McAfee Cloud Workload Security

保護私有雲和公有雲工作負載的安全。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 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 提供無與倫比的防護，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、公共和混合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。

即時可見性

自動化探索

隱密的工作負載例項和 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 Cloud Workload Security 能探索 Amazon Web Services (AWS)、Microsoft Azure 及 Vmware 環境的彈性工作負載例項和 Docker 容器，並持續監控新例項。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。

新型的工作負載安全性

進階威脅防護

McAfee Cloud Workload Security 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。進階威脅防護包括機器學習，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。

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」。
- 探索與監控 Docker 容器，並使用微分段功能來確保其安全。
- 由虛擬機器最佳化的威脅防禦機制提供多層式對策。
- 集中式管理和自動處理工作流程能大幅降低混合雲和多雲端環境的複雜性。
- 與 Chef 和 Puppet 之類的自動處理工具整合，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

統合事件

McAfee Cloud Workload Security 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。這也包括協力廠商技術，例如 AWS GuardDuty。管理員可運用持續性監控和 AWS GuardDuty 找到的未經授權的行為，提供另一層次的可見性。此整合可允許 McAfee Cloud Workload Security 客戶直接從 McAfee Cloud Workload Security 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。當流量對應至由 McAfee Cloud Workload Security 探索到的流量時，GuardDuty 網路連線事件可對應至流量圖表。

優異的虛擬化安全性

McAfee Cloud Workload Security 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。您可以獲得防惡意軟體保護，在 Hypervisor 不會超載狀況下，針對耗用大量資源的工作 (例如按指定掃描) 進行智慧型排程。

具微分段功能的網路管理視覺化

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，並提高修補的效率。

檔案完整性監視 (FIM)

FIM 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。全面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。

應用程式控制

藉由僅允許執行受信任的應用程式，同時封鎖未經授權的承載，應用程式白名單得以防範已知和未知的攻擊。應用程式控制根據當地與全球威脅情報來提供動態防護，並能保持系統處於最新狀態，因此無須停用安全性功能。

簡化管理

透過集中式管理實現一致性

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。

自動處理部署

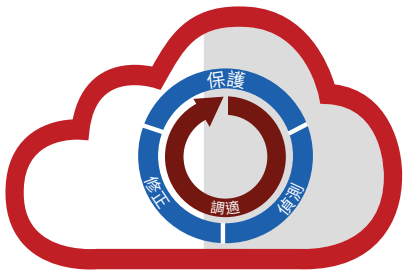
藉由支援來自組織的部署自動化工具 (如 Chef、Puppet 和 Ansible)，您可以在多個雲端環境中自動部署安全性技術。

改善的安全性涵蓋範圍

McAfee Cloud Workload Security 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。

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。
- 無須安裝代理程式也能視覺化和發掘網路威脅。
- 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**

資料工作表

功能	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
集中式管理 (McAfee® ePO™ 平台)	✓	✓	✓
多雲端支援 (AWS、Azure、VMware)	✓	✓	✓
使用微分段功能來隔離工作負載和容器	✓	✓	✓
適用於伺服器作業系統 (Windows 和 Linux) 的威脅防護機制	✓	✓	✓
主機入侵和入侵防護	✓	✓	✓
雲端加密管理	✓	✓	✓
適用於 AWS 和 Azure (安全性群組) 的原生防火牆管理	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (無代理程式和多平台)	✓	✓	✓
主機型防火牆	✓	✓	✓
利用機器學習的適應性威脅保護		✓	✓
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 Global Threat Intelligence 信用評價分數		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
McAfee® Virtual Network Security Platform 整合		✓	✓

深入瞭解

如需詳細資訊，請造訪：**https://www.mcafee.com/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