McAfee Management for Optimized Virtual Environments AntiVirus

適用於私有雲且不降低效能的安全性防護

傳統的防毒軟體在虛擬化基礎架構上無法順利運作。McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) 可為您的虛擬化桌面與伺服器提供最佳化的進階惡意軟體防護功能。跨多個 Hypervisor 實作，或是選擇適用於 VMware NSX 或 VMware vCNS 的無代理程式經調整選項。無論選擇哪一項，您都可獲得首屈一指的即時威脅偵測與遏止之安全防護，並將對虛擬機器 (VM) 效能帶來的影響降至最低。McAfee MOVE AntiVirus 不僅可最佳化虛擬化部署的防惡意軟體保護、釋出 Hypervisor 資源，也可確保根據原則執行最新的安全性掃描。

最佳化掃描控制

訪客桌面與虛擬伺服器具有動態特性，必須謹慎處理。使用者起始工作階段時，映像必須不受惡意軟體的侵擾。但此條件相當難以達成，因為使用者經常群起行動、一起工作，造成所謂的「防毒風暴」尖峰需求消耗所有資源，讓使用者無法取得工作階段。

為避免掃描遭遇瓶頸與延遲，McAfee MOVE AntiVirus 會以卸載掃描服務器分擔個別的訪客映像 (guest image) 的掃描、設定與 .DAT 更新操作。我們為已掃描的檔案建置並維護全域快取，以確保檔案一經掃描並確認安全無虞後，後續虛擬機器無需等待掃描，即可直接存取該檔案。每部虛擬機器的記憶體資源配置將因而減少，而得以釋出給資源集區以更有效的方式加以運用。

McAfee MOVE AntiVirus 可針對常駐和按指定掃描採用個別原則，以啟用微調安全性執行。舉例來說，管理員可針對即時、常駐掃描來假設特定程度的合理風險等級，以防止降低效能；接著，再使用按指定掃描，並隨後在效能影響較小時執行較為精確的原則。

跨雲端間的完整端對端可見度

可見度不佳，將難以針對虛擬化環境實作適當的安全性原則。私有雲的 McAfee Cloud Workload Discovery (涵蓋 VMware 和 OpenStack) 可讓您完整檢視虛擬資料中心，並將重要資產 (例如伺服器、Hypervisor 和虛擬機器) 加入 McAfee ePO 主控台中。一旦管理員掌握所有虛擬機器安全性狀態的可見度，且可在近乎即時的狀態下監控 Hypervisor 與虛擬機器之間的關係時，即可更為輕鬆保護虛擬資料中

主要優點

- **分擔惡意軟體掃描工作量：**提供即時保護，且對記憶體與處理只會有些微影響
- **防範防毒風暴：**可用選項包括常駐與按指定掃描
- **可進行彈性部署：**多平台 (所有主要 Hypervisor、Windows 虛擬機器) 或無代理程式 (VMware、Windows 和 Linux 虛擬機器)
- **改良資料最佳化：**彈性佈建離線掃描程式，並提供事件通知 (多平台)
- **即時封鎖零時差不明威脅：**本機信用評價情報結合沙箱的行為分析 (多平台，另售其他模組)
- **運用 McAfee® ePolicy Orchestrator® (McAfee ePO™) 主控台：**提供端對端可見度，並可跨實體、虛擬及雲端部署控制

心。可自訂的儀表板會顯示安全性掃描狀態、執行概觀以及資產的安全性歷程資料。

McAfee Sever Security Suite Essentials 與 McAfee Server Security Suite Advanced 能擴展可見度，並控制 Amazon Web Services (AWS) 和 Microsoft Azure 公有雲和實體伺服器。

精細的原則管理

熟悉的 McAfee ePO 主控台可讓您設定原則並控制 McAfee MOVE AntiVirus。您可以將虛擬資料與實體系統和公有雲的資料彙總，以提供統一的儀表板和報告。管理員可透過 McAfee Cloud Workload Discovery 為每個虛擬機器、叢集或資料中心設定唯一原則，藉此在建構資料中心時，調整特定安全性。

其他 McAfee MOVE AntiVirus 功能

管理和可見性：

- 立即為一部或多部虛擬機器排定按指定掃描。
- 使用目標按指定掃描提升掃描精準度。
- 透過與 VMware NSX Service Composer 整合，在每個 Hypervisor 上自動部署卸載掃描程式。
- 透過儀表板、報告和電子郵件警示掌握各項問題。

簡化部署和組態：

- 在多個 Hypervisor 上部署和設定分擔負載掃描程式 (無代理程式)。
- 使用 McAfee ePO 主控台還原隔離檔案 (多平台)。
- 防毒效能微調的詳細診斷功能。
- 無縫整合無代理程式和多平台原則管理。

適用於 VMware 的無代理程式選項

McAfee MOVE AntiVirus 利用 VMware NSX 或 VMware vCNS 提升效率。在無代理程式的部署中，這兩者會使用 Hypervisor 做為高速連線，以讓 McAfee MOVE AntiVirus 安全性虛擬機器 (SVM) 從訪客映像外掃描虛擬機器。SVM 在執行掃描時，會指示 VMware NSX 或 VMware vCNS 快取正常檔案或刪除、拒絕存取惡意檔案或予以隔離。

