FIREEYE™

產品型錄

網路鑑識

以高效能的封包擷取與調查分析，將網路攻擊的影響降至最低

企業需要及早發現事件並迅速完成調查以決定其範圍與影響，有效遏止威脅並重新保護本身的網路。

FireEye Network Forensics 解決方案搭配產業最快無丟失網路資料擷取，並配有集中化分析與視覺化的擷取解決方案。它能透過簡化調查且降低風險的單一工作台，加速網路鑑定流程。

FireEye Network Forensics 可以極快速度擷取完整封包，並編製索引，讓您更快速地辨識及解決資安事件。您可以透過 Network Forensics 偵測各種資安事件、改善回應品質，並且精準地量化每個事件的影響。

「調查分析設備」為 FireEye Network Forensics 解決方案的一部分，新增了集中化工作台（具有易於使用的分析介面），以顯示隱藏的威脅並加速資安事件回應。

分析人員還能檢視攻擊發生之前、發生期間及發生之後的特定網路封包和工作階段。由於能夠重建觸發惡意軟體下載或回呼的事件，並加以視覺化，使資安團隊可更有效及迅速地回應事件，並防止日後再次發生。他們可以將常用於在網路中橫向散佈攻擊的通訊協定予以解碼，以擴大查看攻擊者的活動。

此獨一無二，結合高性能封包擷取與深度分析可以快速協助辨識與監視一次攻擊的每個元素。

圖 1. FireEye Network Forensics 封包擷取與分析專用設備。

封包擷取重點

- **高效能：**以高達 20 Gbps 的記錄速度時間戳記，實現絕不間斷、毫無遺漏的封包擷取
- **高保真度：**使用時間戳記與連線屬性，為所有擷取的封包編製索引。以 JSON 格式匯出流量索引與連線中繼資料。流量索引可以轉換成 NetFlow v9、IPFIX 和 Silk Tools 資料格式
- **快速搜尋結果：**使用正在申請專利的索引編製架構，以超快速度搜尋並擷取目標連線與封包
- **豐富內容：**以網路為基礎深入查詢 GUI 可用於搜尋及檢查封包、連線和工作階段
- **廣泛的可視性：**工作階段解碼器支援，可用於檢視及搜尋網路、電子郵件、FTP、DNS、聊天、SSL 連線詳細資料和檔案附件
- **情報擷取：**對可擷取流量選擇性篩選，可消除直播影片、大型檔案傳輸、加密承載等
- **提升效率：**自動化程序運用專有演算法診斷潛在的異常網路行為，從而辨識出資料竊取活動

表 1. 可用封包擷取設備。

機型	擷取連接埠配置	管理連接埠	最大記錄速度	總內建儲存容量	尺寸	電源供應器/一般作業負載
PX 1004S-6	1 個 2GigE	1 個 1GbE	500 Mbps	6 TB	1U 17.2 英吋 (437 公釐) x 19.7 英吋 (500 公釐) x 1.7 英吋 (44 公釐) 18 磅 (8.2 公斤)	交流電、固定交流電壓 100 ~ 240 V @ 50 ~ 60 Hz、 IEC60320-C14 插座
PX 2060ESS-96	4 個 10GE SFP+	2 個 1GbE	2 Gbps	96 TB、可擴充的 SAS 連接儲存裝置	2U 17.24 英吋 (438 公釐) x 24.41 英吋 (620 公釐) x 3.48 英吋 (88.4 公釐) x 57.3 磅 (26.0 公斤)	備援 (1+1) 800 W、100 - 240 VAC 10.5 – 4.0A、50-60 Hz IEC60320-C14 插座、FRU
PX 2060ESS-120	4 個 10GE SFP+	2 個 1GbE	7.5 Gbps	120 TB、可擴充的 SAS 連接儲存裝置	2U 17.24 英吋 (438 公釐) x 24.41 英吋 (620 公釐) x 3.48 英吋 (88.4 公釐) x 57.3 磅 (26.0 公斤)	備援 (1+1) 800 W、100 - 240 VAC 10.5 – 4.0A、50-60 Hz IEC60320-C14 插座、FRU
PX 1004EXT-4G	4 x 1 Gbps、10/100/1000 BaseT、SFP	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	4 Gbps	未搭載內建儲存裝置。透過光纖 HBA 連線至外部 SAN 儲存裝置	1U 機架吊掛 1.7 英吋 (4.3 公分) x 17.2 英吋 (43.7 公分) x 25.6 英吋 (65.0 公分) x 46 磅 (20.9 公斤)	650 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍 230-280 W (額定)
PX 1040EXT-20G	4 x 1 Gbps	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	20 Gbps	未搭載內建儲存裝置。透過光纖 HBA 連線至外部 SAN 儲存裝置	1U 機架吊掛 1.7 英吋 (4.3 公分) x 17.2 英吋 (43.7 公分) x 25.6 英吋 (65.0 公分) x 46 磅 (20.9 公斤)	650 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍 230-280 W (額定)
PX 4000SX440	無	無	無	440TB Raw Storage 架	17.2 英吋 (437 公釐) x 27.5 英吋 (698 公釐) x 7 英吋 (178 公釐) 76 磅 (34 公斤)	1,280 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍

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。

FireEye「調查分析設備」支援數種單一節點和分散式架構設定，讓中繼資料 (metadata) 聚集、查詢、和分析能達到最高頻寬和效能。

調查分析重點

- **視覺化：**透過易於建立的自訂儀表板，檢視並分享網路中繼資料和活動
- **迅速回覆：**進行所有警示、擷取資料流和中繼資料的集中化應用層級關鍵字、regex 和萬用字元查詢
- **靈敏的介面：**立即為感興趣的工作階段進行個別或批次 PCAP 資料樞紐分析與下載
- **強大的搜尋功能：**透過 HTTP、SMTP、POP3、IMAP、SSL、TLS、DNS 和 FTP 等通訊協定提供的中繼資料索引加快搜尋
- **IOC 彙總：**在單個工作台中整合 FireEye Network Security、Email Security 和 Endpoint Security 產品警報以及所有網路中繼資料，並可立即使用「一鍵」樞紐來自警報的工作階段數據
- **可追溯的威脅主動追尋：**透過 FireEye Threat Intelligence、STIX 和 OpenIOC 摘要與自動化 IA 搜尋功能「即時返回」IOC 威脅分析。自動向網路中的 IOC 在數天或數週前發出警報
- **一鍵式檔案重建：**安全快速地重建可疑的檔案、網頁和電子郵件以供進一步分析

表 2. 可用調查分析設備。

機型	總內建儲存容量	尺寸	電源供應器/一般作業負載
IA 1000 DIR	6 TB	17.2 英吋 (437 公釐) x 19.7 英吋 (500 公釐) x 1.7 英吋 (44 公釐)	交流電、固定交流電壓 100 ~ 240 V @ 50 ~ 60 Hz、IEC60320-C14 插座
IA 2100-48	48 TB	17.2 英吋 (437 公釐) x 19.7 英吋 (500 公釐) x 1.7 英吋 (44 公釐)	備援 (1+1) 800 W、100 - 240 VAC 10.5 – 4.0A、50-60 Hz IEC60320-C14 插座、FRU

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。