

# McAfee Server Security Suite Advanced

實體、虛擬與雲端部署的全面安全防護，以及白名單與變更控制。

在當前複雜的 IT 環境中，若無通盤考量的方法，要保護新的伺服器與雲端工作負載不受日益複雜的威脅侵害，益發困難。McAfee® Server Security Suite Advanced 提供涵蓋實體、虛擬及公有雲部署在內的一致且持續的防護。全面的安全防護包括基礎防毒、防火牆防護、入侵防禦、抵禦零時差威脅的白名單與變更控制，以符合法規遵循需求。進階防護將對於實體與虛擬伺服器產生的效能影響降至最低，並且能隨著您的動態雲端工作負載自動擴充。

## 即時探索與控制

適用於混合雲的雲 Cloud Workload Discovery 為 McAfee Server Security Suite Advanced 的重要功能，有了這項功能，在不斷擴展的混合資料中心中追蹤安全性落差並非難事。混合雲的 Cloud Workload Discovery (涵蓋 VMware、OpenStack、AWS 和 Microsoft Azure)，提供所有工作負載及其下層平台的端點對端點可見度。弱點安全性控制、不安全防火牆和加密設定的深入見解，與入侵指標 (例如可疑流量)，可加快偵測速度。McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體或 DevOps 工具能加快進行矯正。

由於眾多不同的雲端工作負載皆有獨特風險設定檔和安全要求，使得雲端安全具有挑戰性。Cloud Workload Discovery 是原則導向的評估，可以將這些多元工作負載需要的安全性控制項與其實際擁有的安全性控制項輕鬆進行對比，以確定適當的防護和法規遵循。一旦發現安全性風險，只要輕輕地按幾下，就可以繼續完成防護。

Cloud Workload Discovery 與 McAfee ePO 管理主控台的整合，可提供組織有效的控制，以協助執行跨實體、虛擬和雲端環境的安全解決方案。藉由此等整合，安全管理員可以使用單一管理平台，並透過簡化的工作流程，處理威脅警示並強制執行原則，藉此縮短識別及解決安全問題的時間。

## 主要優點

- 透過 McAfee ePO 軟體，不分端點、網路、資料、McAfee 法規遵循解決方案及協力廠商解決方案，統一管理安全性產品
- 透過混合雲的 Cloud Workload Discovery，提供深入的可見性、風險評估和矯正措施
- 結合黑名單、入侵防範、進階白名單和變更控制，以保護實體和虛擬伺服器不受惡意軟體侵害
  - 避免執行不需要的應用程式，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
- 使用本機信譽資料結合沙箱分析，在幾秒鐘內封鎖不明的零時差威脅
- 提供最佳化的實體與虛擬安全性，同時將對效能產生的影響降至最低

## 資料工作表

McAfee Server Security Suite Advanced 確保支援 DevOps 的動態雲端環境不會為了靈活度而犧牲安全性。我們的安全性會隨雲端工作負載而彈性擴充；因此，您便可始終受到保護。有了私有雲的彈性佈建，當工作負載有所增減時，離線掃描伺服器便可自動增加至資源集區或從此處卸下。至於 AWS 和 Azure 工作負載，使用者可將安全性設定為範本層級；如此一來，安全性便能隨著工作負載變更而自動擴充。

### 全面性的防護

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，Windows 32 與 64 位元系統上記憶體緩衝區溢位攻擊的防護，連同黑名單、白名單和變更控制的獨特組合，在業界無可匹敵。套件內容包括：



圖 1. 藉由 Cloud Workload Discovery，保有持續優勢。

- **McAfee Application Control for Servers**：此白名單解決方案只允許在伺服器上執行授權軟體，以抵禦未知的惡意軟體以及零時差與進階威脅。此集中管理白名單解決方案使用動態信任模型，可免除需耗費大量人力的清單管理作業。
- **McAfee Change Control for Servers**：可持續偵測不同分佈地點與遠端地點的系統層級變更，協助確保遵循法律和法規，例如沙賓法案 (Sarbanes-Oxley) 和支付卡產業資料安全標準 (PCI DSS)。
- **McAfee Endpoint Security 威脅防護**：屬於協同式、可擴充架構，可保護 Microsoft Windows 和 Linux 伺服器抵禦零時差入侵和進階攻擊。
- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus)**：此防惡意軟體解決方案是專為虛擬環境而設計的。它可當作無代理程式、適用於 VMware NSX 和 VMware vCNS 的經調整選項，也可做為多平台選項，可部署在所有主要的 Hypervisor，包括 Microsoft Hyper-V、VMware、KVM 及 Xen。
- **McAfee Host Intrusion Prevention for Server**：透過監視您伺服器的程式碼行為並分析可疑活動的事件，保護企業不受複雜的安全威脅所攻擊。
- **McAfee Endpoint Security 防火牆**：監視網路和網際網路流量，並攔截可疑通訊。

