解決方案簡介
威脅防禦

50%

資安團隊生產效率提高。[1]

主要優勢

- ✓ 使網路資安工具可查看整個基礎設施中的網路流量，從而提高其效益。
- ✓ 透過最佳化資安工具降低成本，使其更好地保護網路流量和應用程式。
- ✓ 顯著減少測試和部署全新資安技術和工具所需要的時間和努力。
- ✓ 確保 SSL 流量經過有效解密和檢測。
- ✓ 啟用 NetOps 和 SecOps 以更快速部署安全應用程式和全新資安工具，而不會妨礙網路或必須等候維護窗口。

Inline串接威脅防禦策略應不僅僅是一套資安工具。需要是整合式智慧方法。完整的威脅防禦解決方案不僅可提升防禦工具性能，亦可提高運作團隊效率，讓其能夠快速部署程式修補以及實行新技術，而不會影響網路性能或仰賴維護窗口。Gigamon Inline Bypass 威脅防禦解決方案將協助您降低成本，同時獲得最大防禦工具性能、網路彈性和運作效率。

Gigamon Inline Bypass 威脅防禦解決方案是 GigaSECURE® 資安派送平台（GigaSECURE）的一部分，這是專為資安所建構的下一代網路分流設備。讓您在您的整個基礎設施中（內部部署以及在虛擬和雲端環境中）存取資料。您可以透過僅派送專為跨多個工具檢閱、負載平衡，以及卸載 SSL 解密等處理器密集型任務所設計的流量，最佳化資安工具。整合式實體和邏輯旁路功能可提供最高彈性，易於簡單測試和佈建Inline串接工具，而不會影響網路可用性和性能。

提高現有網路資安工具的效益

有效存取資料以偵測和回應威脅的能力是一項挑戰。為了解決這些問題而無需購買更多資安工具或新增機房維運人員，GigaSECURE 讓您能夠：

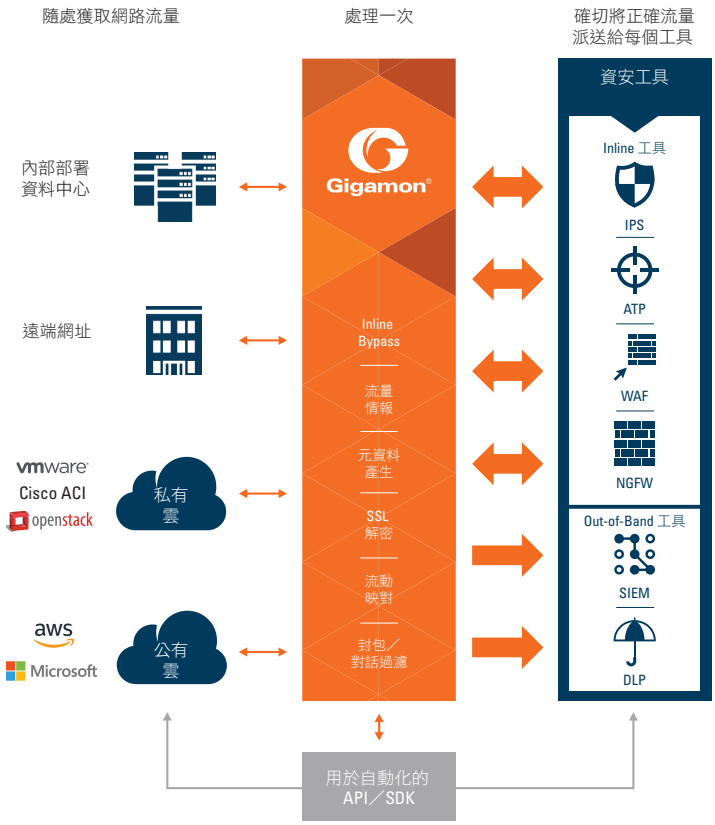
- 透過僅向您的工具提供相關資料最佳化性能。
- 即使網路速度和升級後，既有工具依然可以廣大內外網防禦範圍。
- 在整個組織中存取資料，以加快工具DownTime偵測時間。
- 解密一次，與所有工具共享明文資料。

降低網路資安工具的成本

不斷上升的網路流量迫使企業新增和升級其資安工具。這使得硬體和軟體預算增加，網路資安基礎設施更加複雜，並且提高Capex管理成本。GigaSECURE 資安派送平台可透過有助於下列內容打破這種工具汰換循環：

- 去除重複資料刪除和 SSL 解密等任務。
- 僅向工具傳送其需要的資訊（不能再多）。
- 跨多個工具的負載平衡，以排除容量浪費。
- 降低複雜度和資安管理成本。

[1]Gigamon 的總經濟影響™，這是 2016 年 4 月 Forrester Consulting 公司代表 Gigamon 所執行的委託研究



GigaSECURE 資安派送平台：可排除盲點、提高性能、改善彈性。

可更快速測試和部署全新網路資安技術

隨著新威脅每天皆會湧現，IT 組織需要頻繁地升級或引入全新網路資安工具和技術。憑藉資安派送平台，您可以：

- 測試全新資安工具而不會影響性能。
- 並列評估多個資安工具。
- 部署資安工具而不會影響網路性能。
- 佈建全新工具而無需昂貴網路卡。

運用 Gigamon 生態系統的力量

GigaSECURE 支援援Inline串接資安工具 – 例如思科（Cisco）FirePOWER 入侵防禦系統（IPS）、FireEye 網路資安先進威脅防禦（ATP）解決方案和 Imperva SecureSphere 網頁應用程式防火牆（WAF）– 以在不斷成長的網路流量內和軟體升級期間查看、確保安全以及防止入侵。透過將威脅流量帶到線路前端、卸載 SSL 解密並且提高彈性，Gigamon 及其生態系統合作夥伴使您的網路更加準確有效。

GigaSECURE 資安派送平台

如圖中所例示，GigaSECURE 資安派送平台：

- 提供對整個組織中網路流量的簡化存取。
- 派送Inline串接和旁接個別資安工具所需想要檢測的選定流量。
- 從個別工具卸載 SSL 解密和重複資料刪除等處理器密集型任務。
- 使用流量情報最佳化網路流量或從網路流量提取元資料，並且派送給適當資安工具。
- 提供用於與資安和基礎設施堆疊整合的編程介面，從而能夠動態回應受到影響的基礎設施改變、事件及其他早期指標。

如需更多資訊

如需瞭解 GigaSECURE 資安派送平台可協助您改善資安並且降低成本的方式，請參訪 www.gigamon.com

6114-01 04/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com