# 網路可視化與Inline加解密 全面提昇資安效益

## Gigamon在教育單位的應用案例

**Simon Chien 錢旭光**

*Gigamon 台灣分公司行銷業務總監*

# 主題

- **Gigamon 公司與客戶**
- **新世代資安威脅**
- **網路可視化平台 (Visibility platform) 概略**
- **可視化平台應用構想與實現**
- **教育單位客戶實用範例**

# Gigamon Quick Facts – 美商奇望

創立於
2004
(IPO 2013)

3000+
多個全球客戶

81%
Fortune 100
客戶使用率

~ 800
全球員工數

每年推出的新功能至少
90種

已安裝設備數量達
~25K

>40%
市場佔有率

**Gigamon Vision**

提供主動式全面性訊務可視性，提昇企業客戶下一代創新業務資訊安全平台

# Gigamon 客戶 – 教育產業

尚有許多新客戶進行規劃設計

NARLabs 國家實驗研究院 National Applied Research Laboratories 國家高速網路與計算中心

臺北市政府 教育局 Department of Education, Taipei City Government

宜蘭縣政府教育處
教育資訊網路中心

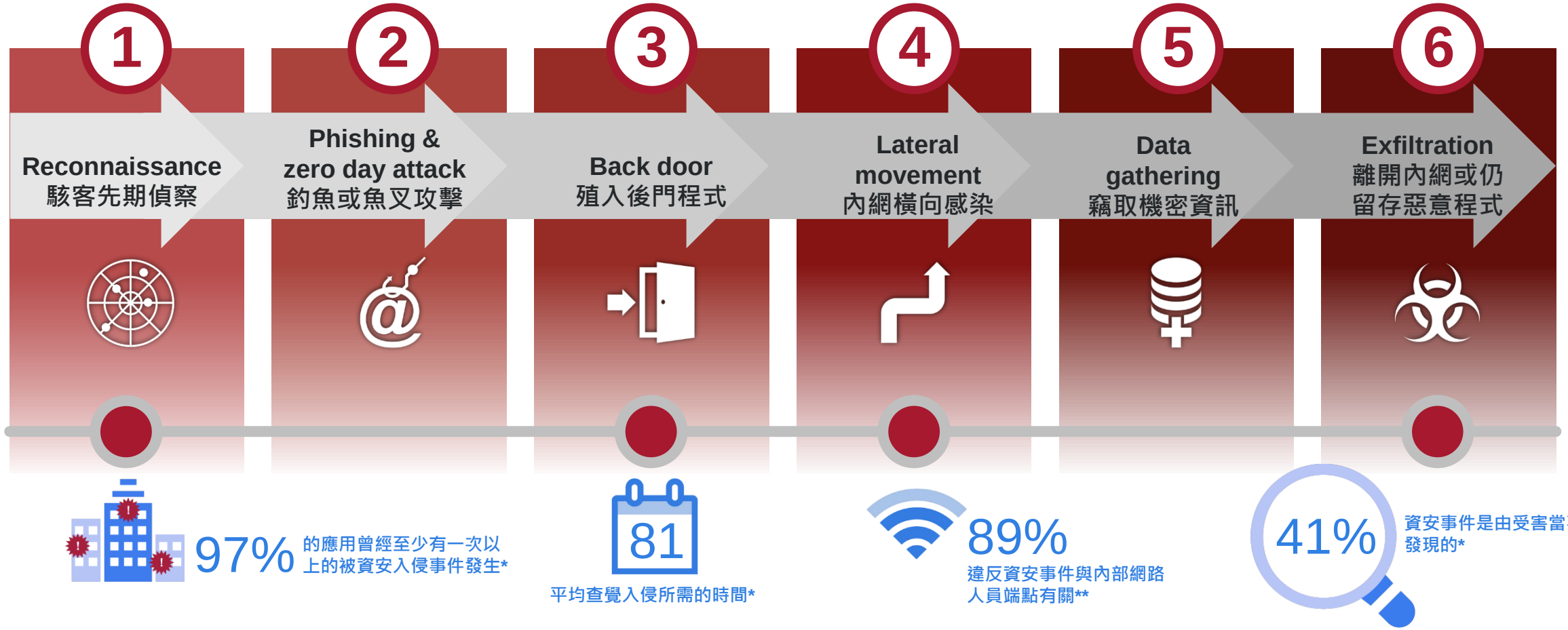
TAIPEI TECH Since1912 國立臺北科技大學 National Taipei University of Technology

國立宜蘭大學 National Ilan University NIU

國立臺東大學 NATIONAL TAITUNG UNIVERSITY

***可視化需求逐日殷切，新客戶持續增加當中!!!***

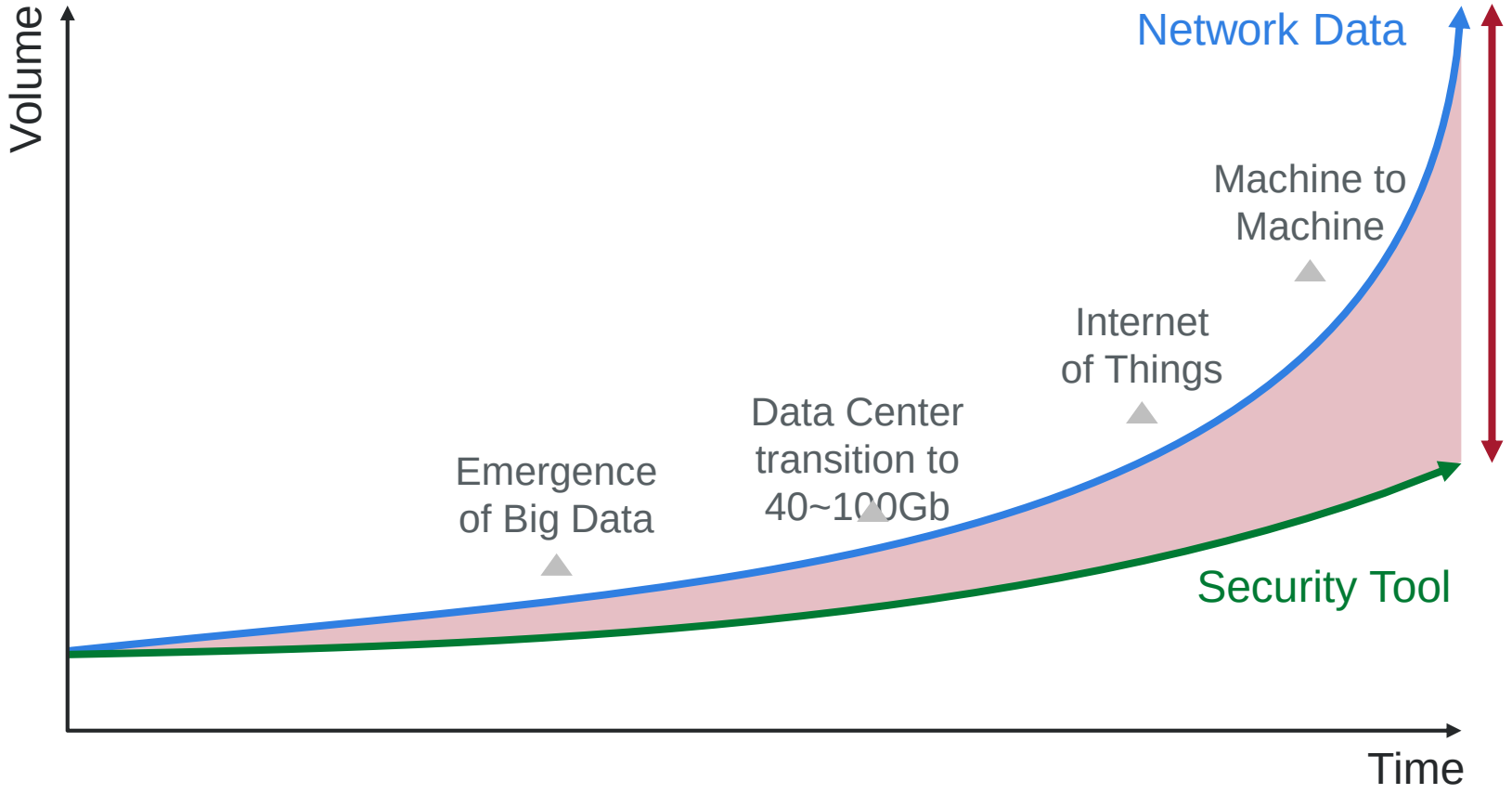
# 新一代資安威脅的變化 – 進階型攻擊不易阻檔




*Trustwave Holdings, Inc. "2016 Trustwave Global Security Report." 2016. Accessed April 5, 2017.
**Verizon. "2016 Data Breach Investivation Report." 2016. Accessed April 5, 2017.

# 新一代資安威脅的變化 – 網路流量與型態變化

資料量大增 + 網速倍增 + 駭客威脅變化多端 = 資安網路維運複雜 + 風險大增 + 成本倍增




資安設備處理效能無法跟上網速與資料量倍增

6.7 ns available to process a network packet on a 100Gb link

4.7ZB of global data center traffic in 2016*

1.7PB of M2M traffic in 2017**

*Cisco Global Cloud Index 2016.
**Statista Global machine-to-machine (M2M) data traffic from 2014 to 2019 (in petabytes per month)

# 新一代資安威脅的變化 – SSL加密流量與日俱增


**>80%** 在2019年企業資料加密流量將超過80%[1]

**80%** SSL加密流量將使資安設備的處理性能降低達80%[2]

**33%** 的Malware程式使用加密方式[3]

SSL流量的可視化需求無所不在因而格外重要 (Internet servers, Cloud services)

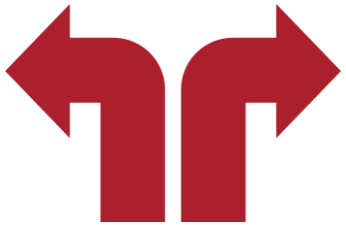
[1] Source: Gartner “Predicts 2017: Network and Gateway Security”, December 13 2016.
[2] Source: SSL Performance Problems, NSS Labs
[3] Source: 2016 Trustwave Global Security Report

