McAfee Endpoint Security

落實專門的安全保護，以主動管理威脅並實行經實證的安全性控制機制

端點安全性：您最關注的是什麼？

在當今企業內，安全性可由一個或多個團隊所擁有。對企業組織而言，安全性是 IT 管理和安全作業等多種團隊共同負責的職務。不論您在企業內擔任何種職務，涉及端點保護平台時，您自然會因為自己關注的內容而更加在意多種不同組合的功能和結果。

您仰賴的端點解決方案應與您最迫切的需求保持一致。不論您做什麼工作，McAfee® Endpoint Security 皆能滿足您的特定關鍵需求，從防護及搜捕威脅到量身訂做的安全控制一應俱全。有了 McAfee® MVISION Insights 功能，即可在攻擊發生前排定明確的安全性優先順序。此解決方案可確保系統正常運作，以供使用者順暢使用，並探索更多實現自動化的機會，而且簡化複雜的工作流程。

確保運作時間與可見性

McAfee Endpoint Security 透過主動式防禦和修補工具，協助客戶回應及管理威脅防禦生命週期。自動復原修補可讓系統復原到健康狀態，不僅提高了使用者和管理員的工作效率，還省去了原本等待系統修補、執行復原以及為受感染電腦重新執行映像處理所花費的時間。端點及 McAfee® MVISION EDR 之間會共用全球威脅情報及即時的當地事件情報，以便收集威脅事件詳細資料、偵測和預防試圖規避偵測的威脅，並將這些威脅對應到 MITRE ATT&CK 架構，供未來調查使用。集中管理主控台提供各種本機、SaaS 或虛擬環境部署，可大幅簡化管理作業。MVISION Insights 針對攻擊傾向偏高的潛在優先威脅，提供獨到的觀察角度和控管機制，並能判斷組織的安全性狀態是否足以防範威脅。這可確保組織能有效防範重大威脅，並在攻擊者發動攻擊前先發制人。

主要優點

- **針對進階威脅提供進階防禦：**機器學習、憑證竊取防禦及復原修補等技術，皆可補足 Windows 桌面型電腦和伺服器系統的基本安全性功能。
- **不增加複雜度：**透過單一原則和主控台管理 McAfee 技術、Windows Defender 防毒軟體原則、Defender Exploit Guard 以及 Windows 防火牆設定。
- **MVISION Insights：**提供現今領先業界的安全性情報解決方案，將情報化為實際行動，針對威脅程度高 (根據是否鎖定您的產業與地理位置) 的潛在持續惡意活動立即做出回應。MVISION Insights 會預測哪些端點缺乏對惡意活動的防護能力，並提供能有效提升偵測效果的引導式指南。這是唯一能同時排定行動優先順序、預測動向及規劃行動的端點安全解決方案。

