產品型錄

FireEye Email Security 雲端版

可辨識、分析和封鎖電子郵件攻擊的雲端平台

重點

- 提供全面的出埠和入埠電子郵件安全
- 使用單一廠商解決方案全面整合多種電子郵件安全
- 支援自定義 YARA 規則，以增強威脅偵測的效率
- 啟用 Office 365 自動修護以移除寄送到使用者收件匣後變為惡意的電子郵件
- 整合任何第三方電子郵件供應商
- 通過前線調查和對攻擊者的觀察提供有關攻擊和攻擊者的深入知識
- 符合 FedRAMP 安全需求

「電子郵件是所有協同作業環境的基礎，因此部署 FireEye Email Security ，我們能夠使用單一解決方案降低這一高度利用通路的風險。」

Nils Göldner
管理合作夥伴與雲端顧問
Blackboat GmbH

概觀

因電子郵件是最大量的資料入口，故是網路攻擊中最脆弱的環節。企業面臨越來越多來自垃圾郵件、惡意軟體及進階威脅的各種威脅。大多數隨電子郵件而來的進階威脅形式包括：連結至憑證式網路釣魚網站的連結、匯款請求詐騙及武器化的附檔。具有高度目標性及自訂性的電子郵件使網路罪犯成功入侵，使電子郵件成為網路犯罪的首選。

FireEye Email Security 可以透過單一電子郵件安全解決方案來減少成本並增加員工的生產力，使進階電子郵件攻擊所造成的昂貴入侵風險降至最低。經雲端部署後，FireEye Email Security 是功能完整的安全電子郵件閘道，可引領業界辨識、隔離及立即阻止連結、變臉郵件及附件型攻擊進入組織環境。利用 Office 365 (O365) 自動修護，可以擷取寄送到使用者收件匣後變為惡意的電子郵件。FireEye Email Security 也會掃瞄出埠的電子郵作流量，查看是否有進階威脅、垃圾郵件與病毒。

透過運用情報主導的背景資料與偵測外掛程式，可偵測真正的大數據、可擴充平台中的惡意連結。可檢查傳送者名稱和電子郵件地址的真確性，並調查內容是否存在變臉郵件詐騙技法，以阻止對進行 CEO 詐騙及其他無惡意軟體的攻擊。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。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，蒐集詳盡的攻擊者威脅情報。Email Security 利用對攻擊與惡意威脅發動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。

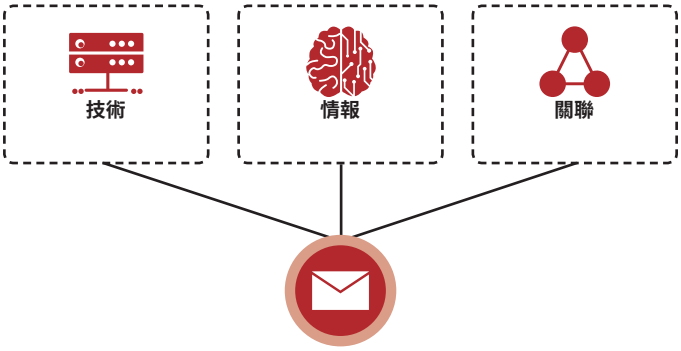

圖 1. 安全的電子郵件閘道。

透過與 FireEye Network 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

在個人資訊皆可隨時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，以對抗能夠規避傳統電子郵件安全性服務的憑證收集、變臉郵件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）：

- 各種附件類型，包括 EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4 以及 ZIP/RAR/TNEF 檔案
- 有密碼保護及加密的附件
- 嵌入在電子郵件、PDF 檔案和 Microsoft Office 文件中的連結
- 憑證式網路釣魚及註冊近似域名的連結
- 未知 OS、瀏覽器和應用程式的漏洞
- 魚叉式網路釣魚電子郵件內嵌的惡意程式碼

雖然勒索軟體的攻擊是從電子郵件開始，但需要回呼命令控制伺服器以加密資料。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和 MVX 引擎。這些技術使用尖端的機器學習和分析來識別逃避傳統特徵碼和基於政策的防禦的攻擊。

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與登入頁面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是 Skyfeed，它是一種專門建構的、全自動的惡意軟體情報收集系統。收集社交媒體帳號、部落格、論壇及威脅摘要以找出誤判。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。

