FIREEYE™

產品型錄

FireEye 端點防禦 (Endpoint Security)

借助來自前線回應的知識來阻止攻擊

重點

- 防止大多數針對環境內的端點的網路攻擊
- 偵測並封鎖入侵，以減少入侵所帶來的影響
- 透過揭露威脅而非追逐警報，來改善生產力和效率
- 使用單一且所佔容量小的代理程式，減低對一般使用者的影響
- 透過可下載模組提供保護與功能
- 符合如 PCI-DSS 與 HIPAA 規範
- 部署至現場或在雲端內

傳統端點防禦對現代的威脅效用不大；它從不是設計來處理複雜或進階的持續威脅 (Advanced Persistent Threat, APT) 攻擊。為了保持端點安全，解決方案必須能快速察覺威脅，並以最有效的技術做出回應。

FireEye 端點防禦結合最頂級的傳統產品，用 FireEye 的技術、專業與情報加以強化，以對抗今日的網路攻擊。端點防禦依據深度防禦的模型，使用預設引擎和可下載模組的模組化架構，來保護、偵測與回應和管理代理程式。

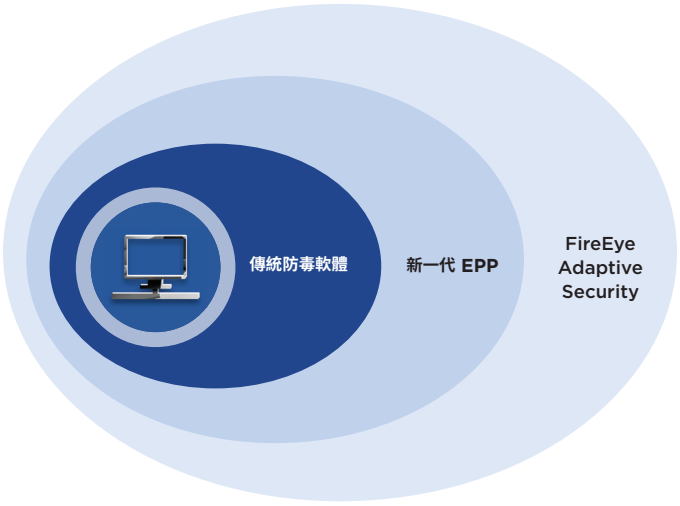
為要避免常見的惡意軟體，端點防禦使用特徵碼式端點保護平台 (Endpoint Protection Platform, EPP) 引擎。為找出尚未存在特徵碼的威脅，MalwareGuard 使用機器學習以獲取來自網路攻擊的第一線知識。為要處理進階威脅，將透過行為分析引擎啟用端點偵測與回應 (Endpoint Detection and Response, EDR) 功能。即時入侵指標 (Indicators of Compromise, IOC) 引擎依靠目前前線情報來幫助發現隱藏的威脅。如果要增添新的引擎和功能，您可以從 FireEye Market 下載模組。

就算有了最佳保護，仍無法避免入侵。為要確保能將企業受到的干擾降到最低，端點防禦提供工具以幫助：

- 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
- 找出用來滲透端點的詳細攻擊媒介
- 確定攻擊是否在特定端點上發生 (並持續發生) 以及其散佈地點
- 建立端點入侵的時間表與持續時間，並追蹤此事件
- 清楚找出要遏止哪些端點和系統以防止進一步損害

IT 是策略上的推手，可推動我們有效教育學生的能力。利用 FireEye 端點防禦可確保我們的 IT 資產可用性，高度運行且安全，這對實現我們的使命至關重要。

— **James D. Perry II**
首席資訊安全長，南加州大學



通常，管理階層認為病毒感染彷彿是世界末日。有了FireEye，我可以帶來實際證據，以展示我們有能力管理，並遏制的問題之相關本質。快速瞭解所有這些未知因素有助於減輕組織中每個人的壓力。

— **Michael Hennessy**，技術服務總監
Alpha Grainer Manufacturing, Inc

支援的作業系統與環境	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	OS X 10.9+
Linux	RedHat Enterprise Linux 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 & 7.6

部署選項：就地實體設備、就地虛擬設備、FireEye Cloud Service

主要功能

- 單一代理程式使用深度防禦來將配置最小化，並將偵測與封鎖最大化
- 單一整合的工作流程可在端點防禦內分析並回應威脅
- 完全整合的惡意軟體防護附有防毒 (Antivirus, AV) 捍衛能力、機器學習、行為分析、入侵指標 (IOC) 和端點能見度等功能
- 用 Triage Summary 與 Audit Viewer 來詳細的檢查和分析威脅

其他功能

- Enterprise Security Search 可快速尋找並揭露可疑活動和威脅
- Data Acquisition 可對指定的時間範圍進行詳細的深度端點檢查與分析
- 端對端可見度讓安全團隊可以快速搜尋、找出並辨別威脅等級
- 偵測和回應功能，以快速偵測、調查和遏制端點過快回應
- 易於瞭解的介面，可快速解譯並回應任何可疑的端點活動

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

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。