# 資安威脅的本質正在改變

## 現有佈建的資安架構並無法解決下面的資安變化

進階式駭客入侵模式導致偵測時間與防制時間大幅拉長

傳統邊際端建置資安工具的模式無法防止駭客入侵或內網監測



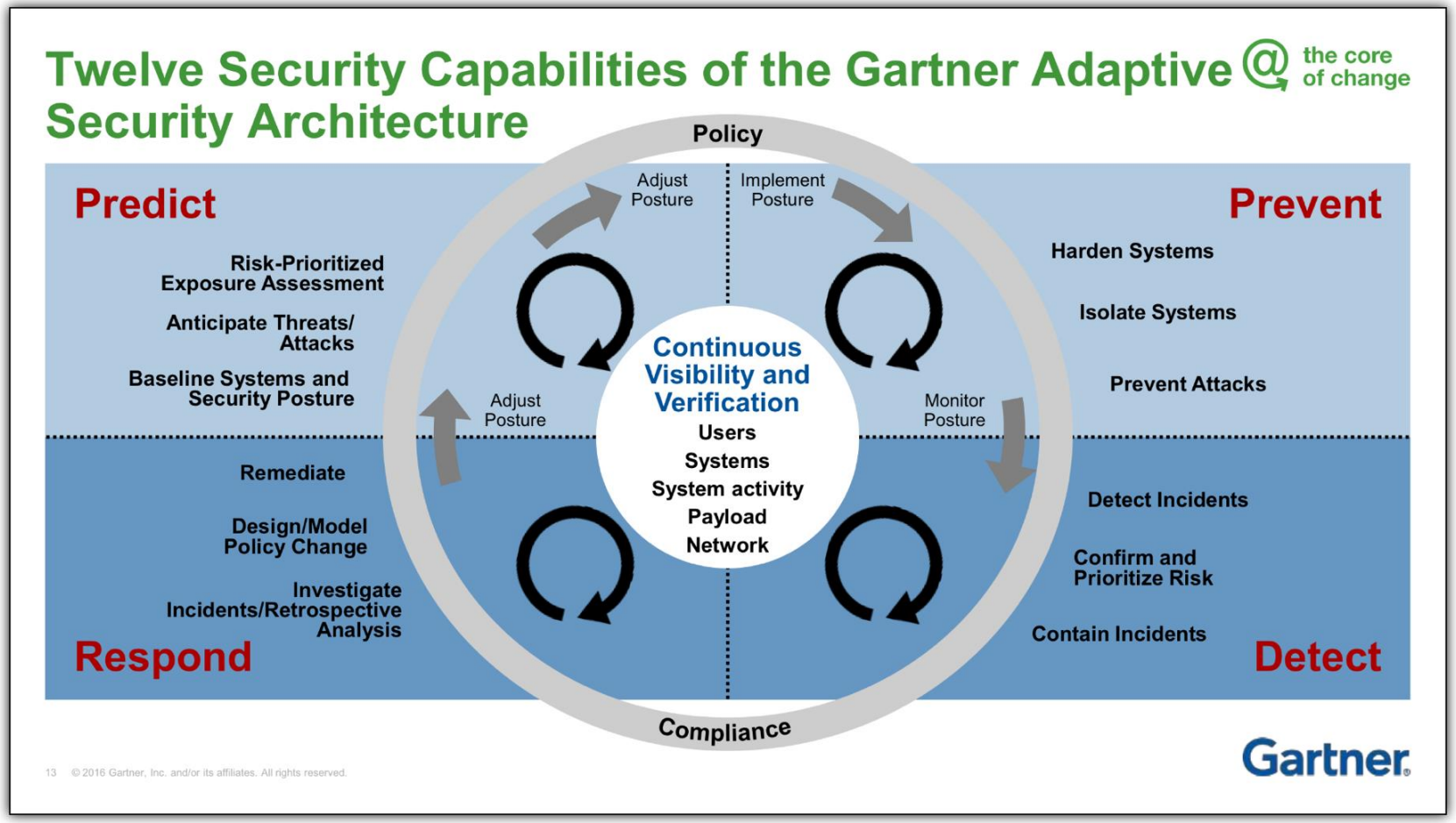
流量虛擬化/行動化讓固定端點偵測或防禦已無良好成效


SSL加密流量大增導致資安工具無法發揮效用

**因此需要一個新的資安運作架構**

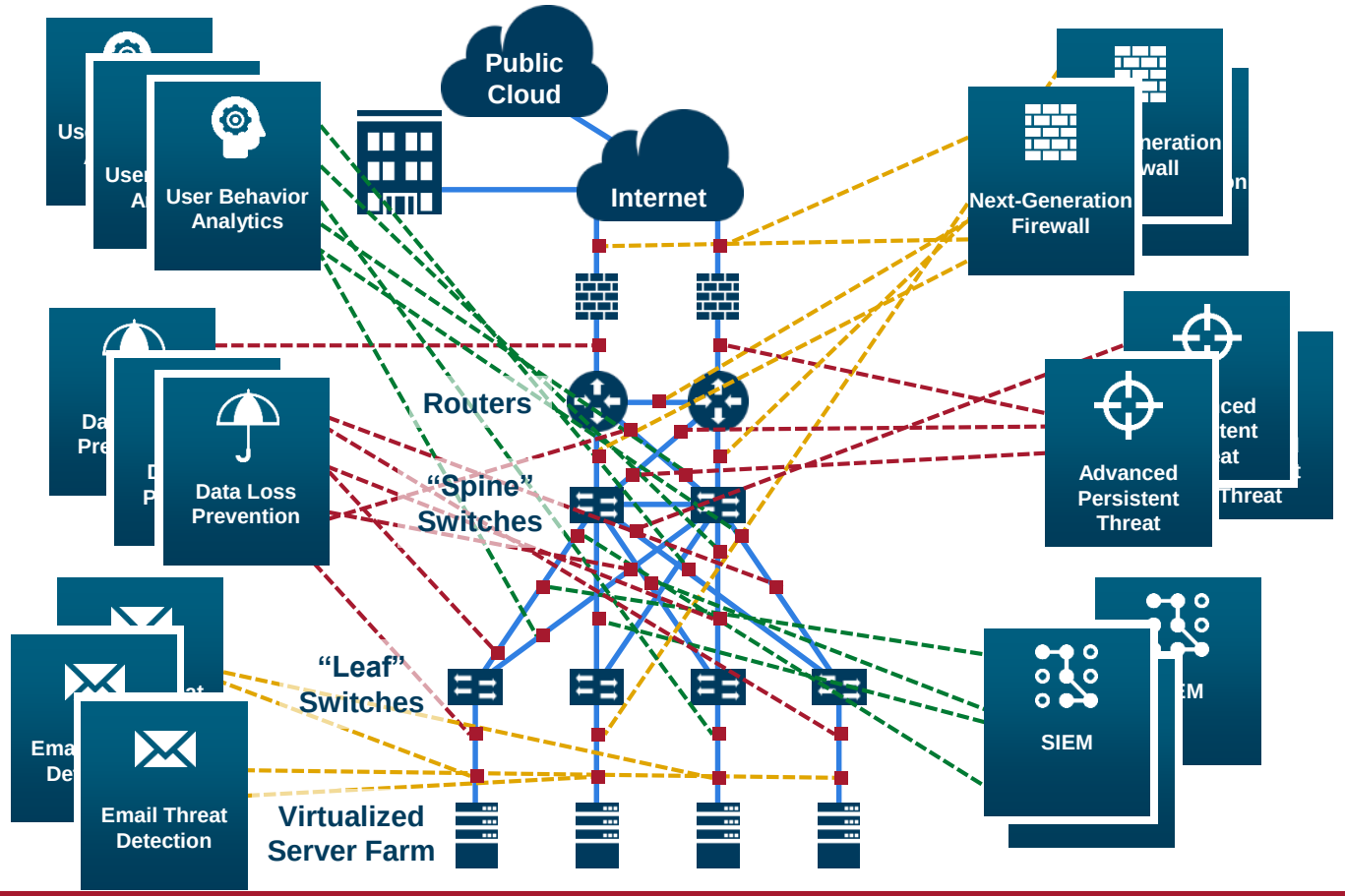
# 持續性網路可視化是資安防禦不可或缺核心基礎

## GARTNER 提出 ADAPTIVE SECURITY ARCHITECTURE 動態資安架構




*Source: Gartner Data Center Infrastructure Operations and Management Conference, December 2016

# 如何鎖定資安威脅: 現有的資安佈建面臨巨大挑戰




**資安防禦的挑戰：設備無法監測全網與分辨各種不同類型的流量**

- 整體網路盲點太多(僅介接某一結點)
- 加密封包無法快速解密或重覆解密
- 封包多層表頭無法去除而監測
- 虛擬主機或雲端作業無法監測其流量
- 工具HA建置時，資料去回不同路徑無法監測

