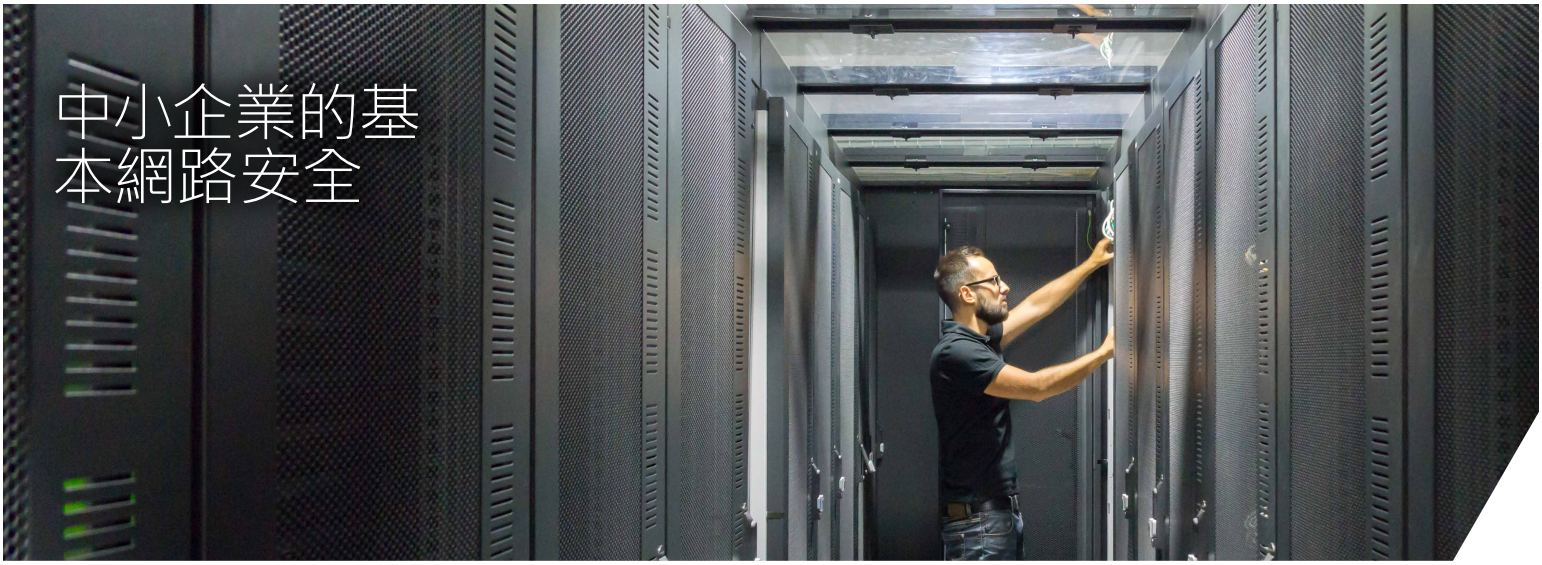
中小企業的基本網路安全



概述

許多產業報告都指出中小企業 (SME) 處於由手段細膩的網路攻擊者策動的風險中。事實上，在所有網路犯罪中，有 77% 是將 SME 當作目標。但預算限制使 SME 難以獲得需要的資源來保護自己並防範進階威脅。

安全機制的基本標準需要兼具「偵測與防護」的策略，才能防範進階威脅，此外還要搭配回應準備計畫以應付突發事件。獲獎項肯定的 FireEye 技術可協助偵測多階段與多媒介攻擊，並加以阻擋。這些技術使資安團隊可獲得準確的資料，並瞭解情境狀況，然後立即自行或交由合作夥伴執行回應計畫。FireEye 及其合作夥伴提供的服務還能彌補這些主動式技術的不足，協助組織對事件做出回應。

這些有效的解決方案皆是為了讓 SME 能輕鬆使用，進而心無旁騖地發展自己的業務。

挑戰

政府機關和大型企業在過去已經知道進階威脅的存在，也逐漸地導入安全機制架構，並採用各種技術來降低資料外洩的風險和衝擊。這類組織通常會有可靈活調整的安全性預算，或是由法務或監管部門將安全機制支出強制列入預算中。SME 面臨的挑戰，就是缺乏同行大型企業所擁有優勢，卻依舊面臨類似的風險。

