FIREEYE™

產品型錄

FireEye Network Security 網路威脅防禦

為中大型組織提供有效的網路入侵防護措施

概觀

FireEye Network Security 網路威脅防禦是有效的網路威脅防護解決方案，能準確偵測並立即阻止進階及目標性威脅，及隱藏在網路流量中的其他規避偵測式攻擊，進而協助組織降低因網路入侵而須付出昂貴代價的風險。它有助於在極短時間內運用具體證據、可行情報及整合回應工作流程，對偵測到的資安事件提出有效的解決方案。不論遭到入侵的是 Microsoft Windows、Apple OS X 作業系統或是應用程式的漏洞；在總部或分公司辦公室；或是隱藏在大量入埠的網際網路流量而必須即時加以檢查，均可透過 FireEye Network Security 網路威脅防禦，讓組織獲得有效防護，避免這些威脅。

FireEye Network Security 網路威脅防禦的核心為 Multi-Vector Virtual Execution™ (MVX) 和動態機器學習與人工智慧 (*Artificial Intelligence*, AI) 技術。

MVX 是無特徵碼的動態分析引擎，能檢查可疑網路流量，以找出規避傳統特徵碼和原則防禦機制的攻擊。多重機器學習、AI 與關聯引擎代表一組情境動態規則引擎，能根據電腦、攻擊者及受害者的最新情報，即時和回溯性偵測，並封鎖惡意活動。FireEye Network Security 網路威脅防禦還包括入侵預防系統 (*Intrusion Prevention System*, IPS) 技術，可透過傳統的特徵碼比對偵測常見攻擊。

FireEye Network Security 網路威脅防禦適用於各種機型、部署及效能選項。這通常會安裝在傳統網路威脅防禦裝置 (例如：新一代防火牆、IPS 及安全網路閘道 [*Secure Web Gateways*, SWG]) 後方的網際網路流量路徑上。FireEye Network Security 網路威脅防禦能以高準確率和極少誤判率迅速偵測已知和未知的攻擊，進而補強這些解決方案，同時有助於以高效率回應每則警示。

圖 1. 一般配置 — Network Security **網路威脅防禦方案。**

功能	優點
偵測	
準確偵測進階、目標性及其他規避性攻擊	有效降低因網路入侵而須付出昂貴代價的風險
模組化與可擴展的資安架構	提供投資保護並支援業務成長
為多種作業系統環境和所有網際網路存取點提供一致的保護層級	建立橫跨整個組織以至到所有類型裝置的強大防禦機制
整合式、分散式、實體、虛擬、內部部署及雲端部署選項	提供彈性以因應組織的偏好與資源
以電子郵件安全和內容安全建立多媒介關聯	全盤掌握更廣泛的攻擊面
預防	
以 250 Mbps 到 10 Gbps 的線速立即封鎖攻擊	即時抵禦規避偵測式攻擊
對加密流量的可視性	應用設備內建 TLS 1.3 解密支援，不需額外支付授權費用
回應	
低誤報率、風險軟體分類並映射到 MITRE ATT&CK 架構	減少分類不可靠警示的作業成本
供調查和警示驗證的樞紐分析、端點遏制及事件回應	自動化和簡化安全工作流程
執行證據和可行威脅情報	加快排定優先順序，並解決已偵測到的資安事件

技術優勢

準確可行的威脅偵測與見解

FireEye Network Security 網路威脅防禦運用多項分析技巧，能以高準確率和低誤判率偵測出攻擊：

- **Multi-Vector Virtual Execution™ (MVX) 引擎**可藉由在安全的虛擬環境中使用動態的無特徵碼分析，偵測出零時差、多流量及其他規避偵測式攻擊。它可找出從未見過的入侵和惡意軟體，在網路攻擊擊殺鏈的感染和入侵階段即予以阻止。
- **多重機器學習、AI 與關聯引擎**能從數千小時的事件回應經驗，在前線收集到即時的深入見解，並從中得出情境相關、規則式分析結果，藉此偵測出偽裝、目標性及其他客製化攻擊並加以封鎖。它能找出惡意入侵、惡意軟體、網路釣魚攻擊及命令與控制 (*Command and Control,* CnC) 回呼，在網路攻擊擊殺鏈的感染、危害及入侵階段予以阻止。它還能擷取可疑的網路流量，並提交至 MVX 引擎，進行最終的裁定分析。除此之外，客戶端的保護、引擎支援伺服器端的偵側、橫向移動偵測和後滲透流量偵測。
- FireEye Network Security 所產生的警示包含具體即時證據，可迅速回應威脅、排定優先順序，並遏止針對性與新發現的攻擊。偵測到的威脅也可映射到 MITRE ATT&CK 架構以取得關聯證據。

