McAfee Virtual Network Security Platform

完整的雲端網路威脅偵測與入侵預防機制

McAfee® Virtual Network Security Platform (McAfee® vNSP) 是完整的網路威脅偵測與入侵預防系統 (IPS)，專為私有雲與公有雲的獨特需求而打造。這套解決方案以準確簡單的方式，快速找出雲端基礎架構中的複雜威脅並加以封鎖，讓組織能安心保護工作負載，恢復到符合法規的狀態。採用的先進技術包含無特徵碼偵測、內置模擬及特徵碼式漏洞修補。精簡的工作流程支援自動縮放、彈性的整合選項以及簡化的授權方式，讓組織得以根據現有和未來的需求，輕鬆管理及調整自家的安全防護機制。

全方位的公有雲安全性

公有雲帶來的便利性與節省成本特性，讓客戶有機會將基礎架構開支轉變為營運支出模式。但這也引進了全新層次的風險，因為存在於可公開存取軟體內的漏洞，可能會讓攻擊者得以入侵雲端，造成敏感資訊外洩；或是不小心將客戶資料暴露給使用同一服務的其他租用戶。McAfee Virtual Network Security Platform 支援 Amazon Web Services (AWS)、Microsoft Azure 和 Oracle Cloud Infrastructure (OCI) 等現今主流的公有雲服務，能鎖定通過網際網路閘道或在伺服器間進出 (東西向流量) 的資料全面掌握威脅，並提供周全防護。

保障虛擬化環境的安全

企業採用虛擬化 IT 基礎架構 (例如私有雲和公有雲) 已是一種快速成長的趨勢，而其中所用的實體伺服器可能同時主控多個虛擬機器 (VM) 與虛擬化工作負載。隨之而來的 VM 間通訊，以及這些工作負載的即時遷移、複製和備份，都使私有雲與公有雲及軟體定義資料中心 (SDDC) 內的東西向流量急遽增加。讓這個混沌局面更加雪上加霜的是，由網路虛擬化所帶來的彈性導致已然驟增的流量更加活躍且難以預測。為了掌握這個局勢，虛擬化安全性解決方案必須兼具彈性與可擴充性，而且更重要的是，必須能在軟體定義網路 (SDN) 平台流暢運作，協調這些通常壽命短暫的虛擬機器與工作負載。

主要優點

- 專為私有雲與公有雲 (AWS、Azure 和 OCI) 打造的全方位防護機制
- 內置 IPS/入侵偵測系統 (IDS) 操作模式
- 滴水不漏的東西向流量防護
- 統一政策和管理工作流程
- 有效防禦已知和未知威脅的先進偵測技術
- 可確保效能的高可用性、嚴重損壞復原和負載平衡功能
- 為私有雲和公有雲提供彈性的雲端授權共用機制
- 與 McAfee 產品組合相互整合，確保裝置到雲端的安全性
- 可從 AWS Marketplace 取得
- 可從 Azure Marketplace 取得

與我們聯絡

私有雲的靈活度

McAfee Virtual Network Security Platform 可做為虛擬設備部署在 VMware ESX 伺服器上，保護私有雲基礎架構中的虛擬網路。作為 Open Virtualization Format (OVF) 映像，虛擬設備可協助檢查特定 ESX 主機上的 VM 之間的流量以及不同 ESX 主機和實體網路之間的流量

進階威脅防禦

McAfee Virtual Network Security Platform 是以新一代檢查架構為基礎，旨在針對虛擬網路流量進行深層檢查。此產品結合多種進階檢查技術，包括完整的通訊協定分析、威脅信用評價、行為分析及進階惡意軟體分析，藉此偵測並防範網路上已知的攻擊和未知的零時差攻擊。

沒有任何一種惡意軟體偵測技術足以抵禦所有的攻擊，因此 McAfee Virtual Network Security Platform 將多個特徵碼及無特徵碼的偵測引擎分層，藉以協助阻止不請自來的惡意軟體大肆破壞您的雲端空間。這採用多種偵測技術，包含內置模擬瀏覽器、JavaScript、Adobe 檔案、殭屍網路、惡意軟體回呼偵測、行為式分散式阻絕服務 (DDoS) 偵測，以及對進階跨站台指令碼與 SQL 植入攻擊的抵禦機制。

McAfee Virtual Network Security Platform 還能與 McAfee® Advanced Threat Defense 整合，將所有檔案送交進行深層行為分析，因而能夠找出潛伏最深的檔案，並加以封鎖。McAfee Advanced Threat Defense 結合深層靜態程式碼分析、動態分析 (惡意軟體沙箱作業) 及機器學習，增強零時差威脅偵測，防禦利用規避技術和勒索軟體的各種威脅。McAfee 也針對 Snort 特徵碼提供原生支援，以利偵測及防禦惡意軟體。

彈性的雲端授權共用

為了支援舊版應用程式、降低對單一廠商的依賴、提升系統備援程度及節省成本，企業組織通常會將 IT 資源與基礎架構分散在多個雲端和平台上。取得虛擬化環境適用的安全性解決方案授權，往往既複雜又所費不貲，因為各大廠商大多要求客戶分別為私有雲和公有雲個別購買授權。

McAfee 透過雲端授權共用機制簡化授權作業並降低成本，組織無論採用何種公有雲與私有雲平台組合，都能共用自有的 McAfee Virtual Network Security Platform 授權。雲端授權共用機制可提供彈性並提升安全性，因為管理員可針對分散各處的虛擬工作負載，迅速提供東西向流量防護和微分段功能，不必辛苦經歷複雜的授權程序和費時的採購過程。

