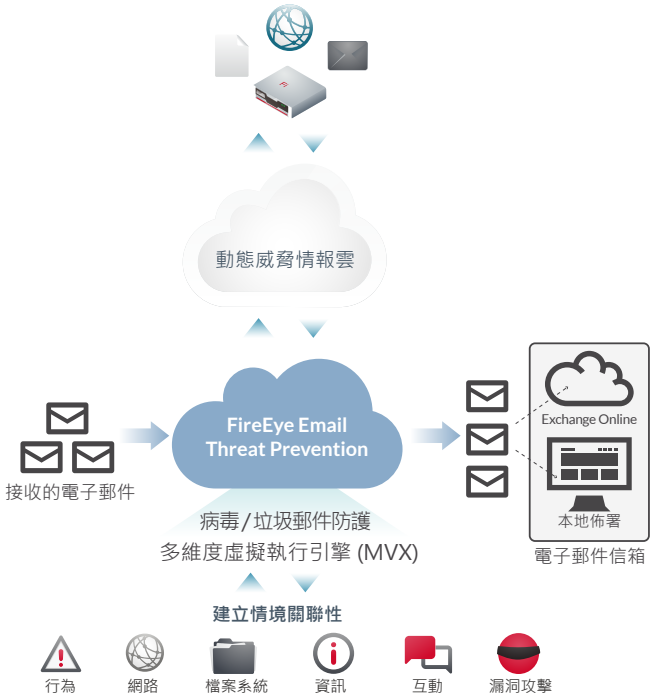
簡 介

FireEye Email Threat Prevention Cloud 為一結合病毒防護與垃圾郵件過濾，又能防禦現今進階電子郵件攻擊的SaaS服務。對希望全然擁抱雲端的企業而言，這個訂閱服務滿足了他們以完整雲端郵件安全產品來防止APT及傳統電子郵件威脅的需求。本服務運用FireEye Multi-vector Virtual Execution (MVX)架構，可與整個FireEye環境執行多媒介威脅的關聯分析。



電子郵件威脅防護雲

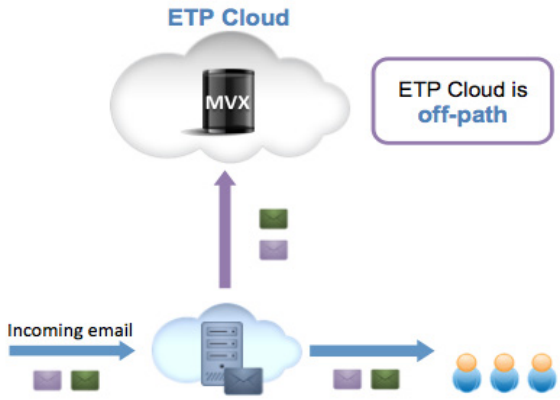
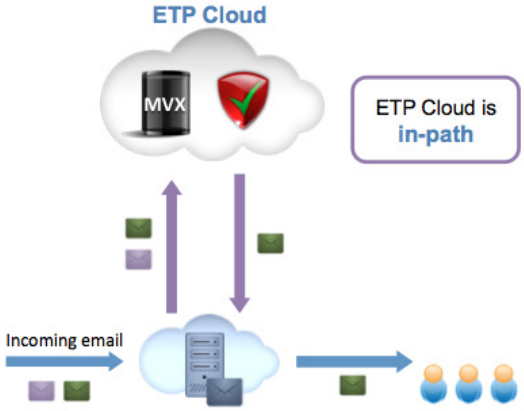
主要效益

- 完整電子郵件安全防護—抵禦進階魚叉網釣郵件攻擊及傳統電子郵件威脅。
- 時程效益—快速部署雲端解決方案，無需安裝軟、硬體。
- 透過與傳統安全及進階威脅防護技術的整合，實現營運效率。
- 藉由使用容易的管理入口網站讀取即時警示通知與通報。
- 低擁有成本—最適合將電子郵件基礎架構搬上雲端的企業組織。
- 榮獲 SOC 2 Type 1 for Security and Confidentiality 認證。

主要特色

- 部署快速—可設定接收端MTA的下一轉發(hop)指向FireEye雲，藉此部署為主動防護模式，或是以BCC規則設立成純監控模式。
- 即時隔離零時差郵件攻擊—在線（inline）模式中，企業可隔離魚叉式網路釣魚郵件、辨識收信者並封鎖使用惡意檔案類型（支援70種以上）開採零時差弱點的進階攻擊。
- 與NX Series整合可封鎖跨多種威脅媒介的混合式攻擊—與來自本地部署的網路威脅防護平台（NX Series）的情報建立關聯，藉此即時防禦混合式攻擊。
- 強化現有郵件控管基礎架構—能和電子郵件環境輕易整合，與現有郵件解決方案相輔相成。

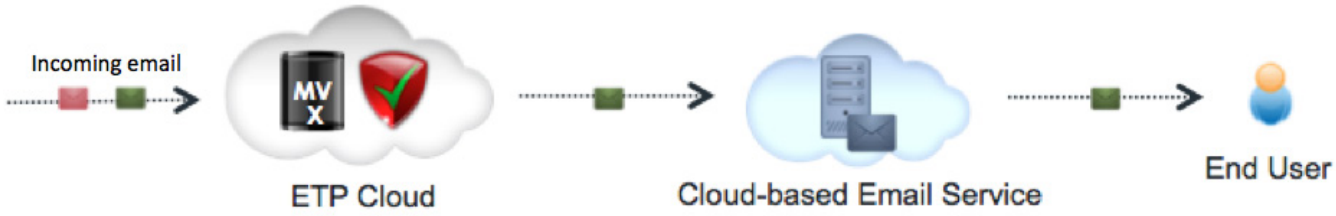
佈署模式

BCC 佈署模式	Inline 佈署模式
	
• 分析送往FireEye雲作MVS分析的郵件複本 • 只要設定透通的BCC規則即可啟動本模式 • 惡意電子郵件將可觸發警示送給管理員	• 分析電子郵件，並將有威脅的郵件隔離 • 設立接收端MTA的下一轉發指向FireEye雲即可啟動本模式。 • 可隔離惡意郵件作為留待管理員日後分析或刪除。

解決方案簡介

過去幾年隨著雲端運算模式的進展，愈來愈多企業與組織轉向雲端郵件方案。雲端郵件有多種效益，包括高可用性、降低基礎架構與IT管理成本。今天企業面臨數量空前的垃圾郵件、病毒和進階威脅，採用雲端郵件服務的組織必須確認他們部署的郵件安全系統足以因應變化多端的威脅樣貌。

FireEye Email Threat Prevention Cloud 提供完整的郵件防護來抵禦進階與傳統型態的郵件威脅。它能與現有本地部署或雲端郵件環境無縫整合，只需將傳入的郵件訊息送到Email Threat Prevention Cloud即可開始防禦郵件形式的攻擊，包括病毒、垃圾郵件和進階惡意程式等。傳入的電子郵件皆會經過垃圾郵件過濾及防毒引擎的分析與隔離，再送到MVX引擎進行進階威脅分析。



Email Threat Prevention Cloud **與雲端郵件服務整合**

目前相容性支援 *

雲端郵件服務	In-line 佈署模式	Bcc 佈署模式
Microsoft Office 365	支 援	支 援
Google Gmail	支 援	支 援

*上表僅列出現有實驗室測試與驗證過的產品整合FireEye Email Threat Prevention Cloud的支援情形，並未完整列出所有支援產品。

資料來源:

http://www.fireeye.com/products-and-solutions/cloud-email-security.html

-