FIREEYE™

產品型錄

FireEye Email Security 伺服器版

自適性、智慧型和可擴充的防護平台，阻絕電子郵件滲透攻擊的威脅

圖 1. 整合式 Email Security 裝置包含 EX 3500、EX 5500 和 EX 8500。

重點

- 提供全面的電子郵件安全，對抗惡意附件、憑證網路釣魚連結、詐騙、零時差和多階段攻擊
- 支援分析 — 用來針對 Microsoft Windows 及 Apple macOS X 操作系統圖示
- 廣泛檢查電子郵件，查看受密碼保護的檔案、加密的附件及連結中是否存在隱藏的威脅
- 從 FireEye DTI 雲端獲取即時威脅情報
- 透過提供警示的背景剖悉，決定優先順序並圍堵威脅
- 以整合式或分散式 MVX 服務來進行內部部署

概觀

電子郵件因其為最大量的資料入口，故是網路攻擊中最脆弱的環節。企業面臨越來越多來自電子郵件進階式威脅的資安挑戰。大多數進階威脅使用電子郵件將連結傳遞至憑證式釣魚網站及武裝的檔案附件。它具有較強的目標性與自訂性，因此電子郵件成為網路犯罪的主要媒介。

FireEye Email Security 可協助組織將進階電子郵件攻擊造成的昂貴的入侵風險降至最低。FireEye Email Security 伺服器版在內部部署，可引領業界辨識、隔離及立即阻止連結和附件型攻擊進入組織。Email Security 整合了情報主導的背景資料與偵測外掛程式，以偵測大數據、可擴充的平台上的惡意與良性的連結。無特徵碼的 Multi-Vector Virtual Execution™ (MVX) 引擎，針對作業系統、應用程式及網站瀏覽器等全面的交叉矩陣上分析電子郵件附件及連結至可下載內容的連結。其可在最小的干擾下辨識威脅，且幾乎不會有誤報情況。

FireEye 透過第一手的入侵調查及數百萬個感測器，蒐集詳盡的敵手威脅情報。Email Security 利用對攻擊與攻擊者相關的實證及情境情報，即時按優先順序處理警示並封鎖威脅。

透過與 FireEye Network Security 和 Endpoint Security 相結合，組織可提供更廣的可見度，以對抗多向量混合式攻擊並協調即時防護。

防禦電子郵件威脅

在所有個人資訊皆可從網路上取得的情況下，網路罪犯可能會對幾乎任何使用者採用社交工程，誘使他們執行動作、點選連結或開啟附件。

Email Security 可提供即時偵測及防護，以對抗能夠規避電子郵件安全性傳統防禦機制的憑證收集、冒充和魚叉式網路釣魚攻擊。如果發現未知和進階威脅隱藏在以下情況中，電子郵件將經過分析與隔離（封鎖）：

- 附件檔案，類型包括（但不限於）：EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4 以及 ZIP/RAR/TNEF 壓縮檔
- 有密碼保護及加密的附件
- 有密碼保護的附件（具有透過圖片傳送的密碼）
- 連結嵌入在電子郵件，MS Office 文件，PDF 及壓縮檔（ZIP，ALZIP，JAR），以及其他檔案格式（Uuencoded, HTML）
- 透過連結下載的檔案 – 以及甚至是 FTP 連結
- 混淆、欺騙、縮短及動態重新導向的連結
- 憑證式網路釣魚及註冊近似域名連結
- 未知 Microsoft Windows 與 Apple macOS X 操作系統圖片，瀏覽器和應用程序漏洞
- 魚叉式網路釣魚電子郵件內嵌的惡意程式碼

勒索軟體攻擊是從電子郵件開始，但需要回呼命令以控制伺服器來加密資料。Email Security 辨識及阻擋難以偵測的多階段惡意軟體活動。

出色的威脅偵測

Email Security 透過辨識和隔離以正常流量偽裝的進階、目標性及其他規避性攻擊，協助降低因網路入侵而須付出昂貴代價的風險。一旦被偵測，將立即停止、分析這些攻擊，並採集指紋以更快辨識未來威脅。

