資料工作表

McAfee Server Security Suite Advanced

利用白名單功能為實體、虛擬與雲端部署取得進階伺服器安全性。

過去數年來，資料中心一直是儲存裝置、伺服器、網路和其所提供應用程式之間的主要傳輸重心。有鑑於資料中心的多樣性本質，以及業界採用雲端運算的急遽轉變趨勢，致使我們必須採用新的方法來保護此環境。企業 IT 人員和安全性專業人員面臨的挑戰，在於如何為實體、虛擬化及雲端環境創造統一且強大的安全性狀態，以協助確保靈活度和成本效益。McAfee® Server Security Suite Advanced 屬於 Intel® Security 產品的供應項目，可為實體、虛擬與雲端部署提供最全面的伺服器防護與管理，同時提供額外的伺服器進階安全性功能 (例如白名單和變更控制)，以協助維持符合性。

主要優點

- 找出所有實體和虛擬伺服器，包括從中央主控台透過單一窗格管理的雲端伺服器。
- 結合黑名單與白名單功能，可保護實體和虛擬伺服器免於惡意軟體的侵擾。
  - 提供動態的白名單功能，透過 McAfee Application Control for Servers 避免執行不需要的應用程式，確保維持主機安全，藉以防範不明威脅。
  - 持續偵測分散和遠端位置中的系統層級變更，協助您符合法規遵循要求。

找出所有工作負荷

如何找出所有工作負荷，並針對實體、虛擬及雲端部署套用合適的安全性原則，時常是一大挑戰。我們讓您使用掃描報告就能輕鬆獲得管理能力，此類報告可偵測到未受保護的端點，並判斷安全性是否符合標準。透過 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體的專用連接器，McAfee Server Security Suite Advanced 可讓您找出所有實體及虛擬伺服器，包括私有雲和公有雲中的同類伺服器。此解決方案也包含 McAfee Data Center Connector for VMware vSphere、Amazon AWS、OpenStack 及 Microsoft Azure。搭配使用後，這些可讓您監視內部部署與外部部署的所有虛擬機器，並套用精細的安全性原則來創造強而有力的安全性狀態。此儀表版提供安全性狀態，包括作業系統記憶體保護、Hypervisor 主機與虛擬機器間的關係、每部虛擬機器所在位置等資訊。

保護伺服器

McAfee Server Security Suite Advanced 為實體、虛擬或雲端中的伺服器提供最全面的防護。此外，亦可提供變更控制，以及在業界無人可及的黑名單與白名單防護技術獨家組合。

intel Security

主要優點 (續上頁)

- 使用 McAfee MOVE AntiVirus 提供最佳化的虛擬化安全性，將其對效能產生的影響減至最少。
- 透過 McAfee Data Center Connector for VMware vSphere、Amazon Web Services、OpenStack 及 Microsoft Azure，全盤掌控私有雲和公有雲中所有虛擬機器的安全性狀態。

McAfee Server Security Suite Advanced 包含 McAfee Application Control for Servers，透過此白名單解決方案，只有獲得授權的軟體才能在伺服器上執行。這項集中管理的白名單解決方案使用動態信任模型與創新的安全性功能，可封鎖未取得授權的應用程式及遏止進階持續威脅 (APT)，完全不需要管理惱人的清單。白名單功能可在無需執行特徵碼更新的情況下，大幅減少主機效能受到的影響。

身為核心伺服器的一員，此套件提供適用於 Microsoft Windows 和 Linux 伺服器的傳統防惡意軟體解決方案，其中的 McAfee VirusScan® Enterprise 軟體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。除了傳統的防惡意軟體工具，此套件也提供專為虛擬環境設計的獨立解決方案。McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus 可最佳化虛擬化環境的防毒軟體、將超大型環境之效能受到的影響減至最少，並為所有主要 Hypervisor 提供支援。McAfee MOVE AntiVirus 可用作 VMware 部署環境的一種無代理程式、經調整的選項，或者可部署於 KVM、Microsoft Hyper-V、VMware 及 Xen 型 Hypervisor 環境的多平台選項。

