



McAfee Security Suite for Virtual Desktop Infrastructure

您不可或缺的安全性，以及應享有的彈性

主要優點

- 使用 McAfee ePO 軟體和 McAfee Data Center Connector for VMware vSphere，探索及全面掌控 VMware vSphere 環境。獨特的黑名單與白名單組合可保護實體和虛擬環境免於惡意軟體的侵擾。
- 最佳化虛擬化安全性，將其對效能產生的影響減至最少。
- 避免虛擬桌面執行不需要的應用程式，藉以防範不明威脅。
- 使用桌面防火牆、記憶體保護以及 Web 應用程式保護，增加入侵與 Web 保護。
- 利用 McAfee ePO 軟體迅速監看、控制與回報所有端點。

今日的解決方案大多已採用虛擬桌面 (VDI)，但是仍須整合強大的桌面安全性，才可以避免造成效能問題，或是影響所需的伺服器密度，妥善保護企業安全。傳統的防毒在虛擬化基礎架構上無法順利運作。如何對應？McAfee® Security Suite for VDI 可為虛擬桌面提供最佳化的全方位安全性。

McAfee Security Suite for VDI 提供最佳虛擬化的防惡意軟體保護、防禦零時差威脅的白名單、桌面入侵保護及資料保護。它也可以向使用者傳送惡意網站警告及/或封鎖惡意網站存取權。

最佳化掃描架構

虛擬桌面具有動態特性，必須謹慎處理。映像必須能在離線時不受惡意軟體的侵擾，而在使用者起始工作階段時立即進行掃描。防惡意軟體並不是唯一啟動的服務，且使用者工作時常會分組，導致耗用掉所有資源的尖峰時段需求「防毒風暴」，並且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 Management for Optimized Virtual Environments (MOVE) 會以強化的虛擬裝置/Offload Scan Server，分擔個別的訪客映像的掃描、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 (VM) 即不須等待掃描，可直接存取該檔案。每個 VM 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。按指定掃描的智慧型排程，可確保掃描作業不會干擾 Hypervisor 的效能。

精細的原則管理

McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體主控台可讓您設定原則並控制 McAfee MOVE AntiVirus 的行為。可在統一的儀表板中，彙總來自虛擬桌面的資料與來自其他系統的資料。管理員可透過 McAfee Data Center Connector 為每個 VM、資源集區、叢集、或資料中心設定唯一原則，藉此在建構資料中心時，調整自己的特定安全性需求。

McAfee Security Suite for VDI 設定

McAfee MOVE AntiVirus for Virtual Desktops (VDI)

- McAfee MOVE AntiVirus
 - 多 Hypervisor 部署
 - 無代理程式部署
- McAfee Data Center Connector for vSphere
- McAfee VirusScan® Enterprise for Windows 軟體
- McAfee VirusScan Enterprise for Linux 軟體
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise 技術
- McAfee ePolicy Orchestrator 軟體

無代理程式的部署利用 VMware vShield 提升效率

在無代理程式的部署中，VMware vShield Endpoint 會使用 Hypervisor 作為高速連線，以讓 McAfee MOVE AntiVirus Security Virtual Appliance (SVA) 從訪客映像外掃描虛擬機器。SVA 在執行掃描時，會指示 vShield 快取正常檔案或刪除、拒絕存取惡意檔案或予以隔離。

在 ESX 伺服器上安裝和設定 SVA 以及必要的 vShield 元件後，隨著在訪客 VM 上安裝的 vShield 驅動程式，每個映像在建立時即會自動受到保護。在每部用戶端 VM 上安裝 McAfee 軟體並無特殊需求。我們的 vMotion 感知實作方式所代表的意義是，虛擬機器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 SVA 縝密的保護，無論是掃描或使用者體驗皆不受影響。McAfee 的整合功能可讓您在 vCenter 內監視 SVA 的狀態，並且在 SVA 的連線中斷時對您發出警示。若有 VM 受到感染，McAfee ePO 軟體會收到說明受影響之特定 VM 的事件資料。

支援多個 Hypervisor 以提供標準及便利的管理

在安裝多個 Hypervisor 期間，McAfee MOVE AntiVirus 代理程式(輕量型端點元件)會與 Offload Scan Server 通訊，以代表每個虛擬桌面進行防毒處理。McAfee ePO 軟體代理程式可管理原則及掃描功能。您也可以指定並掃描參考映像，以作為主要乾淨映像。因此，管理員可以在全域快取中預先填入乾淨映像，協助虛擬桌面迅速開啟。

當使用者存取檔案時，McAfee MOVE Offload Scan Server 即會執行常駐掃描，以回應 VM。若有問題，使用者可透過快顯警示獲得通知，並可將檔案移至隔離區等候處置。您可以在 McAfee ePO 軟體主控台中為各個虛擬桌面設定唯一的個別原則集，或以群組的方式來管理這些 VM。

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。請造訪 www.mcafee.com/tw/products/data-center-security-suite-for-vdi.aspx。

功能	您為什麼需要它
虛擬化安全性	<ul style="list-style-type: none">提升您在虛擬桌面基礎架構上部署的工作負荷安全性，無需犧牲性能和資源使用率。多 Hypervisor 和無代理程式部署選擇：此類部署適用於採用多家廠商設備的虛擬化環境 (VMware、Citrix 及 Hyper-V)。在 VMware 中採用無代理程式部署，協助提供絕佳性能和 VM 密度。每個虛擬桌面皆無需安裝/更新任何 McAfee 代理程式；降低複雜性之餘，也能大幅提升可用性。
核心端點保護	<ul style="list-style-type: none">實體伺服器防毒保護在抵禦零時差入侵和規避攻擊方面榮獲 NSS Labs 評選為第一名。企業使用者可能在無意間引進複雜的安全性威脅或允許其進入企業環境，而主機入侵防禦正可保護企業免於遭受這類安全性威脅的侵擾。McAfee SiteAdvisor® Enterprise 可以防止使用者與危險網站互動，且允許您自訂原則，以限制使用者存取可能有害的網站，藉以確保原則符合性。
應用程式白名單	<ul style="list-style-type: none">大幅減少主機效能受到的影響，遠勝於傳統的端點安全性控制項。無須更新特徵碼即可防阻零時差和進階持續性威脅 (APT)，為您迅速提供所需保護。與舊版白名單技術相比，動態白名單的作業負荷較低。
全盤掌控私有雲中的虛擬機器	<ul style="list-style-type: none">自動探索私有雲 (VMware vSphere) 中的虛擬機器。
檔案和卸除式媒體保護 (加密)	<ul style="list-style-type: none">使用檔案和卸除式媒體保護後，部署加密作業將變得分外輕鬆，風險也大幅降低。最佳化實作 Intel AES-NI 技術，在加密的主機上享受接近本機的效能。提供原則式透明檔案/資料夾自動加密，以及卸除式媒體加密 (USB 磁碟機、CD 和 DVD)。使用者可以為卸除式 USB 媒體加密，並以安全的方式傳送資訊。可以安全存取網路共用資料。
透過 McAfee ePO 軟體的集中式管理	<ul style="list-style-type: none">以單一窗格管理實體和虛擬機器 (包含私有雲和公有雲中的虛擬機器)，以進一步掌控安全性。簡化作業程序並減少管理人員作業時間。減少伺服器使用量以降低硬體成本。



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、McAfee ePO、VirusScan 與 SiteAdvisor 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。
Copyright © 2014 McAfee, Inc. 61145ds_vdl_0614B_fnl