Email Security 的核心是進階連結防禦、MVX 引擎和 MalwareGuard。這些技術使用機器學習與分析功能辨識入侵傳統特徵碼式及政策式防禦的攻擊。

作為進階連結防禦不可或缺的一部份，PhishVision 是一款圖像分類引擎，它使用深度學習功能以針對電子郵件中由連結參考的網頁編譯和比較受信任及常見目標性品牌的螢幕截圖。與 PhishVision 一起協作時，Kraken 是一款網路釣魚偵測外掛程式，該程式套用網域和網頁內容分析以提升機器學習能力。連結偵測的另一個進階 Skyfeed，是一種專門建構的、全自動的惡意軟體情報收集系統。社交媒體帳號、部落格、論壇及威脅摘要被收集用來發現誤判。多重面向的進階連結防禦為受 Email Security 保護的組織提供無與倫比的防禦，可對抗憑證收集和魚叉式網路釣魚攻擊。

MalwareGuard 是一款機器學習實用程式，可將二進位檔案視為可疑活動評分的輸入和輸出。在網路中看到的每個可攜式可執行檔 (PE) 均將由 MalwareGuard 進行分析。決策依據評分所制定，並為由 MalwareGuard 觸發的偵測指定一個名稱。

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、多流量及其他規避性攻擊。它可找出從未見過的入侵與惡意軟體，以阻止感染和入侵。

規避減緩

Email Security 支援受控實時模式功能，可防禦規避遠端物件請求的攻擊。MVX 引擎可偵測需要多個下載的惡意軟體，並傳回樣本二進位請求的遠端物件。受控實時模式可減少對多級下載、進階魚叉式網路釣魚攻擊及進階勒索軟體入侵的誤判。

攻擊者還試圖規避用於連結的技術。作為進階連結防禦的一部份，網絡釣魚網站的逃避緩解措施也在不斷發展。作為進階連結防禦的一部分，逃避緩解措施不斷得到增強。在執行潛在惡意物件時，可對另一個規避減緩，Guest Images 進行自訂以模擬「已使用」端點。確保 Guest Image 重新產生一個端點網域、網域使用者、Outlook 資料及瀏覽器記錄，可防止許多規避技術。

整合有助於提升警示處理效率

Email Security 分析每個電子郵件附件及連結，以準確地辨識現今的進階攻擊。來自 FireEye 整個資安生態系統的即時更新，結合屬於已知威脅者的警示，提供了決定關鍵警示優先順序，並採取行動及封鎖進階電子郵件攻擊的背景。在最小干擾及誤報的情況下辨識已知、未知和非惡意軟體威脅，故可將資源集中在真正的攻擊上，以降低運作費用。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。

能快速因應不斷演變的威脅態勢

透過 FireEye Dynamic Threat Intelligence (DTI) 雲端提供的即時威脅情報，Email Security 可輔助您的組織不斷適應您對電子郵件威脅的主動防禦。關於威脅和攻擊者的深度情報結合了敵意威脅、機器和受害者的多方情資：

- 提供及時且更廣泛的威脅可見度
- 偵測到的惡意軟體和惡意附件，識別其特定功能與特性
- 提供背景剖析，以決定優先順序並加速回應
- 決定可能的攻擊者身分和動機，並追蹤其在貴組織內的活動
- 重寫電子郵件中的所有內嵌連結可防止使用者遭受惡意連結
- 藉由突顯惡意連結，回溯辨識魚叉式網路釣魚攻擊，並防止存取網路釣魚網站

回應工作流程整合

Email Security 可與 FireEye Helix 和 FireEye Central Management 搭配並順暢運作。

- 作為安全操作平台的元件之一 — FireEye Helix — 提供整個基礎架構之間的能見度。FireEye Helix 可運用智慧型功能、端點相關性、自動化功能和調查提示功能來增強電子郵件和第三方警示。運用這些功能，FireEye Helix 能使看不見的威脅浮現，讓專家擁有充分資訊做出決策。
- Central Management 可建立 Email Security 警示和 Network Security 警示間的關聯，以更廣泛地瞭解攻擊，並設定封鎖規則，以防止攻擊進一步擴散。
- Central Management 支援角色型標記功能，藉此得知目前被鎖定的目標是誰。
- Central Management 可根據角色型準則，提供警示回應和補救的支援。