雖然防毒軟體是保護安全性的關鍵，但仍有必要採取額外解決方案，以抵禦進階威脅。McAfee Host Intrusion Prevention 能保護企業不受複雜的安全性威脅所攻擊，而這些攻擊也可能是不慎帶入或放行的。

延伸至雲端

隨著您將部署作業延伸至雲端，要確保新佈建的工作負荷確實套用合適的安全性原則可說益發困難。當虛擬機器佈建至私有雲與公有雲時，McAfee 可自動找出執行中和已停止的虛擬機器，藉此解決這類難題。若要啟用此功能，您只需要在 McAfee ePO 平台中註冊公有雲帳戶。虛擬機器接著可以使用合適的安全性原則加以保護。此外，McAfee 資料中心安全性儀表板中還可以完整看到私有雲與公有雲中的保護狀態和安全事件。

最佳化您的伺服器、最佳化您的企業

唯有賦予虛擬化和雲端運算充分的安全性，才能完全發揮其具備的龐大潛力。McAfee 提供的伺服器安全性解決方案可在組織發展的過程中，隨時支援足以因應成長的各種選項。無論是實體、虛擬化或雲端部署，McAfee 都能提供解決方案套件，維持伺服器的安全之餘，也能保有極佳的運用彈性。McAfee Server Security Suite Advanced 透過進階解決方案為實體、虛擬及雲端伺服器提供安全性，為整個組織建立和維持強而有力的安全性狀態。

瞭解更多關於 McAfee Server Security Suite Advanced 優點的資訊，請造訪：**http://www.mcafee.com/tw/products/server-security-suite-advanced.aspx**。

功能	您為什麼需要它
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。 • 無須更新特徵碼即可抵禦零時差與 APT，有助於更迅速地提供防護。 • 相較於舊版白名單技術，動態白名單需要的營運成本較低。
變更控制	• 防範重要的系統檔案、目錄和設定遭受未經授權的變更，藉以避免發生竄改的情況，進而為管理員節省用於疑難排解安全漏洞的時間。 • 即時追蹤並驗證伺服器上每一個試圖進行的變更，根據時間範圍、來源或是核准的工作單來強制執行變更原則。 • 持續性的控制功能會將臨機操作或未經授權之變更所造成的影響降至最低。
單一主控台管理	• 只需單一窗格即可管理實體與虛擬伺服器，包括私有與公用雲中的伺服器，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。 • 因減少必要的伺服器使用量而降低了硬體成本。
核心伺服器保護	• 在抵禦零時差入侵和規避攻擊方面榮獲 NSS Labs[1] 評選為第一名的實體伺服器專用防惡意軟體防護。 • 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 Host Intrusion Prevention 正可保護企業免於遭受這類安全性威脅的侵擾。
虛擬化安全性	• 最佳化部署於虛擬基礎架構中之工作負荷的安全性，無需犧牲效能和資源使用率。 • 為資料中心的多個 Hypervisor 提供保護，讓所有使用的 Hypervisor 類型具備一般的安全計劃。 • 最佳化 VMware 環境中的無代理程式部署，有助於提供出色的效能與 VM 密度。
全盤掌控私有雲和公有雲中的虛擬機器	• 不僅能探查實體伺服器，還能找出 VMware vSphere、Amazon AWS、OpenStack 與 Microsoft Azure 環境中的 Hypervisor 和虛擬機器，藉此全面掌控需要保護的項目。 • 可在佈建虛擬機器時探索，並以安全性原則自動保護這些機器，藉此確保機器具有適當的安全性狀態。

1. 2013 年 NSS Labs, Inc. Protection & Evasion Test (NSS Labs, Inc. 保護與規避測試)。

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