雖然新聞傾向於著重在大型資安事件的報導，但其實 SME 往往才是網路犯罪的主要目標。[1]原因為何？ 因為與個人相比，SME 擁有更多資產 (例如信用卡號碼、身分識別資訊、醫療保健記錄、智慧財產等)，但如果與大型企業相比，卻又較缺乏安全機制 — 這使 SME 成為攻擊者的「最佳攻擊點」。

許多 SME 也因為向大型組織提供業務流程外包 (BPO) 或資訊科技服務 (ITES) 而成為攻擊目標。攻擊者利用這種信任關係滲透至較弱的連結中，然後橫向移動至更顯著的目標。攻擊者喜歡依循阻力最小的途徑來達成目標。

大型企業越來越重視自身的供應鏈，會判斷供應商是否能克盡職責，展現高度的網路安全性。SME 必須導入更高層級的進階防護和偵測能力，才能符合這些要求並開拓業務。

由於安全性不足，使得魚叉式網路釣魚電子郵件和勒索軟體逐漸成為 SME 的威脅。SME 或許不會認為自己是攻擊目標，但面對勒索軟體「光明正大」的這種攻擊方式，不堪一擊的安全機制卻很容易使自己成為目標。

舊有的特徵碼式安全性技術已無力抵抗這類威脅，因為它們不但有各種變化，甚至還經蓄意設計為避免重複出現過去的所有特徵碼。因此，SME 最終仍須面對進階威脅和勒索軟體的風險並想辦法解決。因為根據估計，所有遭受網路攻擊的中小企業中，有一半會在 6 個月內就歇業。[2]

1 賽門鐵克，《2015 年網路安全威脅報告》，2015 年 4 月
2 https://staysafeonline.org/

FireEye

解決方案

如果要抵禦現今手段細膩的攻擊者，就需要可經由下列方式防範及偵測進階威脅的安全性解決方案：

- 從各個媒介中察覺最大的威脅媒介和惡意活動。
- 發現新的威脅，包括未曾見過的 (零時差) 攻擊，以及各種廣為人知的威脅和商業威脅。
- 辨識進階的多階段與多媒介攻擊。
- 運用最先進的情報快速辨認出嚴重威脅與威脅發動者。

FireEye Essential Security 結合了 FireEye Network Security (NX) Essentials 和 FireEye Email Threat Prevention Cloud (ETP)，可保護組織防範各種網頁型與電子郵件型威脅。這兩種威脅媒介在網路攻擊的比例中就佔了 90%。Essential Security 解決方案只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。

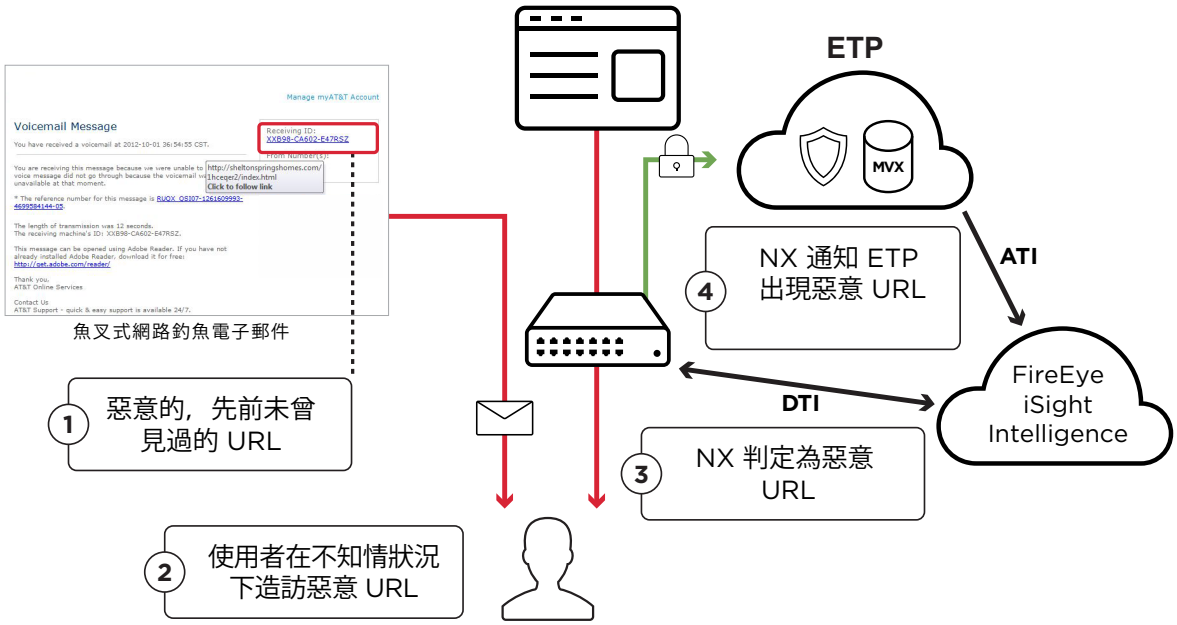
強大的 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎是 FireEye 最核心的關鍵技術。它可以協助辨識出橫跨多個攻擊面的進階多階段攻擊和混合式威脅，包括網頁與電子郵件；如果只從單一面獨立檢視這類攻擊，便可能不會視為惡意活動。

