FireEye

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

重點

- 提供全面的電子郵件安全，對抗魚叉式網路釣魚及其他進階、多階段和零時差攻擊
- 在訊息存取量高峰期間，負載平衡 (Bursting) 提供附加的偵測分析能力
- 支援分析 — 用來針對 Microsoft Windows 及 Apple Mac OS X 操作系統圖示
- 分析電子郵件，找尋隱藏在檔案中的威脅，包括有密碼保護及加密的附件和惡意 URLs
- 自動偵測並降低或完全阻擋憑證式網路釣魚
- 提供警示的背景剖悉，以決定優先順序並圍堵威脅
- 與多種 FireEye 技術完全整合
- 主動防護或純監控部屬模式
- 掌握訊息和警示內容，並加以追蹤和管理

圖 1. EX 3500，EX 5500 及 EX 8500。

概觀

電子郵件因其為最大量的資料入口，是網路攻擊中最脆弱的環節。 企業面臨越來越多來自垃圾郵件、病毒及進階或針對式的各種威脅。 大部分隨電子郵件而來的威脅，形式包括有：具攻擊性的附檔、惡意連結、及憑證授權釣魚詐騙。 雖然反垃圾郵件及防毒軟體可阻擋具有已知惡意附件、連結及內容的傳統群發電子郵件網路釣魚攻擊，但無法阻擋複雜且針對性的魚叉式網路釣魚攻擊，因為這些攻擊是設計用來繞過傳統的解決方案。 電子郵件仍是用來發動進階攻擊或遞送勒索軟體的主要方法，因其具有高度的目標性及客製化能力，可增加利用的機會。

FireEye Email Security 可協助組織將昂貴的入侵風險降至最低。 Email Security 內部裝置可在威脅進入您的環境前，準確偵測並立即遏止進階和目標性攻擊，包括魚叉式網路釣魚及勒索軟體。 Email Security 使用無特徵碼的 Multi-Vector Virtual Execution™ (MVX) 引擎，針對作業系統、應用程式及網頁瀏覽器的全面性交叉矩陣來分析電子郵件附件及 URLs。 其可在最小的干擾下辨識威脅，且幾乎不會有誤報情況。

FireEye 透過數百萬個感測器，蒐集詳盡的敵手威脅情報及第一手的入侵調查。 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。

Email Security 結合 FireEye Network Security 和 Endpoint Security，提供更廣的可見度，以協調即時防護，對抗多向量混合式攻擊。

有效的威脅偵測

Email Security 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，還有隱藏在電子郵件流量中的其他規避型攻擊，進而協助組織降低因網路入侵而須付出昂貴代價的風險。

Email Security 的核心是 MVX 引擎，能檢查可疑電子郵件流量，以找出規避傳統特徵碼式和原則式防禦機制的攻擊。 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、多流量及其他規避型攻擊。 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。

負載平衡 (Bursting) 為 FireEye MVX Smart Grid 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。

防禦電子郵件挾帶威脅

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，誘使他們點選 URL 或開啟附件。

Email Security 可提供即時威脅防護，以對抗能夠規避傳統防禦機制的魚叉式網路釣魚、勒索軟體及憑證式網路釣魚攻擊。 可偵測「相似但不同」網域（註冊近似域名）以降低憑證式網路釣魚。

若確認為攻擊，Email Security 將隔離惡意電子郵件，以便進一步分析或刪除。 可分析隱藏在以下情況中的惡意軟體：

- 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
- URL 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 URL 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 URLs
- 憑證式網路釣魚及註冊近似域名 URLs
- 未知 Microsoft Windows 與 Apple Mac OS 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。

高效警示回應

Email Security 分析每個附件及 URL，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，並採取行動及封鎖魚叉式網路釣魚電子郵件的背景。 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

Email Security 藉由使用深度的威脅和攻擊者情報，協助企業持續調整主動防禦，對抗來自電子郵件的威脅。 結合潛在的敵意威脅、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
- 藉由突顯惡意 URLs，回溯辨識魚叉式網路釣魚攻擊，並防止存取網路釣魚網站

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。 然後再運用無特徵碼的引爆室 MVX 引擎分析每個附件與 URL，以偵測威脅並即時阻止進階攻擊。

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 FireEye 進行 MVX 分析。

安全操作控制

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。

以 YARA 為基礎的規則可幫助自訂化

Email Security – 伺服器版支援自訂 YARA 規則，因此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。

訊息佇列、警示、與隔離管理

Email Security 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。

表 1. 技術規格

	EX 3500	EX 5500	EX 8500
效能*	最高達 700 個單一附件／小時	最高達 1,800 個單一附件／小時	最高達 2,650 個單一附件／小時
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
散熱最大功率瓦特 (Btu/h)	245 瓦特 (836 Btu/h)	456 瓦特 (1,556 Btu/h)	530 瓦特 (1,808 Btu/h)
平均故障間隔 (MTBF) (小時)	54,200	57,401	53,742
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

*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 1. 技術規格

	EX 3500	EX 5500	EX 8500
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 & 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 & 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 & 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。

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

DS.EX.ZH-TW-032018

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。 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網路安全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。