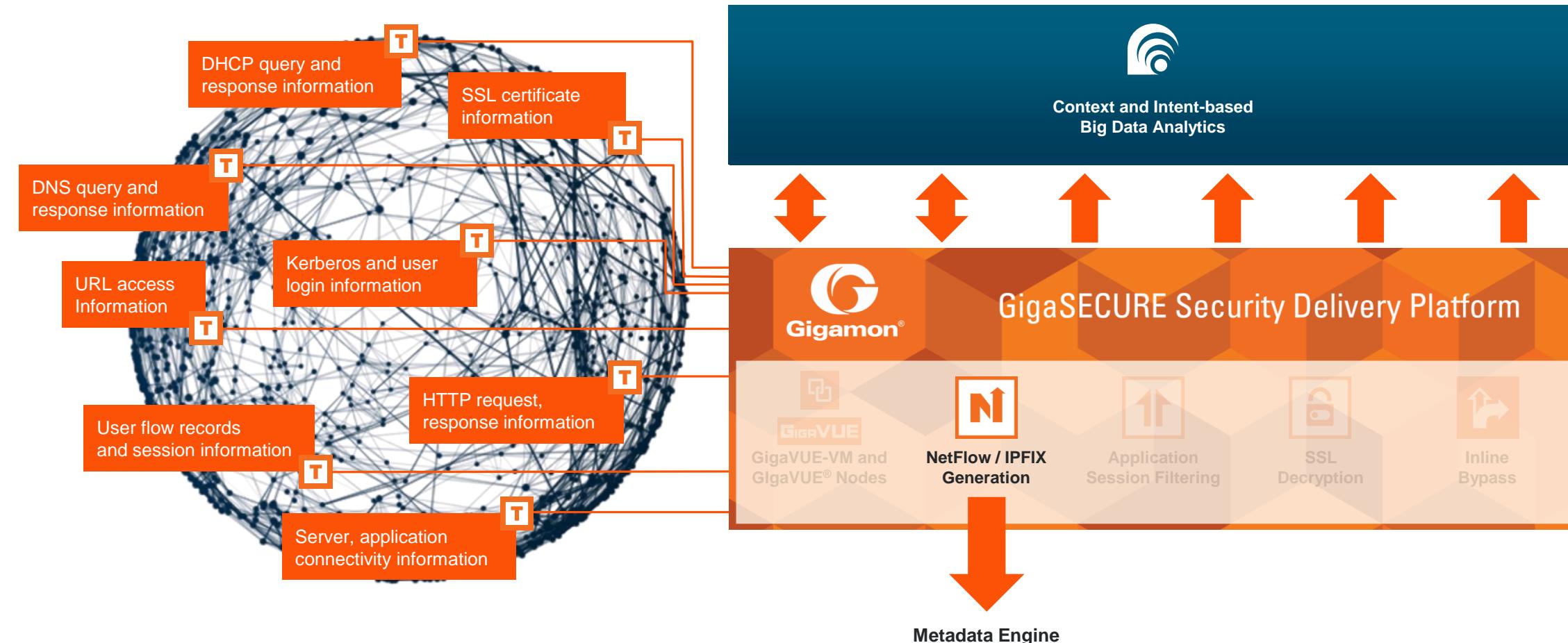
應用二：全網NetFlow / IPFIX Generation

NETFLOW/IPFIX應用在資安偵測的範例



應用二：全網NetFlow / IPFIX Generation

NETFLOW與GIGAMON加值資訊可讓資安設備更快速地偵測問題所在



應用二：全網NetFlow / IPFIX Generation

已適用多家FLOW 分析與資安設備方案

plixer

Currently
Available

splunk®