即時而強韌的防護

FireEye Network Security 提供靈活的配置模式，包括：

- 透過 TAP/SPAN、In-line 監控或 In-line 主動式封鎖的頻外監控。Inline 封鎖模式會自動封鎖入埠入侵與惡意軟體以及出埠多重通訊協定回呼。在 Inline 監視模式下，會產生警示，並讓組織決定因應攻擊的對策。在頻外防護模式下，FireEye Network Security 網路威脅防禦會發出 TCP 重設，以在頻外封鎖 TCP 或 HTTP 連線。
- 特定模式可提供主動式高可用性 (*High Availability,* HA) 選項，以便在網路失效或裝置故障時提供恢復能力。

涵蓋廣泛的攻擊面

FireEye Network Security 網路威脅防禦可為現今多樣化的網路環境提供一致的保護層級：

- 支援最常見的 Microsoft Windows 與 Apple Mac OS X 作業系統。
- 可分析超過 160 種的檔案類型，包括可攜式可執行檔 (*Portable Executables,* PE)、活躍型網路內容、壓縮檔、影像、Java、Microsoft 和 Adobe 應用程式，以及多媒體。
- 在數千個作業系統、Service Pack、IoT 應用程式類型及應用程式版本組合上執行的可疑網路流量。
- 預防高階攻擊和較難透過特徵碼偵測的惡意軟體類型：web shell 上傳、現存的 web shell、勒索軟體、加密貨幣挖礦。

經驗證並排定優先順序警示

除了偵測真正的攻擊之外，FireEye MVX 技術還能用來驗證透過傳統特徵碼比對方法所偵測的警示，以及識別重大威脅並排定其優先順序：

- 入侵預防系統 (IPS) 結合 MVX 引擎驗證，能縮短對特徵碼式偵測進行分類所需的時間，而傳統上這類偵測容易出現誤報的情況
- 風險軟體分類會將真正的嘗試入侵行為與不受歡迎、但惡意程度較低的活動 (例如廣告軟體和間諜軟體) 區分開來，藉此排定警示回應的處理順序

回應工作流程整合

可利用多種方式增強 FireEye Network Security 網路威脅防禦，以自動執行警示反應工作流程：

- **FireEye Central Management** 可將 FireEye Network Security 網路威脅防禦和 FireEye Email Security 的警示與對攻擊更廣泛的瞭解建立關聯，並設定封鎖規則，以防止攻擊進一步擴散。
- **FireEye Network Forensics** 會與 FireEye Network Security 網路威脅防禦整合，提供與警示相關的擷取封包詳細資料，並進行深入調查。
- **FireEye Endpoint Security** 端點威脅防禦可識別、驗證並遏止 FireEye Network Security 網路威脅防禦偵測到的入侵，以簡化受影響端點的遏制和修復作業。

彈性的部署選項

FireEye Network Security 網路威脅防禦提供各種部署選項，以符合組織的需求與預算考量：

- **Integrated Network Security：**使用整合式 MVX 服務，以保護位於單一站點之網際網路存取點安全的全方位獨立硬體裝置。FireEye Network Security 是易於管理的無用戶端平台，無需必要規則、政策或微調即可快速部署。
- **Distributed Network Security：**可延伸的裝置搭配，從中心位置共用的 MVX 服務，以確保組織內網際網路存取點的安全。
  - **網路智慧型節點：**可分析網際網路流量以偵測和封鎖惡意流量，並經由加密連線提交可疑活動給 MVX 做最終裁定分析之實體或虛擬裝置。
  - **MVX 智慧型網格：**由內部部署、座落於中央位置，並具彈性的 MVX 提供透明的可擴充性、內建的 N+1 容錯以及自動負載平衡。
  - **FireEye Cloud MVX：**FireEye 代管的 MVX 服務訂閱項，可分析網路智慧型節點上的流量，以確保隱私安全。只有可疑物件經由加密連線提交至 MVX 服務，經裁定為良性的物件之後便會被排除。
  - **就地部署或在雲端的防護：**除了獨立的虛擬應用設備，FireEye 使用 Amazon 和 Azure 提供公共雲端的網路威脅防禦。

圖 2. Integrated Network Security **的範例包括：**NX 2550、NX 3500、NX 5500 **及** NX 10550。

圖 3.

針對 Network Security 網路威脅防禦的分散式部署模型。

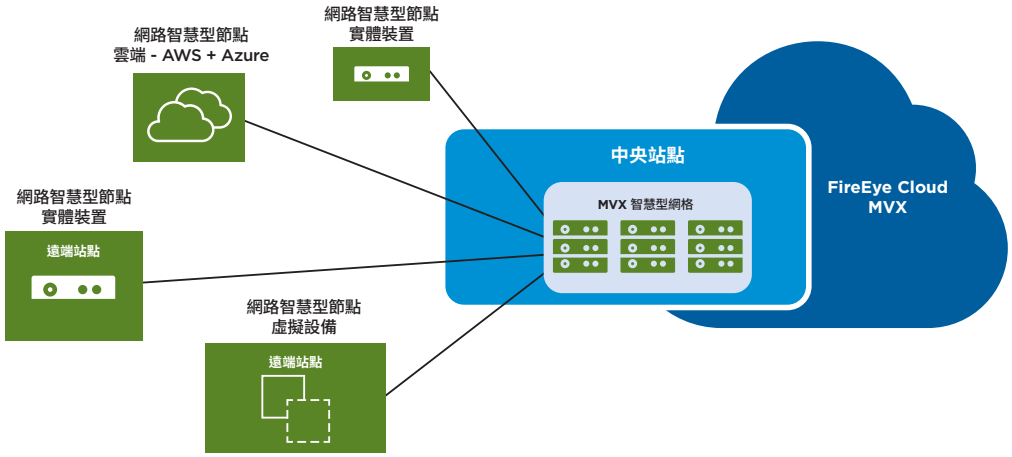

圖 4.

