資料工作表

McAfee Public Cloud Server Security Suite

為 AWS 和 Azure 雲端工作負載提供全方位的安全保護

主要優點

- 專為 AWS 和 Azure 工作負載設計。
- 即時探索。
- 安全性評估和威脅修復。
- 可彈性調整的安全性。
- 全方位的保護。
- 利用 McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理主控台。
- 多樣部署選項，包括 Chef、Puppet 及 OpsWorks。
- 具有法規遵循能力。
- 整合其他 Intel Security 解決方案。

正當各大企業為了納入公有雲伺服器例項 (而且經常以此為領導) 而轉變自家的資料中心策略之際，他們也留意到，採用共享責任機制[1]以提供保護是相當重要的考量要素。Amazon Web Services (AWS) 和 Microsoft Azure 之類的公有雲提供者會確保其周邊的安全性，而使用者則必須自行保護內容。但是眼光遠大的企業該如何在保護雲端工作負載不受零時差和進階持續性威脅 (APT) 的影響同時，讓成本保持在其雲端策略的預算範圍內呢？企業採用雲端後，可能會遇到的一些重大難題：

- 零時差和進階威脅越來越難防範。
- 在擁有多個雲端基礎架構的情況下，無法監看環境狀態及從中央集中管理，使得執行安全性作業異常艱困。
- 雲端工作負載安全性會帶來效能下降的隱憂。

McAfee® Public Cloud Server Security Suite 可讓您即時探索及控制 AWS 和 Azure 工作負載和威脅，以持續提供完整且一致的保護，同時將效能影響降到最低。您可以探索數個雲端資料中心、雲端帳戶、虛擬機器及新興的威脅。

McAfee Public Cloud Server Security Suite 提供全方位的安全保護，內含基礎防毒、入侵防禦及進階白名單，可以保護環境不受零時差威脅攻擊，更改控制設定以符合相關法規遵循需求，以及管理加密方式以保護資料。單一管理主控台可讓您輕鬆管理數個雲端及強制執行原則。彈性靈活的部署選項 (包括 Chef、Puppet 及 OpsWorks DevOps 工具)，可讓您進行無縫作業，同時將影響降到最低。

圖 1. 單一管理主控台採用數種 Intel Security 技術，可管理數個雲端基礎架構。

intel Security

支援的平台

- Windows Server 2008、2008 R2、2012、2012 R2
- Linux (Red Hat、CentOS、SUSE、Ubuntu、Amazon Linux)

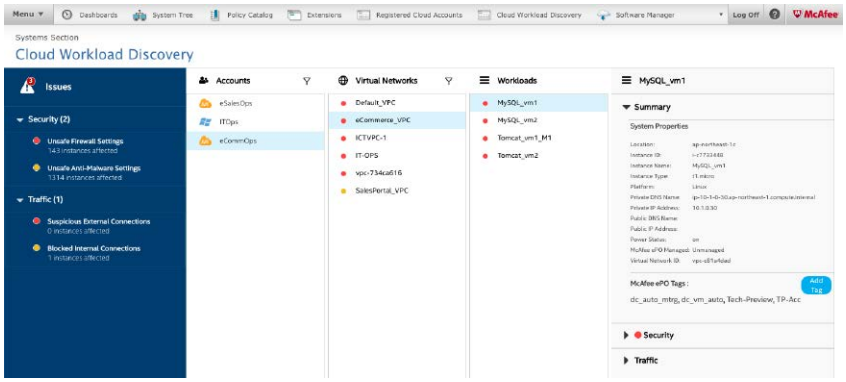

圖 2. 探索及監視數個雲端基礎架構和新興的威脅。

探索雲端基礎架構和威脅

若想加強控制雲端基礎架構和威脅，您必須提高監控能力。

- 在短短幾分鐘之內，探索 AWS 和 Azure 雲端基礎架構中所有虛擬網路或虛擬私有雲 (VPC)、範本及工作負載。要確實保護好雲端基礎架構的第一步，便是可以深入瞭解有關雲端基礎架構帳戶的詳細資訊，分辨使用者的雲端基礎架構權限，熟悉指派給範本和 VPC 的工作負載，以及快速掌握與雲端基礎架構相關聯的系統樹狀目錄。
- 從單一位置集中監控數個雲端的安全性。利用端對端威脅資訊 (包括攻擊來源)，提升安全性控制能力。
- 檢視工作負載間的流量，管理工作負載間的資訊如何流動，以及如何從組織外存取這些資訊。

