解決方案概要

面對日新月異網絡威脅大挑戰

為其他人錯過的攻擊做好準備

現今的資安挑戰

進階，目標性及其他規避性攻擊讓組織很難有效預防網絡入侵：

- 網絡犯罪者會使用進階攻擊規避新一代防火牆、IPS 及防毒解決方案，並且在組織內隱匿數個月 (2015 年，在收到外部單位通知時，網絡犯罪者平均已隱匿 320 天)[1]
- 超過 68% 的惡意軟體會針對特定組織，而其中的 80% 只使用一次[2]，令特徵碼式防禦機制無法有效對抗目標性攻擊
- 超過 80% 的特徵碼式和原則式安全警示皆不可靠[3]，不但佔用資源，也錯失了專注處理重大警示的機會

現今業務導向的 IT 轉型擴大了組織的攻擊面，而讓此挑戰的難度也隨之增加：

- 到了 2020 年，公有雲應用程式將佔企業支出的三分之二以上。[4] 以雲端為基礎的營運將組織的入埠和出埠網際網絡流量 - 以及潛在威脅 - 提高 40%。[5]所有這些流量必須經過檢查
- 現今 96% 的組織所支援的非 Windows 裝置[6]在傳統上並沒有獲得良好的防護
- 40% 的分公司會採用直接網際網絡連線[5]，使得他們在獲得嚴密防護的中央辦公室外暴露在攻擊威脅下的風險增加

防護網絡入侵的四大要素

為了徹底降低因網絡入侵而須付出昂貴代價的風險，各種規模的組織都需要有效抵禦攻擊的解決方案。其必須：

1. 能偵測和阻止傳統安全性產品遺漏的威脅
2. 能迅速回應並遏止資安事件所造成的影響
3. 不斷適應持續變化的威脅形勢
4. 在組織擴張或 IT 服務的提供模式變更時，能隨之調整並保持靈活性

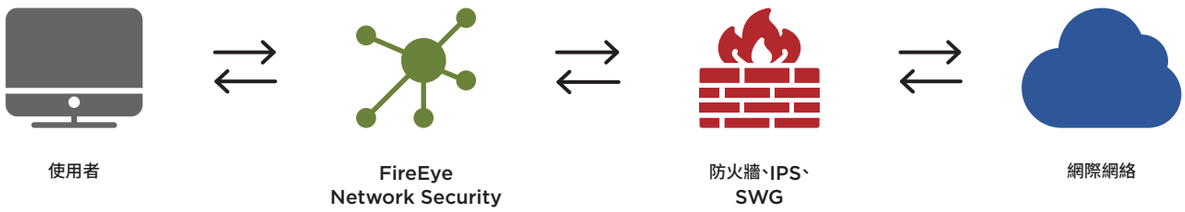
FireEye Network Security

FireEye Network Security 能準確偵測，並立即阻止進階，目標性及隱藏在網際網絡流量中的其他規避性攻擊，進而協助各種規模的組織降低因網絡入侵而須付出昂貴代價的風險。FireEye Network Security 的核心為 Multi-Vector Virtual Execution™ (MVX) 和情報導向分析 (IDA) 技術。MVX 是一種無特徵碼的動態分析引擎，能檢查可疑物件，以找出目標性、規避性及未知的威脅。IDA 引擎會依據電腦、攻擊者和受害者情報，偵測並封鎖惡意物件。

FireEye Network Security 適用於各種機型和部署模式。這通常會安裝在傳統網絡安全裝置 (例如：新一代防火牆、IPS 及安全網絡閘道 [SWG]) 後方的網際網絡流量路徑上。

1 FireEye (2016 年 2 月)。M-Trends 2016。
2 Joshua Goldfarb (2016 年 9 月 19 日)。"Detection Innovations." (偵測技術上的創新。)
3 Ponemon Institute LLC (2015 年 1 月)。"The Cost of Malware Containment." (惡意軟體遏制的成本。)
4 Forrester (2016 年 9 月)。"The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020." (到了 2020 年，公有雲服務的市場產值將迅速成長至 2,360 億美元。)
5 IDC (2016 年 2 月)。"Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services." (通訊服務供應商採用的 SD-WAN 技術及其對 MPLS VPN 服務的影響。)
6 JAMF Software (2015 年)。2015 年調查：管理企業中的 Apple 裝置。

