中小型企業可負擔的企業級資安防護

概觀

大部分的組織使用電子郵件和網頁通訊協定做為商業用途。因此，大部分的網路攻擊會從這些通訊協定進入。有效防護能偵測，並防止已知的商業攻擊和先進的未知攻擊。獲獎肯定的 FireEye 技術，可準確地偵測先進多階段與多媒介攻擊，並加以阻擋。FireEye 提供資安團隊有效工具，透過大幅降低誤報率來增加作業效率。這些強大的解決方案皆是為了讓組織能輕鬆使用，進而心無旁騖地發展自己的業務。

FireEye 率先推出此技術用於偵測先進未知攻擊，但一開始僅提供大型企業進行部署。然而，不論組織的規模大小，網路攻擊者皆將其視為攻擊目標。中小型企業 (SME) 發現自身也暴露在危險中，而進階威脅防護成為了他們安全架構的基本要求。

資安挑戰

中小型企業面臨許多資安挑戰，一方面是因為網路威脅型態持續變動，另一方面是因為中小型企業嘗試在組織內有效地進行資安管理。

有關威脅型態的挑戰，通常源自於組織內缺乏資安可視性。傳統周邊偵測和防護技術須透過攻擊特徵碼來識別威脅，這已無法對付現今的威脅。攻擊者使用更先進的技術，更改惡意軟體的特徵碼，因此它在任何指定的組織中只會出現一次。在許多案例中，惡意軟體甚至未參與攻擊事件。

有關資安作業中心的挑戰，則是因為中小型企業經常收到過多的資安警示，但缺乏足夠人力去回應所有警示。其中許多警示為誤判，導致浪費了分析時間在調查這些非資安問題的警示上。過多的誤判警示也會隱藏真正的威脅警示，導致無法立即處理威脅以減少進一步影響。

還有其他複雜性的問題。為了調查警示，中小型企業須雇用具備相當資安專業知識的員工。在大部分的組織內，安全性資源為 IT 部門的一部分，容易引起利益衝突。執行多層級深度防禦方法的中小型企業，可能會面臨許多資安技術工具經常缺乏有效管理的問題，或是由資安服務提供者管理，甚至是完全不管理。最好的情況是，這些問題造成過多成本負擔，而最壞的情況，則是讓公司暴露在資安危險中。這些挑戰皆互相關聯：中小型企業須一邊控制成本，一邊透過有限的員工，管理許多發出過多警示的資安工具。

FireEye

解決方案

FireEye 解決方案結合 Network Security Essentials (NXE) 和 Email Threat Prevention Cloud (ETP) 以保護組織免於網站型和電子郵件型的威脅。[1] 90% 的網路攻擊透過這兩項媒介進行攻擊。這項解決方案會找出重大安全性問題，避免因誤判而無謂加大事件回應的規模，並損及即時性，進而讓您徹底發揮安全性預算的效益。

強大的 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎是這些 FireEye 最核心的關鍵技術。它可以協助辨識出橫跨多個攻擊媒介的進階多階段攻擊和混合式威脅，包括網頁與電子郵件；如果只從單一面向獨立檢視這類攻擊，便可能不會視為惡意活動。

如果要找出大多數多媒介攻擊的初期手段，惡意 URL 與魚叉式網路釣魚電子郵件的關聯性是一項關鍵線索。Cloud MVX 引擎能夠發現這些連結，讓組織瞭解這兩起事件的相關性，並自動封鎖該攻擊的後續階段，例如攻擊者嘗試經由網路傳送遭竊資料。此方法也同樣會辨識出利用類似策略、工具及程序 (TTP) 的後續攻擊，並加以封鎖。

由於此解決方案兼具高度自動化、高效率和高功效的特性，因此組織不但能改善安全性狀態，還能簡化網路和電子郵件安全機制的部署工作及日常管理作業。

Network Security Essentials

Network Security Essentials 是一項經濟實惠、隨插即用的網路安全性解決方案，60 分鐘內即可完成部署，降低因網路入侵而須付出昂貴代價的風險。

除了無特徵碼 Cloud MVX 引擎這項專利，Network Security Essentials 還包括情報導向分析技術，可識別已知及未知威脅，並加以封鎖。情報導向分析技術是一組情境式規則型引擎，能根據電腦、攻擊者及受害者的最新情報，偵測並封鎖惡意活動。入侵預防系統 (IPS) 可透過傳統的特徵碼比對來偵測出常見的攻擊，並提供對風險軟體的防護，以封鎖間諜軟體和廣告軟體。與傳統或新一代防火牆、單一 IPS 或防毒 (AV) 軟體不同之處在於，Network Security Essentials 能以高準確率偵測出已知與未知的零時差攻擊，且誤判率低，讓資安團隊能專注在真正重大的威脅警示上。