電子郵件一開始可能會呈良性，以通過安全防禦。只有當郵件寄到收件者的收件匣後，才變成惡意郵件。在電子郵件寄出並變成惡意郵件後，Email Security－雲端版會回溯分析及發出警示。透過 O365 API，建立一個 O365 自動修護政策，可以使變成惡意的電子郵件自動從收件匣中被隔離出來。

MVX 引擎可藉由在安全的虛擬環境中，利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。

增強型 AVAS 防護

Email Security－ 雲端版可提供反垃圾郵件及防毒 (AVAS) 保護，偵測使用傳統特徵比對的常見攻擊以及變臉郵件技術。

變臉郵件攻擊，如：CEO 詐騙（通常被稱為商務電子郵件入侵），將繼續對企業財務造成重大影響。一部分是因為缺少如惡意附件或連結這類傳統威脅指標，因為這種攻擊並不附帶惡意軟體且依賴社交引擎技術。為對抗這些攻擊並保護客戶，FireEye 開發了專注於變臉郵件偵測和防禦的創新算法、系統及工具。

電子郵件攻擊的一個常見指標是傳送者網域的使用年期。在建立變臉郵件活動時，網路罪犯通常會在建立該網域的幾小時內，透過與其模擬的該人員或公司的網域相似的網域發出攻擊電子郵件。

Email Security 能夠使用內部開發的現有新網域 (NED) 和新觀察域 (NOD) 工具，準確判斷網域的使用年期和成熟度。判斷新建立的網域是否為可疑內容，並予以廣泛調查以查看是否存在其他攻擊指標，例如：註冊近似域名和傳送者顯示或使用者名稱詐騙。

網路罪犯只用變更顯示名稱或傳送者名稱，以使電子郵件看起來出自可信來源即可，而無需完成購買和注冊網域的程序。Email Security 透過使用易記名稱判斷顯示名稱及使用者名稱的真確性來防範此傳送者的詐騙。

出埠掃瞄

Email Security 偵測未知的進階威脅，包含透過出埠電子郵件訊息傳遞的惡意附件和網路釣魚連結。同時也會掃瞄出埠電子郵件流量的惡意軟體與垃圾郵件，以保護公司的網域不被列入黑名單。

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。

能快速因應不斷演變的威脅態勢

Email Security 可協助企業持續調整主動防禦，對抗來自電子郵件的威脅。Email Security 可建立其自有的威脅情報，而不是依賴落後的第三方摘要。特定於電子郵件的內部威脅情報（或智慧型 DNS）、資料收集功能、電子郵件安全專家及威脅分析，為增強型防垃圾郵件技術及變臉郵件偵測提供了潛在的基礎架構。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
- 藉由修改惡意連結，回溯辨識魚叉式網路釣魚攻擊，防止存取網路釣魚網站

企業可存取 Email Security 入口網站，以檢視即時警示、建立智慧型自訂規則及產生報告。智慧型自訂規則允許組織依據多重精細條件建立政策和規則。

回應工作流程整合

Email Security 與多項其他 FireEye 解決方案搭配運作，協助自動警示回應工作流程：

FireEye 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。

FireEye Helix 平台與 Email Security 流暢運作，且專門設計用以簡化、整合及自動進行資安操作。

部署簡單、跨企業防護

Email Security— 雲端版以雲端為基礎，不需要安裝硬體或軟體。最適合將組織的電子郵件基礎設施轉移至雲端。轉移工作完成後，企業即可省去採購、安裝和管理實體基礎架構的煩惱。

Email Security— 雲端版流暢整合雲端電子郵件系統，例如：Microsoft Office 365 與 Exchange Online Protection 和 G Suite。

為防範惡意電子郵件，組織只要將訊息轉至 Email Security，先對電子郵件進行垃圾郵件、已知惡意軟體和變臉郵件手法分析即可。然後再運用連結防禦技術和無特徵碼的引爆室 MVX 引擎分析每個附件與連結，以偵測威脅並即時阻止進階攻擊。

其他功能

以 YARA 為基礎的規則可幫助自訂化

Email Security 讓分析師可以使用自定義 YARA 規則來管理並強化偵測、阻止最新的威脅並識別進行中的活動。

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。企業只需要更新 MX 紀錄，訊息將自動發送至 FireEye。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。

