McAfee Enterprise Security Manager

探索。回應。遵循。

最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 是 McAfee 安全性資訊和事件管理 (SIEM) 解決方案系列的基礎，可以適當的速度與規模為安全性組織提供所需的效能、可動作的情報和即時情境感知，協助組織識別、瞭解和回應各種隱形威脅；同時，內嵌符合性架構還能簡化規範。

主要優點

- 可即時檢視歷程資料，以達到全面性的威脅偵測與回應能力。
- 立即提供已排定優先順序且可動作的資訊，讓您迅速因應威脅。
- 進階分析和資料擴充功能，將資料轉變成安全性情報。
- 適用於超過 240 種全球法規的符合性架構。

McAfee Enterprise Security Manager 不僅能提供真實現況(威脅資料、信用評價摘要與弱點狀態)的即時資訊，也能讓瞭解企業內的系統、資料、風險和活動。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為考量的決策，進而投入相關資源以妥善因應變動的威脅態勢。在調查潛伏式攻擊、搜尋入侵的跡象或修補符合性控制項時，這是左右成敗的關鍵。為了最佳化安全性作業，McAfee Enterprise Security Manager 也提供了用於組態與變更管理、案例管理及原則集中化管理的整合式工具，而這些都是改善工作流程以及安全性作業團隊的效率所不可或缺的管理工作。

先進的威脅情報

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，或是您的資料或基礎架構正面臨風險。McAfee Enterprise Security Manager 可對所有收集到的資訊即時計算基準活動，這是為了在潛在威脅發生前依照優先順序對您發出警示，同時分析該資料的型態是否潛藏更大的威脅。McAfee Enterprise Security Manager 還能運用內容相關資訊 (例如來自弱點掃描以及身分識別與驗證管理系統的資訊)，為每個事件加入對應的內容，以進一步瞭解安全性事件對實際商業程序有何影響。這些情報可讓組織正確對應資料與人員，以便即時採取行動，做出更明智的決策。

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 (APT) 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，而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。

可擴充的部署選項

- 混合式發佈選擇，包含實體和虛擬裝置以及高可用性選項。
- 單一裝置部署 (小型企業適用) 或分散式解決方案 (大型企業適用)。
- 具備高度擴充能力的裝置，可自各種安全性和基礎架構資產收集大量資料。

專為巨量資料建置

巨量資料安全性極其重要，但不斷增加的大量事件以及資產、威脅、使用者和其他相關資料已經讓安全團隊面臨艱鉅挑戰。為了克服這項挑戰，McAfee Enterprise Security Manager 採取的第一步就是針對 SIEM 進行這類作業的需求來建置資料管理系統 (獲 Gartner 認可為 McAfee SIEM 解決方案的核心優勢)。

McAfee Enterprise Security Manager 的設計旨在儲存大量內容相關資料 (來自數億個資料點)，並即時為每個事件加入對應的內容。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 Enterprise Security Manager 的索引系統效率極佳，可針對簡易和複雜兩種查詢迅速給予回應，還可進行同時、即時及歷程作業，以便最佳化威脅調查與鑑識作業。採擷巨量資料以找到重要的安全性資訊，則是 SIEM 的關鍵要素之一。McAfee Enterprise Security Manager 可運用這些大量的安全性資料並發揮超越模式比對的效益，以提供入侵行為長期指標以及可動作的威脅情報。

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。

最佳化安全性作業

McAfee Enterprise Security Manager 簡化了安全性作業，可集中顯示組織的安全性狀態、符合性狀態，並優先顯示需要調查的安全性問題。

您可以立即使用 McAfee Enterprise Security Manager 以及數百種現成的報告、檢視、規則和警示，更可以輕鬆加以自訂。無論是想設定基準以便瞭解一般網路使用情形，或只是想要自訂警示，McAfee Enterprise Security Manager 的儀表板都能輕鬆顯示、調查並報告最相關的安全性資訊。您的組織現在可以存取所有需要的相關資料與內容，迅速做出明智決策。