與我們聯絡

資料工作表

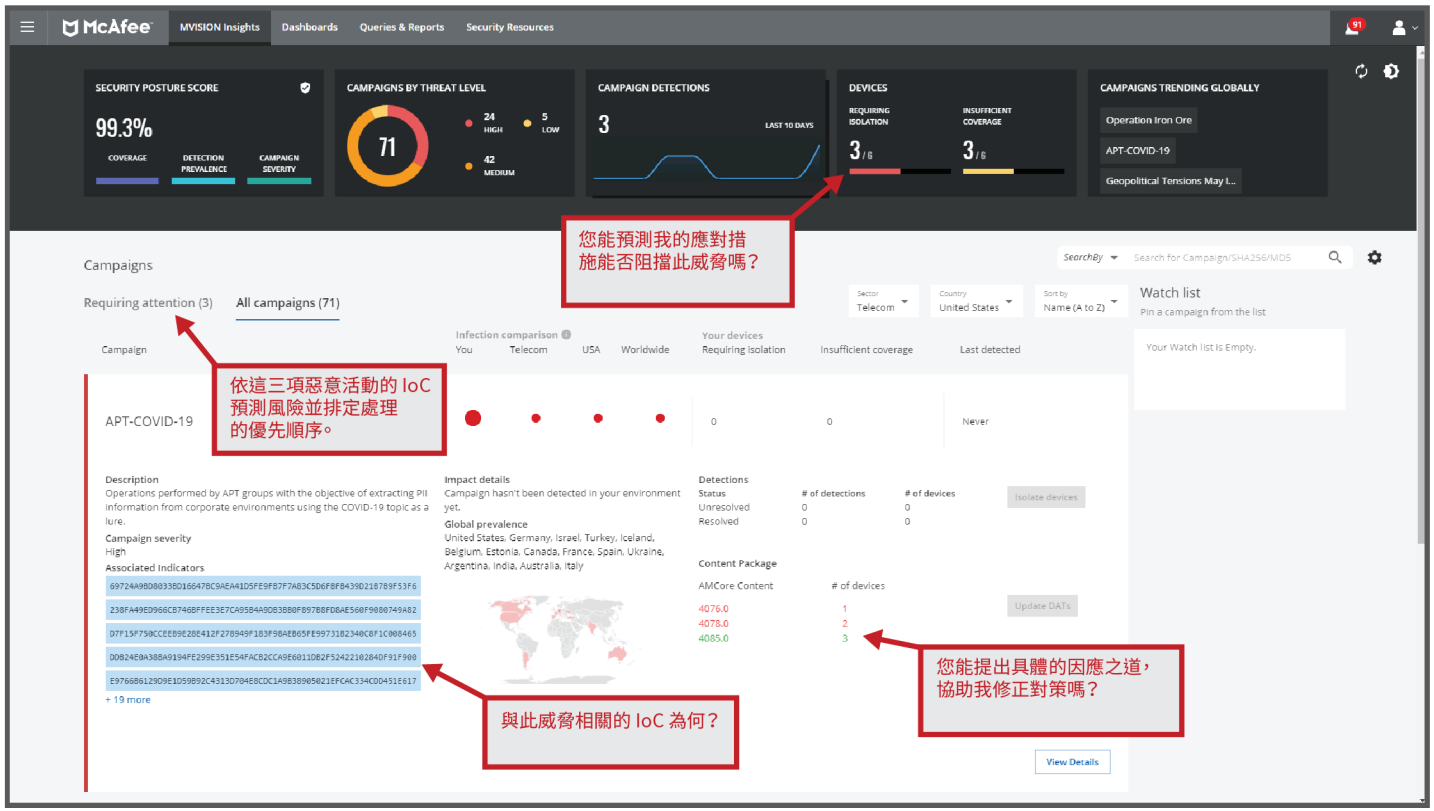

圖 1. MVISION Insights 儀表板。(MVISION Insights 需有 McAfee Endpoint Security 遙測 (選擇加入) 才能正確運作。)

在 MVISION Insights 的輔助下，組織能主動掌握可能發動攻擊的潛在威脅，依產業和地區取得警示和通知，了解應優先處理哪些事件。此外，MVISION Insights 可根據所在地的情報評估安全性狀態，確認當下的防禦機制能否防範此威脅。MVISION Insights 也會找出易受威脅的端點，並提供更新項目的相關指示。如此一來，您就能主動防禦可能會發動攻擊的敵人，先發制人。