簡化的工作流程和分析

現今的威脅往往會引致大量的警示，其速度之快可能超過資安管理人員能力範疇，而難以排定優先順序並加以追蹤。若反應速度太慢，真正的威脅可能會因此躲過偵測而不被發現。McAfee Virtual Network Security Platform 包含進階分析功能和可行的工作流程，能將多個 IPS 警示建立關聯，整合成單一可行的事件，協助管理員迅速掌握相關資訊。此外，更與 McAfee 安全性解決方案整合，打造出真正全方位且相互連結的網路威脅偵測與緩解平台。

統一政策和管理工作流程

McAfee® Network Security Manager 可部署為 VMware ESX 伺服器和 AWS/Azure/OCI 環境中的虛擬例項。當工作負載會轉向雲端平台之時，這可協助安全管理員在混合資料中心之間一致地擴展內部部署安全設定檔，並使用統一管理主控台和工作流程進行管理。McAfee Virtual Network Security Platform 支援 AWS Identity and Access Management (IAM)，讓管理員能根據指派給特定使用者與群組的權限，輕鬆且安全地管理 AWS 服務與資源的存取權。

高可用性、嚴重損壞復原和負載平衡

McAfee Virtual Network Security Platform 透過多種方式自動提供不間斷的控制能力、防護及效能。McAfee Network Security Manager 可主動監控環境，提供高可用性。例如，新的控制器例項會在活躍的控制器變為不可用時啟動。此外，待命的 McAfee Network Security Manager 還可部署於 AWS、Azure 和 OCI環境，提供嚴重損壞復原功能。

McAfee Virtual Network Security Platform 還為 IPS 偵測器提供高可用性。如果偵測器無法使用，自動調整功能會自動建立新的虛擬 IPS 偵測器，藉此提供不間斷的完善防護。此外，如果網路流量增加，偵測器之間的自動負載平衡可確保效能最佳化，且為了達到所需的輸送量效能，系統還會自動部署額外的偵測器。

整合式安全性

縝密型攻擊不會區分產品界線，而會快速利用基礎架構上的任何缺口侵入，尤其是安全性產品之間的弱點。McAfee Virtual Network Security Platform 是唯一無縫整合多種安全性產品的 IPS，可充分利用不同解決方案的資料和工作流程以提供卓越安全性和防護，並提高投資報酬率。McAfee 安全性解決方案整合的範例包含：

- **McAfee® ePolicy Orchestrator® (McAfee ePO™)：**全盤掌握端點的所有 IPS 事件和警示
- **McAfee® Endpoint Intelligence Agent：**結合網路與端點透視，以防止資料外洩
- **McAfee® Enterprise Security Manager：**針對 IPS 警示提供豐富的資料共用和 IPS 隔離機制

- **McAfee® Threat Intelligence Exchange：**共用不同類型裝置的學習成果
- **McAfee® Global Threat Intelligence：**全球最大型也最活躍的信用評價服務
- **McAfee® Network Threat Behavior Analysis：**將掌握範圍延伸至整個網路
- **McAfee® Virtual Advanced Threat Defense：**提供深層檢查以偵測規避性威脅
- **McAfee® Management for Optimized Virtual Environments (McAfee® MOVE)：**適用於虛擬環境的防毒解決方案
- **協力廠商漏洞掃描程式：**適用於端點的主機和風險分析

其他功能

進階威脅防禦

- 進階惡意軟體防護
- 原生輸入 SSL 檢查
- Microsoft Office 深層檔案檢查
- PDF JavaScript 模擬引擎 (輕量級沙箱)
- Adobe Flash 行為分析引擎
- 進階規避防護

殭屍網路和惡意軟體回呼保護

- 網域名稱伺服器 (DNS)/網域產生演算法 (DGA)/快速變動網域回呼偵測
- DNS 沉洞技術
- 啟發式殭屍病毒 (Bot) 偵測
- 多重攻擊關聯
- 命令與控制資料庫

進階入侵防禦功能

- IP 重組與 TCP 資料流重組
- McAfee、使用者定義、開放原始碼等各種特徵碼
- 主機隔離及速率限制
- 虛擬環境檢查
- 阻絕服務 (DoS) 及分散式阻絕服務 (DDoS) 防護
- 支援 Structured Threat Information eXpression (STIX) 中的黑/白名單
- 閾值與啟發式偵測
- 主機式連線限制
- 針對 Snort 特徵碼提供原生支援
- 以設定檔為基礎的自我學習型偵測

McAfee Global Threat Intelligence

- 檔案信用評價
- IP 信用評價
- URL/網域信用評價
- 以地理位置為基礎使存取權受限
- IP 位址型存取控制

資料工作表

	偵測器類型 1	偵測器類型 2
平台	VMware ESX	AWS Azure OCI
虛擬 IPS 偵測器機型	**IPS-VM600**	**IPS-VM600-VSS**
虛擬 IPS 部署類型	獨立式	分散式
AWS 支援	否	是
Azure 支援	否	是
OCI 支援	否	是
邏輯 CPU 數目	4	4
所需記憶體	8 GB	8 GB
儲存空間	40 GB	40 GB
虛擬偵測器規格		
最高輸送量	最高 1 Gbps	最高 1 Gbps
監視埠配對數目	3	1 (監視埠，非埠配對)
每台偵測器虛擬介面 (VIDS)	100	100
DoS 設定檔	300	300
管理連接埠	是	是
回應連接埠	否	否
部署模式	虛擬機器間的檢查、實體到虛擬機器間的檢查、實體到實體機器間的檢查、SPAN/內置埠檢查	

深入了解

- 保護您的 Amazon Web Services 虛擬網路
- 保護您的 Microsoft Azure 虛擬網路

McAfee 技術的特色和優勢將因系統設定而有所不同，並且可能需要啟用軟硬體或啟動服務。若需深入了解，請前往 mcafee.com/tw。任何網路皆非絕對安全。

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

2021 年 1 月