資安防護進入綜觀全局的時代

網路資訊專訪 Gigamon 台灣區銷售總監錢旭光

「資安威脅正在改變，8 月份台積電資安事件即是最明顯的例子。」Gigamon 台灣區銷售總監錢旭光說。

過去的資安威脅多屬於縱向，即由企業外攻向企業內，而今卻逐漸橫向化、內網化，威脅順利滲透後，開始在企業內的網路移動，一台機器跳過一台機器，而後發作。然而很遺憾的，今日多數資安設備無法掌握內網動向，也就無從察覺、防範此一新趨向的威脅。

內網動向僅為企業內諸多「不可視」的一項。錢旭光持續列舉，進出企業的加密資訊一樣躲過現行資安設備的檢查；或者是虛擬化環境中虛擬機器(Virtual Machine, VM)間的溝通聯繫也是另一種內網活動，同樣不在現行資安設備監管範轄內；其他如企業內的非軍事區(Demilitarized Zone, DMZ)，或企業放置於公有雲資料中心的系統，或高可用性(High Availability, HA)產生的資料路徑轉移，都是資安死角、盲區之所在。

特別是加密，愈來愈多的企業連線是採加密方式進行，預計明(2019)年即有超過 80%的連線採 SSL 加密傳輸，若加密內容不能掌握，即可能包藏惡意程式等資安威脅在其中，並躲過查核監視。此外資安攻擊也朝高階應用程式下手，如透過社交媒體滲透，或魚叉式網路釣魚(Spear Phishing)等，看似正常使用者行為，實已為駭客開啟大門。

有效防禦之前要先能看得見

有鑑於此，Gigamon 強調資安設備介接企業網路的做法，可以換個想法去重新思考介接的方式，方能使資安監控更全面，並以此提出「可視化平台」的主張，將 Visibility Appliance 設備導入到企業網路內。過去企業內層層介接的交換器連線，改以 Visibility Appliance 設備為交通中樞，所有企業內外封包均會流入流出設備，而在設備內即可進行各種流量辨視、分類篩選、以及派送的行動。

錢旭光舉例，有些封包需要硬體防火牆檢查，設備即把封包轉導入防火牆內，檢查完再行由設備處理其後續流向，或有的封裝需要導入進階持續性威脅(Advanced Persistent Threat, APT)的系統中，也由設備統管進出，另有些封包如 YouTube 影像資料已確定安全無虞則可直接通行，不需要再行檢查。

由於所有封包活動均透過設備進出，一切動向均掌握，也就一切均在監控視野內，使過去片段局部的資安檢測躍升綜觀全局的新境界。錢旭光說明，如此即可支援全盤的資安訊息彙整，如安全性資訊與事件管理(Security Information Event Management, SIEM)，或觀察可能的潛在威脅活動，如使用者行為分析(User Behavior Analytics, UBA)。

更全面性的資安監控是「可視化平台」一大特點，但除此之外也為企業資訊管理帶來多項助益。

首先是資訊設備的固定成本投資可以減緩，過去的企業網路常有封包重複查核的情形，拖累企業網路效能，而在導入可視化平台後，對封包路徑進行軟體規劃設定，必要查核只進行一次，不再重複，如此企業更有效運用網路頻寬資源，也使資安設備負荷減輕，過去企業可能設備每年升級網路及設備，而今採購週期得以延長。

其次是協助網管人員找尋網路瓶頸，可視化平台可以發出節奏式的心跳封包給資安設備，而後聆聽資安設備的回應，若資安設備的回應過慢，即可了解該設備處理效能逐漸不合需求，當列入優先汰換。同理，當企業資訊環境發生問題時，可視化平台也會是網管人員最佳的故障排除檢視工具。

進一步的，可視化平台既已掌握所有進出封包，如此企業若需改變網路連線架構，也只要在平台上進行軟體設定即可，不再需要網管人員親自到現場更動實體接線，網路的維護管理更為便利容易。

硬體設備只是可視化平台的一種實現型態，適合企業內網路運用，然實際上還有軟體型態的可視化平台。錢旭光說明，軟體型態的可視化平台可安裝在 Hypervisor 虛擬環境上，對環境上的各虛擬機器封包進行管理與監控，或安裝在公有雲環境上，對多個企業所屬的虛擬機器進行監控。

對用戶端的「干擾」極小化

可視化平台如此強大，但更重要的是，對終端用戶、網路設備而言這一切都是透通的，在背景般運作於無形，設備認為它採行固有的連線運作方式，終端用戶一樣日常操作使用，不需要再行安裝代理程式(Agent)等工作，可視化平台會自動檢視各封包的檔頭，從而辨識此為網路瀏覽封包、資料庫運作封包、應用程式封包等，並進行管理追蹤。
對於尚未建立網路環境的企業，建議在初始階段便可導入可視化平台，至於已有網路環境的企業也只需要變更一次網路接線工程，之後即可長久享受可視化平台的益處。
最後，錢旭光也分享台灣企業對可視化平台的接受進度，現階段以大型網路環境、複雜網路環境的企業或機構，或高安全性要求的企業機構，較優先快速導入可視化平台。例如金融業即屬於網路龐雜亦有高安全性的需求，政府機構亦屬於此。

另外教育機構也因校內單位眾多而有複雜的網路，需更全面的管理，因而積極導入可視化平台。或者電信業同樣有龐雜網路需要妥善監管的需求。展望未來，台積電資安事件太具指標性與震撼，估計台灣的高科技製造業也將開始評估與導入可視化平台，往後更多類型的大型企業也將有需求。

受訪人簡介

錢旭光 (Simon) 目前擔任 Gigamon 台灣區域銷售總監 一職，深耕 IT 產業超過 30 年，經歷橫跨網通及資安領域，曾服務於中山科學研究院、九鼎科技、訊康科技國內部經理、Cabletron Networks 業務協理，以及擔任 Extreme Networks 區域總經理近 15 年。