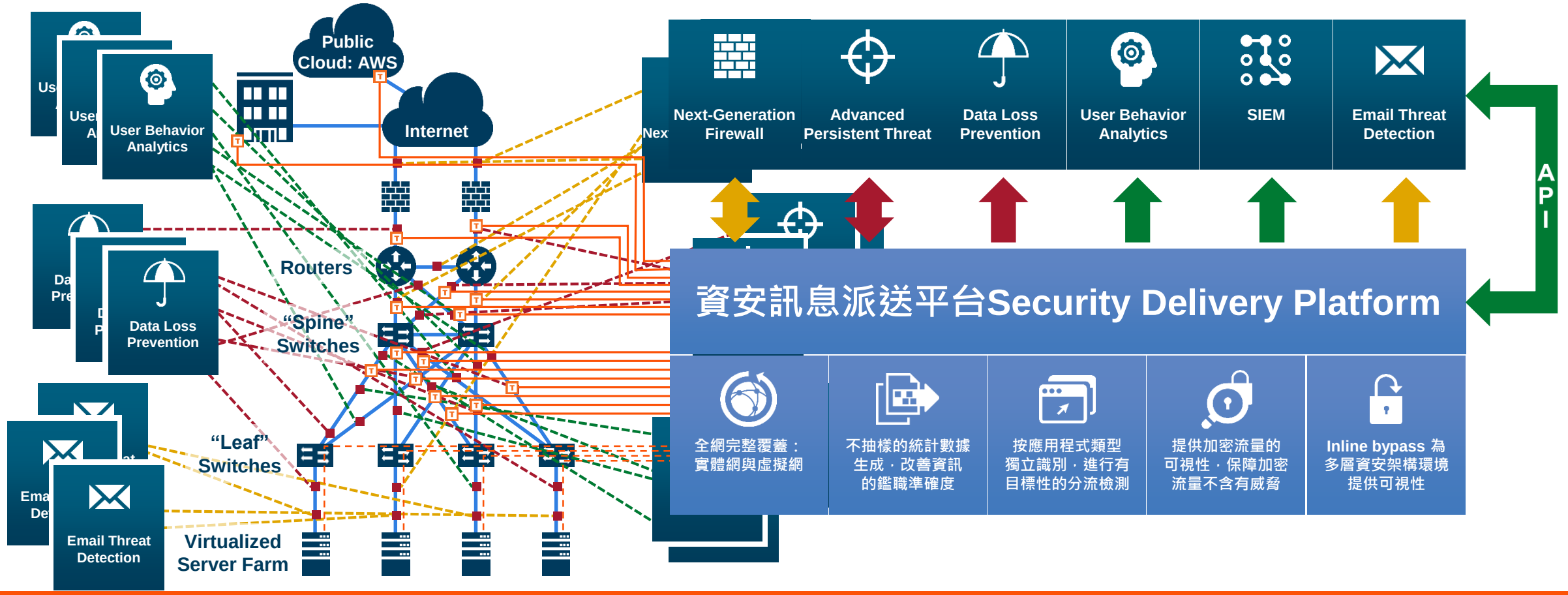
**工具介接網路設備的限制**

- 任何工具設備需更新均會影響網路
- 為達網頻相當的資安效能，成本甚高
- 資安、偵錯、分析設備日增，介接埠不足

***是該將主動權由攻擊者手上移轉至防禦者的時候了***

# 網路可視化應用 – 資安訊息派送平台

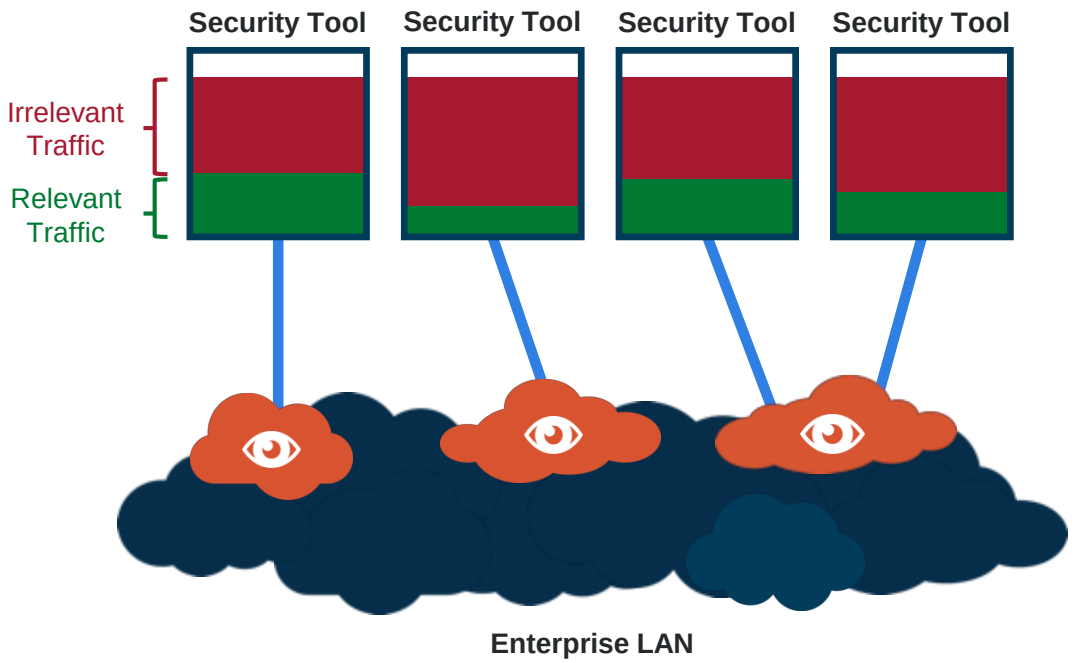
## LOOK INSIDE THE NETWORK




***Security Delivery Platform: A foundational building block to effective security***

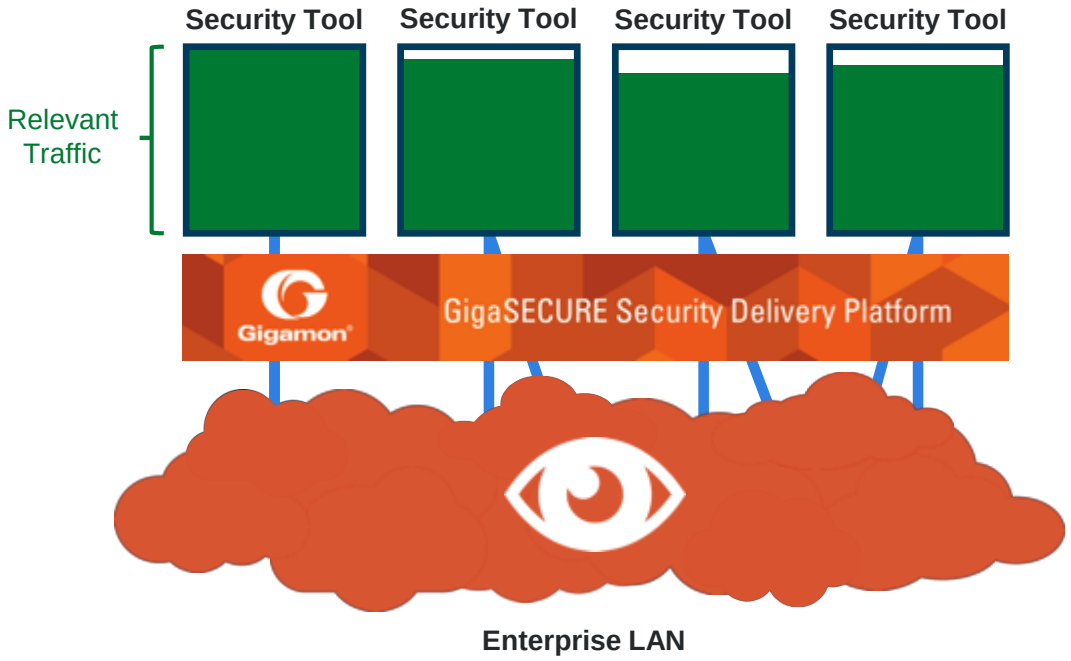
# GigaSECURE® 的優勢

## Legacy Approach Without Gigamon



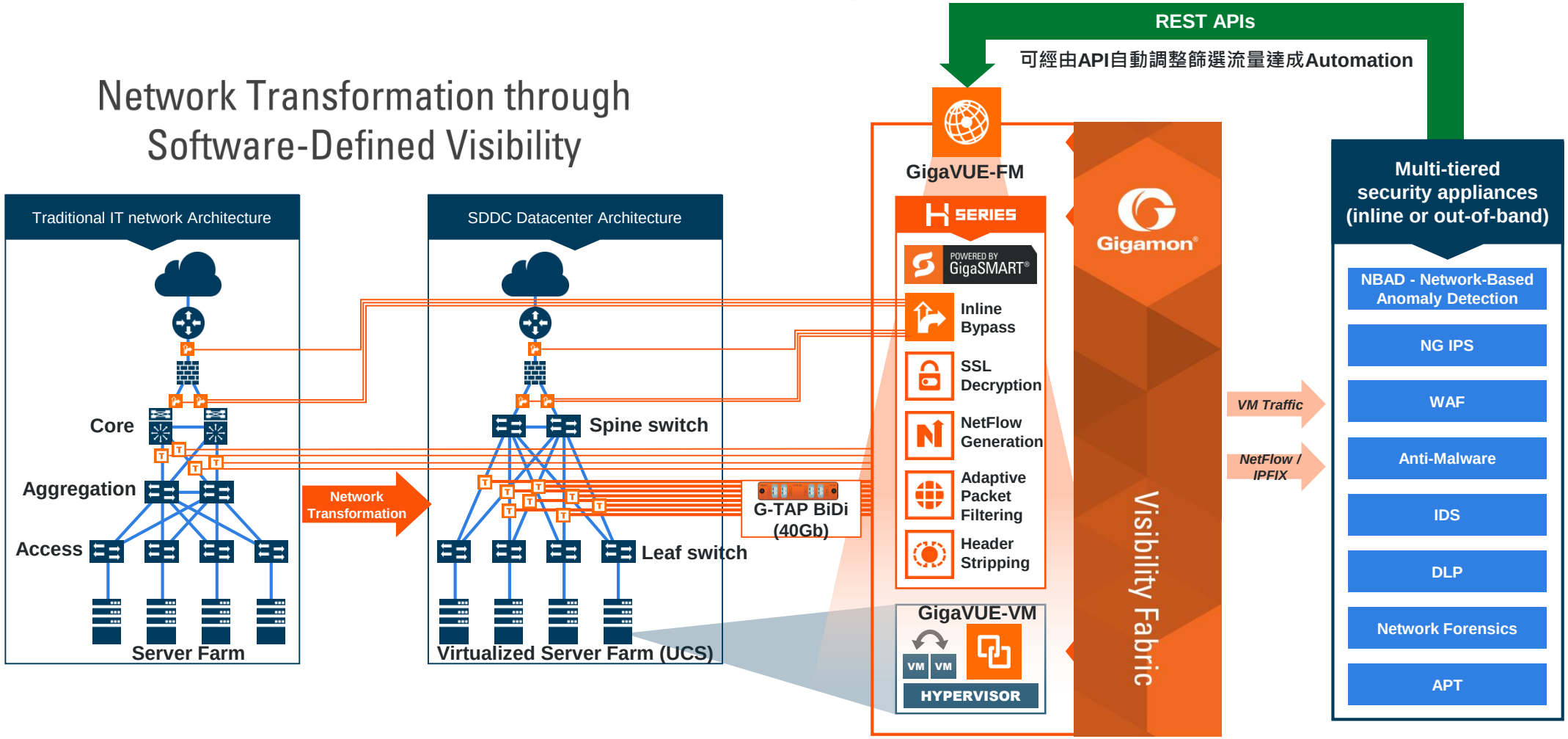

- 只見局部網路點之訊務
- 無法控制要取得哪種訊務
- 資訊設備的效能無法善用

## 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

# 全方位資安架構示意圖 – Gigamon結合資安設備




*經由Gigamon與各種資安工具整合方案達到偵測異常流量並自動反制或導向之能力*

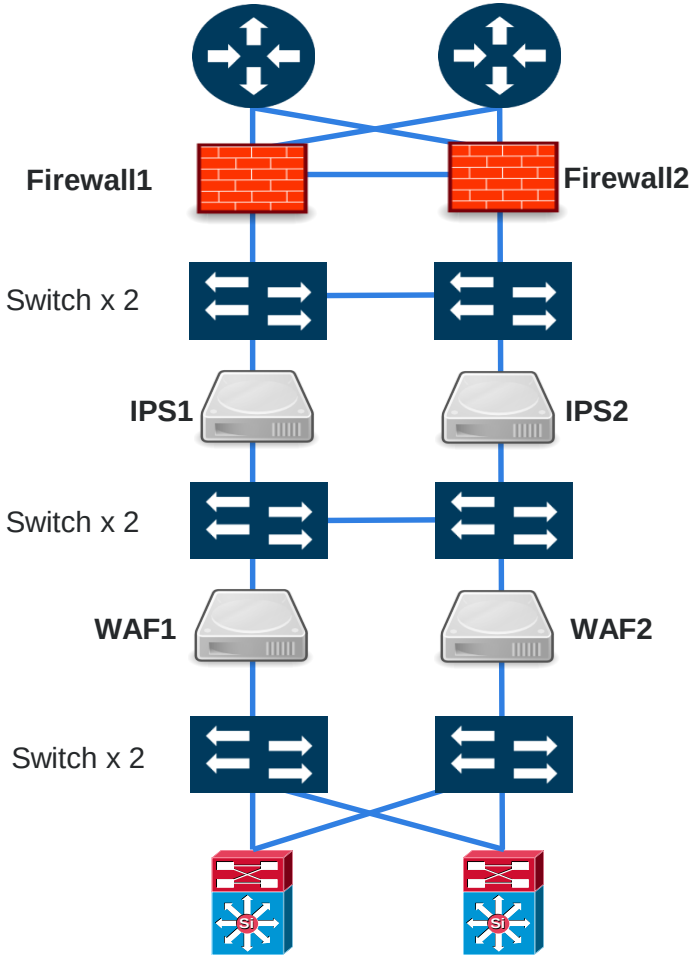
# Gigamon適用於各種不同資安, 分析設備應用

# 可視化提昇之加值應用

- In-Line Bypass與一機多用
- IPv4/IPv6同時Netflow輸出
- Inline SSL 加解密

# In-Line Bypass 管理讓人頭痛

## 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

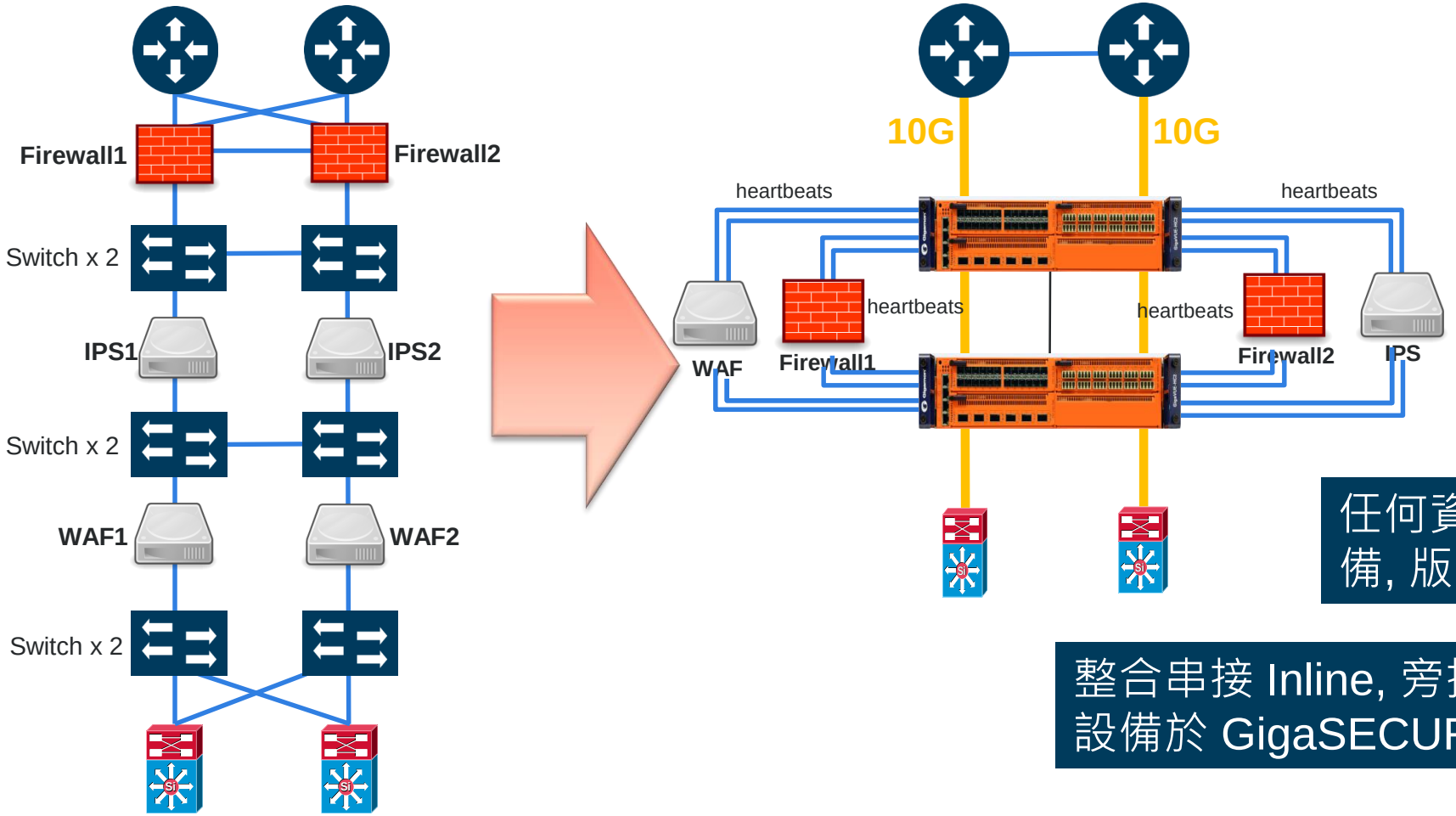
新增設備測試時, 必須以實際運作的流量做測試, 導致測試時網路運作受到斷斷續續的影響

# Use Case：In-Line Bypass 增進資安效能與彈性

Inline Bypass

Gigamon

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

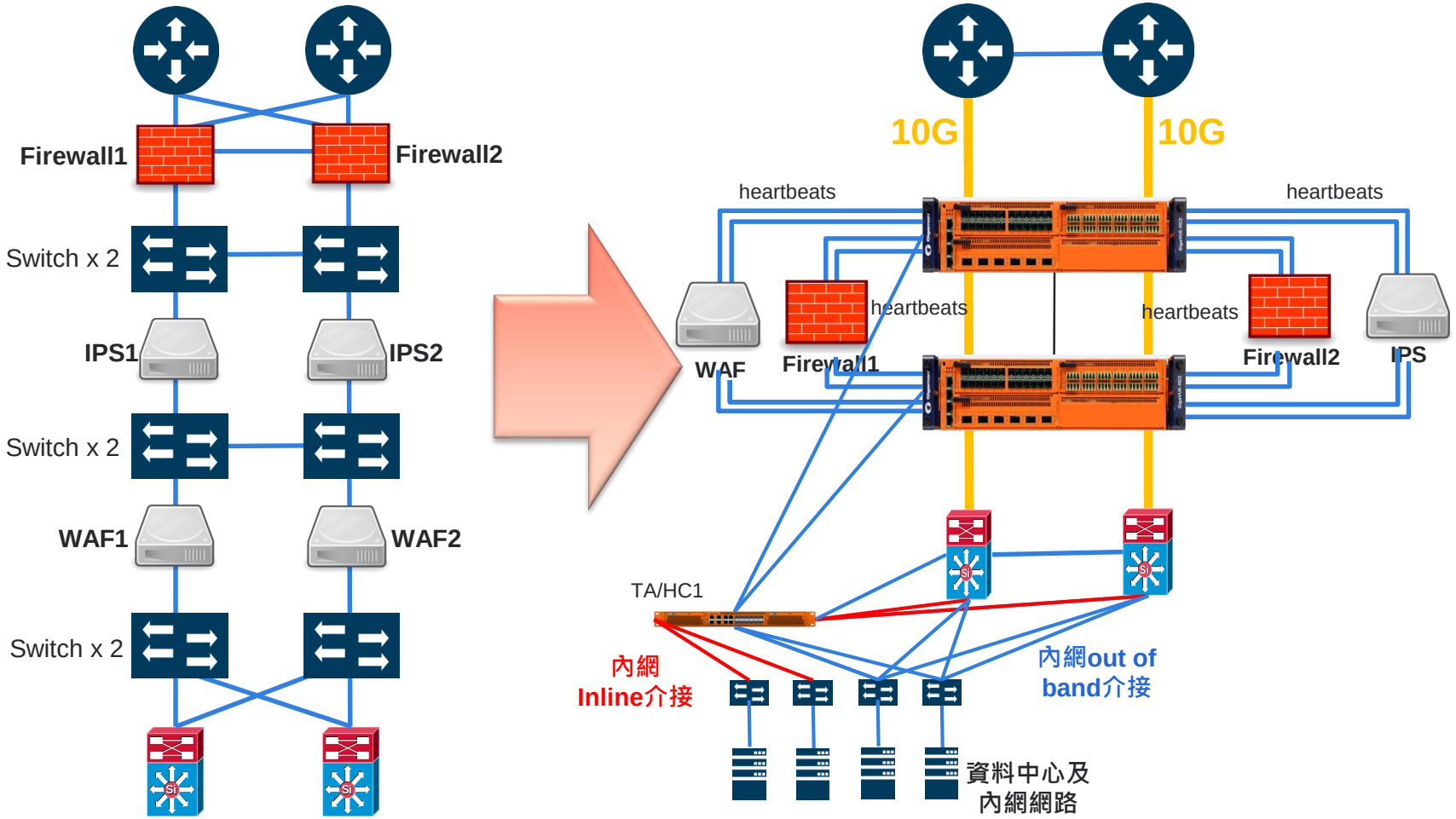
任何資安設備的變動, 如新加/移除設備, 版本升級, 並不影響網路運作

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

# Use Case：In-Line Bypass 利用原有資安設備防禦內網與資料中心

Inline Bypass

解決了資安與網路組的棘手問題




進出流量可篩選無資安威脅的流量不經過某些資安設備，進而降低其使用率

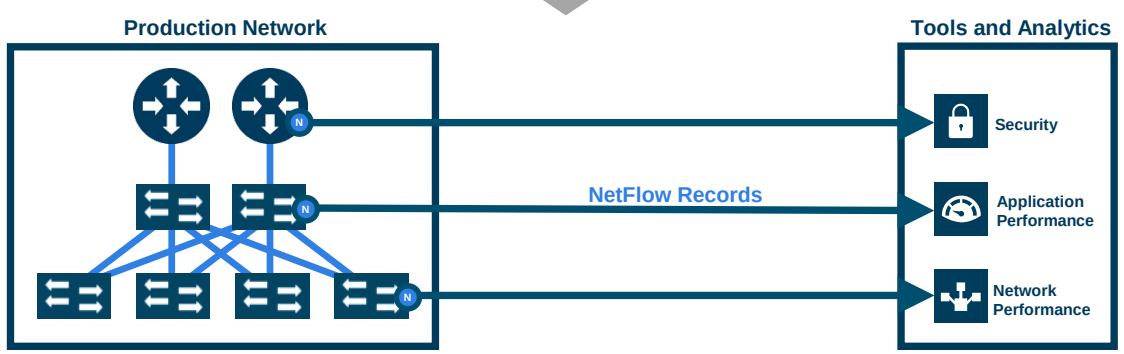
多出的效能容量可讓原有Inline資安設備同時監看資料中心或內網流量，達到全網資安防禦之效果