其他功能

以 YARA 為基礎的規則可幫助自訂化

Email Security 使安全分析人員能為組織量身指定並測試規則，用以分析內含鎖定其組織之威脅的電子郵件附件。

執行模擬防護

Email Security – 伺服器版具有封鎖商務電子郵件入侵 (BEC) 的功能，可防止重要員工免受欺騙。建立一個將入埠電子郵件顯示名稱與符合核准信封傳送者的核准清單相比的政策。

訊息佇列、警示、與隔離管理

Email Security – 伺服器版能高度掌控所掃描的電子郵件訊息。在主動防護模式中，訊息會在通過 MTA 佇列時進行追蹤和管理。可透過搜尋及驗證電子郵件屬性，確認已收到、已分析的和已送到下一個階段的訊息，還能透過直覺式儀表板監視長期發展趨勢。明確允許和封鎖清單，可針對電子郵件的處理流程提供自訂控制。可搜尋和選取一般的警示屬性。並且對於警示及隔離訊息可以採批次操作。

主動防護模式或純監控模式

Email Security 可透過分析電子郵件，並隔離潛在威脅，以達到主動防護的作用。對於純監控的部署，企業只需設定透明的 BCC 規則，將電子郵件複本傳送至 Email Security 進行分析。

彈性的部署選項

Email Security – 伺服器版提供各種部署選項，以符合組織的需求與預算考量：

- **Integrated Email Security：**使用整合式 MVX 服務，以保護位於單一站點之電子郵件入口安全的全方位獨立硬體裝置。FireEye Email Security 是易於管理的解決方案，可在 60 分鐘內部署完畢。而且無須規則、原則，或額外調整。
- **Distributed Email Security：**可延伸的裝置搭配，從中心位置共享的 MVX 服務，以確保組織內電子郵件入口的安全。
- **Email 智慧型節點：**可分析電子郵件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。

  整合硬體設備至 MVX 智慧型網格的負載平衡 (Bursting) 提供的附加功能，能在訊息存取量高峰期間偵測，並分析來自於電子郵件所產生的威脅。
- **FireEye Cloud MVX：**MVX 服務訂閱項，可分析電子郵件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。