FireEye Network Security **網路威脅防禦的模組化元件。**

高效能與可擴充性

FireEye Network Security 網路威脅防禦能以線速保護網際網路存取點，並為各種分公司與中央辦公室規模提供效能選項：

MVX 智慧型節點和 FireEye Cloud MVX 可擴充架構，讓 MVX 服務能支援一到上千個網路智慧型節點，並且視需要順暢擴充。

外觀尺寸	效能
Integrated Network Security	50 Mbps 到 5 Gbps
實體網路智慧型節點	**50 Mbps 到 10 Gbps**
實體或公共雲端網路智慧型節點	50 Mbps 到 8 Gbps

業務優點

FireEye Network Security 網路威脅防禦能滿足單一站點和分散式多站點組織的需求，提供以下優點：

有效降低網路入侵風險

FireEye Network Security 網路威脅防禦為高效的網路防禦解決方案，其可：

- 防止入侵者闖入組織竊取寶貴資產或藉由阻止進階、目標性及其他規避偵測式攻擊以避免其中斷業務
- 藉由具體證據、可行情報、In-line 封鎖及回應工作流程自動化，更快阻止攻擊並遏止入侵
- 為不同作業系統、應用程式類型、分公司及中央站點提供持續的防護，以消除組織網路防禦機制中的弱點

縮短投資回收期

根據 Forrester Consulting 的研究指出[1]，FireEye Network Security 網路威脅防禦的客戶預計可因三年期間節省的成本而達到 152% 的投資報酬率，初期投資也可在短短 9.7 個月內回收。FireEye Network Security 網路威脅防禦：

- 將安全團隊的資源集中在處理真正的攻擊上，以降低營運成本
- 透過可以共用的 MVX 服務，以及可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
- 可在分公司數量或網際網路流量成長時，為未來擴充的整備安全投資更為順暢
- 藉由容許從整合式部署，轉移到分散式部署的免成本轉移以保護現有投資
- 以模組化的可延伸架構減少未來資金投入

1 Forrester (2016 年 5 月)。The Total Economic Impact Of FireEye (FireEye 的總體經濟影響)。

獎項與認證

FireEye Network Security 網路威脅防禦產品組合已多次榮獲產業和政府獎項與認證：

- 2020 年，FireEye 贏得海軍資訊作戰系統司令部 (NAVWAR) 人工智慧網路安全挑戰賽的第一名[2]
- 2020 年，KuppingerCole 授予 FireEye 網路偵測與回應領導地位指南的榮耀[3]
- 2020 年，Forrester 認定 FireEye 為網路分析與可見度的大型供應商[4]
- 2018 年，Frost & Sullivan 確認 FireEye 的市場領導者地位無庸置疑，其擁有 46% 市佔率，甚至超過僅次於它的十名競爭對手的總和[5]
- FireEye Network Security 擁有包括 Common Criteria、FIPS 140-2 和 SOC 2 在內的認證
- FireEye Network Security 網路威脅防禦已多次榮獲 SANS Institute、SC Magazine、CRN 及其他機構頒發的獎項
- FireEye Network Security 網路威脅防禦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

2 FireEye (2021 年 1 月 6 日)。在海軍資訊作戰系統司令部 (NAVWAR) 人工智慧網路安全挑戰賽中，FireEye 榮獲第一名。
3 KuppingerCole (2020 年 6 月 10 日)。網路偵測與回應領導地位指南。
4 Forrester (2020 年 6 月 23 日) Now Tech：網路分析和可見度，2020 年第 2 季。
5 Frost & Sullivan (2018 年 7 月 5 日) 預測至 2022 年的全球進階惡意程式沙箱 (AMS) 解決方案市場。

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
Taiwan@FireEye.com

©2021 FireEye, Inc. 保留一切權利。
FireEye 和 Mandiant 為 FireEye, Inc. 的註冊商標。
所有其他品牌、產品
或服務名稱分屬各擁有人之商標或服務標記。
NS-EXT-DS-US-EN-000048-13

關於 FireEye

FireEye **是一間情報主導的資安公司。作為客戶資安監控的無縫、可擴展的延伸，**FireEye **提供單一平台，將創新的資安技術、國家級別的威脅情報和世界知名的** Mandiant® **諮詢融合在一起。藉由此方法，**FireEye **得以讓對於準備、預防及回應網路攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。**