在 VMware ESX 伺服器上安裝和設定完 SVM 和 VMware NSX 或 VMware vCNS 元件，並在訪客虛擬機器上安裝完 VMware NSX 或 VMware vCNS 端點驅動程式後，各映像會自動受到保護，無需在每部用戶端虛擬機器上安裝 McAfee 軟體。我們的 vMotion 感知實作方式所代表的意義是，您的 VM 可在不同的主機間移動，且在此期間同樣能受到目標主機上的 SVM 縝密的保護，無論是掃描或使用者體驗皆不受影響。

McAfee MOVE AntiVirus 組態

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus：
  - 多平台部署
  - 無代理程式部署
- 適用於私有雲 (VMware 及 OpenStack) 的 Cloud Workload Discovery
- McAfee ePO 軟體

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus：
  - 多平台部署
  - 無代理程式部署
- 私有雲的 Cloud Workload Discovery (涵蓋 VMware 和 OpenStack)
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- 記憶體保護與 Web 應用程式保護
- McAfee ePO 軟體

McAfee 產品與 VMware vCNS 的整合，可讓您監控 VMware vCenter 內的 SVM 狀態，並在 SVM 連線中斷時收到警示。若有虛擬機器受到感染，McAfee ePO 主控台會收到說明受影響之特定虛擬機器的事件資料。與 VMware NSX 深入整合，即可同步 McAfee ePO 主控台中建立的原則，以及 VMware NSX 指派的原則。為缺乏防惡意軟體保護或存在惡意軟體的機器，標記為容易受到攻擊的機器，以透過 VMware NSX 防火牆進行立即隔離。

同時支援無代理程式的 McAfee MOVE AntiVirus 與 VMware vCNS 和 VMware NSX 的部署，使 VMware vCNS 客戶能非常輕鬆順利轉移至 VMware NSX。

適用於所有主要 Hypervisor 的多平台安裝

在多平台安裝 (包括 vSphere、Hyper-V、KVM 和 XenServer) 期間，McAfee MOVE AntiVirus 代理程式 (輕量型端點元件) 會與安全性虛擬裝置通訊，以代表每個虛擬機進行防毒處理。McAfee MOVE AntiVirus 代理程式會維護本機快取並管理原則和掃描功能。您可以指定並掃描參考映像，以作為主要乾淨映像。在本機快取中預先填入乾淨映像，可讓虛擬機器迅速開機。

存取檔案時，McAfee MOVE Offload Scan Server 即會執行常駐掃描，以回應 VM。使用者可透過快顯警示收到問題通知，並可採取行動選擇刪除、拒絕存取或隔離惡意檔案。

當多平台部署中的掃描需求量劇烈變化時，會自動從資源集區新增或移除安全虛擬裝置，以擴充或縮減功能，使資源使用能獲得無限擴充與效率。事件通知可協助管理員瞭解安全虛擬裝置的使用趨勢，以最佳化資源管理。

多平台部署中的 McAfee MOVE AntiVirus 可增強 McAfee Global Threat Intelligence (McAfee GTI) 的全域信用評價情報與 McAfee Threat Intelligence Exchange (額外模組，另售) 的本機資料，以立即辨識和對抗日益增長的獨特惡意軟體樣本。若搭配使用 McAfee Threat Intelligence Exchange，McAfee MOVE AntiVirus 可與 McAfee Advanced Threat Defense 協同合作，在沙箱中動態分析未知應用程式的行為，使各端點自動免受最新偵測的惡意軟體襲擊。透過 McAfee Threat Intelligence Exchange 將 McAfee MOVE AntiVirus 與 McAfee Network Security Platform 整合，提供統合邊界分層式的安全防護與虛擬機器保護。

適用於無代理程式和多平台部署的統一原則管理

許多組織可能會需要運用 McAfee MOVE AntiVirus 的功能，以支援無代理程式和多平台部署。McAfee MOVE AntiVirus 可讓安全管理員透過 McAfee ePO 主控台的延伸點定義和管理一致的安全性原則，使不同原則方式的管理變得順利輕鬆。

架構	多平台部署	無代理程式部署
Hypervisor/平台支援	所有主要 Hypervisor，包括 VMware、Citrix、Hyper-V 及 KVM	VMware
掃描平台	Windows 2008、Windows 2012 R2、Windows Server 2016	Linux Ubuntu 16.04
部署擴充性	一部安全虛擬裝置即可保護多部 Hypervisor 的虛擬機器。安全虛擬裝置可彈性佈建	每部 ESX 主機有一部安全虛擬裝置
與 VM 通訊	透過網路	透過 Hypervisor
虛擬機器保護	Windows	Windows 和 Linux

深入瞭解

McAfee 解決方案可讓您獲得不可或缺的安全性，以及應享有的彈性。

若要深入瞭解，請至 www.mcafee.com/tw/products/move-anti-virus.aspx

台灣
台北市信義區忠孝東路五段 68 號 29 樓，11065
電話：+886 2 8729 9222
www.mcafee.com/tw