監視雲端，依照安全性警告加快並採取適當行動

由於加快修補作業近年逐漸成為防禦關鍵，有了此解決方案之後，您便可以快速進行安全性問題深度評估，立即採取採取適當行動。

- 識別需要即時關注的問題，並使用顏色編碼威脅，採取適當的行動。
- 建立自訂標籤，並根據您特有的需求，將標籤指派給工作負載。
- 運用更正方法減少安全性問題，並以採用原則或定義威脅信用評價的方式，保護基礎架構日後不受安全性事件影響。
- 運用自訂的個人工作負載或群組工作負載原則，管理雲端防火牆。管理 AWS 安全群組原則，控制單一或多重例項流量。
- 識別 VPC 中出現的可疑流量，採取修補步驟以避免重要資訊落入有心人之手

全方位威脅保護

McAfee Public Cloud Server Security Suite 利用單一代理程式提供多層的安全性，方便您在數個雲端平台上，使用單一管理主控台進行管理。此解決方案也可搭配部署 DevOps 支援工具，以提供最佳的防禦體驗。

若要深入瞭解

請造訪產品頁面：**http://www.mcafee.com/tw/products/public-cloud-server-security-suite.aspx**。

您也可前往 **AWS Marketplace** 購買。

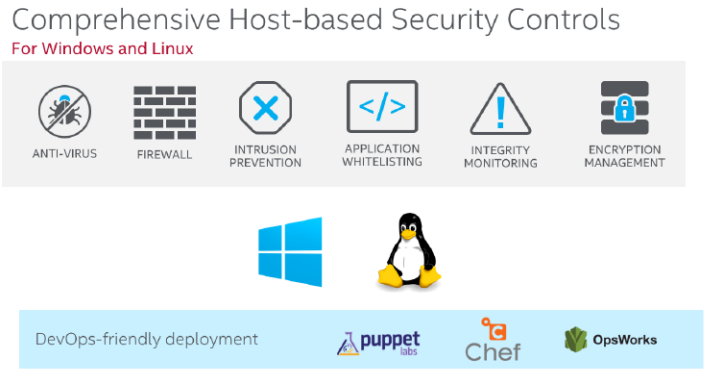

圖 3. 為公有雲端工作負載提供全方位的安全保護

功能	優點
Chef、Puppet 及 AWS OpsWorks 部署選項	• DevOps 部署工具可讓您及早做好安全性考量，且部署方式極為簡單。 • 您可以將安全機制內建為作業系統的一部分。
雲端工作負載探索	• 即時監控雲端基礎架構，探索虛擬資料中心、雲端工作負載及雲端防火牆。 • 具備安全性狀態評估的快速威脅警示通知。 • 藉由依威脅關鍵性排定優先順序的警示，以及快速針對警示採取行動的步驟，更快速修補威脅。
適用於多個雲端基礎架構安全性解決方案的單一管理主控台 (McAfee ePO 軟體)	• 對混合環境設定極其有利。 • 單一窗格即可管理實體、虛擬與雲端工作負載與原則。 • 整合 Intel Security 與合作夥伴的雲端與內部部署安全性技術 • 透過整合的安全性程序與快速解決方案步驟，降低整體擁有成本
防惡意軟體	• 最有效的惡意軟體防護。保護系統與檔案，免受病毒、間諜軟體、蠕蟲、特洛伊木馬程式及其他安全性風險的危害。它可偵測出惡意軟體並加以清除，並讓使用者輕鬆設定原則來管理隔離的項目。
主機防火牆	• 保護工作負載，避免未經授權的存取與攻擊。
主機入侵防禦	• 可以使用取得專利權且屢獲獎賞的技術，封鎖不需要或有害的網路流量，並主動封鎖零時差與已知攻擊。 • 透過限制對指定連接埠、檔案、共用資源、登錄機碼和登錄值的存取，防止對工作負載進行不需要的變更。 • 將資料寫入緩衝區時，記憶體保護可避免異常程式或威脅滿溢緩衝區的邊界，並覆寫鄰近的記憶體。遭到入侵的緩衝區溢位可以在您的電腦上執行任意程式碼。
應用程式白名單	• 無需更新特徵碼即可抵禦零時差與進階持續性威脅。 • 動態白名單可強化安全性及降低擁有成本，還能自動接受透過受信任通道所新增的軟體。 • 安全的應用程式白名單與先進的記憶體保護可縮短修補週期。
檔案完整性監視	• 可持續偵測不同分佈地點與遠端地點的系統層級變更。 • 封鎖對關鍵系統檔案、目錄及組態進行的未經授權變更，藉此避免任意變更。 • 即時追蹤並驗證工作負載上每一個試圖進行的變更，根據時間區段、來源或是核准的工作票證來強制執行變更原則。
加密管理	• 透過 AWS Advanced Encryption Standard (AES)，加密儲存於 AWS EBS 磁碟區的資料。 • 亦可輕鬆地加密原本即含有資料的磁碟區。 • 整合 Amazon 的 Key Management Service (KMS) 進行加密。

1. http://www.mcafee.com/tw/resources/white-papers/wp-cloud-security-primer-techtarget.pdf

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