Currently
Available



Lancope®

In
progress

LogRhythm™

In
progress



In
progress

RSA

In
progress



In
progress

應用三

虛擬環境流量可視式

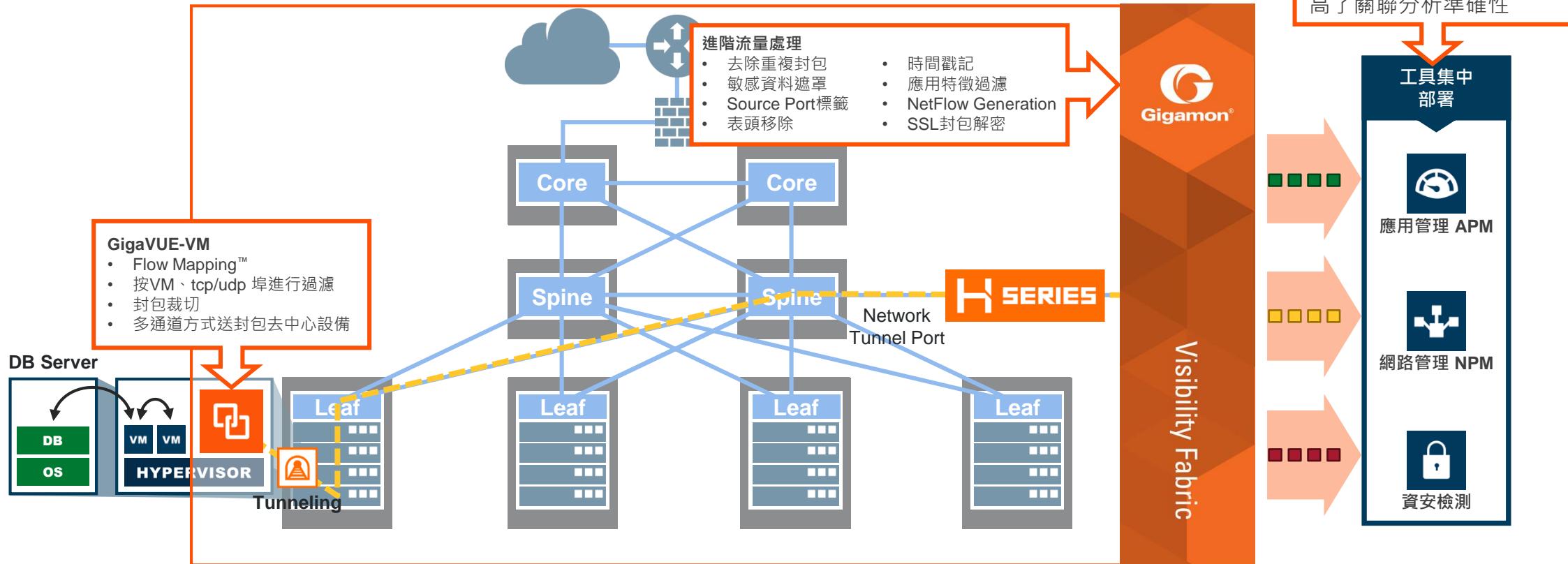


GigaVUE

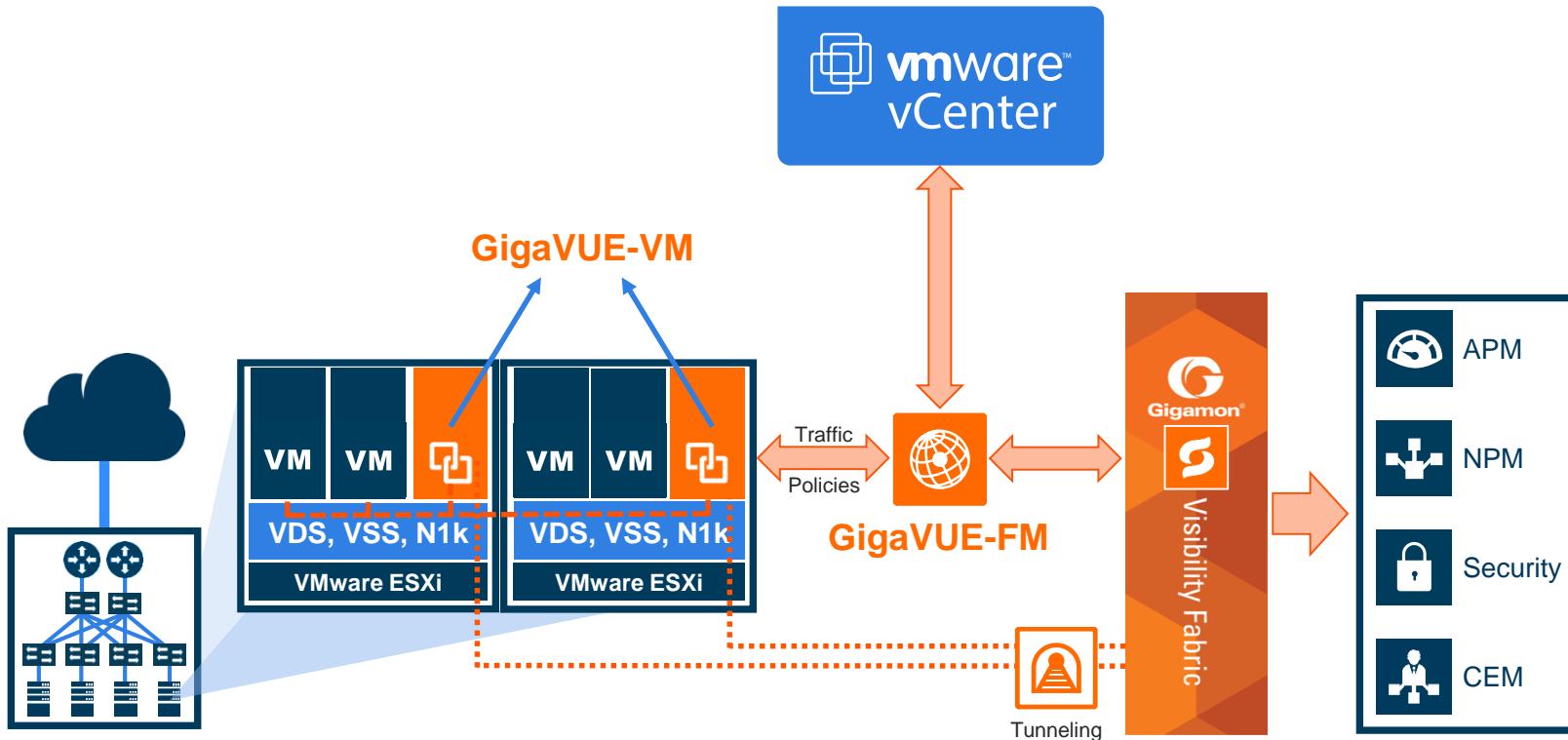
GigaVUE-VM and
GigaVUE® Nodes