圖 1. 一般配置：Network Security 解決方案。



為了有效保護各種規模的組織免於網絡入侵的威脅，FireEye Network Security 提供：

- **準確偵測：**MVX 和 IDA 技術具備高準確率、低誤報率的攻擊偵測能力。這些技術也能橫跨多個流量和威脅媒介建立事件關聯性，藉此抵禦其他解決方案無法偵測或阻止的多階段攻擊。
- **即時而強韌的防護：**In-line 封鎖入埠的入侵和惡意軟體以及出埠的多重通訊協定回呼，立即阻止攻擊。高可用性選項，可在網絡連結失效或裝置故障時，提供更強的恢復能力和防護。
- **可行的深入見解：**警示包括從前線取得的具體證據以及情境式情報，以迅速對威脅做出回應、排定其優先順序，並加以遏止。
- **指標擷取：**結構化威脅資訊表示 (STIX) 格式讓自訂情報得以帶入 IDA 引擎。
- 全新推出！ **可延伸架構：**軟體和系統設計，使得多重威脅防護技術得以軟體模組的方式提供。

- **全方位防護：**支援多種環境，除了最常見的 Microsoft Windows 與 Apple OS X 作業系統外，還包括超過 140 種的檔案類型以及數千種作業系統、Service Pack 及應用程式的組合，以涵蓋極為廣泛的攻擊面。
- **回應工作流程整合：**供深入調查的警示驗證、風險軟體分類以及封包擷取的樞紐分析能自動化警示回應工作流程，並加快其速度。

適合貴組織的完美防護

FireEye Network Security 提供彈性且可擴充的部署選項，最多可達 8 Gbps，以滿足中大型組織的需求與預算考量。

- **Integrated Network Security：**使用 MVX 服務以保護單一網際網絡存取點安全的全方位獨立硬體裝置。
- 全新推出！ **Distributed Network Security：**網絡智慧型節點與共用的 MVX 服務將防護擴展至整個組織。
  - **網絡智慧型節點：**部署在網際網絡存取點上，以辨識並抵禦可疑活動的實體或虛擬裝置
  - **MVX 智慧型網格或 FireEye Cloud MVX：**可執行進一步的分析以偵測進階攻擊，讓安全團隊能更有效率的提供內部部署或雲端型 MVX 服務

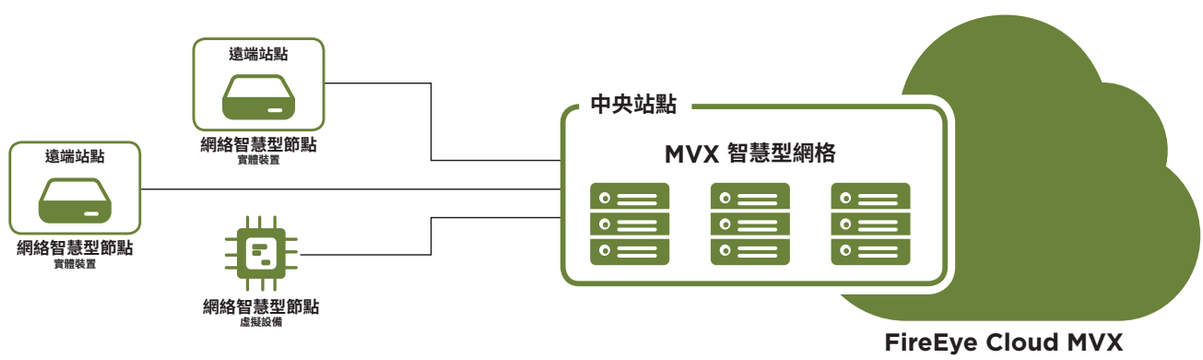


圖 2. Distributed Network Security。

FireEye Network Security Essentials 提供從 10 Mbps 到 2 Gbps，符合成本效益的整合式與分散式部署選項，以符合中小型組織的需求。

表 1. FireEye Network Security 部署選項。

	整合式裝置	網絡智慧型節點	MVX 智慧型網格 需要網絡智慧型節點	FireEye Cloud MVX 需要網絡智慧型節點
FireEye Network Security（適用於中大型組織）	內部部署	實體或虛擬	內部部署和分佈式	以雲端為基礎的和分佈式
FireEye Network Security Essentials（適用於中小型組織）	內部部署	實體或虛擬	不適用	以雲端為基礎的和分佈式