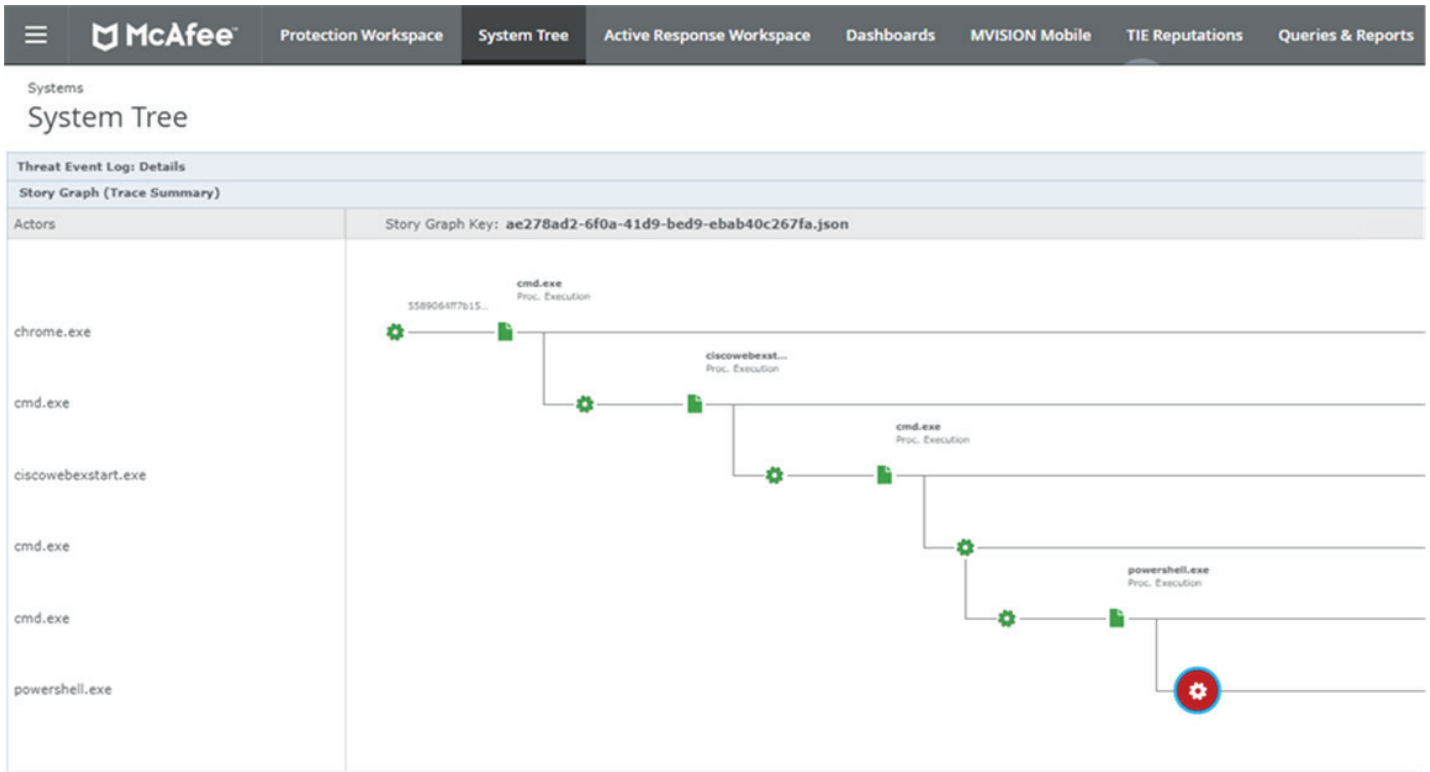

圖 2. Story Graph

McAfee Endpoint Security 使用單一軟體代理程式來收集多層業務的威脅情報，進而消除多點產品產生的冗餘。系統會採用整合式安全措施，去除手動威脅關聯，將需進一步調查的威脅詳細資料自動提交給事件回應程式。Story Graph 以簡單易讀的格式展示威脅事件資料，將威脅詳細資料視覺化，使管理員能輕鬆分析及調查惡意行為的來源。

整合式進階威脅防禦自動處理及快速回應

其他進階威脅防禦功能 (如動態應用程式遏止技術 (DAC)) 已與 McAfee Endpoint Security 架構完成整合，可協助組織抵禦最新進階威脅。[1]例如，DAC 將分析灰色軟體等新興惡意軟體並採取相應行動，阻止其執行動作以防感染。

另一項針對進階威脅的技術是 Real Protect，這一技術結合機器學習的行為分類，可協助偵測零時差惡意軟體及加強偵測能力。免簽章分類會在雲端執行，在提供近乎即時偵測功能的同時，維持較小的用戶端使用量。可化為實際行動的情報將一併傳遞給系統，系統能使用這些情報建立攻擊指標 (IoA) 及入侵指標 (IoC)。這對於水平擴散偵測、零號受害者探索、威脅執行者屬性、鑑識調查及修補而言尤其有用。藉助靜態和執行階段功能，Real Protect 還能透過自動更新行為分類來識別各種行為，並可增加規則以識別未來的類似攻擊，進而加速進一步的分析作業。

最後，為即時預防感染並減少 IT 安全管理員所需花費的時間，用戶端會將端點修復至已知的最新良好狀態。

智慧端點保護功能即時為您展示攻擊者

智慧與結果息息相關。McAfee Endpoint Security 即時與其框架中的多項端點防禦技術共享觀察，以協作及加速可疑行為的識別，促進更佳的防禦協調作業，並提供更好的保護來抵禦鎖定式攻擊及零時差威脅。系統將追蹤檔案雜湊、來源 URL、AMSI 及 PowerShell 事件等情報，並將這些情報與其他防禦以及用戶端和管理介面共用，進而協助使用者瞭解攻擊並為管理員提供可化為實際行動的威脅鑑識機制。

