McAfee Enterprise Security Manager

探索、回應、遵循。

有效的安全性就從即時監看所有系統、網路、資料庫與應用程式上的所有活動開始。McAfee® Enterprise Security Manager 可讓您的企業即時獲知實際現況，並擁有足夠的速度與規模能夠識別重大威脅並敏捷因應，而且能夠持續監控符合性。McAfee Global Threat Intelligence™ (McAfee GTI™) 與 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體整合，可協助您在幾分鐘內偵測、關聯及補救整個 IT 基礎架構內的威脅。

主要優點

- 在幾分鐘 (而不是數小時) 內找出可行的資訊
- 在大範圍的資訊來源間收集大量資料
- 即時的威脅與風險資料整合，以及事件關聯
- 可立即存取數年的事件與流程資料
- 支援對 240 餘項法規進行監視與報告
- 整合式工具可用以改善安全性工作流程
- 彈性的混合式傳送選項，包含實體裝置與虛擬裝置
- 高可用性選項

McAfee Enterprise Security Manager 整合了企業現況感知所需的安全情報與資訊管理，而革新了安全資訊與事件管理 (SIEM) 功能。我們將真實現況 (威脅資料、信用評價資料與弱點的相關消息) 的即時資訊，與您企業內的系統、資料和活動的即時資訊相連結。

IT 最終將可存取完整而關聯所需的內容以迅速做出以風險爲考量的決策，進而投入相關資源以妥善因應變動的威脅態勢。

有鑑於符合性的工作負荷持續增長，我們因而將稽核與符合性活動整合到單一平台內，以盡可能減少稽核的工作量與成本。我們透過在 Unified Compliance Framework 內統籌支援 240 餘項法規，讓符合性更容易達成、維護及記錄。

在幾分鐘內找出關鍵事證，而無需延宕數小時

我們具有高度調整性的資料庫裝置可依照企業所需的速度收集及處理數年來多達幾十億筆的記錄事件，並使其與其他資料流相關聯。McAfee Enterprise Security Manager 可儲存數十億個事件與流程，讓所有的資訊皆可立即用於特定查詢、鑑識、規則驗證與符合性工作。

在調查潛伏式攻擊、搜尋進階持續性威脅的跡象、或試圖補救失敗的符合性稽核時，能否快速存取長期儲存的事件資料將是關鍵 - 這些作業全都有賴於詳查歷史資料，以及完整存取每項特定事件的所有詳細資料。

大量資料收集

一個 McAfee 接收器每秒最多可收集 18,000 個事件。McAfee Enterprise Security Manager 本身可支援多個分散的接收器，且每秒能夠處理數十萬個未經壓縮或彙總的事件。若經過彙總，則單一裝置每秒將可處理數千萬個事件，足以因應最大型企業網路的需求。

進階風險與威脅偵測

無論是網路流量、使用者活動還是應用程式的使用，任何異於正常型態的活動，都可能意味著潛在的威脅，或是您的網路面臨風險。McAfee Enterprise Security Manager 可對所有收集自企業的資訊即時計算基準活動，並且在潛在威脅發生之前對您發出警示，同時分析該資料的型態是否潛藏更大的威脅。

內容感知

有可用的內容時 (來自弱點掃描程式、身分識別與驗證管理系統、隱私權解決方案或其他支援的系統)，每個事件中都會加入對應的內容，以進一步瞭解網路和安全性事件對實際商業程序與原則有何關聯。

McAfee Enterprise Security Manager 的調整性與效能可讓您從更多來源收集更多資訊 (包括文件、交易與通訊等應用程式內容)，而產生更深入的鑑識價值。這些資訊全都經過嚴密的索引編排、標準化與關聯化，以擴大偵測風險與威脅的範圍。

McAfee Global Threat Intelligence

選用性的 McAfee GTI IP 信用評價資料即時摘要，可針對收集自全球各地數億個偵測器的外部惡意成分提供重要而即時的資訊，讓您能夠辨識您網路上的惡意活動。McAfee ESM 可使用 GTI IP 信用評價資料，快速識別出內部主機與已知惡意成分通訊的情況。

根據風險與資產價值做出決策

與 McAfee Risk Advisor 整合，可進行即時風險管理。McAfee Risk Advisor (MRA) 可根據指定的值計算內部資產的分數，搭配 McAfee GTI 對外部風險係數的評估，爲您提供環境風險評估。MRA 可根據資產組態、弱點以及已部署的控制功能與可用的對策選項，提供精確的端點風險分數。

McAfee ESM 關聯引擎可讓外部 GTI 威脅摘要與內部 MRA 風險分數產生關聯，以突顯對您的組織具有重要性的事件，而爲您省下寶貴的時間，並迅速警告您有潛在的問題需注意。視覺化指標可顯示所有儀表板上的趨勢活動，以便進行迅速分析。

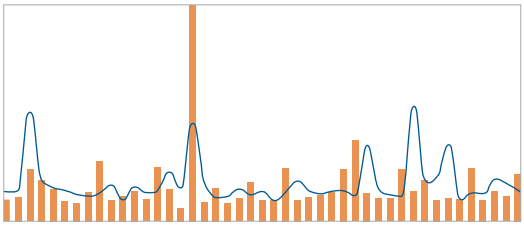

圖 1：動態基準可迅速指出異常。

更理想的事件管理與工作流程

自動化動作可讓您透過優先順序的指定，隨著風險的變化妥善管理安全性。例如，您可以設定監視清單以標示危險活動，例如與已知的惡意 IP 位址聯絡。或者，您可以使用 McAfee ePO 執行特定範圍的更正動作：發出新組態、實作新原則或部署軟體更新等。

爲強化安全性作業，McAfee Enterprise Security Manager 也提供了用於組態與變更管理、案例管理與原則集中化管理的整合式工具 - 這些都是改善工作流程與加速日常資訊安全性作業所不可或缺的管理工作。

原則感知符合性管理

McAfee Enterprise Security Manager 根據 PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、SOX 等標準預先建置了數百個儀表板、完整的稽核追溯與報告，可讓您輕鬆管理符合性工作。我們對統一符合性架構 (Unified Compliance Framework) 的支援，也可讓您根據 240 餘項全球性的法規與控制架構報告您的原則。

連結您的 IT 基礎架構

與 McAfee ePO 軟體間的雙向整合，可延伸整個安全性與符合性管理環境的可見性與控制能力。McAfee Enterprise Security Manager 可自動向 McAfee ePO 管理的資料來源偵測及收集資料。

McAfee Enterprise Security Manager 也可將事件 (包括關聯的事件) 送回到 McAfee ePO 系統，而接下來可再傳輸至其他 SIEM、IT 控管、風險與符合性解決方案，以及 McAfee Security Innovation Alliance 合作夥伴產品。

如需相關資訊，請造訪
www.mcafee.com/tw/products/enterprise-security-manager.aspx。

遇克菲台北辦公室
台北市 104 南京東路三段132 號 4 樓 A2
886-2-2721-7766
www.mcafee.com/tw

41708ds_esm_0412_fnl_ETMG