資料工作表

McAfee Vulnerability Manager

即時、高效能地持續監控資產

主要特色

- 無人可及的延展性、準確度和彈性
- 對出現在網路上之新裝置進行即時評估、全面清查軟體與硬體資產、對應使用者與資產，及自動網路拓撲
- 結合主動式與被動式網路探索和監控，來找出虛擬化、行動及隱藏裝置
- 對裝置進行的深入稽核可以引導掃描作業，並對授權資產資料庫提供摘要
- 動態系統標記可以全面自動化弱點評估作業
- 已透過 McAfee Global Threat Intelligence™ 更新最新的弱點及威脅
- 已透過 Cyber-Ark 整合提升憑證型安全性
- 同時掃描 IPv4 及 IPv6 網路
- 充分彈性的報告 - 掃描資產一次，並根據其狀態隨時進行報告
- 自動化風險管理工作流程可以包括 McAfee、自製及協力廠商應用程式

採用業界最彈性、經過驗證且具延展性的解決方案來保護您的企業，讓全方位弱點管理變得更簡單且能即時執行。McAfee® Vulnerability Manager 搭配 McAfee Asset Manager 功能，提供了無與倫比的延展性和效能，主動及被動地徹底檢查您網路上的所有項目。如果裝置或資產具有IP位址或正在使用您的網路，McAfee Vulnerability Manager 就可以在即時的狀況下自動找出它並對其進行評估，揭露您網路上所有資產的符合性。

McAfee Vulnerablity Manager 樹立業界的標準，根據您公司的實際狀況運作，覆蓋所有類型的網路和資產設定。它可以於您所需的時間及位置進行被動、不間斷或主動掃描，讓您針對所有資產進行探索、評估、修補及報告。您可以找出隱藏於網路中的裝置，以及在排程掃描之間進入及離開網路的智慧型手機、平板電腦及筆記型電腦。您先前未能看到或掃描到的內容將會令您大吃一驚，且可能會危及您的符合性。上千家組織依賴 McAfee Vulnerability Manager 爲它們快速找出弱點並排定處理的優先順序，其規模從只有幾百個節點的部署到需要持續掃描超過四百萬個 IP 位址的部署都有。

輕鬆實作

McAfee 將實作可靠的掃描變得簡單。McAfee Vulnerability Manager 可輕鬆安裝在您的實體或虛擬硬體上，或者您也可以使用強化的 McAfee 裝置。只要幾分鐘，您就可以開始進行第一次掃描。

載入和維護您的資產庫存也同樣簡單。在搭配 McAfee Asset Manager 模組的情況下，資產資料庫可以在新裝置上線時立即更新，確保您即時掌握裝置資訊。此外，McAfee Vulnerability Manager 可以直接與企業資產管理工具整合，這些工具包括 LDAP、Microsoft Active Directory 及 McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理平台，您只要維護一個中央存放庫即可管理資產資料。

取得所有資產的可見度

McAfee Asset Manager 選項可透過全天候的被動式探索和監控功能，增強可見度。這個可快速部署於 SPAN 連接埠的系統會監視流量，探索網路上所有項目並進行對應，其中包括未管轄的裝置、被遺忘的 VMware 主機及行動裝置。在監視的同時，它會列舉所監看到的裝置、模式及通訊，這些詳細資料可協助您評定並降低風險。裝置詳細資料會自動傳送至 McAfee Vulnerability Manager，供立即評估之用。此外，McAfee Asset Manager 可以針對它所探索到的每個資產執行全面的軟體及硬體清查。

自訂掃描以符合您的需求

McAfee Vulnerability Manager 提供多項選項，協助您建立基準並記錄符合業界法規的規範。若要快速定義原則，您可以掃描「黃金級標準」系統來建立基準、利用提供的符合性範本，或是載入運用 Security Content Automation Protocol (安全性內容自動通訊協定，SCAP) 的原則。

McAfee Vulnerability Manager 會掃描所有網路資產，甚至掃描位於氣隙式環境和重要基礎架構環境之中難以辨識的資產。舉例來說，如果您的網路沒有外部連線，則您可以部署以筆記型電腦爲基礎的掃描器或虛擬掃描器，來探索及掃描這些資產。您可以選擇將結果保留在受限環境中，如有必要，也可以將這些結果彙總至中央系統。

大部分作業系統都需要先進行資產認證，然後才會顯示機密的設定資訊，但部分安全小組難以存取這些認證。與 Cyber-Ark 的 Privileged Identity Management 套件進行整合，即可在輕鬆安全且效能優異的情況下，進行高度安全的認證型探索和掃描。

掃描覆蓋範圍

- 掃描超過 450 種作業系統，包括 Microsoft Windows、UNIX、Cisco、Android、Linux、Apple Macintosh、Apple iOS 及 VMware 平台
- 深入掃描 Web 應用程式 (OWASP Top 10 與 CWE Top 25)
- 尋找下列項目中的弱點及惡意軟體：Adobe、AOL、Apple、Microsoft (Office、IIS、Exchange)、Blue Coat、CA、Cisco、Citrix、Facebook、Google、HP、IBM (Lotus Notes 與 WebSphere)、Novell、Oracle、Real Networks、RIM (BlackBerry Enterprise Server)、SAP、Oracle Java、Symantec 及 VMware 軟體
- 掃描主流資料庫，包括 DB2、MySQL、Oracle、Microsoft SQL Server 和 Sybase