內網介接可選擇Inline做阻斷效果或out of band監看用途

# Use Case：全網Netflow/IPFIX 及Metadata 生成

ROUTER/SWITCH無法產生不同需要的NETFLOW內容，並同時輸出至多個不同NETFLOW V5/V9及IPFIX的接收/分析工具設備

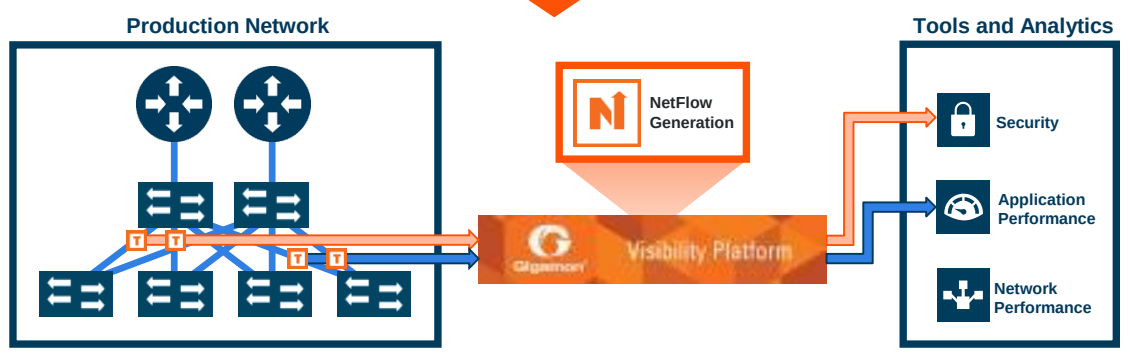
## Without Gigamon




現有挑戰:

- Router/Switches產生大量NetFlow紀錄造成設備過載
- 採樣(Sampling) 的NetFlow紀錄無法滿足資安分析使用
- 部分Router/Switch 不支援NetFlow輸出
- 使用Netflow統計工具收網路流量產出Netflow無法達到全網並需極大型設備，成本甚高

## With Gigamon




NetFlow 1:1輸出, 可增強 “慢速攻擊” 的偵測:

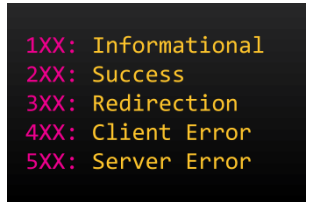
- 經由全網Netflow做分析，對有異常的節點流量機動的導流至工具設備做進一步深層監測
- 全流量不失真Netflow的視別可達成全域性 (End-to-End) 資安防禦 ，有效協助偵測C&C中繼站通訊連線行為
- 與各SIEM廠家或NetFlow統計鑑識工具均有結合運作，至多可同時輸出6個不同NetFlow v5/v9/IPFIX接收/分析設備
- 可產生多樣Metadata資料供SIEM分析工具偵測異常狀況

# Netflow / IPFIX加Metadata 應用

NetFlow / IPFIX Generation

Gigamon

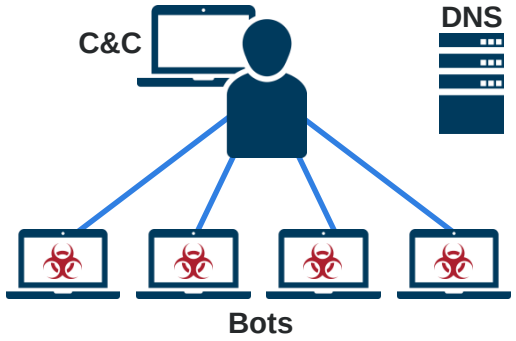
## HTTP Response Codes





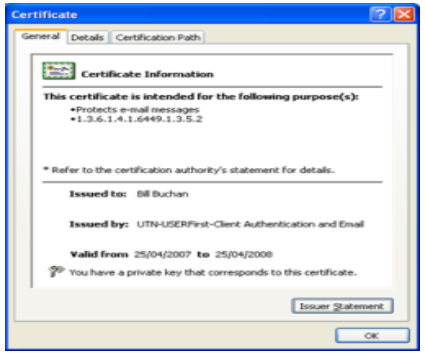

經由HTTP行為可發現DDOS攻擊以及內部網站主機被入侵情形

## DNS Discovery*



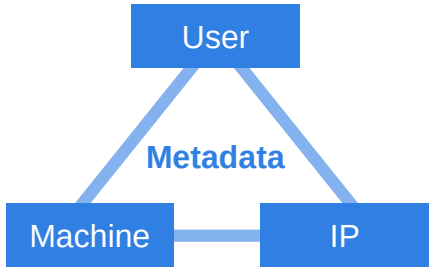

DNS transactions可發現惡意程式利用C&C控制內部端點情形

## HTTPS Certificate Anomalies*




分析 HTTPS certificates 可發現異常憑証使用

## 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

* Planned

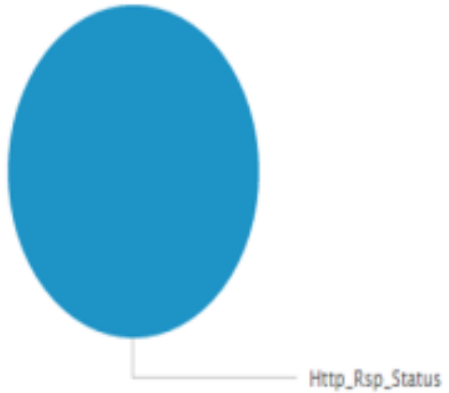
Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and subject to change.