應用三：虛擬環境流量可視式- GigaVUE-VM

LIGHTWEIGHT VM，非侵入式的NFV架構流量收集



應用三：虛擬環境流量可視式- GigaVUE-VM



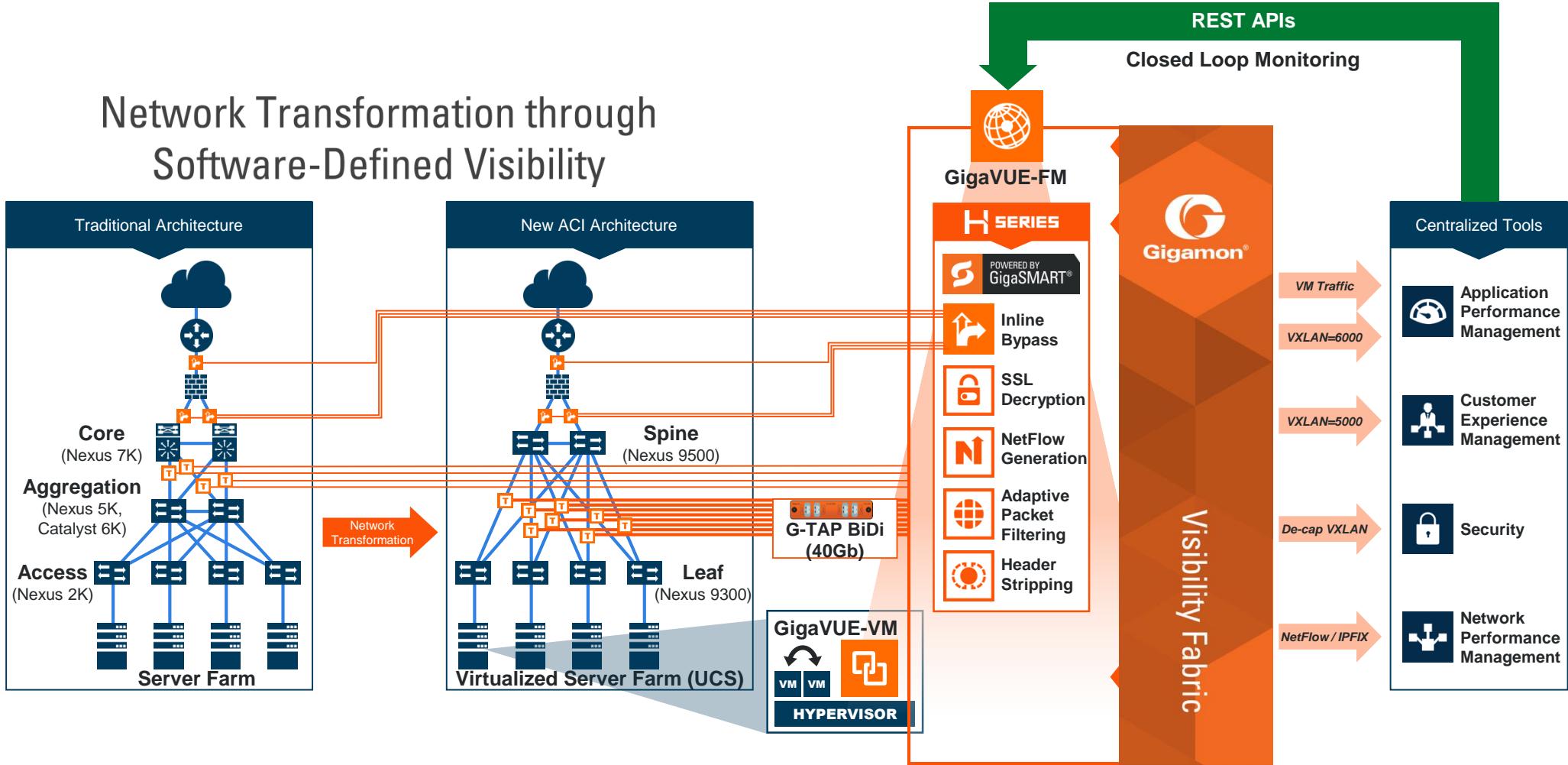
- 只在主機Hypervisor 佈放建置
 - GigaVUE-VM on every ESXi host
- 篩選所需流量輸出
 - VDS, VSS, Nexus 1k
- 與vCenter整合, 可偵測vMotion
自動找出所要監看的虛擬主機所在Hypervisor位置

