McAfee Cloud Workload Security

保護您的混合式基礎架構工作負載。更安全。更快速。更簡單。

隨著企業資料中心不斷演進，每天都有愈來愈多的工作負載遷移至雲端環境。大多數的組織建置了混合式環境，並具有包括容器等位於內部部署和雲端不斷變化的工作負載。而由於雲端環境 (包括公有和私有) 需要新的防護方法和工具，同時也帶來了新的安全性挑戰。組織需要集中掌控所有雲端工作負載，以全面防堵錯誤設定、惡意軟體和資料外洩的風險。

McAfee® Cloud Workload Security (McAfee® CWS) 會自動探索和保護彈性工作負載和容器，以消除盲點、提供進階威脅防禦，以及簡化多雲端管理作業。McAfee 提供出色防護功能，能透過單一自動處理的原則，有效確保工作負載在虛擬的私有、公共和多雲端環境中轉移時安全無虞，並且使網路安全性團隊得以順暢運作。

新型的工作負載安全性：使用案例

自動化探索

未受管理的工作負載例項和 Docker 容器會產生安全管理作業的缺口，提供攻擊者在滲透您的組織時所需要的據點。McAfee CWS 能探索 Amazon Web Services (AWS)、Microsoft Azure、OpenStack，以及 VMware 環境的彈性工作負載例項和 Docker 容器。而且還會持續監控新例項。您可以集中而完整地檢視整個環境，消除導致您暴露於風險當中的作業和安全盲點。

瞭解網路流量

McAfee CWS 可利用雲端工作負載提供的原生網路流量，藉此增強和應用來自 McAfee® Global Threat Intelligence (McAfee® GTI) 資料摘要的情報。豐富的資訊可以顯示風險評分、地理位置和其他重要網路資訊之類的屬性。此資訊可用於建立自動修補動作，以保護工作負載。

主要優點

- 自動處理原本需要耗費大量人力的原則部署，同時持續監控彈性工作負載例項，可消弭運作的「盲點」。
- 集中式管理和自動處理工作負載，能大幅降低混合雲和多雲端環境的複雜性。
- 無須安裝代理程式也能視覺化和發掘網路威脅。
- 由虛擬機器最佳化的威脅防禦機制，提供多層式對策。
- 與 Chef 和 Puppet 等自動處理工具整合，在部署時將安全性套用到公有和私有雲端工作負載。

與我們聯絡

整合至部署架構

McAfee CWS 會建立部署指令碼，將 McAfee® 代理程式自動部署到雲端工作負載並進行管理。這些指令碼允許其整合至 Chef、Puppet 和其他 DevOps 架構等工具中，以便將 McAfee 代理程式部署到由雲端供應商 (例如 AWS 和 Microsoft Azure) 執行的工作負載。

統合事件

McAfee CWS 允許組織使用單一介面來管理多項對策技術，無論是內部部署或是在雲端環境皆然。這也包括與 AWS GuardDuty、McAfee® Policy Auditor，以及 McAfee® Network Security Platform 等其他技術的整合。

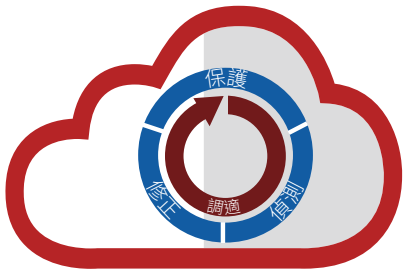
- 管理員可運用持續性監控功能和由 AWS GuardDuty 找到的未經授權之行為，提供全面的可見性。此整合可允許 McAfee CWS 客戶直接從 McAfee CWS 主控台檢視 GuardDuty事件，包括網路連線、連接埠探查以及針對EC2 例項的 DNS 要求。
- McAfee Policy Auditor 根據已知或使用者定義的組態稽核內容，執行代理程式型的檢查作業，確認其是否遵循 Health Insurance Portability and Accountability Act (HIPAA)、Payment Card Industry Data Security Standard (PCI-DSS)、Center for Internet Security Benchmark (CIS Benchmark) 或其他產業標準。McAfee CWS 對任何失敗的稽核作業都會進行報告，以便即時查看雲端中工作負載的錯誤設定。
- McAfee Network Security Platform 是另一個雲端安全平台，可對混合式環境以及 AWS 和 Microsoft Azure 環境中的流量執行網路檢查。它會對網路流量執行更深層的封包檢查，並透過 McAfee CWS 報告任何差異或警報。這樣一來，透過單一窗格即可掌握多雲端環境，以便進行修補。

強制執行網路安全性群組原則

McAfee CWS 允許使用者和管理員建立基準安全性群組原則，並根據這些基準，對在工作負載上執行的原則進行稽核。任何基準的偏差或變更都可以在 McAfee CWS 主控台建立警示以進行修補。管理員也可以在 McAfee CWS 手動設定原生網路安全性群組，讓他們能夠直接控制雲端原生安全性群組原則。

主要優勢 (續)

- 以易於使用的多層級防護功能，抵禦進階惡意軟體和入侵行動。
- 探索與監控 Docker 容器，並使用微分段功能來確保其安全。
- 從解決方案中直接採取修正行動來保護環境安全。