# HTTP&URL

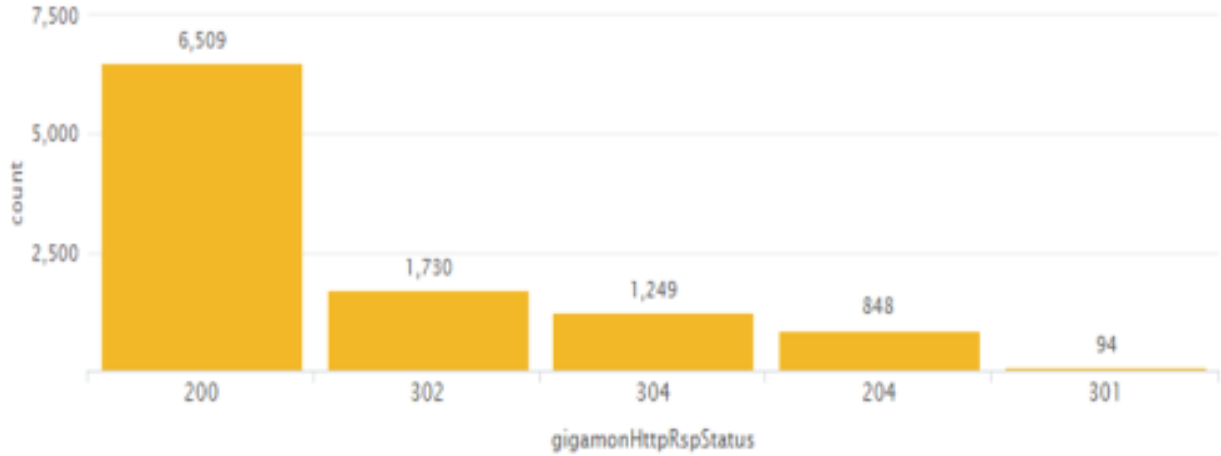
Edit More Info

Last 2 hours

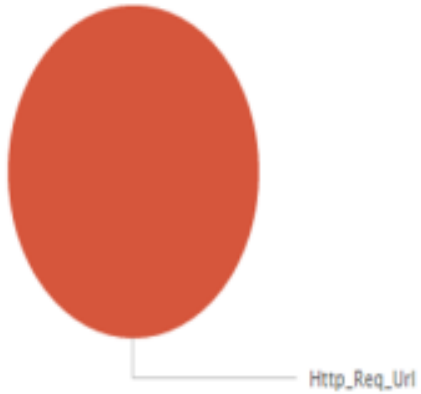
## http_Meta_Data



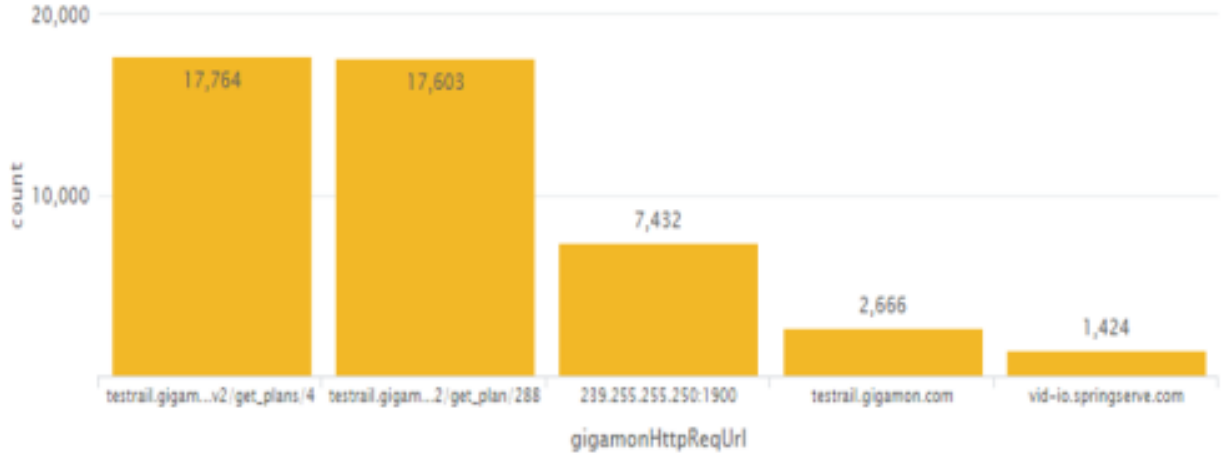

## Top 5 ResponseStatusCodes




## url_Meta_Data




## Top 5 UrlRequested

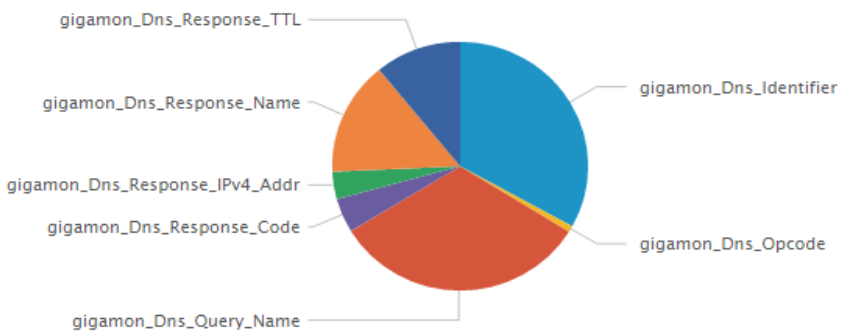


# DNS

Edit | More Info

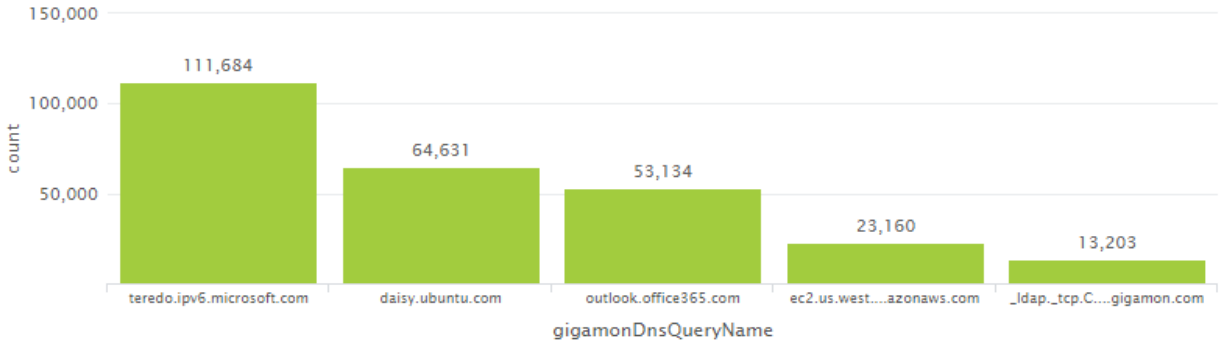
Last 24 hours

## dns_Meta_Data_Fields

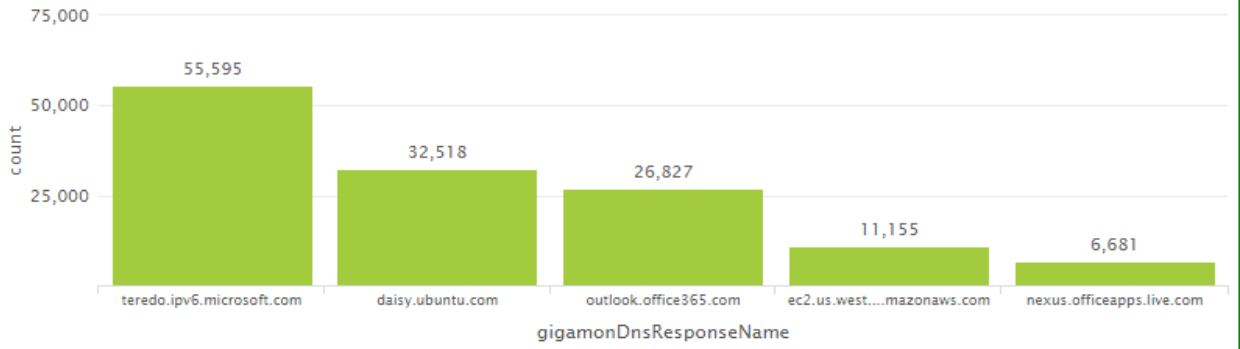



## INTERESTING DNS FIELDS

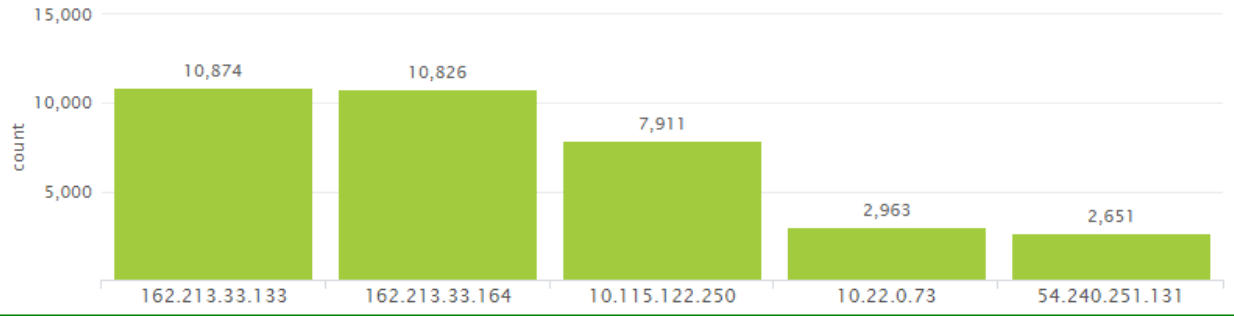
### Top 5 DnsQuery



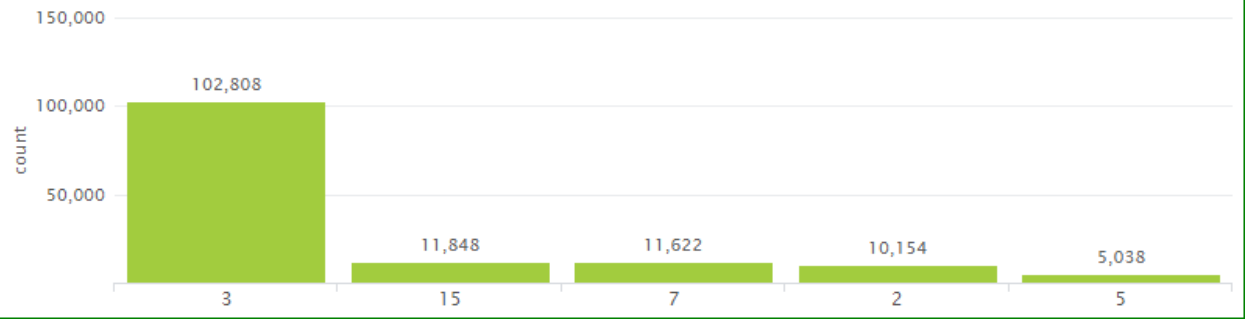

### Top 5 DnsResponse




### Top 5 DnsResponseIPv4Addr




### Top 5 DnsResponseCode

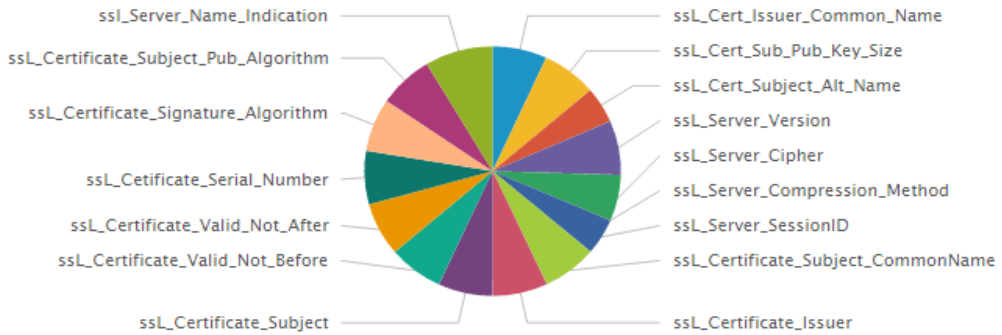


# SSL

Edit | More Info

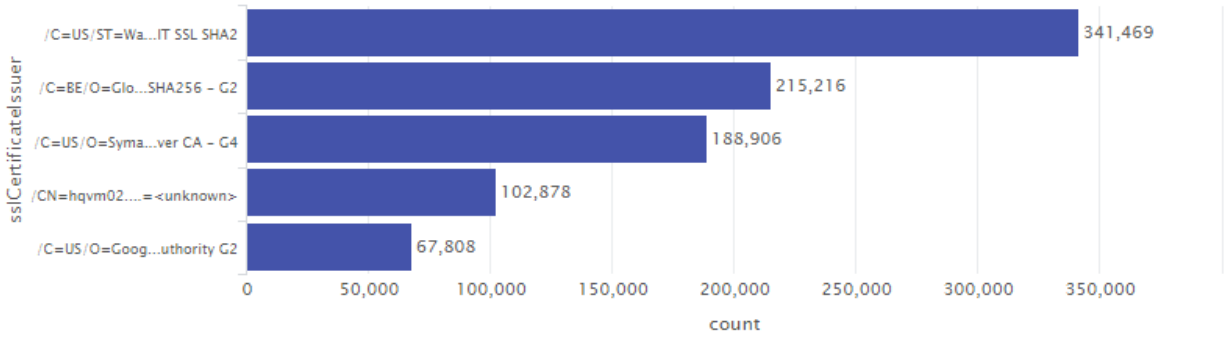
Last 24 hours

## ssl_Meta_Data_Fields

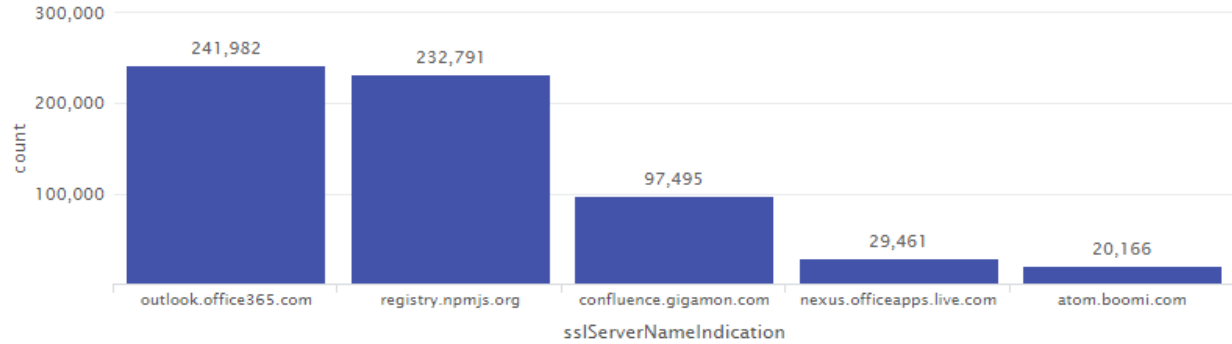



## INTERESTING SSL FIELDS

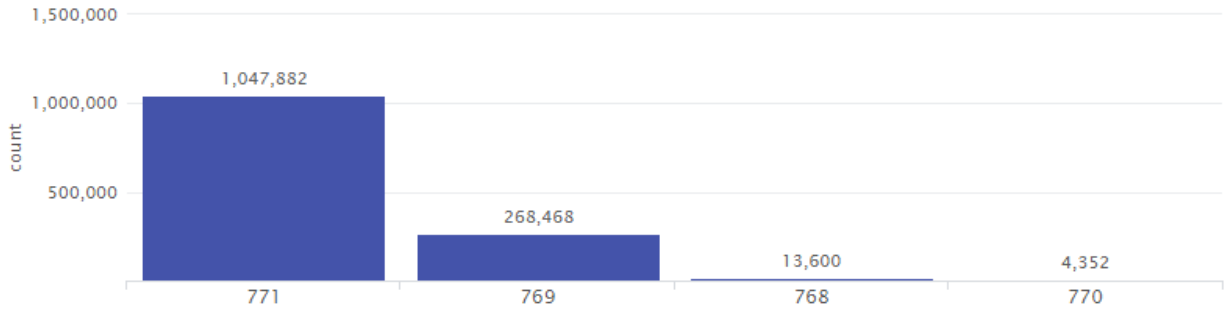
### Top 5 CertificateIssuer



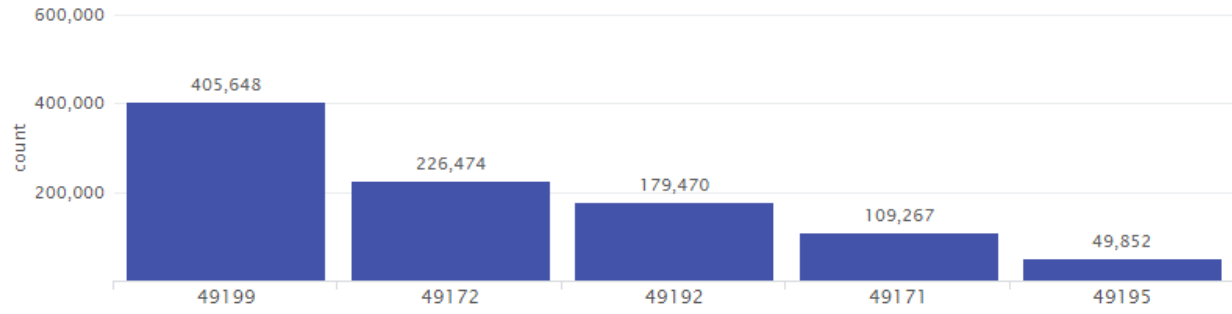

### Top 5 ServerNameIndication




### Top 5 ServerVersion




### Top 5 ServerCipher



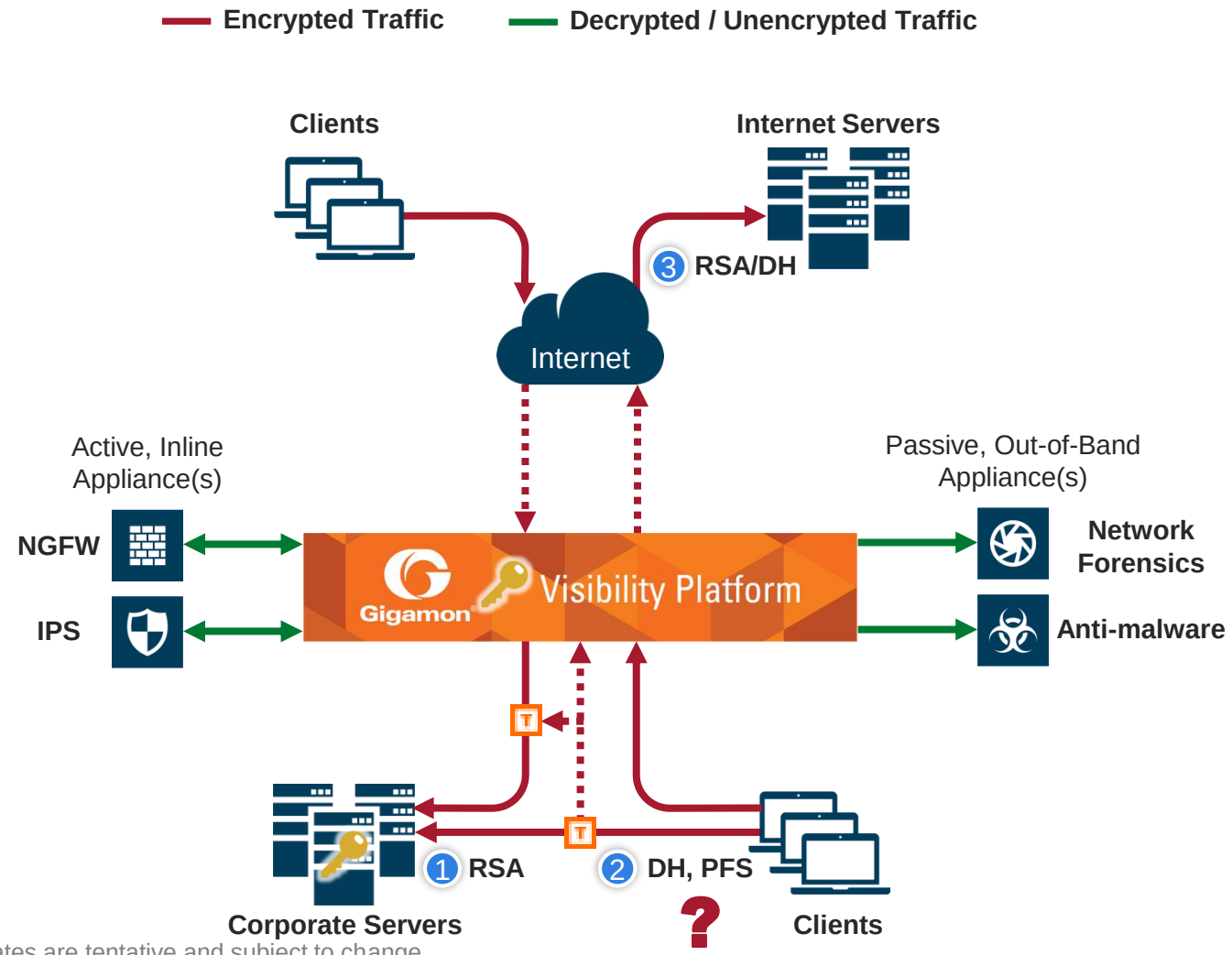
# Use Case：SSL 加解密解除工具設備負擔

## OUT OF BAND與IN-LINE加解密

1. • Corporate servers
   • 企業已有 server keys
   • RSA key exchange
   • *Gigamon 已於2014支援Out of band解密*