應用三：虛擬環境流量可視式- GigaVUE-VM Cisco ACI 架構亦可應用



- 利用原有資安工具監看ACI架構流量
- 解析ACI 打包封包格式, 並去除 VXLAN報頭再派送給工具設備
- 流量分類篩選再派送給工具設備, 提昇工具設備效益而無需更新資安設備
- 因而降低資安設備成本

Network Transformation through Software-Defined Visibility



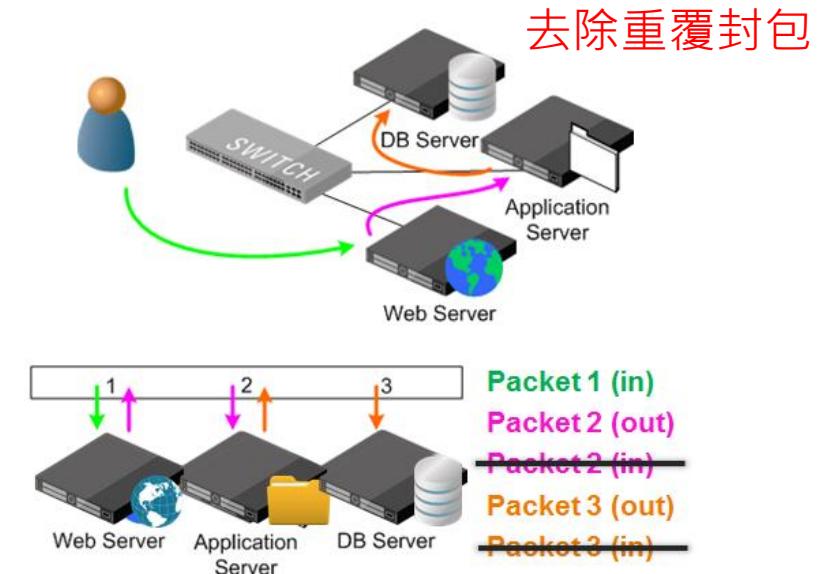
應用四

大幅減少記錄容量

應用四：大幅減少記錄容量

• 去除重覆封包

- 單一session流量經由數個網路結點，會產生多個相同而重覆的封包
- De-Dup功能可辦識相同session流量而將重覆封包只留取一筆，而可減少33~75%的封包量



• 封包裁切

- 對不同屬性流量可裁切不同長度的封包，可以減少側錄或大數據設備的容量
- 平均網路流量封包長度約為800Byte，如果依需要裁切為平均200Byte，則可節省80%流量

