端點安全

內部部署及遠端端點防護，對抗已知和未知的威脅與入侵

現今的專業攻擊者能繞過傳統端點防護平台 (EPP)，因為這些 EPP 只聚焦於單一元素來辨識威脅。FireEye Endpoint Security 透過整合 AV 與惡意軟體防護、威脅情報、行為分析以及 Endpoint Detection and Response (EDR) 功能，提供更多更強大的 EPP 選項，供您偵測和防護多種威脅特性。這麼做可提高資安自動化，同時啟用主動檢查及分析，藉此找出並消除可疑活動。其功能包括：

- Triage Viewer 與 Audit Viewer 可檢查和分析威脅指標
- Enterprise Security Search 可快速搜尋、尋找並判斷可疑活動與威脅的行動
- Data Acquisition 可進行深入端點檢查及分析
- Exploit Guard 可偵測和預防試圖入侵端點和應用程式的攻擊，並發出警示

使用 FireEye Endpoint Security，組織就可以主動偵測、預防、檢查、分析，並遏制任何端點上的已知和未知威脅。

偵測和預防隱藏端點入侵程序

若涉及到入侵偵測，傳統的端點保護 (EPP) 能力會因入侵不符合某個簡單的特徵碼或模式，而受到限制。FireEye Endpoint Security 則可透過名為 Exploit Guard 的功能提供靈活、資料導向的入侵行為情報。此功能還會藉由收集傳統端點解決方案遺漏的區域詳細資訊，來提供 Endpoint Detection and Response (EDR) 功能。它使用詳細的 FireEye 獨家情報，來關聯多項獨立活動，並藉此揭露入侵行為。

將威脅情報延伸至每個端點

威脅情報必須在攻擊點出現，才能有效進行防護。Endpoint Security 提供的 Endpoint Detection and Response (EDR) 功能，可將其他 FireEye 產品的威脅情報能力緊密延伸至端點。若 FireEye 產品在網路中的任何位置偵測到攻擊，端點便會自動更新，分析人員可使用 Triage 與 Audit Viewer 在每個端點快速檢查並收集資訊，檢查是否有 IOC。

取得強化的端點可見性

完整的端點可見性對於找出警示的根本原因，和對威脅進行深入分析，以判斷其威脅狀態而言至關重要。Endpoint Security 中的回顧快取功能，可讓您檢查和分析任一端點上當前和過去的警示，從而進行深入的鑑識調查並獲得最佳回應。

重點

- 部署為內部裝置和端點代理程式軟體，用於偵測和預防入侵，以及監控遠端及網路端點的活動，以便快速回應已知和未知威脅
- 提供新的 AV (僅偵測至 Q3) 功能，在單一端點代理程式中整合 Advanced Threat Intelligence 及端點行為分析
- 使用單一工作流程的通盤活動時間軸，協助進行詳細的端點調查，以識別和遏止 IOC
- 在極短時間內搜尋、偵測、識別並遏止上萬個端點 (已連線或未連線) 中的威脅
- 運用 Triage 與 Audit Viewer 從單一介面輕鬆評估所有端點活動，只需按一下按鍵即可找出並制止事件，然後加以分析和遏制，實現更及時的回應決策

獲得完整的端點涵蓋率

企業網路外的現場和遠端端點往往都更容易遭受攻擊。Endpoint Security 可涵蓋所有端點，不論使用何種網際網路連線類型，都能將情報推送至端點。如此一來，您無須額外的 VPN 連線，即可偵測和預防威脅，以及調查和遏止世界各地的端點。

遏止遭入侵端點，並防止橫向擴散

在端點發動的攻擊會透過您的網路快速傳播。在發現攻擊後，Endpoint Security 可讓您按一下按鍵便立即隔離遭入侵的裝置，進而阻止攻擊，並預防橫向擴散，或以其他方式造成更大的威脅。接著您便可對事件進行完整的鑑識調查工作，而不會有進一步感染的風險。

Endpoint Security 的運作方式

Endpoint Security 能在極短時間內搜尋，和調查上萬個端點中的已知和未知威脅。它會使用 FireEye Dynamic Threat Intelligence 來關聯由 FireEye 和網路安全性產品產生的警示與安全性記錄，進而驗證和判斷以下情形：

- 用來滲透端點的攻擊媒介
- 攻擊是否在特定端點上發生 (並持續)
- 是否有橫向擴散情形，並到達哪些端點
- 端點遭入侵的時間長度
- 智慧財產是否已被竊取
- 要遏止哪些端點和系統以防止進一步損害

Endpoint Security 需求

Endpoint Security 需要 1 GHz 或更高的 Pentium 相容處理器以及至少 300 MB 可用磁碟空間。相容於以下作業系統：

作業系統	最低系統記憶體 (RAM)
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1 或更新版本	1 GB (32 位元)、2 GB (64 位元)
Windows 2008 (包括 R2)	2 GB (64 位元)
Windows 7	1 GB (32 位元)、2 GB (64 位元)
Windows 2012 (包括 R2)	2 GB (64 位元)
Windows 8	1 GB (32 位元)、2 GB (64 位元)
Windows 8.1	1 GB (32 位元)、2 GB (64 位元)
Windows 10	1 GB (32 位元)、2 GB (64 位元)
Windows Server 2016	2 GB
Mac OS 10.9 或更新版本	1 GB

硬體裝置規格

Endpoint Security 的硬體部署選項，使用單一裝置進行通訊，且最多可支援 100,000 個端點的威脅情報。

規格	HX 4402/HX 4400D
儲存容量	4 個 1.8 TB 硬碟、RAID 10、2.5 吋、FRU
機殼	1RU、適合 19 吋機架
機箱尺寸 (寬 x 深 x 高)	17.2 x 27.8 x 1.7 吋 (437 x 706 x 43.2 公釐)
AC 電源供應器	備援 (1+1) 750 W、100 - 240 VAC
消耗功率上限 (W)	313 W
MTBF (h)	35,200 小時
裝置本身	32 磅 (15 公斤)

如需 FireEye 的詳細資訊，請造訪：
www.FireEye.com

關於 FIREEYE, INC.

FireEye 是一間情報主導的資安即服務領導公司。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 在全球超過 67 個國家/地區擁有超過 5,000 位客戶，其中包括富比士全球 2000 大公司中的 940 家以上公司。

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

www.FireEye.com