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 (如圖 1 所示)。只要能夠發現這種連結，便可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運用類似策略、工具及程序 (TTP) 的後續攻擊，並加以封鎖。

Essential Security 解決方案可利用具有情境關聯狀況的可行情報，協助組織更快對威脅做出回應。它還能整合技術部署、自動封鎖重大攻擊並產生實質有幫助的警示，將浪費資源的情形減至最低，藉此讓 SME 充分利用有限的網路安全預算，同時減少營運開支。

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，還能改善安全性狀態。

圖 1. NETWORK SECURITY ESSENTIALS　EMAIL THREAT PREVENTION 的多媒介關聯



偵測與防護技術

Network Security Essentials

FireEye 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。它可偵測已知與未知的網路型網路攻擊，將破壞所帶來的風險成本降至最低。此解決方案會運用 MVX 引擎分析網路流量，藉此偵測是否有入侵、惡意軟體執行檔及多通訊協定回呼活動。其也包含入侵預防系統 (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、獨立 IPS 或防毒 (AV) 解決方案不同之處在於，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。

Email Security: Email Threat Protection Cloud (ETP)

電子郵件是多數入侵事件的初期手段。FireEye ETP 是一項軟體即服務 (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 除了憑藉雲端服務簡化部署工作外，還能運用具專利的 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，可同時保護內部部署與雲端信箱。

Threat Intelligence

以雲端為基礎的 FireEye Threat Intelligence 可擷取我們專有的情報資料，這些資料來自 FireEye 解決方案在全球部署的偵測器和附帶的警示。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 MVX 引擎對進階威脅偵測的不足之處。

FireEye Dynamic Threat Intelligence (DTI) 會每小時更新匿名交換資料，這些資料包括遍佈於 FireEye 全球雲端網路中的各種網頁、電子郵件及檔案型威脅。這些更新內容可確保 FireEye 能在全球客戶網路中找出最新發現的攻擊資料並加以封鎖。Network Security Essentials 中已隨附 DTI。

FireEye Advanced Threat Intelligence (ATI) 可提供由威脅情報分析師和資安事件處理人員收集而來的詳盡對手資料與受害者情報。因此，FireEye 攻擊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。這讓解決方案在偵測具高度目標性的零時差攻擊與已知惡意軟體時，顯得更有效率，還能協助專業資安人員搶先取得優勢並阻止威脅發動者。ATI 是 ETP 的標準功能。