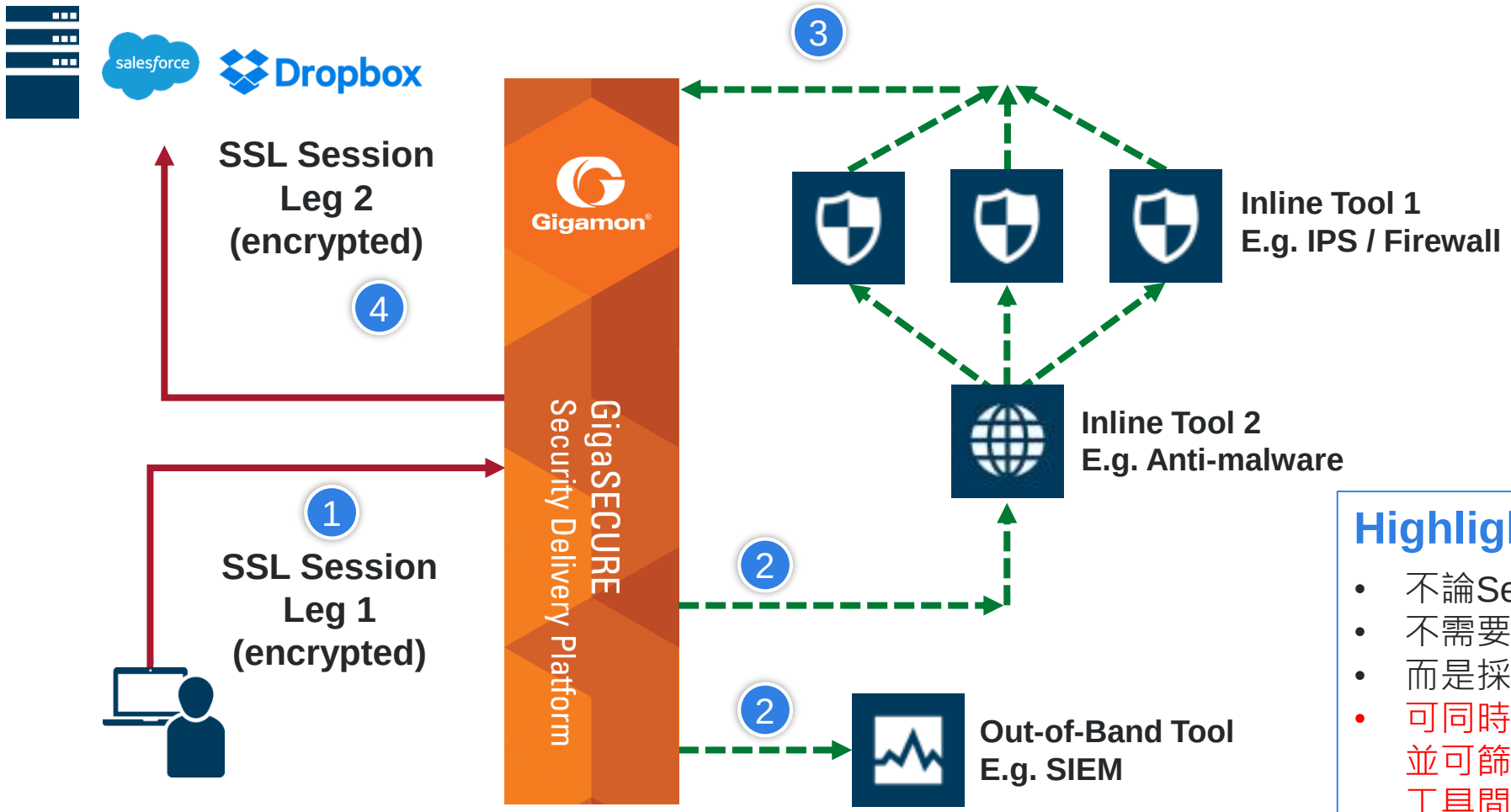
2. • Corporate servers
   • Diffie-Hellman (DH) key exchange
   • Emerging TLS 1.3 standard
   • *必須在 inline 執行 SSL解密*

3. • Internet Servers or SaaS services
   • 企業並無 Internet server keys
   • *必須在 inline 執行 SSL解密*




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

# SSL 加解密結合分流與平衡負載減輕工具負担

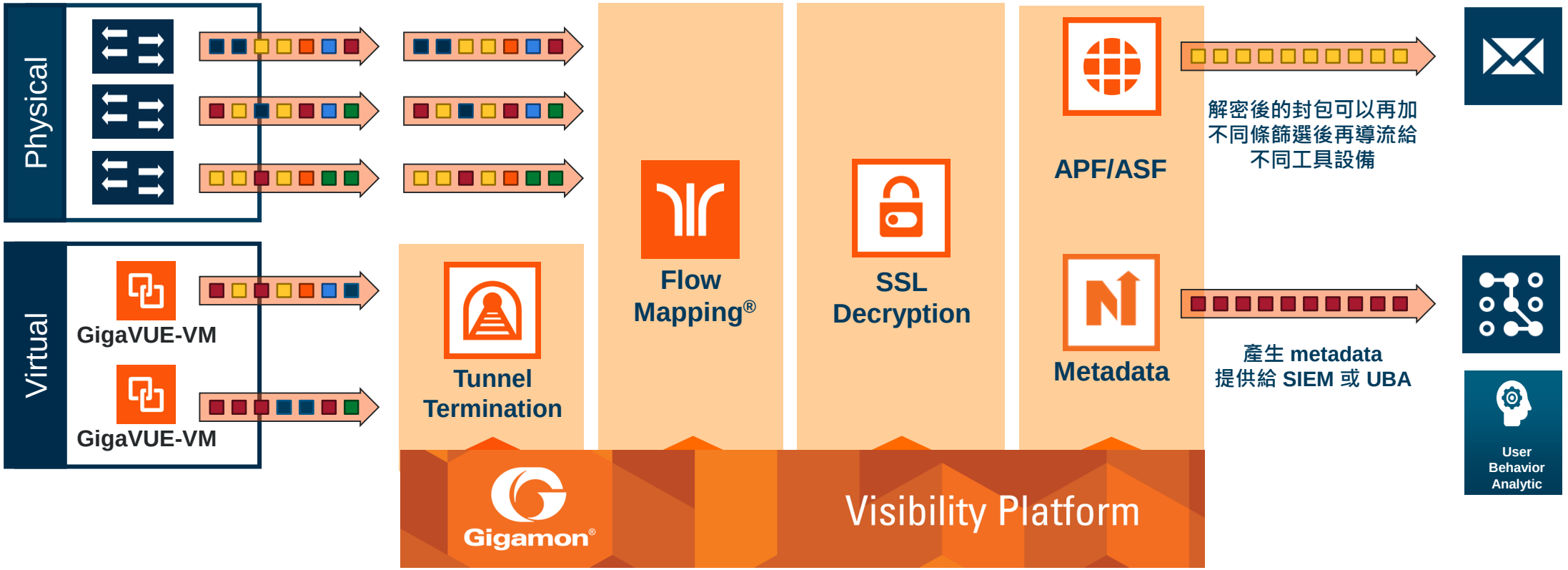



## Highlights

- 不論Servers/clients 位於內部或外部
- 不需要拿到Private keys做解密
- 而是採用RSA, DH, PFS
- 可同時支援多個inline與out-of-band工具, 並可篩選分流、Bypass、負載平衡、與工具間客製化Heartbeat檢測

# SSL可與GigaSMART® 其他功能整合服務縺

在解密後可再進行其他智慧流量篩選處理，讓派送到不同工具設備的流量更精減




先以Flow Mapping®,篩選需要解密的量再執行深度封包過濾 (Adaptive packet filtering) ，可同時產生Netflow與多元的Metadata給不同工具分析與處理

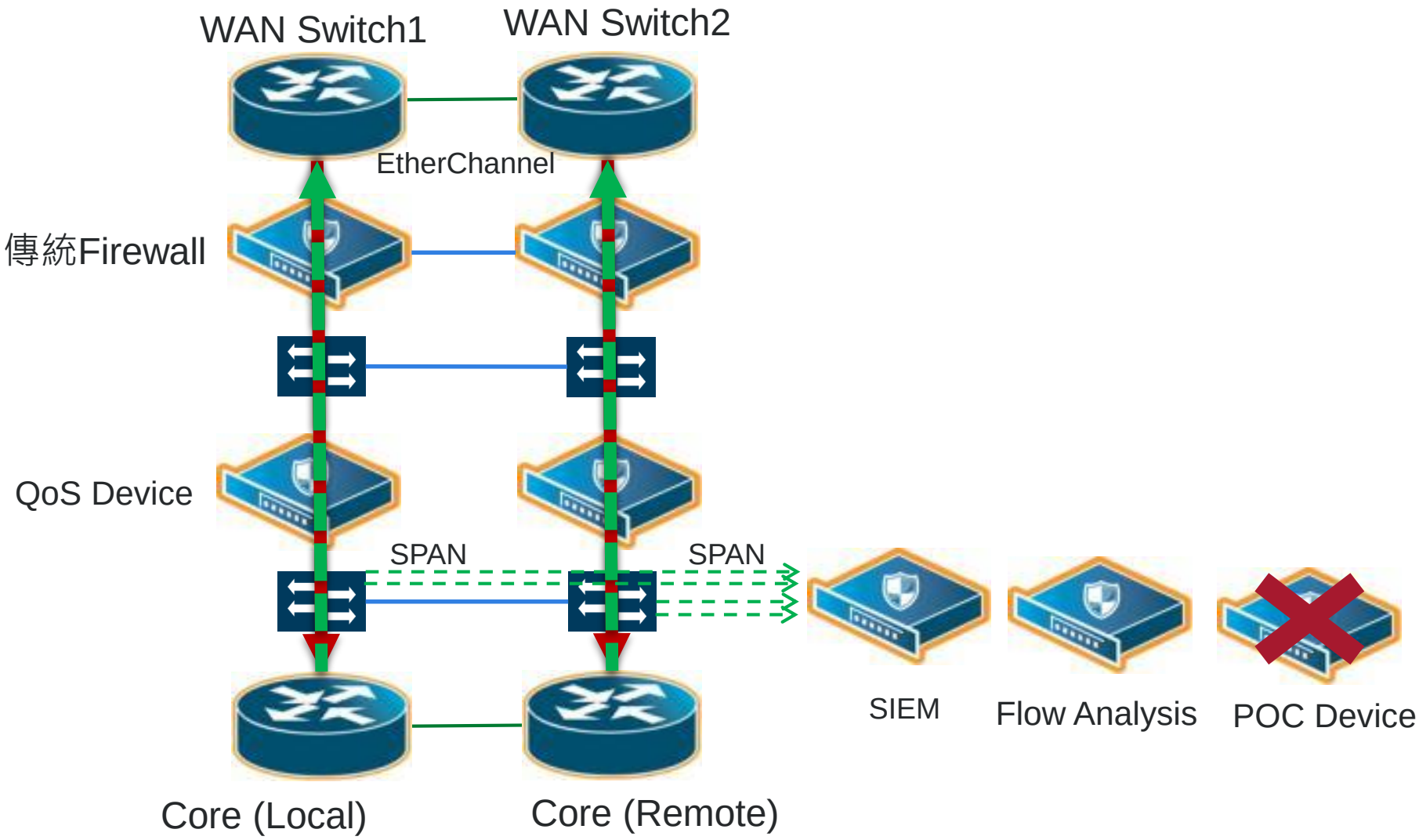
# Gigamon 客戶實用案例分享

## 某科技大學

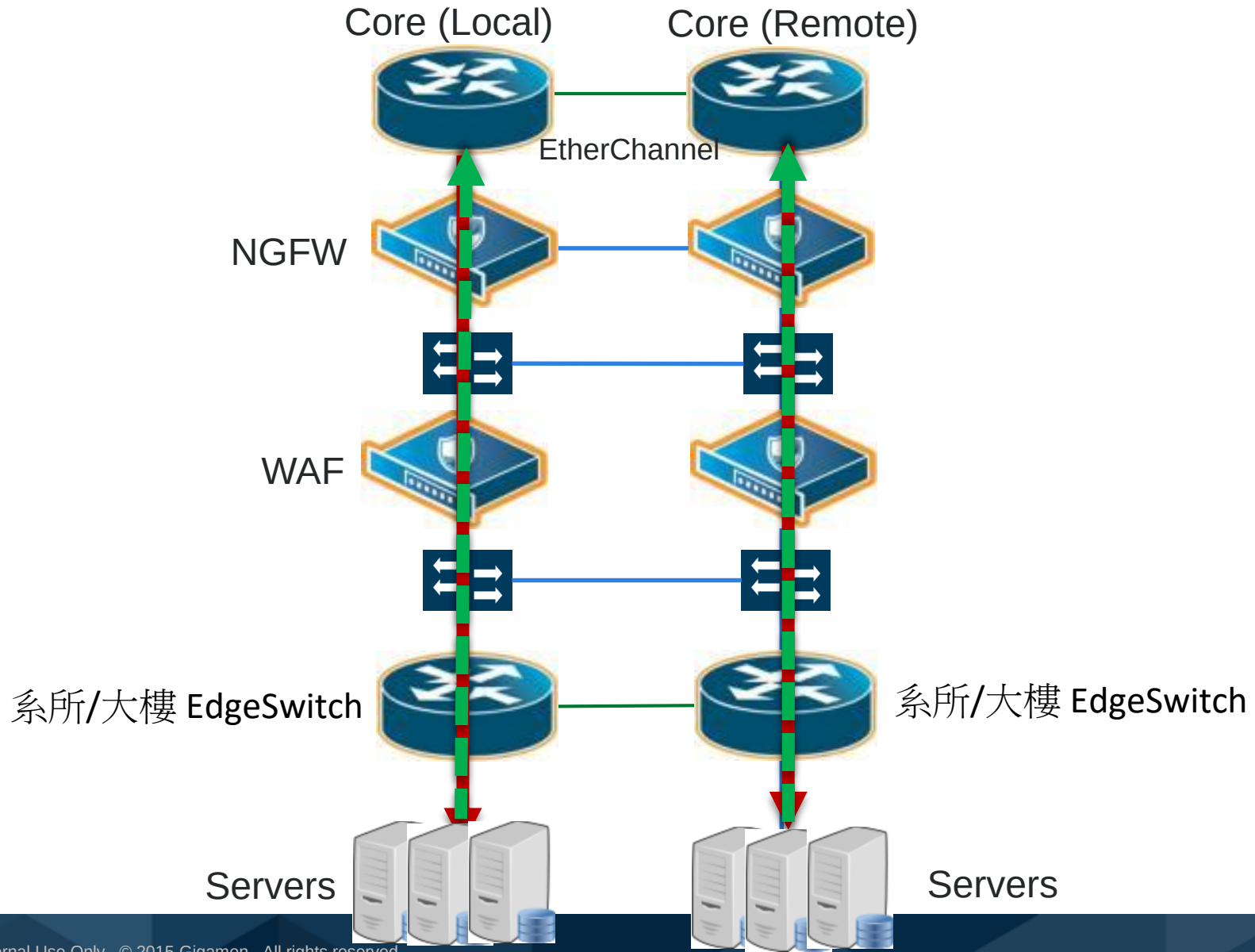
# 未建置Gigamon架構前困擾問題

- 該科技大學因相關業務及因應教育部校園資安管理原則，資安等級必須提升
- 對外網路頻寬為10Gbps，現今使用平均流量超過3Gbps
- 需將Core Switch介接對校內、校外網路流量轉接至各工具設備檢測，IP Dst 到Server Farm相關流量才須經過第二層NGFW做檢測
- 現有FW、WAF對應流量日增，更換設備之型號預算必須大增影響預算規劃
- POC測試設備困擾
  - 核心交換器無法提供足夠Mirror Port
  - 某些測試設備為Inline模式，上線時調整線路造成斷線，測試時亦影響校內網路流量
  - 測試設備異常無法即時拔除而造成斷線狀況