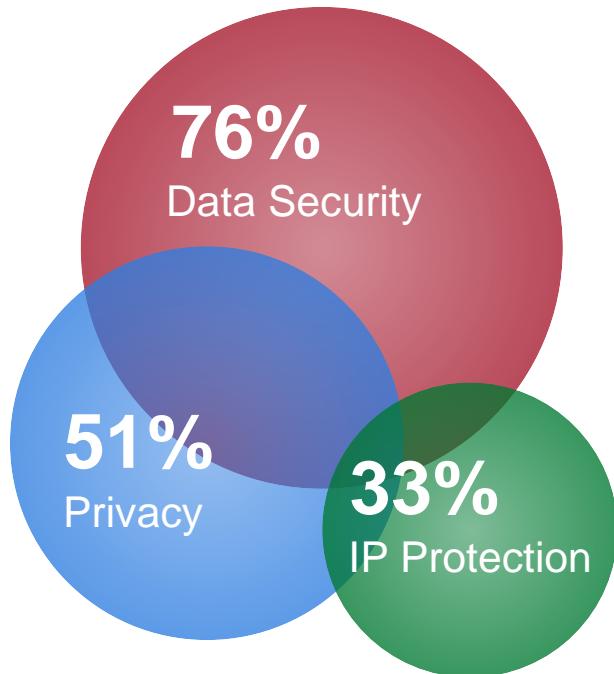




雲端的佈建有資安風險嗎？

雲端應用資安需求日趨強烈

資安議題是公眾雲客戶
的首要¹



- AWS: 每年近百億美金雲端營業額⁴
 - 2016第一季 達 \$257億美金營業額, 64% YoY

¹Goldman Sachs

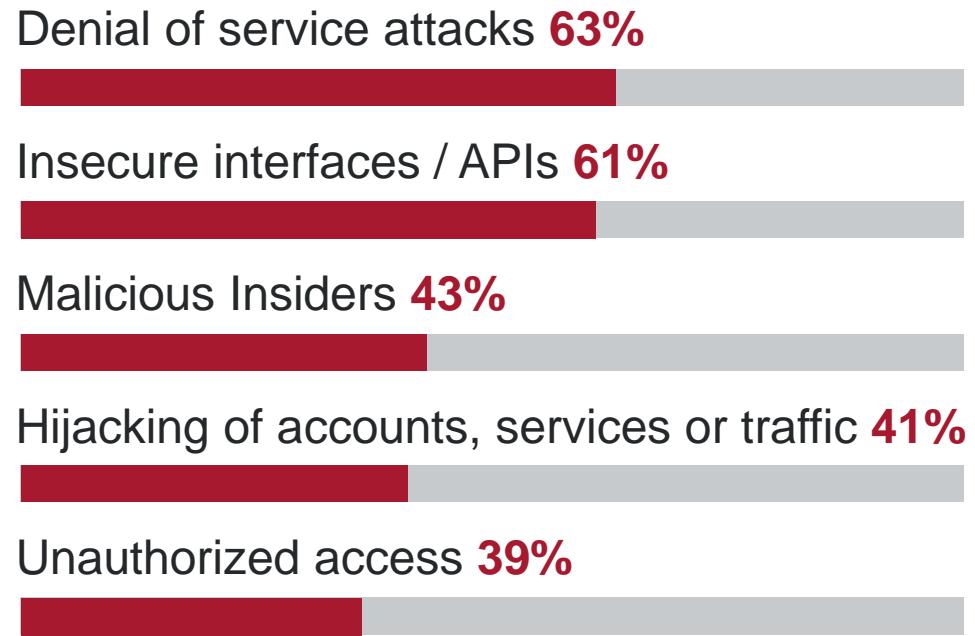
²CIO Insight 2015

³J.P. Morgan, May 2016

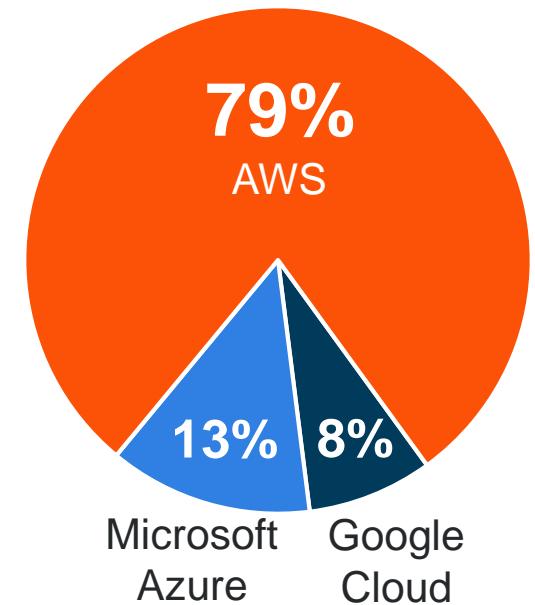
⁴Amazon Q1 2016 earnings

⁵AWS re:Invent 2015

公眾雲前5大資安威脅²



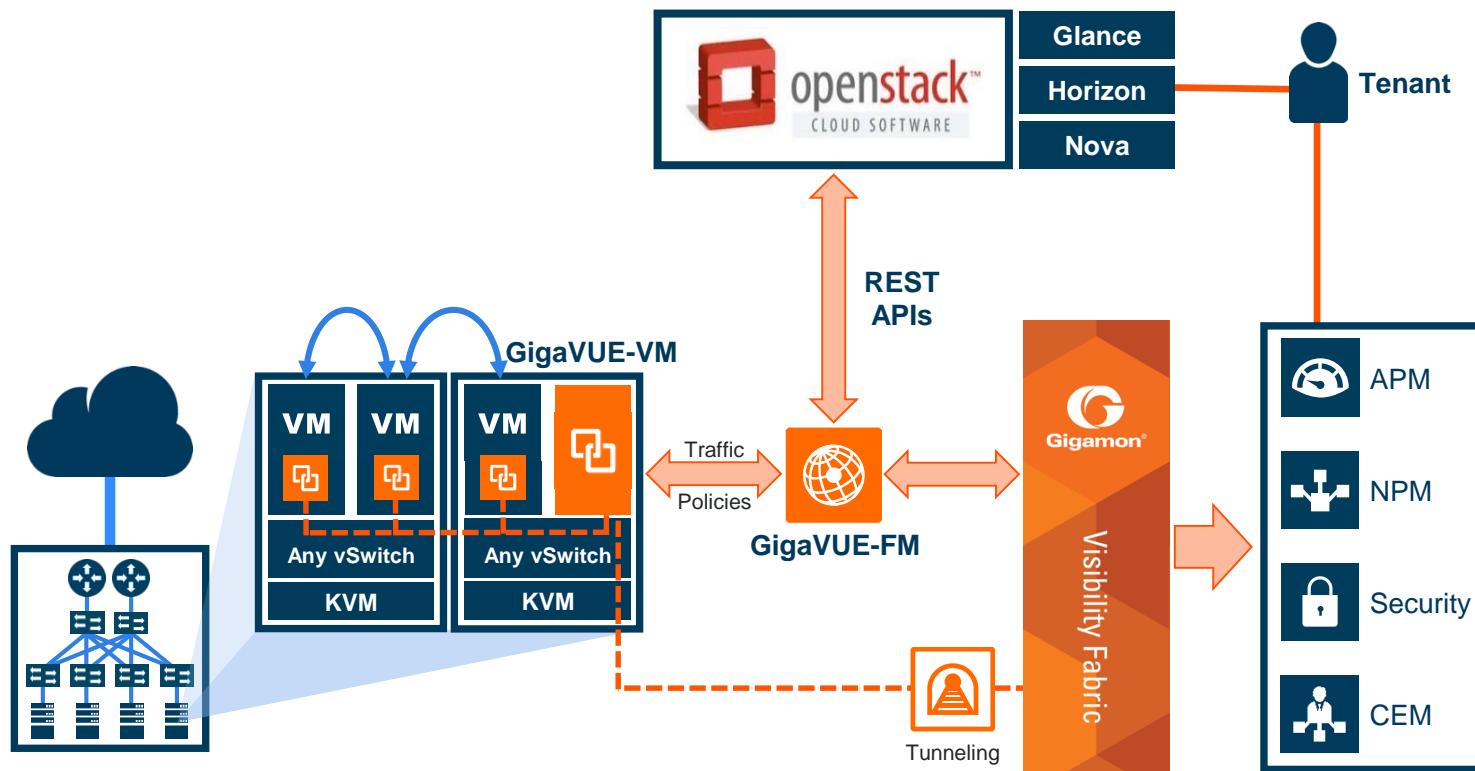
2015 公眾雲服務市場佔
有率³



- 已有百萬企業客戶數⁵

雲端環境用戶流量可視式 – OpenStack