部署選項

Essential Security 解決方案可 In-Line 部署，以換取更高的掌控能力和即時回應速度，以便阻止正在進行中的攻擊活動 (如圖 2 所示)。

圖 2A. NETWORK SECURITY ESSENTIALS – IN-LINE 部署

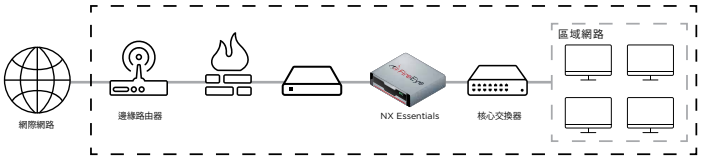
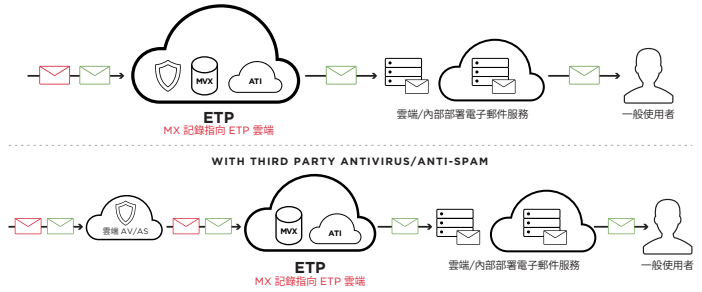


圖 2B. EMAIL THREAT PREVENTION – IN-LINE 部署



部分組織偏好以較保守的方式著手進行，所以此解決方案也能以頻外或純監控模式 (ETP 則為 BCC 模式) 進行部署 (如圖 3 所示)。在此種部署中，系統會監控所有流量中是否有惡意活動，且會產生報告，但沒有任何自動化防護機制。FireEye 或我們的合作夥伴可幫您判斷及部署最符合您需求的選項。

圖 3A. NETWORK SECURITY ESSENTIALS – 頻外 (TAP/SPAN) 部署

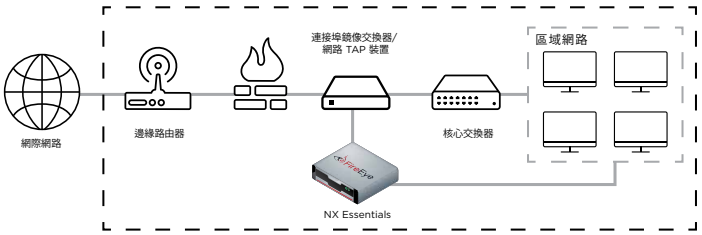
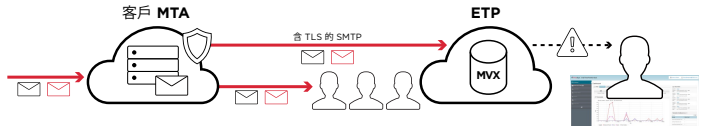


圖 3B. EMAIL THREAT PREVENTION – BCC 模式



入侵事件準備措施

請記住，偵測與防護只能解決一半的問題。針對突發事件所造成的技術、法務、財務及公關連帶影響，也同樣有必要進行分析並做出回應。FireEye 強烈建議您制定一套回應計畫，而且最好與安全機制合作夥伴一同討論。FireEye 及其合作夥伴對於回應計畫部署、回應計畫驗證及資安事件調查均有提供服務。

後續步驟

SME 是進階攻擊者的目標首選，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威脅警覺意識較薄弱。為了讓您能專心拓展業務並將風險降至最低，我們建議您至少採取基本層級的安全措施。這包括專為抵禦及因應現今手段細膩的網路攻擊者而設計的安全性技術和程序。這些措施最終可讓您對組織的安全性狀態有更多信心。

若要深入瞭解專為偵測及防範進階攻擊而設的 FireEye 安全性解決方案，以及準備一套合適的回應計畫以因應入侵事件，請造訪 www.FireEye.com 或聯絡您當地的銷售代表。

關於 FIREEYE

FireEye 保護世界上最寶貴的資產，免於現今網路攻擊者的侵擾。我們的技術、情報及專業知識組合有助於化解入侵事件所造成的衝擊。FireEye 全球防禦社群在全球 67 個國家/地區擁有 4,400 名客戶，其中財星五百大企業就超過 250 家公司。

如需 FireEye 的詳細資訊，請造訪：
www.FireEye.com

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 / Taiwan@FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com