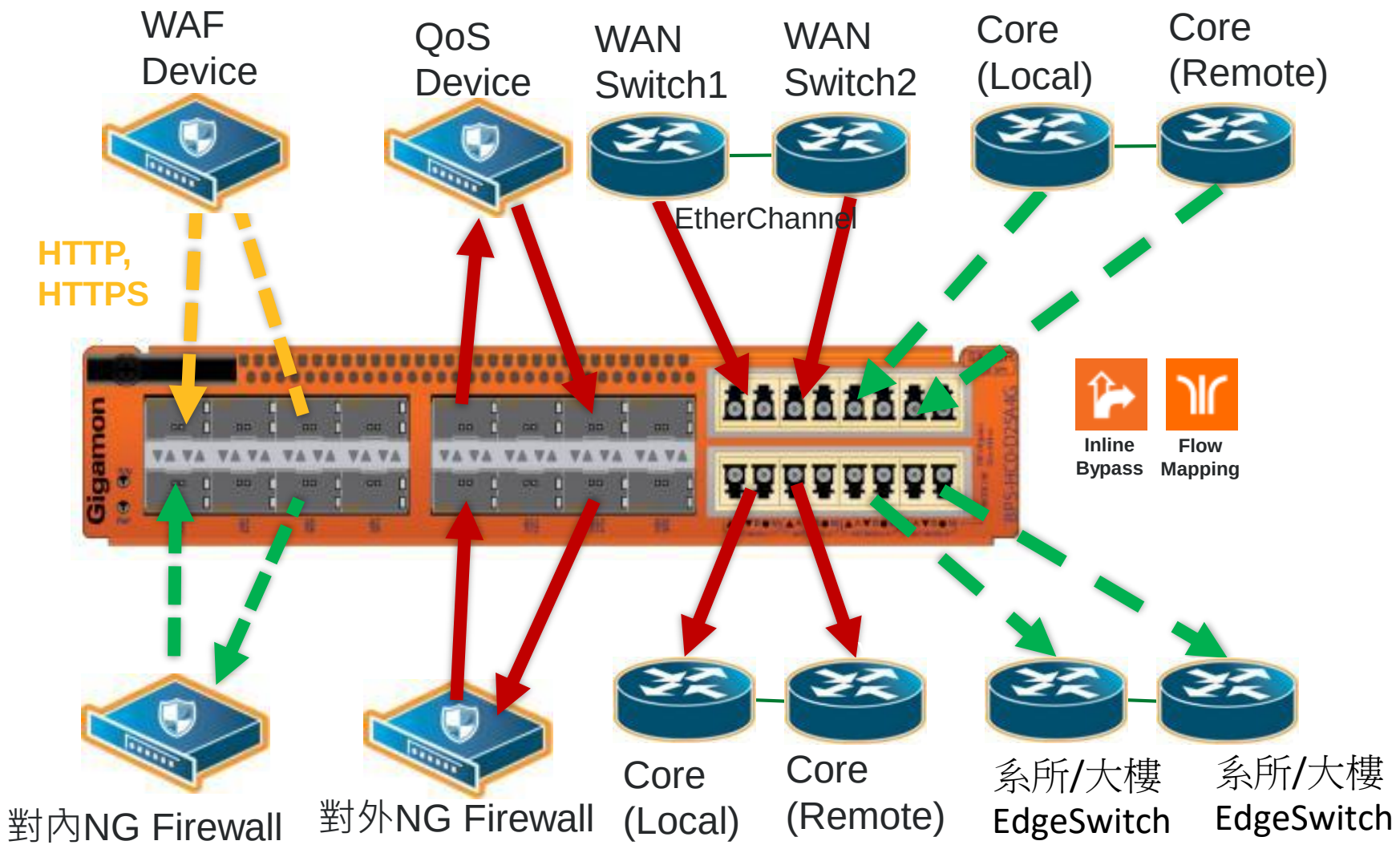
# 未建置Gigamon前對外網In-Line介接架構



# 未建置Gigamon前各系所Server Farm介接架構

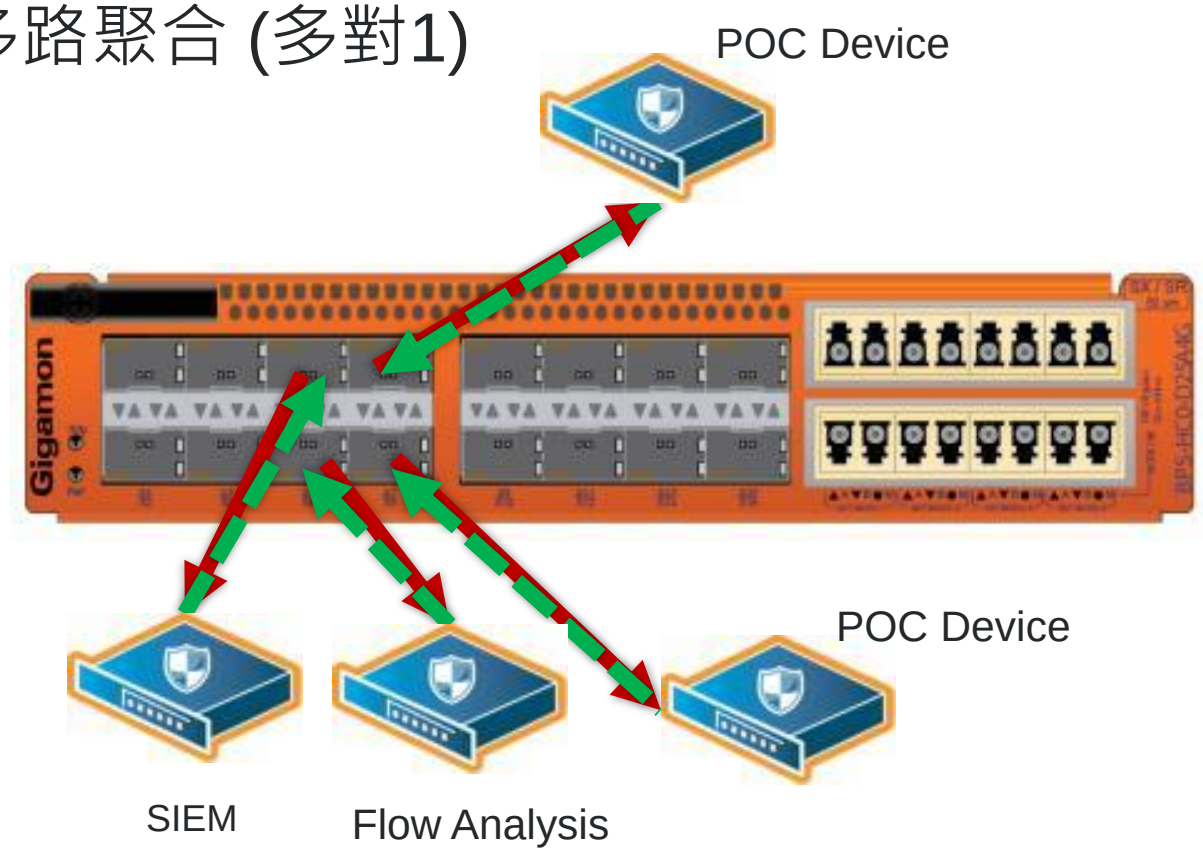


# Gigamon對外網及各系所ServerFarm介接架構



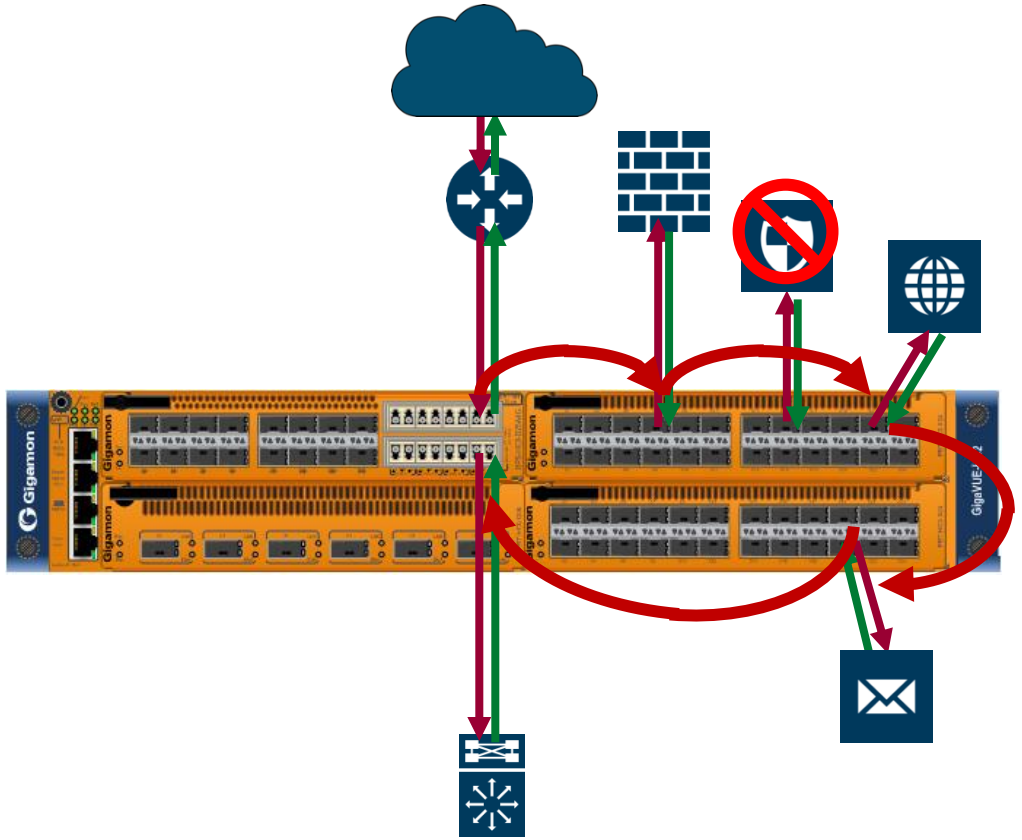
# Out-of-band 輸出架構

- 可透過設定將多路聚合 (多對1)

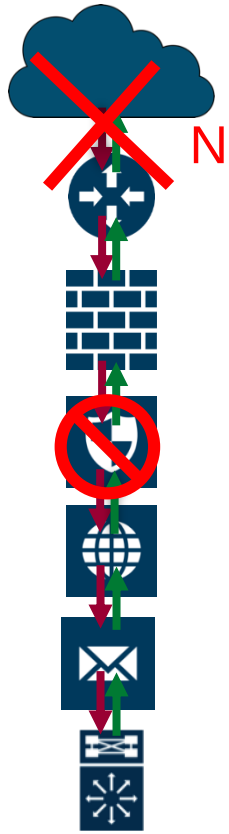


# 建置前後的分別

## SOLVING PAIN POINTS OF BOTH SECURITY & NETWORK TEAMS



Service continue



No service !!

Inline
Bypass

# 建置後效益與未來延展概念

- 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 Rule 依照條件決定校內外的流量路徑。6Gb流量也能用3Gb設備，如：
    - IP Dst 非各系統Server Farm 且非80、443流量，不通過WAF設備，直接進入校內網路
    - SSL加密封包可以Bypass FW
- 高度彈性
  - 若工具設備有故障或效能問題時，可依自動啟用設備故障政策(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
- 未來擴充延展概念
  - Inline SSL解密，分階段測試對主機存取加密流量監看，防止外來駭客殖入木馬程式
  - 因應未來資安法要求，若有需要，可對必要監看加密流量予以解密存証

