McAfee Endpoint Threat Protection

不可或缺的有效防護，且可與您的企業一同成長

威脅態勢會持續演進，這是無庸置疑的。您已意識到要從端點開始部署強而有力的防禦機制。但是，若沒有可隨時間變遷而加入新技術的能力，要取得您現在所需的防護會很困難，最終只會演變成建立複雜又各自不相干的安全性作業。McAfee® Endpoint Threat Protection 提供您現在所需的防護能力，還能使您具備能抵擋未來進階威脅的防禦需求。此產品提供整合式威脅防護、防火牆、Web、電子郵件及裝置控制防禦機制，它們可即時共同運作以分析並合作抵禦威脅，在威脅還未影響您的系統或使用者之前，便先加以封鎖並快速修正。

主要優點

- 使用多層協作式防護技術，可強化您的安全計劃。
- 擁有可視需求改變而輕鬆擴展防護能力的靈活性。
- 以集中式管理、零干擾使用者掃描提高生產力，且對系統資源的影響極小。

協作式端點架構

建立此架構時即考慮到整合性，使得 McAfee Endpoint Threat Protection 防禦機制具備更高水準的防護能力，可協同作業並共用所擁有的即時資料，以協調識別機制並阻止可疑檔案、網站及可能不需要的程式執行。

使用案例
網路上的惡意檔案下載

檔案雜湊從 Web 控制傳送至威脅防護，觸發 ODS。

在惡意檔案取得系統完整存取權之前，偵測到它們並加以封鎖。

獲得鑑識資料（來源 URL、檔案雜湊及其他資訊）。

事件資料與其他模組和 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體共用，且顯示在用戶端使用者介面中。

圖 1. McAfee Endpoint Threat Protection 防禦機制共同運作。

intel Security

當前與未來都適用的整合式解決方案

有了 McAfee Endpoint Threat Protection，您就能以連結的協作式架構與近乎即時且囊括多種防護技術的防護能力，取代原本未互相連結的端點產品部署。這不僅讓您獲得更具威力的威脅分析結果，還能讓收集的威脅鑑識資料與其他防禦機制共用，讓它們變得更聰明，並協助它們更快識別及封鎖在其他端點，或於其他進入點所遇到的威脅。

而多虧了這種作法，部署也能變得更靈活。您可以安裝目前所購買的產品隨附的所有軟體，並決定目前和日後要設定與啟用的功能。只要變更原則，您即可輕鬆啟用決定之後再使用的功能。

最後，由於架構的設計可包含其他技術，因此我們的架構可在您的需求改變時輕鬆擴展防護能力。如此可確保您隨時都能導入其他進階防護功能，以抵禦更多複雜威脅。

經濟實惠又不犧牲效能

McAfee Endpoint Threat Protection 提供搭配核心防護技術的可擴充架構，不會帶來複雜度或犧牲效能，為您和您的使用者帶來提高的生產力。舉例來說，由於透過 McAfee ePolicy Orchestrator 軟體的集中式管理，您的作業可更有效率地執行。此軟體提供的單一介面可部署、監控及管理整個環境的安全性原則。環境中有多種作業系統的客戶，將可藉由 Microsoft Windows、Apple Macintosh 及 Linux 系統的跨平台原則提高生產力。此外，由於 McAfee Endpoint Threat Protection 元件所使用的共同語言 (McAfee Data Exchange Layer)，您可最佳化技術之間的處理程序、加快回應威脅的時間，進而大幅縮短曝露時間以降低風險。

您的使用者也會因為零干擾使用者掃描、記憶體及 CPU 使用率而提高生產力，這些功能已經過最佳化可有效減少對系統的影響。直覺式使用者介面也是標準功能，可讓您與使用者更輕鬆使用，並快速取得已採取之動作的分析資料且瞭解背後原因。