Cloud Workload Security

全方位的**可見性**
與**控制能力**

與眾不同的 McAfee Cloud Workload Security：主要功能與技術

雲端原生組建支援

客戶使用 McAfee CWS，即可在單一管理主控台中整合管理多個公有雲和私有雲，包括 AWS EC2、Microsoft Azure 虛擬機器、OpenStack 和 VMware Vcenter。McAfee CWS 可透過 Amazon Elastic Container Service for Kubernetes (Amazon EKS) 和 Microsoft Azure Kubernetes Service (AKS) 的全新雲端原生組建支援來匯入客戶，並允許客戶在雲端中執行作業。

簡單的集中式管理

單一主控台可在跨越伺服器、虛擬伺服器和雲端工作負載的多雲端環境中，提供一致的安全性原則和集中式管理。管理員也可以在 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體中建立多個以角色為基礎的權限，讓他們能夠更具體、更恰當地定義使用者角色。

具微分段功能的網路視覺化

雲端原生網路管理視覺化、區分優先順序的風險警示和微分段功能可帶來感知和控管能力，防止虛擬環境發生橫向攻擊並防範外部惡意資源。一鍵關閉或隔離功能有助於降低設定錯誤的可能性，並提高修補效率。

優異的虛擬化安全性

McAfee CWS 套件使用 McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus)，妥善保護您的私有雲虛擬機器免於遭受惡意軟體威脅。既不會耗盡基礎資源，也不會增加額外的作業成本。McAfee MOVE AntiVirus 允許組織將安全性卸載到專用的虛擬機器，以最佳化其虛擬化環境的掃描作業。

使用者透過 McAfee® Endpoint Security for Servers 獲得防惡意軟體保護。此解決方案會聰明地排程資源密集的任務 (例如按指定掃描)，以避免對關鍵業務流程產生影響。

標記與自動化工作負載安全性

自動為所有工作負載指派適當原則，亦即將 AWS 和 Microsoft Azure 標記資訊匯入 McAfee ePO 軟體，並根據這些標記指派原則。現有的 AWS 和 Microsoft Azure 標記會與 McAfee ePO 軟體標記同步，進而實現管理作業自動化。

自動修補

使用者會定義 McAfee ePO 軟體原則。如果 McAfee CWS 發現系統未受 McAfee ePO 軟體安全性原則保護，並且發現其中包含惡意軟體或病毒，將自動隔離此系統。

適應性威脅防護

McAfee CWS 整合全方位的對策，包括機器學習、應用程式遏止、虛擬機器最佳化的防惡意軟體、白名單、檔案完整性監控和微分段的整合對策，可保護工作負載，預防勒索軟體和目標式攻擊等威脅。McAfee® Advanced Threat Protection 採用機器學習技術，並根據程式碼屬性和行為來判定惡意承載，足以抵禦前所未見的複雜攻擊。

應用程式控制

應用程式白名單僅允許執行受信任的應用程式，同時封鎖未經授權的承載，藉此防範已知和未知的攻擊。McAfee® Application Control 根據當地與全球威脅情報來提供動態防護，並確保系統處於最新狀態，而無需停用安全性功能。

檔案完整性監視 (FIM)

McAfee® 檔案完整性監視可持續監控，確保您的系統檔案和目錄不會遭到惡意軟體、駭客或惡意內部人員的入侵。全方位的稽核詳細資料可提供有關伺服器工作負載之檔案變化情況的相關資訊，並提醒您主動式攻擊的存在。

適用於多雲端環境的安全涵蓋範圍

McAfee CWS 可確保您在充分運用雲端優勢的同時，還能維持最高品質的安全性。本產品涵蓋多種防護技術、簡化安全管理作業，並防止網路威脅影響您的企業營運，讓您可以放心拓展商業版圖。以下是可用套件選項的功能比較。

資料工作表

特色	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
集中式管理 (McAfee ePO 平台)	✓	✓	✓
多雲端支援 (AWS、Microsoft Azure、VMware)	✓	✓	✓
使用微分段功能來隔離工作負載和容器	✓	✓	✓
McAfee MOVE (無代理程式及多平台)	✓	✓	✓
適用於伺服器作業系統 (Windows 和 Linux) 的 McAfee Endpoint Security 威脅防護	✓	✓	✓
主機型防火牆	✓	✓	✓
適用於 AWS 和 Microsoft Azure (安全性群組) 的原生防火牆管理	✓	✓	✓
主機入侵和入侵防護	✓	✓	✓
將 AWS 和 Microsoft Azure 標記資訊匯入 McAfee ePO 軟體	✓	✓	✓
自動修補不符合規範的工作負載	✓	✓	✓
利用機器學習技術的適應性威脅保護		✓	✓
網路流量視覺化和微分段功能		✓	✓
雲端原生網路流量分析結合 McAfee GTI 信用評價分數		✓	✓
McAfee® Virtual Network Security Platform (McAfee® vNSP) 整合		✓	✓
透過 McAfee Application Control，動態建立伺服器的白名單。			✓
透過 McAfee 檔案完整性監視持續進行稽核記錄			✓
透過 McAfee® Change Control for Servers 保護檔案和資料夾			✓

深入瞭解

如需詳細資訊，請造訪：
https://www.mcafee.com/zh-tw/products/cloud-workload-security.aspx.

McAfee Together is power.

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