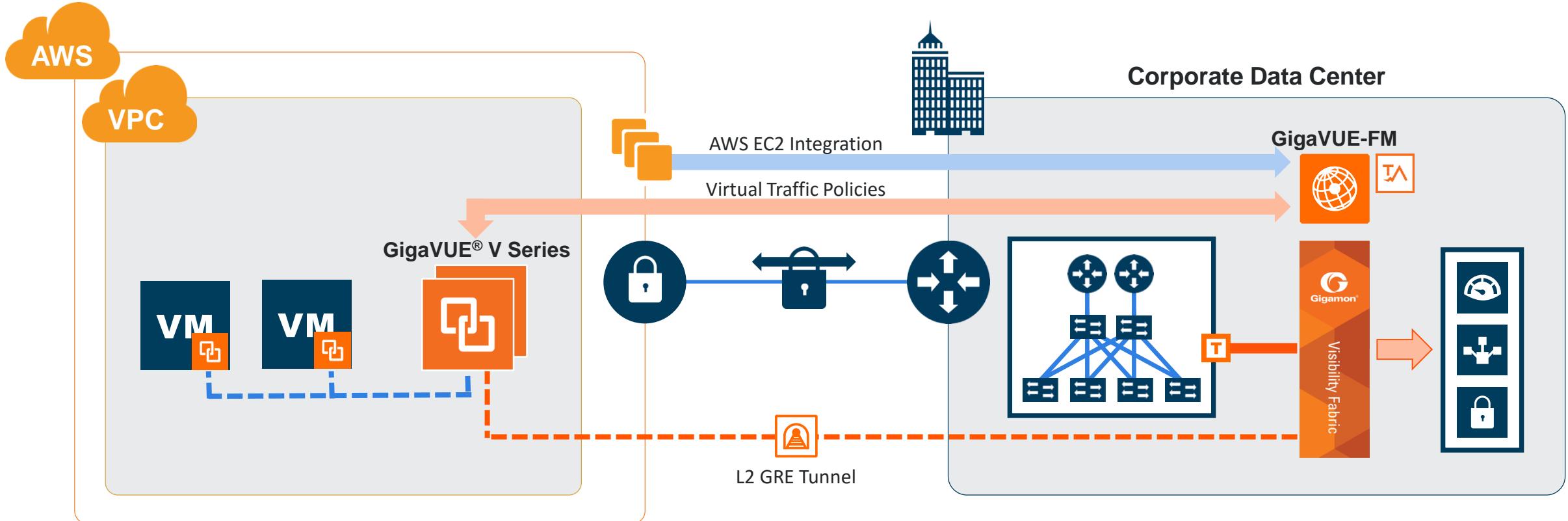
G-VTAP & GIGAVUE-VM 的協同運行



- 於客戶欲監視之雲端VM應用程序建置G-vTAP
- G-vTAP篩選該VM應用程式的訊務流量 Gigamon virtual appliance (GigaVUE-VM)集中
- GigaVUE-VM 可過濾, 裁切, 篩選後Tunnel至Gigamon Visibility Fabric設備再統一企業全網流量派送給暨有資安設備
- GigaVUE-FM 可統一管理企業全網與公眾雲的篩選與派送條件

雲端環境用戶流量可視式 – AWS 公眾雲

應用範例：資安工具設備置於單位內亦可監控雲端應用系統效能與安全



將AWS公眾雲上的VM應用程式負載流量導回企業資料中心的資安設備

VPC: Virtual Private Cloud. Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and subject to change.