簡化規範

McAfee Enterprise Security Manager 可將符合性監控與報告作業集中化和自動化，藉此免除耗時的人工作業。此外，與統一符合性架構 (UCF) 整合後，「只要收集一次即可適合多種用途」的方法不但可滿足符合性需求，還能有效減少稽核的工作量與成本。支援 UCF 後即可將各項法規的細節標準化，方便將一組集合事件對應到相關法規，藉此提高符合性效率。

McAfee Enterprise Security Manager 提供數百種預先建立的儀表板、完整的稽核追蹤項以及適用於超過 240 種全球法規和控制架構 (包括 PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX 和 SOX) 的報告，以簡化並加快符合性管理作業。McAfee Enterprise Security Manager 除了提供廣泛的立即可用支援之外，還可讓您完全自訂所有符合性報告、規則及儀表板。

連結您的 IT 基礎架構

整合的安全性與符合性解決方案可提供任何單一解決方案所無法給予的優勢，讓您以前所未有的即時性全盤掌握組織的安全性狀態。McAfee SIEM 解決方案可透過單一基礎架構自安全性廠商的數百種裝置收集保貴資料，McAfee Enterprise Security Manager 則能主動與 McAfee® ePolicy Orchestrator® (McAfee ePO™) 平台、McAfee Network Security Manager 及 McAfee Vulnerability Manager 整合，分別提供原則式端點管理、入侵預防以及弱點掃描與修補功能。

McAfee Enterprise Security Manager 已與 McAfee Threat Intelligence Exchange 整合。有別於標準安全性方法，這兩者的結合能為組織提供從發現攻擊到遏止攻擊為止的封閉迴路式詳細工作流程。McAfee Threat Intelligence Exchange 會根據端點監控資料來彙總盛行範圍小的攻擊，有效運用全域、協力廠商及本機的威脅情報。此外，McAfee Threat Intelligence Exchange 還能利用任何整合的 Security Connected 產品 (例如 McAfee Advanced Threat Defense)，進一步分析和判斷檔案。這項方法可提供全面性的情境感知，讓組織瞭解安全性事件對實際商業程序與政策有何影響，進而瞭解應將安全性措施部署於何處。

與 McAfee 安全性解決方案深入整合後，可讓安全性情報發揮更大效用，讓您只需透過 McAfee Enterprise Security Manager 主控台即可採取明智的行動。McAfee Enterprise Security Manager 可運作這些整合功能來變更端點的原則、隔離網路上的可疑系統，以及透過弱點掃描收集重要情報；當然，只需透過 McAfee Enterprise Security Manager 主控台即可完成。McAfee Global Threat Intelligence (McAfee GTI) 與 McAfee Enterprise Security Manager 整合後，便可包含 McAfee Labs 超過 1 億個全球威脅偵測器的資料，持續提供最新的已知惡意 IP 位址。McAfee Enterprise Security Manager 有了這類整合後，即可將許多必須率先回應的行動自動化，有助於組織更快速有效地因應攻擊。

McAfee 的 Security Connected 平台為數百種產品、服務及合作夥伴提供了可互相合作的統一架構。有了 McAfee Enterprise Security Manager 等 Security Connected 解決方案，安全團隊就能即時檢視特定內容的相關資料，讓組織能立即瞭解整個基礎架構的安全性狀態，進而有效縮短從發現威脅到進行修補之間的回應時間。

深入瞭解

如需 McAfee Enterprise Security Manager 的詳細資訊，請造訪 **www.mcafee.com/tw/products/siem/index.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

Intel 和 Intel 標誌皆為 Intel Corporation 在美國及/或其他國家/地區的註冊商標。McAfee、McAfee 標誌、ePolicy Orchestrator 及 McAfee ePO 是 McAfee, Inc. 或其附設公司在美國及其他國家地區的商標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。本文中的產品計劃、規格和描述僅供參考，並且不包含任何明示或暗示的保證，如有變更，恕不另行通知。Copyright © 2014 McAfee, Inc. 61292ds_esm_0914_fnl_ETMG