資料工作表

HX 系列

端點威脅防護平台可偵測、分析和解決端點上的安全事件

重點

- 整合網路和端點安全：找出端點上相符的活動，驗證和分析網路警告。
- 全面防護各處的端點：創新的 Agen Anywhere 技術可到達到企業網路外和 NAT 後端的端點。
- 運用強大的威脅情報偵測威脅：套用 Fire Eye 的威脅情報，找出 IT 環境中的先進威脅。
- 按一下即可壓制遭入侵的裝置：按一下滑鼠鍵即可隔離遭入侵的裝置，拒絕攻擊者存取系統，同時又能進行遠端調查。
- 快速調查各端點：幾分鐘內即可調查成千上萬的端點。

概觀

各大企業無不花費數百萬美金投資於尖端安全團隊和建立安全網路來防止威脅，並將攻擊者隔離在 IT 環境之外。即使做了這麼多的投資，堅決的攻擊者仍千方百計想要入侵企業，盜取智慧財產和財務資產。Endpoint Threat Prevention 平台讓安全團隊萬事俱足，更有信心地偵測、分析和解決威脅事件，並比使用傳統措施花更少的時間。

搜尋先進攻擊者和 APT

主機式偵測入侵指標 (IOC) 可辨識防毒軟體所忽略的威脅，包括先進攻擊者和進階持續威脅 (APT)。IOC 發現有裝置遭入侵時會立即通知使用者。

FireEye 偵測延伸到端點

將其他 FireEye® 威脅防護平台，如 FireEye 網路威脅防護平台 (NX 系列) 全面延伸至端點。端點代理程式將會自動更新入侵指標，對多數重大威脅提供整合式的「深度防禦」：尤其是那些正在發生的威脅。

驗證網路警告

確認網路上所看到的攻擊是否真的入侵端點。針對其他 FireEye 產品的每一項警告，找出所有受影響的端點。分析人員可檢視受影響的代理程式自動收集的事件時間表，進一步分析造成任何網路警告 (包括 SIEM 中的警告) 的原因。

Agent Anywhere 提供全面防護

運用 Agent Anywhere 技術，將防護範圍擴展到企業網路外的遠端端點，無論使用哪一類網路連線均適用。目前攻擊的指標會推送到不在 FireEye 產品保護之網路上的遠端端點。這樣讓分析員無需額外連接 VPN，即可調查和壓制全世界各地的端點。

壓制端點

立即採取行動隔離遭入侵的裝置，並拒絕攻擊者存取系統，同時仍允許遠端調查。

運作方式

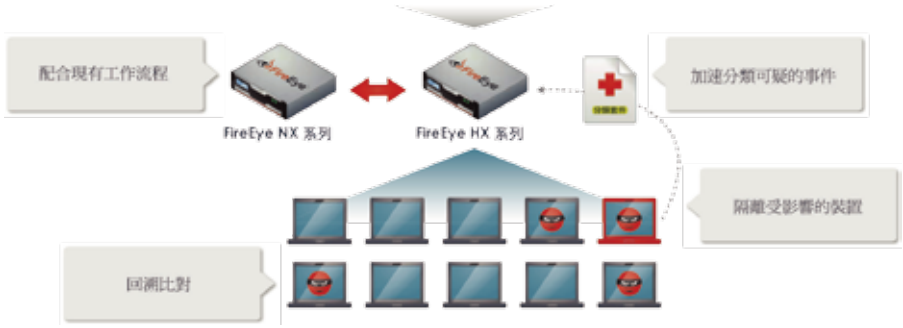
Endpoint Threat Prevention 平台讓安全作業團隊可將網路和端點活動相關聯。企業可自動調查 FireEye 威脅防護平台、記錄管理和網路安全產品所產生的警告，套用 FireEye 專屬情報，找出遭入侵的裝置和分析潛在危機。此外，企業還可快速將事件分流以瞭解入侵的細節。企業可進一步快速將事件分流以瞭解其細節，並用一鍵操作即可壓制遭入侵的端點。

自動調查網路裝置上的警告 - 從網路裝置上所產生的警告自動建立IOC。確認各端點的威脅警告以找出重大問題。

快速審查各端點 - 可在幾分鐘內調查成千上萬個端點。

Agent Anywhere - 可調查任和端點，即使端點不在網路中亦適用。

一目了然的介面 - 將前線分析員轉變成調查員，用簡單而直覺的介面快速解讀資料，並採取適當後續行動。



技術規格

	HX 4000 / HX 4000D
CPU	6核心、2.5 GHz
記憶體	16 Gb
硬碟	(4) 2 TB (RAID 10)
端點數量	多達 100.000 個端點
網路介面	(4) 10/100/1000 BASE-T 連接埠 (2 個主動)
尺寸 (寬 x 深 x 高)	17.2 x 27.5 x 1.7吋 (43.7 x 69.9 x 4.3)
電源供應器 /RAID	Dual、熱插拔
最大功率	700 W

附註：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。

台灣區授權代理商 | 創泓科技股份有限公司 | 台北市內湖區內湖路一段322號6樓 | 02-2658-3077 | 02-2658-3079 | www.uniforcetech.com.tw

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | APAC@FireEye.com | **www.FireEye.com**