## 資料工作表

McAfee Server Security Suite Advanced 可以強化來自 McAfee Global Threat Intelligence (McAfee GTI) 的全球信用評價情報，搭配來自 McAfee Threat Intelligence Exchange 的本機資料（個別銷售的附加模組），藉此立即辨識及對抗數量不斷增加的唯一惡意軟體樣本。使用套件中 McAfee Threat Intelligence Exchange 解決方案可與 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，並使各端點自動免受新近偵測到的惡意軟體侵襲。

McAfee 合作夥伴採用 Rapid7 來漏洞管理。Rapid7 的 Nexpose 解決方案可探索漏洞並排定其處理的優先順序，同時確認所暴露之弱點的修正時間。

### 將對效能的影響減至最低

雖然對大多數公司而言，安全為優先考量，但有些公司由於顧慮到效能方面的影響，而對於進行伺服器防護裹足不前。McAfee Server Security Suite Advanced 可以保護您的實體和虛擬伺服器，即使在掃描惡意軟體時，也能兼顧效能。

McAfee Endpoint Security 和 McAfee MOVE AntiVirus 與其他防惡意軟體產品不同，不會大量耗費運算資源。McAfee Endpoint Security 提供快速掃描，並將 CPU 和記憶體的使用最佳化；比起其他防惡意軟體產品，能提供更理想的防護。McAfee MOVE AntiVirus 分擔虛擬機器的惡意軟體掃描工作量，提供即時保護，而且對記憶體與處理僅有些微影響。常駐和隨選掃描的獨立原則提供更優異的效能周轉和安全控制。

### 最佳化您的伺服器安全、讓您的企業享有最佳績效

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、虛擬或是在雲端，我們都能提供解決方案套件，在不斷變遷的環境中，保持伺服器和雲端工作負載安全。

功能	您為什麼需要它
單一主控台管理	<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></ul>
即時探索與控制	<ul style="list-style-type: none"><li>探索實體伺服器並取得深入 VMware vSphere、OpenStack、AWS 和 Microsoft Azure 工作負載及平台的完整檢視。</li><li>確保您不但始終獲得安全保護,還能隨著動態雲端工作負載而彈性擴充。</li></ul>
虛擬化安全性	<ul style="list-style-type: none"><li>最佳化部署於虛擬基礎架構中之工作負荷的安全性,同時兼顧效能和資源使用率。</li><li>選擇多重平台 (所有主要 Hypervisor) 或適用於 VMware NSX 及 VMware vCNS 的無代理程式部署,以提供優異的效能和虛擬機器密度。</li></ul>
公有雲的安全性	<ul style="list-style-type: none"><li>適用於 AWS 和 Microsoft Azure 的稽核平台安全性,包括防火牆和加密設定。</li><li>確保針對 AWS 提供兼具流量與網路威脅能見性的完整防護。</li></ul>
應用程式白名單	<ul style="list-style-type: none"><li>大幅減少主機效能受到的影響,遠勝於傳統的伺服器安全性控制項。</li><li>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。</li><li>透過動態白名單,降低營運成本。</li></ul>
變更控制	<ul style="list-style-type: none"><li>可封鎖對重要系統檔案、目錄及組態的未經授權變更來防止竄改,藉此節省管理員花費在難排解安全性漏洞的時間。</li><li>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、來源或是允許的工作單來強制執行變更原則。</li></ul>
核心伺服器保護	<ul style="list-style-type: none"><li>執行防惡意軟體防護,抵禦零時差入侵和進階攻擊。</li><li>防禦複雜的安全性威脅,這些威脅可能是透過 McAfee Host Intrusion Prevention System 不慎引入或允許進入。</li></ul>
本機信譽評價情報	<ul style="list-style-type: none"><li>使用 McAfee Threat Intelligence Exchange (個別銷售的附加模組),在幾秒鐘內封鎖未知的零時差威脅。</li></ul>

## 深入瞭解

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>。



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 與 McAfee ePO 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. 2719\_0317  
2017 年 3 月