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

- **防止大多數針對端點的網路攻擊**
- **偵測並封鎖入侵以減少其影響**
- **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**
- **透過可下載模組取得新增的保護與功能**
- **符合如 PCI-DSS 與 HIPAA 規範**
- **在現場或在雲端內部署**

每一天都有全新的網路攻擊、全新的安全漏洞或全新的勒索軟體目標。資安團隊發現越來越難跟上針對使用者、公司資料和智慧財產權的威脅，並且他們並不總能帶來額外的幫助。資安回應人員被太多的工具所累，這些工具不能相互協作，產生的噪音多於有用的信號。現有系統並不總是對這些進階威脅提供充分的偵測和回應。

FireEye 端點防禦透過使用 FireEye 的技術、專業知識和情報來增強傳統安全產品的最佳部分，從而抵禦當今的網路攻擊。使用依據深度防禦的模型、此端點防禦單位預設引擎的模組化架構和可下載模組，來保護、偵測與回應和管理端點安全。

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前線知識。對於常見軟體和瀏覽器漏洞的攻擊，ExploitGuard 使用行為分析引擎來確定是否有人正在利用漏洞並阻止其執行。此外，FireEye 不斷創造防禦攻擊技術的偵測模組，並加速對新興威脅的回應。例如，Process Guard 流程防護的開發目的就在於阻止憑據洩露。

> 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

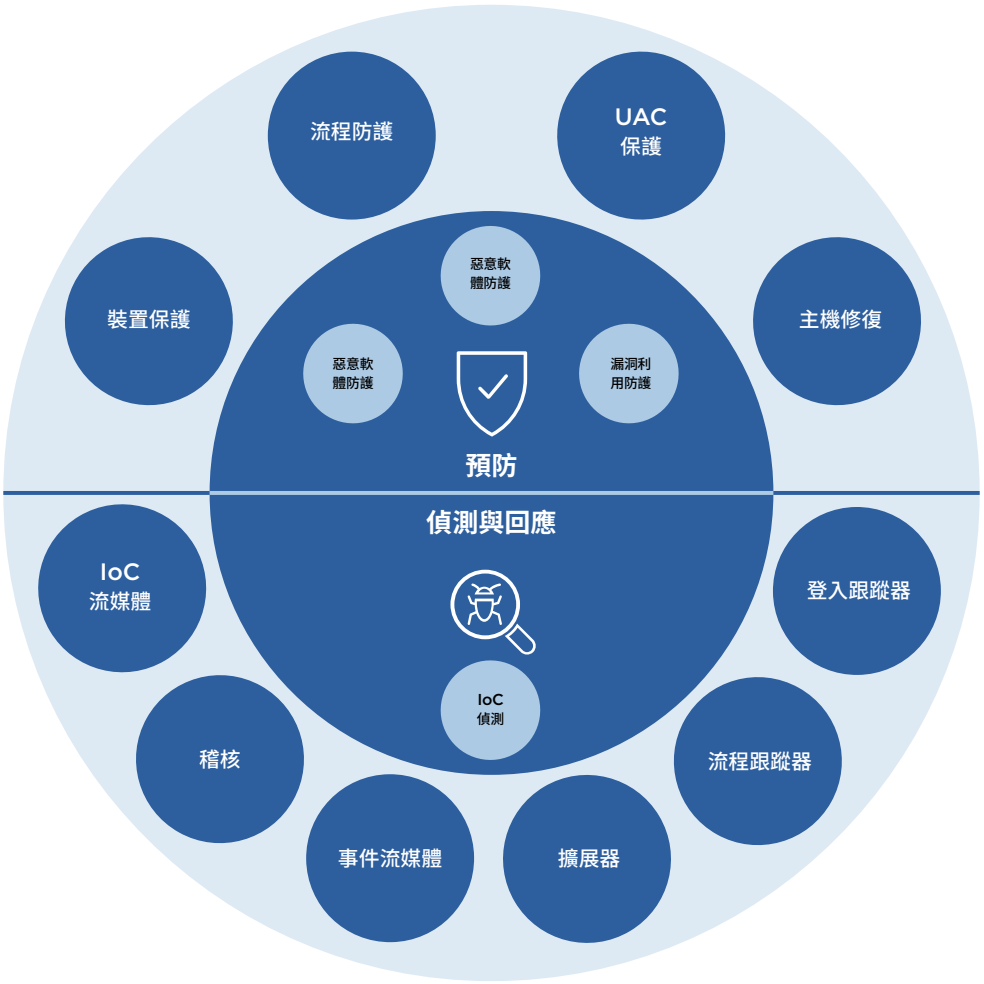
就算有了最佳保護，仍無法避免入侵。為確保做出能最大限度地減少業務中斷的實質性回應，Endpoint Security 端點威脅防禦包含端點偵測和回應（*Endpoint Detection and Response*, EDR）功能，這些功能依賴 Mandiant 的前線資安回應者的幫助下開發的即時入侵指標（*Indicators of Compromise*, IOC）。FireEye 工具還可以：

- 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

現代威脅不會止步於一個端點，因此在單個端點上進行補救並不能解決大多數的入侵。有效地全面修復通訊和指向可能隱藏威脅的所有設備，並即時關聯此資料。Endpoint Security 端點威脅防禦為 FireEye Helix XDR 中的一個元件，它能流暢地連結所有 FireEye 技術與服務，以偵測並回應所有最複雜的威脅。

圖 1.

FireEye Endpoint Security **端點防禦核心引擎（中心）以及可用模組（外圍）。**



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

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
- 整合的工作流程可在端點防禦內分析並回應威脅
- 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
- FireEye Helix XDR 元件可全面修復組織中的所有威脅

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

支援的作業系統與環境	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	10.9 – 10.15, 11
Linux	RHEL 6.8 – 6.10, 7.1 – 7.7, 8–8.2 CentOS 6.9 – 6.10, 7.1 – 7.7, 8 SUSE 11.3, 11.4, 12.2 – 12.5 15 Open SUSE 15.1, 15.2 Ubuntu 12.04, 14.04, 16.04, 18.04, 19.04, 20.04, 20.10 Amazon Linux AMI 2018.3, AM2 Oracle Linux 6.10, 7.6, 8 (1 **和** 2)

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

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
Taiwan@FireEye.com

關於 FireEye
FireEye 是一間情報主導的資安公司。作為客戶資安監控的無縫、可擴展的延伸，FireEye 提供單一平台，將創新的資安技術、國家級別的威脅情報和世界知名的 Mandiant® 諮詢融合在一起。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。