Gigamon解決了公眾雲用戶的使用障礙

用戶使用公眾雲的障礙

- 機密與重要應用系統上雲端的資安問題無法完全放心
- 無法取得雲端用應用負載的流量分析
- 雲端環境資安與分析工具不多
- 取得雲端流量回企業增加線路費用

Gigamon Solution

- 提供完整而可用的訊務篩選，讓公眾雲端應用負載流量可視化
- 第一階段提供在AWS EC2，爾後會增加在其他公眾雲端服務系統
- 佈建方式極為彈性：
 - Hybrid cloud: Tools in the enterprise
 - Tools in the same VPC
 - Tools in a different VPC

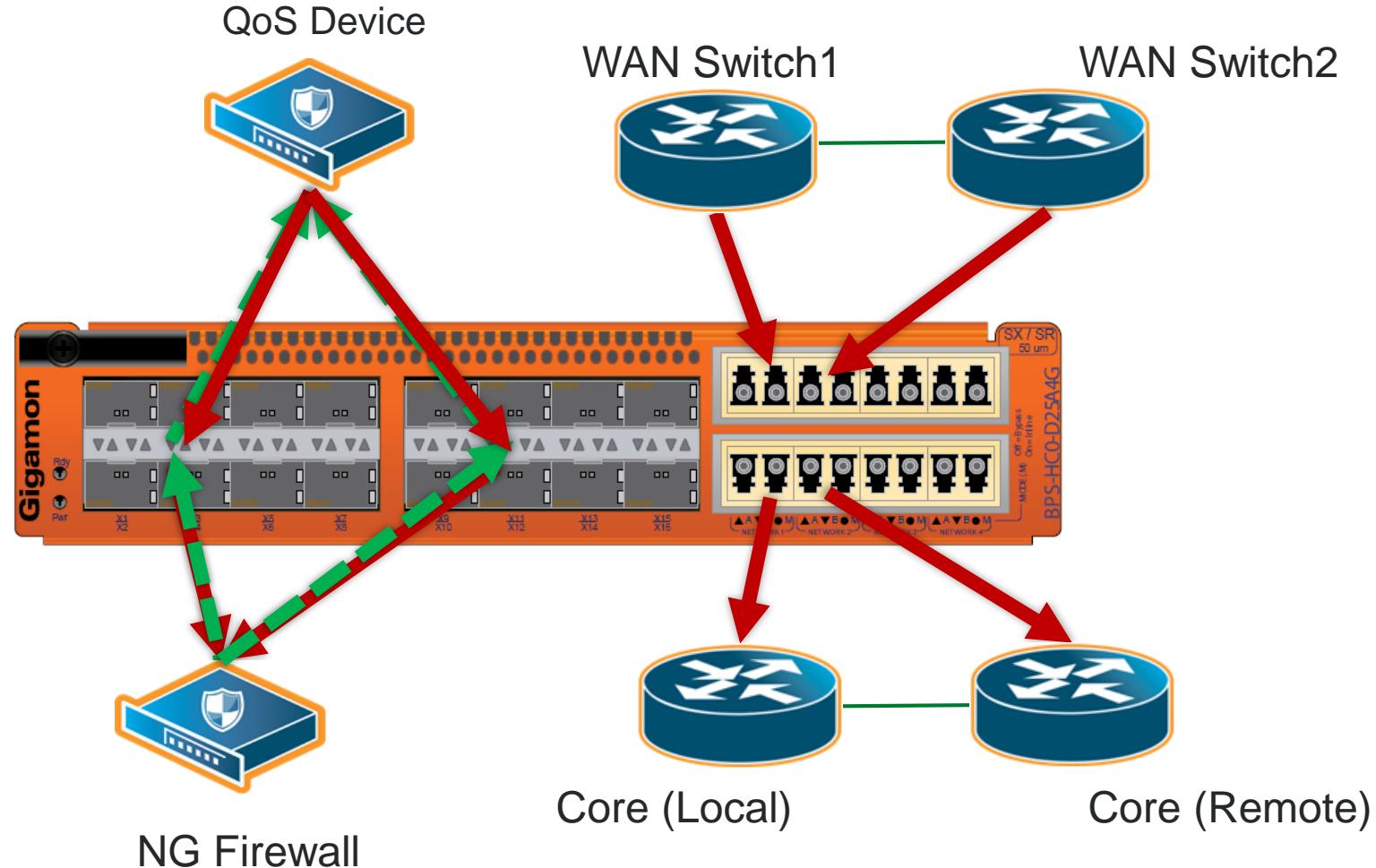
Gigamon 客戶實用案例分享

臺北某科技大學 計算機與網路中心

未建置Gigamon架構前困擾問題

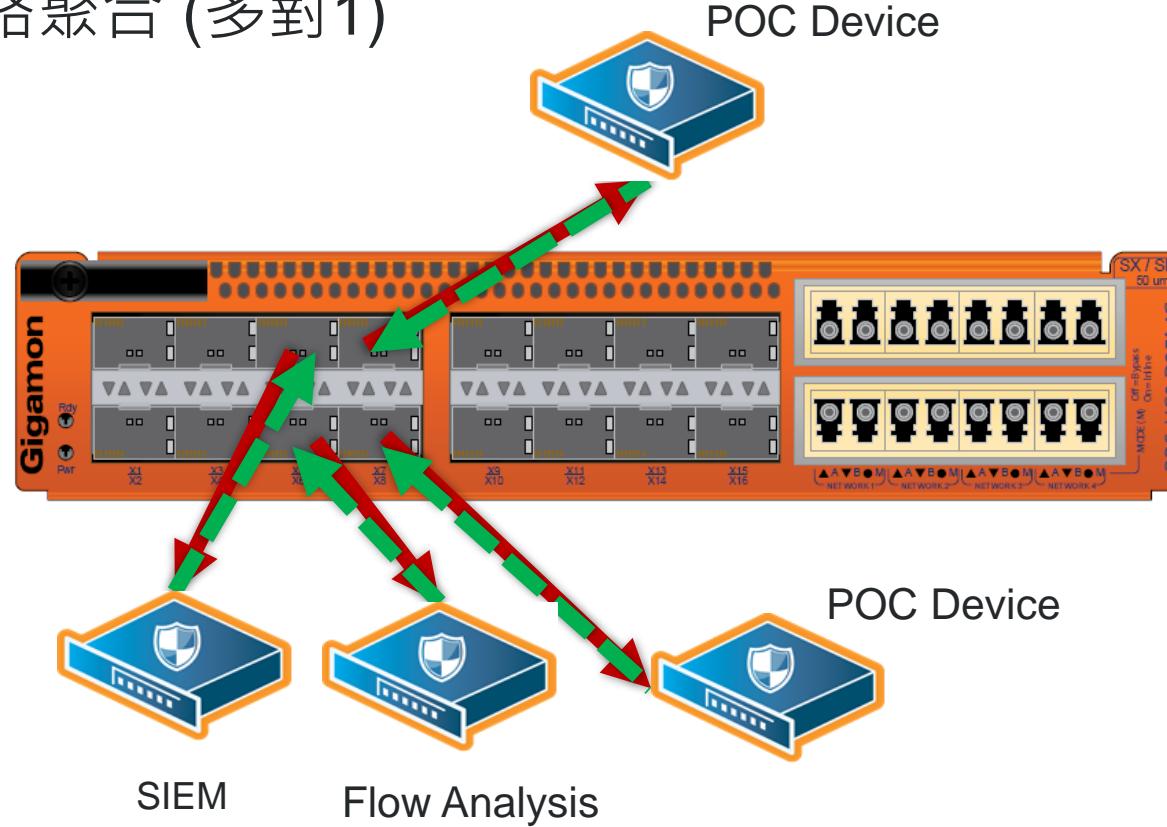
- 該科技大學因承辦技專校院招生委員會聯合會相關業務。因應教育部政策，資安等級提升為A級
- 評估峰值流量於一年內將增加為6Gbps至8Gbps
- 現有APT、WAF不是無對應流量之型號或是無法負荷之預算金額
- POC測試設備時無法克服
 - 核心交換器因Mirror Port過多無法負荷
 - 某些測試設備必須Inline，上線時調整線路造成斷線
 - 測試設備異常無法即時拔除

該校 In-Line 連接架構示意



該校 Out-of-band 連接示意

- 可透過設定將多路聚合 (多對1)



建置後現階段效益

- 設備採購成本降低
 - 緩衝資安設備HA一次到位預算壓力
 - 使用Map Filter 依照條件決定流量路徑。8Gb流量也能用4Gb設備，如：
 - IP Dst 非Server Farm 不通過WAF設備
 - 非SSL封包不通過SSL解密設備
 - 非關鍵業務網段不通過APT設備
- 高度彈性
 - 可控制介面，依需求彈性切換使用模式不浪費
 - 依政策需求可調整個別設備故障政策(Fail Open、Fail Close)
 - 設備測試、維護及升級不斷線，提升業務持續運作成效

**See More
Secure More**