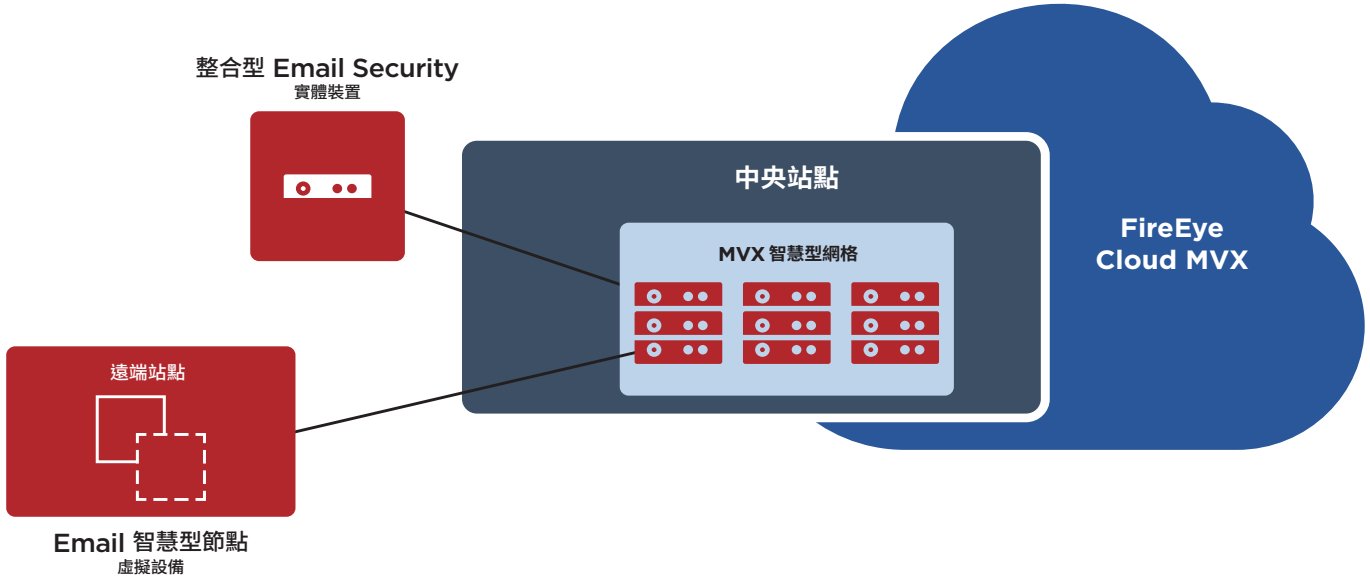

圖 2. Email Security 分散與負載平衡部署模式。

表 1. 技術規格。

	EX 3500	**EX 5500**	**EX 8500**
效能*	最高達每小時 700 個單一附件	最高達每小時 1,800 個單一附件	最高達每小時 2,650 個單一附件
網路介面連接埠	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (支援 10GigE 光纖、10GigE 銅線、1GigE 銅線)、 2x 1GigE BaseT
管理連接埠	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI 監控	內含	內含	內含
VGA 連接埠 (後面板)	內含	內含	內含
USB 連接埠 (後面板)	4x USB Type A (後端)	2x USB Type A (前端)、 2x USB Type A (後端)	2x USB Type A (前端)、 2x USB Type A (後端)
序列連接埠 (後面板)	115,200 bps、無同位檢查、8 位元、1 停止位元	115,200 bps、無同位檢查、8 位元、1 停止位元	115,200 bps、無同位檢查、8 位元、1 停止位元
儲存容量	4 個 2 TB 硬碟、RAID 10、3.5 吋、FRU	4 個 2 TB 硬碟、RAID 10、3.5 吋、FRU	4 個 2 TB 硬碟、RAID 10、3.5 吋、FRU
機殼	1RU、適合 19 吋機架	2RU、適合 19 吋機架	2RU、適合 19 吋機架
機箱尺寸 (寬 x 深 x 高)	17.2 x 25.6 x 1.7 吋 （437 x 650 x 43.2 公釐）	17.24 x 24.41 x 3.48 吋 （438 x 620 x 88.4 公釐）	17.24 x 24.41 x 3.48 吋 （438 x 620 x 88.4 公釐）
AC 電源供應器	備援 (1+1) 750 瓦、 100 - 240 VAC、9 – 4.5A、50-60 Hz、 IEC60320-C14 插座、FRU	備援 (1+1) 800 W、 100 - 240 VAC、9 – 4.5A、50-60 Hz、 IEC60320-C14 插座、FRU	備援 (1+1) 800 W、 100 - 240 VAC、9 – 4.5A、50-60 Hz、 IEC60320-C14 插座、FRU
DC 電源供應器	不適用	不適用	不適用
散熱最大功率	245 瓦特 (每小時 836 BTU)	456 瓦特 (每小時 1,556 BTU)	530 瓦特 (每小時 1,808 BTU)
平均故障間隔 (MTBF) (小時)	54,200 小時	57,401 小時	53,742 小時
裝置淨重／出貨重量，磅 (公斤)	30.0 磅 （13.6 公斤）／41.0 磅 （18.6 公斤）	44.1 磅 (20.0 公斤)/65.3 磅 (29.6 公斤)	44.4 磅 (20.2 公斤) ／65.6 磅 (29.8 公斤)
安全法規遵循	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
EMC 法規遵循	FCC 第 15 部分 ICES-003 類別 A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 和 V-3/2015	FCC 第 15 部分 ICES-003 類別 A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 和 V-3/2015	FCC 第 15 部分 ICES-003 類別 A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 和 V-3/2015
安全性認證	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
環保法規遵循	RoHS 指令 2011/65/EU；REACH； WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU；REACH； WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU；REACH； WEEE 指令 2012/19/EU
運作溫度	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)
作業相對濕度	10 ~ 95% @ 40°C，非冷凝	10 ~ 95% @ 40°C，非冷凝	10 ~ 95% @ 40°C，非冷凝
作業高度	3,000 公尺 / 9,842 英尺	3,000 公尺 / 9,842 英尺	3,000 公尺 / 9,842 英尺