彈性的部署選項

Network Security Essentials 需要內部虛擬或實體裝置，可在 In-line 或純監控模式中進行部署。Network Smart Node 為內部裝置，可橫跨範圍內的位置進行部署，從主要網路邊界到遠端和分公司辦公室 — 只要可以直接存取網路的位置皆可部署。可下載的虛擬機器影像 (圖 1) 為最常用的方法，因為其符合成本效益且可以快速進行部署。Network Smart Node 使用情報導向分析技術及特徵碼型 IPS 偵測功能，來辨識並抵禦可疑活動。他們使用加密連線，來傳送需要進一步分析的可疑物件至 FireEye 私有雲端中的 Cloud MVX 服務。Network Smart Node 及 Cloud MVX 服務也可做為整合硬體裝置 (圖 2)。FireEye 向小型企業推薦 50 Mbps 選項，中型企業則推薦 100 Mbps 選項。

Email Security: Email Threat Protection Cloud

電子郵件是多數入侵事件的開端。ETP 是一項雲端型軟體即服務 (SaaS) 產品，可針對魚叉式網路釣魚、商業病毒或垃圾郵件威脅，分析電子郵件中是否有相關徵兆。ETP 運用專利 MVX 技術來主動防範進階電子郵件攻擊。ETP 也提供 In-Line 防垃圾郵件與防毒保護，透過 In-Line 或純監控部署，同時保護內部與雲端信箱。

Threat Intelligence

雲端型 FireEye 威脅情報附帶 FireEye 解決方案的警示。此情報 (每 60 分鐘更新一次) 內含新型惡意軟體描述檔、弱點入侵、對手資料與受害者情報及威脅調查結果等資訊。此服務可透過雲端化分析和機器學習技術，彌補 Cloud MVX 引擎對進階威脅偵測的不足之處。因此，FireEye 警示可能會含有寶貴的情境關聯資訊，例如威脅發動者可能的身分、可能的動機以及惡意軟體詳細資訊，以協助資安專業人員偵測具高度目標性的零時差攻擊與已知惡意軟體，並加以阻止。

[1] Verizon 2015 年資料破壞調查報告 (Data Breach Investigations Report)

範例設定

組裝解決方案時需要考慮的因素包括：監控的電子信箱數、系統內的網路流量大小、虛擬化或實體環境、採用的雲端傳送服務、以及高階業務主管和董事會所具備的安全意識等級。FireEye 與合作夥伴可協助您選擇或設計符合您需求的解決方案，並在這些範例設定後建立模型。

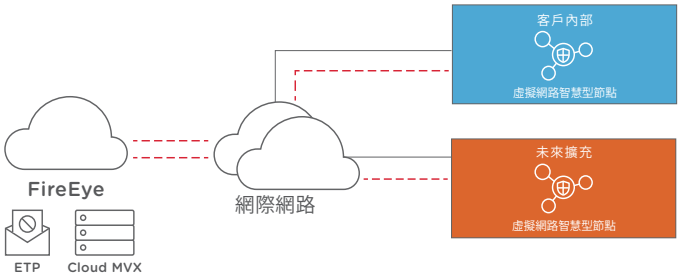

圖 1. ETP CLOUD 及具虛擬裝置的 CLOUD MVX

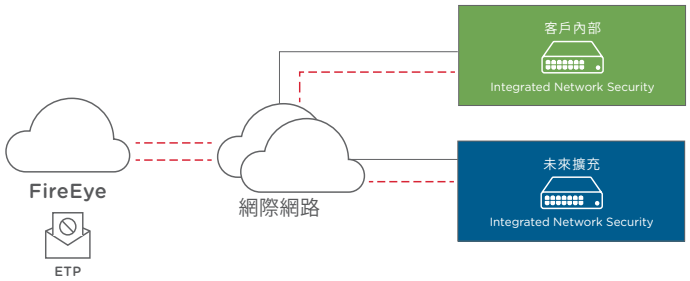

圖 2. ETP CLOUD 及實體整合網路安全性裝置

	小型 #1	小型 #2	中型 #1	中型 #2
部署類型	虛擬/雲端	實體裝置	虛擬/雲端	實體裝置
員工數量	200-250	200-250	450-550	450-550
網路流量	50 Mbps	50 Mbps	100 Mbps	100 Mbps
範例解決方案提案	ETP 200-250 位置 Virtual NX1500 Cloud MVX	ETP 200-250 位置 Integrated 2500NXE1	ETP 450-550 位置 Virtual NX2500 Cloud MVX	ETP 450-550 位置 Integrated 2500NXE2

後續步驟

SME 是進階攻擊者的首選目標或機會，因為他們的安全性措施往往較為不足，而這大部分要歸因於其資源有限且警覺意識較薄弱。為了拓展業務及降低風險，維持基本層級的安全措施非常重要。這需要對安全性狀態的信心，以及安全性計劃、工具和程序。

若要深入瞭解 FireEye，請前往：
www.FireEye.com

關於 FIREEYE, INC.

FireEye® 是一間情報主導的資安即服務領導公司。FireEye 以流暢、可擴充的客戶安全作業延伸，提供了混合創新安全技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平台。FireEye 在全球 67 個國家/地區擁有超過 5,000 位客戶，其中包括富比士全球 2000 大公司中的 940 家以上公司。

FireEye Taiwan
台灣火眼有限公司 / 10683 台北市信義路四段6號6樓
+886 2 5551 1268 / FIREEYE / taiwan@FireEye.com

www.FireEye.com