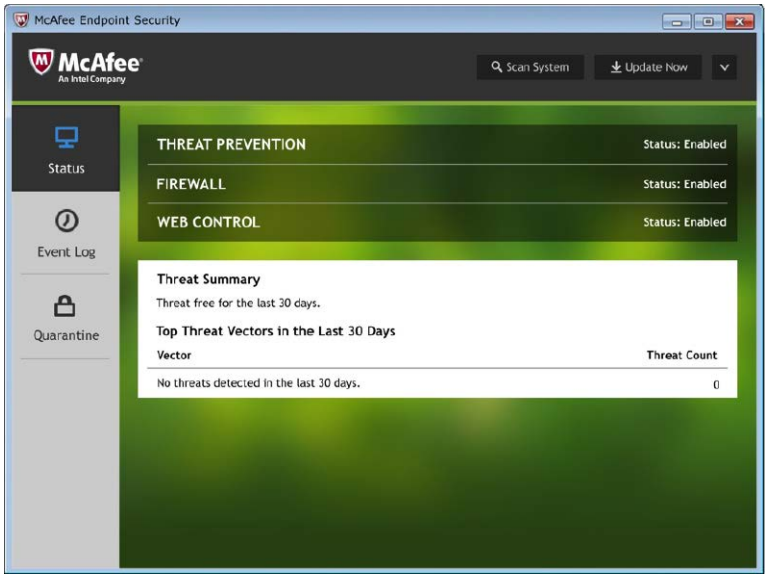

圖 2. 直覺式使用者介面讓管理員和使用者更輕鬆操作。

支援平台

- Windows：Windows 7、Windows To Go、Windows 8、Windows 8.1、Windows 10、Windows 10 November、Windows 10 Anniversary
- Mac OS X 10.5 版或以上版本
- Linux 32 和 64 位元平台：RHEL、SUSE、CentOS、OEL、Amazon Linux 及 Ubuntu 最新版本

伺服器：

- Windows Server (2003 SP2 或以上版本、2008 SP2 或以上版本、2012)、Windows Server 2016
- Windows Embedded (Standard 2009、Point of Service 1.1 SP3 或以上版本)
- Citrix Xen Guest
- Citrix XenApp 5.0 或以上版本

元件	優點	客戶利益	獨到之處
威脅防護	可運用多層防護機制快速尋找、凍結並修正惡意軟體的全方位防護。	• 透過啟發式常駐掃描技術阻止已知與未知惡意軟體。 • 運用跨 Windows、Mac 及 Linux 平台的防護機制，簡化原則與部署作業。 • 避免掃描信任的處理程序並優先處理可疑的處理程序，藉此提高效能。	多層防惡意軟體可與 Web 和防火牆防禦機制合作並通知這兩者，以進行更強大的分析，並聰明地套用規則以封鎖潛在威脅。
整合式防火牆	保護端點，防範殭屍網路、分散式阻絕服務 (DDoS) 攻擊、不受信任的執行檔、進階持續性威脅和有風險的 Web 連線。	• 強制執行原則以保護使用者與生產力。 • 封鎖不需要的入埠連線並控制出埠請求以保護頻寬。 • 通知使用者目前有信任的網路、執行檔、具風險的檔案或連線，讓他們做好準備。	應用程式與位置原則可在筆記型與桌上型電腦不使用企業網路的狀況下，提供進一步防護。
Web 控制	利用 Web 保護與端點篩選功能，確保瀏覽網路時安全無虞。	• 在使用者造訪惡意網站前即先警告使用者，藉此降低風險與保護符合性。 • 授權或封鎖危險或不適當的網站，以防止威脅並保護生產力。 • 在下載有危險的項目前即加以封鎖，藉此安全地阻止危險下載行為。	全面保護 Windows、Mac 及多種瀏覽器 (由 McAfee Global Threat Intelligence 發出通知)。
McAfee Data Exchange Layer	連結所有安全機制，以整合並簡化 Intel Security 與其他協力廠商產品之間的通訊作業。	• 整合可降低風險並縮短回應時間。 • 較低的營運開支與作業人員成本。 • 最佳化流程與實用建議。	• 在多個安全性產品間共用最重要的威脅資訊。 • 立即與其他所有端點共用感染源的威脅分析資料，以防止感染並更新防護機制。
McAfee ePO 管理	此單一介面適用於具高度延展性、靈活性且自動化的安全性原則管理作業，讓您找出安全性問題並做出回應。	• 可統一並簡化安全性工作流程，達到經實證的效率。 • 得以放心採取行動的更高可見性與彈性。 • 運用可自訂的原則強制執行快速部署和管理單一代理程式。 • 透過動態的自動化查詢、儀表板及回應機制，縮短從取得資料到做出回應的時間。	• 透過單一主控台更有效掌控、降低成本並更快進行營運安全管理作業。 • 經實證有效的介面已廣獲業界公認極為出色。 • 適用於廣大安全性生態系統的拖放式儀表板。 • 開放式平台有助於快速採用安全性創新技術。

深入瞭解 McAfee Endpoint Threat Protection 的優勢：**www.mcafee.com/tw/products/endpoint-threat-protection.aspx**。

McAfee. Part of Intel Security.
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.intelsecurity.com