縮短投資回收期

FireEye Network Security 的設計旨在滿足單一站點及分散式多站點組織的需求，能降低網絡入侵風險，並縮短投資回收期。

根據 Forrester Consulting 的最近一項研究指出，[7]FireEye Network Security 的客戶，預計可因三年期間節省下來的費用而達到 152% 的投資報酬率，初期投資也可在短短 9.7 個月內回收。透過以下機制即可節省您目前和未來的各項費用：

- 將安全團隊的資源集中在處理真正的攻擊上，以降低營運費用。
- 透過可以共用 MVX 容量的選項以及調整為最理想部署規模的各種效能點，達成最理想的資本支出。
- 容許依分公司數量或網際網絡流量成長，而逐漸擴充容量的未來整備度投資。
- 從整合式部署移轉到分散式部署的免成本轉移，保護現有投資。
- 以模組化的可延伸架構減少未來資金投入。

為何選擇 FireEye Network Security?

FireEye MVX 引擎是市場上具原創性且最成功的進階[8]威脅防護解決方案：

- 從 2013 年開始，FireEye 發現「流傳在外」並且十分猖獗的零時差攻擊數量比其他解決方案的總和還多。
- 2016 年，Frost & Sullivan 確認 FireEye 的市場領導者地位無庸置疑，其擁有 56% 市佔率，甚至超過僅次於它的十名競爭對手的總和。[9]
- FireEye Network Security 已多次榮獲 SANS Institute、SC Magazine、CRN 及其他機構頒發的獎項。
- FireEye Network Security 是市場上第一個榮獲美國國土安全部安全法認證的安全性解決方案。

7 Forrester（2016 年5 月）。“The Total Economic Impact Of FireEye.”（FireEye 的總體經濟影響。）
8 IDC（2015 年）。全球專業化威脅分析與防護的市佔率。
9 Frost & Sullivan（2016 年 9 月）。“Network Security Sandbox Market Analysis.”（網絡安全沙盒市場分析。）

表 2. FireEye Network Security 優點。

功能	優點
能偵測和阻止傳統安全性產品遺漏的威脅	
無特徵碼的威脅偵測 (MVX)	可偵測多流量、多階段、零時差、多型態、勒索軟體及其他規避性攻擊
即時和回溯性偵測	即時偵測已知和未知威脅，同時並啟用回溯性威脅偵測功能
多媒介關聯	自動驗證和封鎖橫跨電子郵件、端點及檔案媒介的攻擊
多種作業系統、檔案及應用程式支援	支援多種應用程式的異質端點環境
強化型 Hypervisor	提供規避防護
能迅速回應並遏止資安事件所造成的影響	
即時 In-line 封鎖	立即阻止攻擊
整合式安全工作流程	從偵測到調查的樞紐分析和回應
高可用性 (HA)	具備恢復能力的防禦機制
特徵碼式 IPS 偵測以及降噪功能	自動化和加快分類傳統上不具意義的警示，以免除人工負擔
風險軟體偵測與分類	對重大和非重大惡意軟體進行分類，以排定回應資源的優先順序
可行的內容情報	藉由對攻擊和攻擊者的深入瞭解，加快遏制進階威脅的速度
不斷適應持續變化的威脅形勢	
即時共用威脅情報	全球共用真實證據，以立即封鎖先前未知的攻擊並加快回應速度
全新推出! 客製化及第三方威脅情報 (結構化威脅資訊表示，STIX)	將 FireEye 和第三方指標導入具 STIX 功能的 IDA 引擎
策略威脅情報	對威脅形勢轉變進行主動評估，並賦予採取前瞻性安全狀態的能力
在組織擴張或 IT 服務的提供模式變更時，能隨之調整並保持靈活性	
支援的頻寬	10 Mbps 至 8 Gbps
支援的規模	單一站點到分散式部署的數千個站點
支援的機型	實體、虛擬、雲端
部署模式	具備網絡智慧型節點與 MVX 服務架構的 Integrated Network Security 以及 Distributed Network Security

要知道更多關於 FireEye，請前往：**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 |
FIREEYE /taiwan@FireEye.com

關於 FireEye, Inc.
FireEye 是一間情報主導的資安公司。FireEye 以流暢、可擴充的客戶資安作業延伸，提供了混合創新資安技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平臺。藉由此方法，FireEye 得以讓對於準備、預防及回應網絡攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。FireEye 在全球各地 67 個國家/地區擁有超過 6,600 位客戶，其中包括富比士全球 2000 大公司中百分之 45 的多家公司。