# Gigamon 客戶實用案例分享

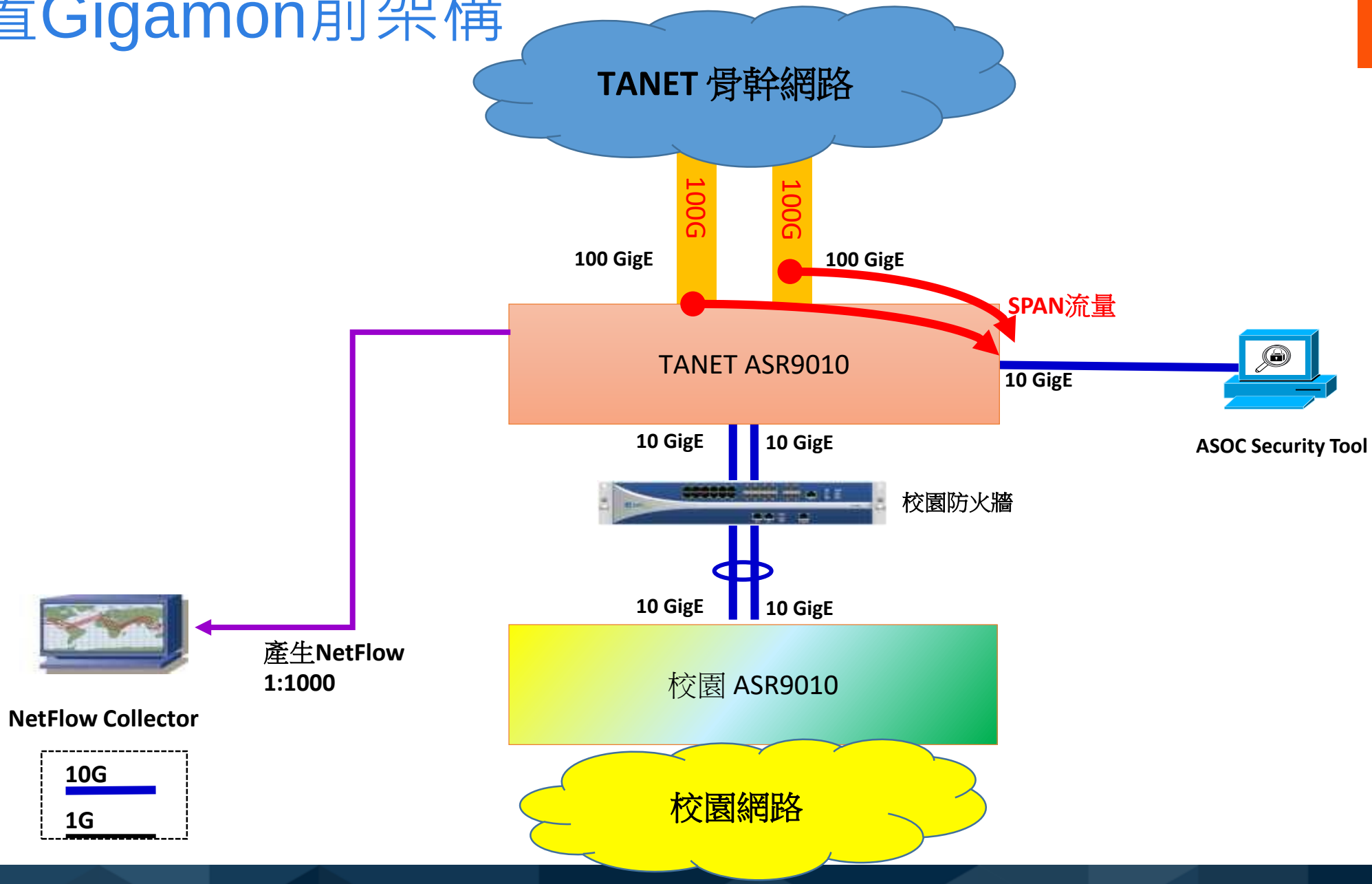
## 某區網中心

# 未建置Gigamon架構前困擾問題

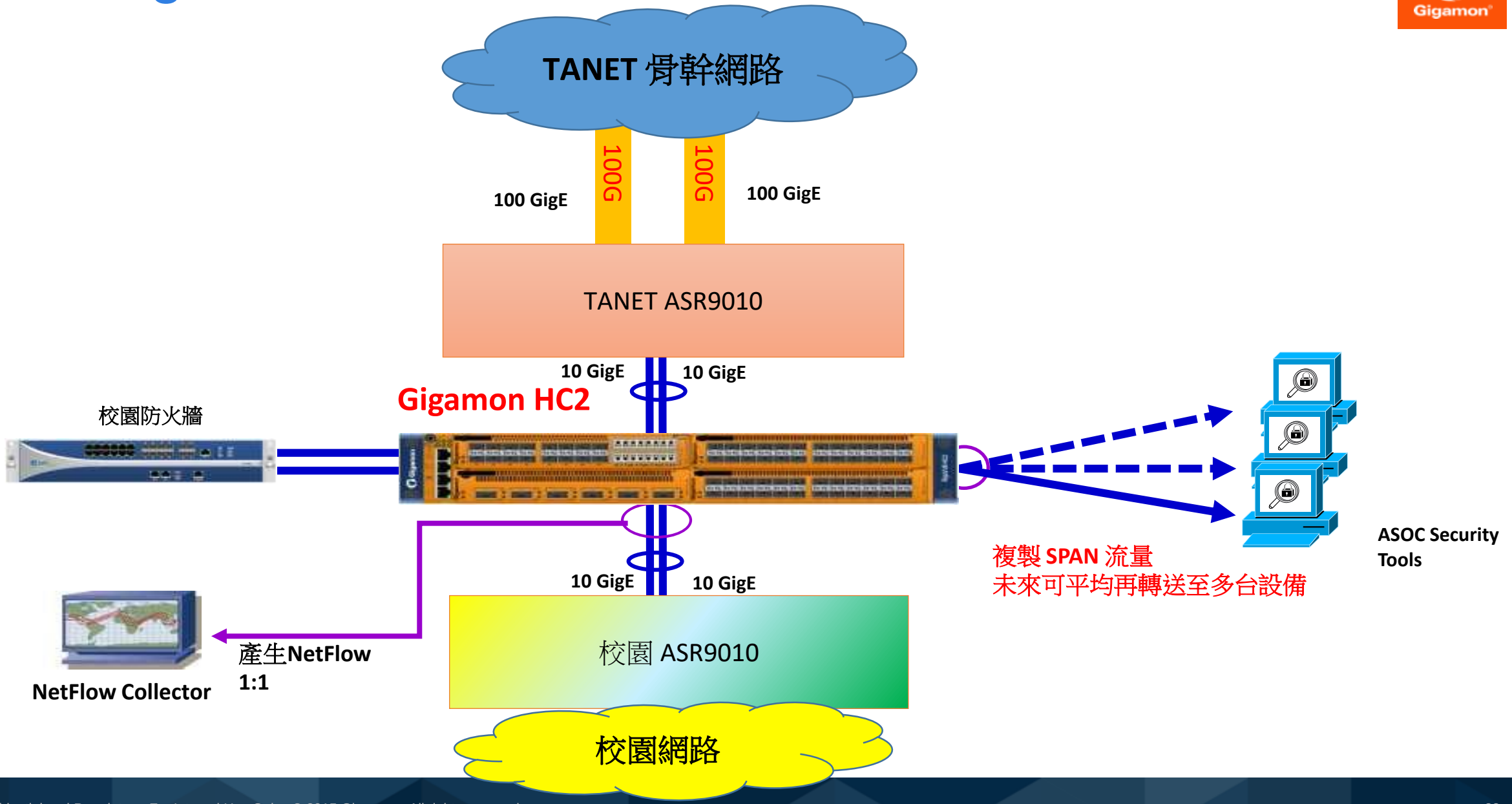
- Inline 設備與斷線問題
  - 現有透通資安設備缺少Bypass功能，如果發生異常將造成校園網路斷線。
  - 資安設備須以Inline方式測試時，上線與離線均需因調整線路造成短時間斷線，測試前需提早公告相關人員也須配合上線時間，測試期間設備異常時無法即時Bypass測試設備。
- 原有資安設備在網路流量不斷提昇下，亦會產生效能瓶頸

- Netflow 取樣率問題
  - Router在佈建時期考慮效能問題，故產出Netflow時使用1:1000取樣率，取樣率比例的高低會造成分析的精準性誤差，分析或DDoS防禦工具可能會因此造成誤判。

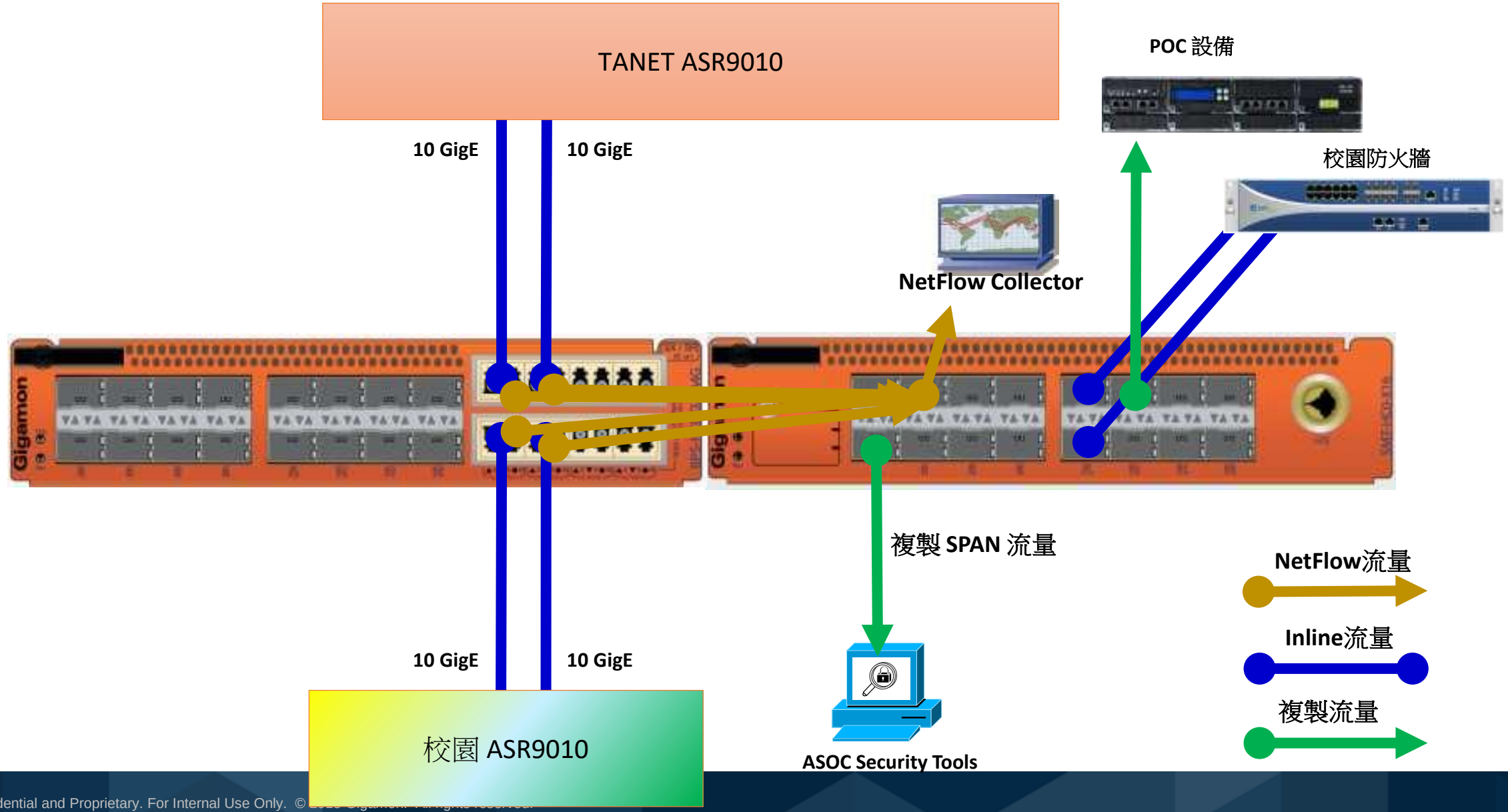
# 未建置Gigamon前架構



# 建置Gigamon後架構



# Gigamon實體線路介接示意圖



# 建置後效益與未來延展概念

- 現行資安設備 (PA) 缺乏 Bypass功能，Gigamon提供PA檢測與Bypass功能，避免設備異常時造成校園網路斷線。
- 日前校園引進A10 DDoS設備，介接方式可任意由Out of Band介接由Gigamon設定轉接為Inline方式而完全不影響校園網路的運作
- 未來新購設備時，可評估需採購多少效能之工具設備，而非僅依頻寬大小考量型號 Model
- 由Gigamon同時產出 IPv4/IPv6 的1:1 NetFlow 至N-partner分析設備，讓Router減輕負擔
- 未來需進行資安設備測試時，不須公告斷線，可多家產品以相同流量同時測試，縮短測試時間也避免測試流量不同造成測試的效果差異
- 未來可擴充加解密功能

# 可視化可達到的效益

**資安設備效用優化**
流量篩選過濾增進效益

**保障暨有設備投資**
暨有設備不需網路頻寬變動而丟棄

**一次加值供多種工具設備使用**
處理或篩選後的流量可複製給多台工具設備使用

**大幅提昇架構穩定性**
資安工具或網路變動不會互相影響

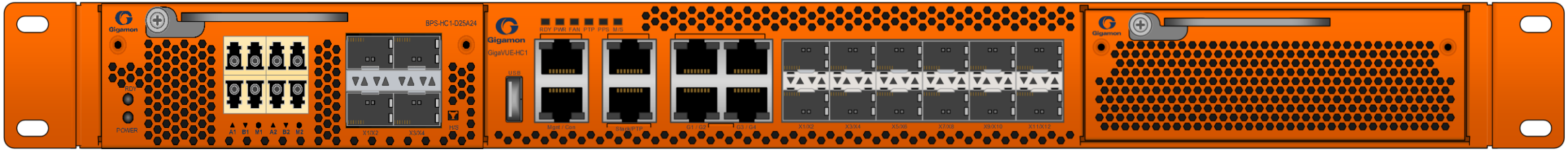
**資安防禦政策的一致化**
不論是實體網路、虛擬網路、雲端網路資安防禦一致作業

**可以保証法規依循**
不論是公司內部規定或政府資安法規範均可任意佈建

# Gigamon有特惠方案嗎？

# GigaVUE-HC1促銷方案

專供大學校內INLINE BYPASS, 並可擴充未來不同功能如NETFLOW, SSL, APF/ASF等



- **1RU 標準機架 – 不佔機架空間**
- **硬體配置:**
  - **12 x 10Gb + 4 x 1Gb ports**
  - **配有一片 2 x 10G Fiber Bypass與 4 x 10Gb ports**
  - **10G SX GBIC 10顆**
  - **尚餘1個擴充插槽可擴充**
- **主要功能:**
  - **Flow Mapping®可依L2~L4組合條件分流與Bypass**
  - **實體TANet線路 1/10G介面Inline Bypass**
  - **各種工具設備的Inline bypass保護 (IPS, WAF, ATP, DLP, etc.)**

- **GigaSMART的多種可擴充應用，但需依流量效能有所限制:**
  - **NetFlow / IPFIX Generation (Metadata Generation)**
  - **De-duplication**
  - **Inline SSL 加解密**
  - **Header stripping**
  - **Packet slicing/masking**
  - **APF/ASF 依資料內容篩選欲監看的流量**

***含3年原廠軟體支援與硬體保固***
***原價：NT4,958,140未稅***
***校園教育特惠價：NT1,490,000未稅***


Gigamon
Cybercriminals
Now there's nowhere to hide
#wefightsmart