

產品型錄

FireEye Helix

世界一流的資安作業偵測和情報



重點

- **偵測進階威脅:**整合超過 600 種 FireEye 和非 FireEye 安全工具, 覆蓋情境威脅情報和行為分析, 提供無與倫比的環境警覺。
- **將事件影響降至最低程度:**利用前線經驗取得的安全協調和自動化的工作流程來加速回應。
- **獲得所有威脅媒介和部署類型的可見性:**無論是內部部署或是雲端, 都需要利用新一代 SIEM 集中處理安全資料和架構以全面掌握威脅與漏洞。

簡介

網路安全正面臨前所未有的挑戰。幾乎每一天, 都有新的威脅暴露出公司的脆弱性, 迫使他們購買更多產品並僱用更多的人才。這些反應式方法導致複雜性不斷升級, 使得另一個漏洞攻擊者可以趁機利用。資安監控 — 無論大或小 — 都需要全面和基礎的方法。FireEye Helix 幫助組織建立資安監控的基礎。

FireEye Helix 是一種 SaaS 資安監控作業平台, 可讓組織控制從偵測到回應的任何事件。在任何 FireEye 解決方案中, FireEye Helix 均會整合您所有的資安工具並利用新一代 SIEM、協調性和威脅情報功能增強它們, 以擷取資安投資中未被開發的潛力。由資安專家設計, 對於資安專家, 它讓資安團隊能有效地執行主要功能, 例如: 警報管理、搜尋、分析、調查和報告。

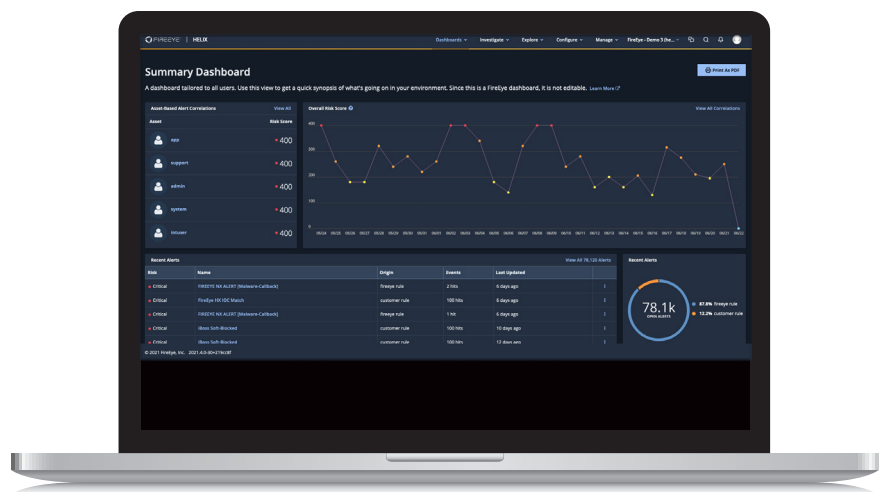


圖 1. 提供即時的环境警覺操作介面。

FireEye Helix 的功用



由多個工具資料透過交叉對比以偵測資安事件



透過情境威脅情報做出明智高效的決定



集中處理資安資料與基礎架構



威脅情報

偵測、強化、探索和瞭解最新情報威脅。



新一代 SIEM

利用先進的使用者行為分析技術增強威脅和漏洞偵測能力。



資安協調與自動化 (Security Orchestration and Automation, SOAR)

利用前線從業人員建立的預製操作手冊進行自動回應。



使用者與實體行為分析 (User and Entity Behavior Analytics, UEBA)

將警示與機器學習相關聯，以識別顯示存在內部威脅、橫向移動或最後階段攻擊的高風險的活動。



工作流程管理

透過自動化和手動工作流程，在調查程序中進行組織、指派、合作和採取行動步驟。



法規遵循報告

使用與自訂儀表板和工具可確實彙總、呈現和探索最重要的資訊。

如何取得 FireEye Helix 平台

購買任何 FireEye 以訂閱制 (subscription-based) 授權模式為基礎的解決方案時可購買 FireEye Helix。它適用於所有 FireEye 技術，並可集成您已安裝的非 FireEye 資安產品。隨著您組織的成長和改變，FireEye 解決方案可以在不中斷組織作業的情況下重新配置、增添或升級。

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 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE | taiwan@FireEye.com

©2020 FireEye, Inc. 保留一切權利。FireEye 為 FireEye, Inc. 的註冊商標。所有其他品牌、產品或服務名稱分屬各擁有人之商標或服務標記。
H-EXT-DS-US-EN-000050-07

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® 諮詢服務的單一平台。藉由此方法，FireEye 為那些正在努力準備、預防和應對網路攻擊的組織，消除資安機制的複雜性和重擔。

