

# McAfee Security Suite for Virtual Desktop Infrastructure

這是您所需要的安全防護，而且對效能影響最小

當前的解決方案大多已採用虛擬桌面，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 Virtual Desktop Infrastructure (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/或封鎖這些網站。

## 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「防病毒風暴」，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 AntiVirus (McAfee MOVE AntiVirus) 會以強化的虛擬裝置/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 (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。按需求掃描的智慧型排程，可確保掃描作業不會干擾 Hypervisor 的效能。

## 精細的原則管理

The McAfee® ePolicy Orchestrator® (McAfee ePO™) 主控台可讓您設定原則並控制 McAfee MOVE AntiVirus。可在統一的儀表中，彙總來自虛擬桌面的資料與來自其他系統的資料。管理員可透過私有雲的 Cloud Workload Discovery，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。

## 主要優點

- 透過 McAfee ePO 軟體及 Cloud Workload Discovery，提供探索能力及可見性
- 提供獨特的黑名單與白名單組合功能，保護虛擬桌面免於惡意軟體威脅
- 最佳化虛擬化安全性，將其對效能產生的影響降至最低
- 藉由記憶體保護以及 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
- 可靈活進行無代理程式及多平台部署
- 支援離線掃描程式的彈性佈建，以便根據需求進行調整 (多平台)
- 整合本機信譽評價情報，以加快威脅回應速度 (多平台)

### VMware 的無代理程式部署

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。

只要在 VMware ESX 伺服器安裝並設定 VMware SVM 及 VMware NSX 或 VMware vCNS 元件，並在訪客 VM 上安裝 VMware NSX 或 VMware vCNS 端點驅動程式，即使不在每個用戶端 VM 上安裝我們的軟體，也能自動為所有映像提供保護。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的體驗皆不受影響。

McAfee MOVE AntiVirus 整合了 vCNS，可讓您在 VMware vCenter 內監視 SVM 的狀態，並在 SVM 的連線中斷時獲得警示。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。與 NSX 深度整合，同步 McAfee ePO 軟體內建立的原則與 VMware NSX 指派的規則。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。

### 適用於所有 Hypervisor 的多平台

在多平台安裝期間，McAfee MOVE AntiVirus 代理程式 (輕量型端點元件) 會與 McAfee MOVE 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並進行掃描。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 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。

隨著多平台部署的工作負載提高或降低，系統可自動從資源集區新增或移除 SVM，上下調整您的電力需求，藉由不斷調整的方式有效利用資源。事件通知可協助管理員瞭解 SVM 使用趨勢，藉此達到最佳資源管理。

### McAfee Security Suite for VDI 設定

---

- 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 VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise 技術
- McAfee ePolicy Orchestrator

## 資料工作表

多平台部署的 McAfee MOVE AntiVirus 可利用 McAfee Threat Intelligence Exchange (個別銷售的附加模組) 的本機資料, 增強 McAfee Global Threat Intelligence 的全球信用評價情報, 藉此立即辨識及對抗數量不斷增長的唯

一惡意軟體樣本。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。並可使各虛擬桌面免受最新偵測的惡意軟體襲擊。

---

### 功能

### 您為什麼需要它

---

#### 虛擬化安全性

- 提升您在虛擬桌面基礎架構上部署的工作負荷安全性, 無需犧牲效能和資源使用率。
- 在 VMware 中採用無代理程式部署, 協助提供絕佳效能和 VM 密度。每個虛擬桌面皆無需安裝/更新任何我們的代理程式; 降低複雜性之餘, 也能大幅提升可用性。
- 為所有 Hypervisor 提供多平台部署, 支援離線掃描程式的彈性佈建, 以便根據需求進行調整, 並整合本機信譽評價情報, 藉此加快威脅回應速度。

---

#### 核心端點保護

- McAfee 防毒保護的掃描速度、使用的記憶體、需要的 CPU 週期及保護能力均優於其他產品。
- 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

- 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。
- 無需更新特徵碼即可抵禦零時差與進階持續性威脅 (APT), 提供更即時的防護。
- 與舊版白名單技術相比, 動態白名單的作業負荷較低。

---

#### Cloud Workload Discovery

- 可完整看到私有雲工作負載及其基礎平台, 藉此辨識安全性不足的控制項。
-

功能	您為什麼需要它
檔案和卸除式媒體保護 (加密)	<ul style="list-style-type: none"><li>▪ 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。</li><li>▪ 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。</li><li>▪ 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)。</li><li>▪ 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。</li><li>▪ 可以安全存取網路共用資料。</li></ul>
透過 McAfee ePO 軟體的集中式管理	<ul style="list-style-type: none"><li>▪ 集中管理實體、虛擬及雲端部署, 提供更優秀的安全控制, 包括所有平台的原則管理、部署、可見性與安全性管理。</li><li>▪ 簡化作業程序並減少管理人員作業時間。</li><li>▪ 減少伺服器使用量以降低硬體成本。</li></ul>

## 深入瞭解

McAfee 解決方案可讓您獲得不可或缺的安全性, 同時將對效能的影響降至最低。請造訪 [www.mcafee.com/tw/products/data-center-security-suite-for-vdi.aspx](http://www.mcafee.com/tw/products/data-center-security-suite-for-vdi.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](http://www.mcafee.com/tw)

McAfee 和 McAfee 標誌、ePolicy Orchestrator、McAfee ePO、VirusScan 與 SiteAdvisor 是 McAfee, LLC 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 © 2017 McAfee, LLC. 2065\_1216  
2016 年 12 月