標準與認證

- 針對 ASCI 33、BASEL II、BILL 198 (CSOX)、BSI IT (GR)、COBIT、FDCC、FISMA、GLBA、HIPAA、ISO 27002、JSOX、MITS、PCI、SOX、NIST SP 800-68、SANS Top 20、SCAP、OVAL 等等提供範本
- 支援的標準包括經 CIS 認證的稽核、COBIT、CPE、CVE、CVSS、DISA STIG、FDCC/SCAP、ISO17799/ISO 27002/FINRA、ITIL、NIST-SP800、NSA、OVAL 和 SANS Top 20
- 通過公用準則認證
- FIPS-140-2 加密法驗證

技術規格

請造訪 www.mcafee.com/tw，看看目前硬體和軟體的規格與需求。

在數分鐘內即可判定風險

當 McAfee Asset Manager 識別到您網路上的新系統時，即會將該系統的相關詳細資訊傳送給 McAfee Vulnerability Manager 以觸發目標掃描。幾分鐘後，您即可掌握該系統的狀態及其對您的環境所帶來的風險。

標記資產以提升掃描效率

您也可以使用標記原則，根據每個裝置的設定檔及風險，將新裝置自動納入掃描群組中。適當的掃描依您所定義的原則而定，可以是立即的掃描，或屬於下一次定期掃描。

同時偵測弱點與惡意軟體

其他產品只會尋找表面的開放連接埠和設定，McAfee Vulnerability Manager 則會更加深入地探索。它可實現系統和應用程式層級的評估，包括資料庫橫幅、原則設定、登錄機碼、檔案、磁碟機權限和執行中的服務。爲了要偵測最大範圍的弱點，該產品測試超過 450 個作業系統版本。我們的檢驗也會抓取惡意內容，包括特洛伊木馬程式、病毒和其他惡意軟體。

除了預先定義的檢查和零時差威脅的更新外，您也可以編寫自訂指令碼和檢查，測試專利和舊有程式。McAfee Vulnerability Manager 也可以評估遵循 XCCDF、OVAL 和其他 SCAP 標準的協力廠商內容。

特別注意 Web 應用程式

McAfee Vulnerability Manager 可讓管理員管理 Web 應用程式，方法正如他們管理傳統網路型資產一樣。Web 應用程式資產可以進行分組，並擁有其專屬的關鍵性、資產擁有者及特性。McAfee Vulnerability Manager 運用完全自動化的功能，針對各種 Web 弱點進行深入 Web 應用程式掃描。

保持最新

全球數百萬個偵測器告訴上千名 McAfee Labs 研究人員威脅世界中的最新變化。McAfee Global Threat Intelligence 會將即時風險評估和威脅建議直接送至 McAfee Vulnerability Manager，保護您不受新興威脅的攻擊。

根據需要進行管理、延展及整合

McAfee 的彈性讓您可以用喜愛的方式設計掃描、報告和管理。只監視掃描程式本機的資產，或從單一主控台查看數百個遠端掃描引擎的進度。我們的多層式架構可符合所有尺寸組織的需求。

透過開放式的應用程式開發介面 (API)，McAfee Vulnerability Manager 可以與大部分的應用程式整合。

根據風險進行回應

弱點的單一可動作的檢視可降低修補與稽核成本。例如，在 Patch Tuesdays 定期發佈更新時，您可以快速判斷哪一台機器會受到 Microsoft Windows 或 Adobe 弱點的影響。只要幾分鐘，而且不必重新掃描整個網路，McAfee Vulnerability Manager 就可以根據現有的設定資料和風險指數，針對新的威脅將潛在風險視覺化並排名。

有了此資訊，您就可以根據關鍵性選取資產，並按一下滑鼠右鍵執行即時的目標掃描。

符合規範、擁有信心

決定性的證據 - 像是預期結果和實際掃描結果、任何未掃描的系統和失敗的掃描 - 提供特定系統「不易受攻擊」的記錄、增加的共同稽核需求的文件。透過主動式與被動式監控的結合、滲透測試、驗證掃描及非認證掃描，McAfee Vulnerablity Manager 讓您可以正確無誤地指出弱點和原則違規。全方位的弱點管理，前所未有的簡單。

McAfee
An Intel Company

邁克菲有限公司台灣分公司
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.mcafee.com/tw

McAfee、McAfee 標誌、ePolicy Orchestrator、McAfee ePO 和 McAfee Global Threat Intelligence 皆為 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。其他名稱與品牌可能為他人所宣告的財產。本文中的產品計劃、規格和描述只提供參考，如有變更，恕不另行通知，並且不包含任何明示或暗示的保證。Copyright © 2012 McAfee, Inc.
53000ds_mvm-mam_1012_fnl_ETMG