* 所有效能值將依據系統組態和要處理的流量設定檔而有所不同。尺寸大小應用則是依據每小時單一附件數量。

表 2. FireEye MVX 智慧型網格規格。

	VX 5500	VX 12500
OS 支援	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
效能*	最高達每小時 480 個單一附件	最高達每小時 3,780 個單一附件
高可用性**	N+1	N+1
管理連接埠 (後面板)	1 個 10/100/1000 Mbps BASE-T 連接埠	1 個 10/100/1000 Mbps BASE-T 連接埠
叢集連接埠 (後面板)	3 個 10/100/1000 Mbps BASE-T 連接埠	1 個 10/100/1000 Mbps BASE-T 連接埠、 2 個 10 Gbps BASE-T 連接埠
IPMI 連接埠 (後面板)	內含	內含
前端 LCD 螢幕和鍵台	不適用	內含
VGA 連接埠	內含	內含
USB 連接埠 (後面板)	4 個 Type A USB 連接埠	2 個 Type A USB 連接埠
序列連接埠 (後面板)	115,200 bps、無同位檢查、8 位元、1 停止位元	115,200 bps、無同位檢查、8 位元、1 停止位元
磁碟機容量	2 個 2 TB 3.5 吋 SAS HDD、RAID 1、可熱交換、FRU	4 x 4TB、3.5 吋、SAS3 HDD、RAID 1、FRU
機殼	1RU、適合 19 吋機架	2RU、適合 19 吋機架
機箱尺寸 (寬 x 深 x 高)	17. 2x25.6x1.7 吋 (437 x 650 x 43.2 公釐)	17.2x33.5x3.5 吋 (437 x 851 x 89 公釐)
DC 電源供應器	不適用	不適用
AC 電源供應器	備援 (1+1) 750 W、100 - 240 VAC、 8-3.8 A、50-60 Hz、IEC60320-C14、插座、 可熱交換、FRU	備援 (1+1) 800 W：100-127 V、 9.8 A-7 A 1,000 W：220-240 V、7-5 A、50-60 Hz、 FRU IEC60320-C14 插座、FRU
消耗功率 (上限)	285 W	760 W
最大散熱量	每小時 972 BTU	每小時 2594 BTU
MTBF	54,200 小時	38,836 小時
裝置本身/出貨重量	33 磅 (15 公斤)/48 磅 (21.8 公斤)	46 磅 (21 公斤)/90 磅 (40.2 公斤)
安全性認證	FIPS 140-2 等級 1, CC NDPP v1.1	FIPS 140-2 等級 1, CC NDPP v1.1
安全性法規遵循	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* 所有效能值將依據系統配置和要處理的流量設定檔而有所不同。

**有適當的備援硬體配置。

表 3. FireEye Email Security 智慧型節點、虛擬感測器規格。

	EX 5500V
OS 支援	Microsoft Windows、Apple macOS X
效能*	最高達每小時 1,250 個單一附件
網路監視連接埠	2
網路管理連接埠	2
CPU 核心	8
記憶體	16 GB
磁碟機容量	384 GB
網路介面卡	VMXNet 3、vNIC
Hypervisor 支援	VMware ESXi 6.0 或更新版本

* 所有效能值將依據系統配置和要處理的流量設定檔而有所不同。

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 臺北市信義路四段 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、預防及回應網路攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。