此外，McAfee® Threat Intelligence Exchange 技術將賦權給適應性防禦功能，以便與其他 McAfee 解決方案協作，包括閘道、沙箱以及我們的安全資訊和事件管理 (SIEM) 解決方案。收集和分散本機、社群和全球安全情報，可將攻擊、探索和遏止的時間從數週或數月縮短到數秒。

透過與 McAfee® Global Threat Intelligence (McAfee® GTI) 相結合，McAfee Endpoint Security 架構可利用雲端來監控及全面掌握所有媒介 (檔案、Web、郵件及網路) 中層出不窮的新型和新興威脅。本機和全球威脅情報有助於強化既有的端點使用量和管理系統，即時防禦未知與目標式惡意軟體。抵禦可疑應用程式及處理程序的自動化動作，可在通知其他防護與全球社群的同時快速向上呈報層出不窮的新型攻擊形式。

使用 DAC 和 Real Protect 的客戶將深入瞭解更進階的威脅及其執行的動作。例如，DAC 提供有關遏止應用程式及其嘗試取得之存取類型 (例如登錄或記憶體) 的資訊。

如果組織是透過關注端點程序所收集的威脅情報，搜捕惡意軟體和配備事件回應程式，Real Protect 將能深入分析其判斷為惡意的行為，並將威脅分類。若想深入調查檔案型惡意軟體如何透過封裝、加密或誤用合法應用程式等技術來規避偵測，這些深入分析尤其有用。

強大有效的效能助您及時回應

如果智慧型防禦的掃描較慢、安裝時間較長或者較難管理，則智慧型防禦幾乎沒有價值。McAfee Endpoint Security 透過通用的服務層及我們全新的反惡意程式碼核心引擎，可減少使用者系統所需的資源數量和功能，進而保護使用者的工作不受影響。端點掃描僅在裝置處於閒置狀態時執行並在裝置重新啟動或關閉時直接回復作業，因此不會影響使用者的日常工作。

適應性掃描程序還會透過瞭解受信任的程序和來源來協助降低 CPU 需求，以便集中資源處理可疑或未知來源的程式。McAfee Endpoint Security 採用 McAfee GTI 的整合式防火牆，可保護端點免受殭屍網路、分散式阻斷服務 (DDoS)、持續性進階威脅，以及富有風險的 Web 連線攻擊。

降低複雜性及提高永續性以緩解壓力

安全產品的數量快速增加，不僅功能重複，其管理主控台也各自為政，導致許多組織很難一窺潛在攻擊的全貌。McAfee Endpoint Security 具備可擴充的開放性架構，以此為集中管理當前及未來端點解決方案的基礎，藉此提供強大的長期保護。此一架構運用 Data Exchange Layer，實現了與現有安全投資的跨技術協作。整合式架構可與其他 McAfee 產品無縫整合，不僅顯著減少安全上的漏洞、技術孤島以及冗餘等情形，還能降低運作成本及管理複雜性，大幅提升工作效率。

McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體提供單一介面供您監控、部署和管理端點，可顯著降低複雜性。可自訂的檢視及可操作的工作流程均使用容易理解的語言，清楚呈現，並提供各種專門隔離系統、終止惡意程序或阻止資料外流的工具，快速存取安全性狀態、定位感染程式，並減緩威脅帶來的影響。此外，還提供了單一位置來管理每個端點、其他 McAfee 服務以及超過 130 個協力廠商安全解決方案。