授權和符合性認證

ISO 27001

Email Security— 雲端版符合 ISO 27001 資訊安全標準，可確保資料中心受到妥善管理。

FedRAMP

Email Security— 雲端版（具有 AVAS 防護）符合政府和公共教育機構所運作之雲端服務的 FedRAMP 安全要求。

SOC 2 Type 2

Email Security— 雲端版在資安及機密性上符合美國註冊會計師協會 (AICPA) 服務機構控制 (SOC 2) Type 2 認證。

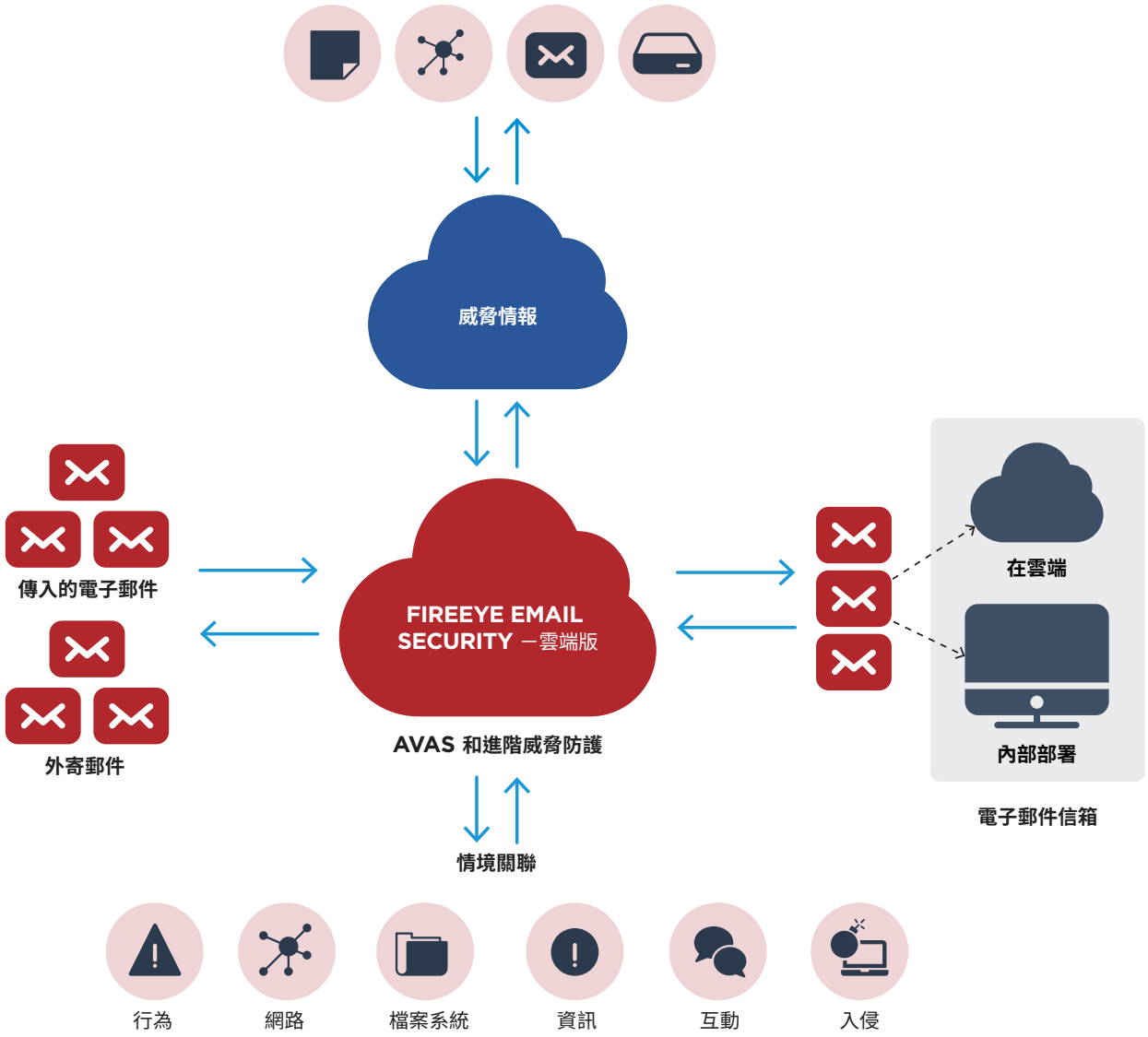

圖 2. FireEye Email Security—雲端版。

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。