資料工作表

功能	採用理由
主動威脅偵測與回應 (MVISION Insights)	▪ 根據所屬產業和地區預測及主動偵測潛在威脅。 ▪ 針對潛在威脅，在本機上評估安全性狀態，並提供有助於改善現狀的修正指示。 ▪ 在攻擊發生前率先採取保護措施，領先敵人一步。
Real Protect	▪ 機器學習行為分類機制可近乎第一時間偵測零時差威脅，提供可化為實際行動的威脅情報。 ▪ 這能自動更新行為分類，以利識別各種行為，並且增加規則來識別日後遭逢的攻擊。
抵禦鎖定式攻擊的端點保護	▪ 端點保護能縮短從遭遇攻擊到遏止之間的時間，從數日縮短到幾毫秒。 ▪ McAfee Threat Intelligence Exchange 從多個來源收集情報，允許安全組件之間就層出不窮的多階段進階攻擊即時通訊。 ▪ AMSI 及 PowerShell 事件記錄功能可挖掘並協助抵禦無檔案型攻擊和指令碼型攻擊。
智慧型適應性掃描	▪ 略過掃描信任的處理程序，並優先處理可疑的處理程序和應用程式，藉此提高效能和生產力。 ▪ 適應性行為掃描程序可監控及鎖定可疑活動，並向上呈報為保證狀態。
復原修補	▪ 復原修補會自動還原惡意軟體所做的變更，並將系統回復至已知的最新健康狀態，確保使用者能保持較高的工作效率。
主動式 Web 安全性	▪ 主動式 Web 安全性利用 Web 保護與端點篩選功能，確保網路瀏覽安全。
動態應用程式遏制功能	▪ DAC 能抵禦勒索軟體和灰色軟體，並保護「零號受害者」。[2]
封鎖惡意網路攻擊	▪ 整合式防火牆可使用 McAfee GTI 提供的信用評價分數來保護端點，抵禦殭屍網路、DDoS、進階持續威脅及可疑 Web 連線。 ▪ 防火牆保護功能在系統啟動時僅允許出埠流量，藉此在端點不在企業網路內時加以保護。
Story Graph	▪ 管理員可在短時間內得知感染之處、發生原因及曝險時間長度，進而瞭解威脅並迅速應變。
多種部署選擇實現集中式管理 (McAfee ePO 平台)	▪ 實際集中式管理功能可提供全面掌握能力、簡化複雜作業、提高 IT 生產力、整合安全產品及降低成本。
可擴充的開放型端點安全架構	▪ 整合式架構允許端點防護產品相互協作及通訊，強化防禦功效。 ▪ 如此一來，透過消除冗餘及最佳化程序，即可減少作業成本。 ▪ 此外，還能與其他 McAfee 及協力廠商產品無縫整合，減少防護漏洞。

表 1. 關鍵功能及您需要這些功能的原因。

輕鬆抵禦網路威脅

McAfee Endpoint Security 為現今的資安從業人員提供了戰勝攻擊者的優勢：情報、協作防禦機制及簡化複雜環境的架構。威脅偵測機制強大有效，效率卓絕，通過協力廠商測試驗證，在此機制的輔助下，組織將能保護其使用者，確保在安心工作的同時也能提高工作效率。

端點安全的市場領導品牌 McAfee 提供全方位的解決方案，集功能強大的保護功能與高效率的管理機制於一體，使安全團隊能在動用更少資源的情況下更快解決威脅，大幅提升防禦能力。

遷移從此輕鬆不已

如果已在環境中使用最新版 McAfee ePO 軟體、McAfee VirusScan® Enterprise 及 McAfee® Agent，可利用我們的自動遷移工具，將您現有的原則遷移至 McAfee Endpoint Security，最多 20 分鐘即可完成。[3]

McAfee Endpoint Security 還提供以下優勢：

- 零干擾使用者掃描，確保更優異的使用者工作效率
- 將更強大的鑑識資料同步至 Story Graph，讓您輕鬆掌握情報及簡化調查，進而強化防禦原則
- 復原修補功能可自動回復惡意軟體所做的變更，並將系統維持在健康狀態
- MVISION Insights 能主動深入分析需優先處理的潛在威脅，並提供相關指示，協助您調整威脅對策
- 無需管理過多的代理程式，同時避免不必要的掃描，減少手動輸入
- 協作型防禦機制可共同採取行動，對抗多種進階威脅
- 新一代架構能與其他進階威脅以及端點偵測與回應 (EDR) 解決方案相容

深入了解

若要深入了解 McAfee Endpoint Security，請按下此處造訪我們。

若要進一步了解 McAfee Endpoint Security 如何實作 McAfee 產品組合，請造訪：

- MVISION Endpoint
- MVISION 產品系列
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. 大多數 McAfee 端點套件均已隨附。請洽詢銷售代表以取得詳細資料。
2. 同上。
3. 遷移時間需視您現有的原則和環境而定。

台灣
台北市信義區忠孝東路五段 68 號 29 樓，11065
www.mcafee.com/tw

2020 年 7 月