資料工作表

Trellix Virtual Network Security Platform

完整的雲端網路威脅偵測機制

Trellix Virtual Network Security Platform 是完整的網路威脅與入侵預防系統 (IPS) 解決方案，專為私有雲與公有雲的獨特需求而打造。其可準確俐落地探索並封鎖雲端架構中的複雜威脅，使組織能回復符合性，並安心地採用雲端安全技術。進階技術包括了無特徵碼偵測、內置模擬、特徵碼式漏洞修補，以及對 Amazon Web Services (AWS) 和網路虛擬化的支援。透過簡化的工作流程、多種整合選項以及簡化的授權方式，組織得以在最複雜的雲端架構中輕鬆管理並調整自己的安全防護機制。

以進階安全性技術達到完整的公有雲安全性

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。Trellix Virtual Network Security Platform 支援 AWS——現今的主流公有雲服務，能針對通過網際網路閘道以及進入橫向流量的資料提供完整的威脅可見性。有了此產品，您便可透過能真正檢查橫向流量的入侵預防系統 (IPS) 平台，回復公有雲架構中的威脅可見性和安全性符合性。

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，而其中的實體伺服器可能同時主控多個虛擬機器 (VM)，甚至是整體的虛擬化工作負載。因此產生的 VM 間通訊，連同這些工作負載的即時遷移、複製和備份，合而為私有雲與公有雲以及 SDDC 內急遽增加的

主要優點

無可比擬的進階威脅防護

- 無特徵碼進階惡意軟體分析。
- 抵禦跨站台指令碼與 SQL 植入攻擊。
- 進階殭屍網路回呼與惡意軟體偵測。
- 行為式分析及分散式阻絕服務 (DDoS) 保護。
- 與 Trellix Advanced Threat Defense 整合。
- IPS 與入侵偵測系統 (IDS) 部署。
- 全天候 VMware ESX-Trellix Virtual Network Security Platform 解決方案。

雲端就緒架構

- 一份授權即可讓客戶跨越任意組合的公有雲與私有雲共用輸送量。

橫向流量。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。

提高私有雲的靈活度

為符合確保虛擬化環境安全性的需求，Trellix Virtual Network Security Platform 無縫整合了各種熱門的私有雲平台，包括 VMware NSX 和 OpenStack SDN 環境。事實上，Trellix Virtual Network Security Platform 是唯一專門設計且經認證能與 VMware NSX 相容的虛擬 IPS 解決方案。它能在虛擬化環境中自動維持 VM 的微分段以及針對橫向流量的深層檢查功能；甚至在工作負載迅速產生、遷移及停用的環境中，依然能維持其運作。

無與倫比的威脅防護

Trellix 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。此產品結合了多種進階檢查技術，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 Trellix 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。它提供了多種偵測技術，例如內置模擬瀏覽器、JavaScript 及 Adobe 檔案、殭屍網路與惡意軟體回呼偵測、行為式 DDoS 偵測，以及對進階攻擊 (如：跨站台指令碼與 SQL 植入攻擊) 的防護。Trellix Virtual Network Security Platform 還能與 Trellix 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。Trellix Advanced Threat Defense 結合了深層靜態程式碼分析、動態分析 (惡意軟體沙箱作業) 與機器學習，可增強零時差威脅偵測，包括利用規避技術和勒索軟體的威脅。

以雲端授權共用簡化授權作業

時至今日，不論是為了支援舊版應用程式、降低對單一廠商的依賴、系統備援度，或是為了節省成本，許多企業都將他們的 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，因為大多數的廠商需要購買各個私有雲和公有雲以及不同 SDN 平台的個別授權。

Trellix 透過雲端授權共用簡化授權作業並降低成本，這個雲端共用的新概念讓客戶得以跨越任意組合的公有雲與私有雲端平台，共用自己的 Trellix Virtual Network Security Platform 輸送量和授權。雲端授權共用還能提升安全性，因為管理員可針對位於各處的虛擬工作負載，迅速提供橫向流量防護和微分段功能，而不必辛苦經歷費時的採購過程。

- 創新的 AWS 檢查方法可在公有雲中提供橫向流量防護。
- 支援 VMware NSX 與 OpenStack SDN 環境之間的協調，以利私有雲工作負載間自動進行微分段與流量檢查。
- 與 VMware 整合後具備含隔離強制功能的 VM 感知儀表板。
- 不論是內部部署或雲端中，實體和虛擬偵測器皆適用的單一集中式管理主控台。

智慧型安全性管理

- 透過單一主控台管理內部部署和雲端偵測器。
- 智慧型警示關聯及優先順序。
- 強大的惡意軟體調查儀表板。
- 預先設定的調查工作流程。
- 可擴充的網頁式管理。

可見性及控制

- 應用程式識別。
- 使用者識別。
- 裝置識別。
- AWS 中所有 VM 的安全性狀態。

簡化工作流程和分析

輕輕鬆鬆就能探索並封鎖最複雜的威脅。Trellix Virtual Network Security Platform 內含先進的分析功能，並整合額外安全性解決方案，打造出一個真正全面性且相互連結的網路威脅偵測與緩解平台。

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。如果無法及時勾勒出全貌，真正的威脅就可能因此躲過偵測而不被發現。Trellix Virtual Network Security Platform 立即可用的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，協助管理員迅速釐清思路，找出相關的可行資訊。

即時掌控即時資料以集中管理

單一 Trellix Virtual Network Security Manager 裝置不僅提供集中式 Web 型管理，在使用方便性上更是無可比擬。最新的主控台與強化的圖形化使用者介面，可讓您充分掌控即時資料。您可以透過單一主控台輕鬆管理、設定及監控橫跨傳統、私有雲及公有雲資源的 Trellix Network Security Platform 虛擬或實體裝置，以及 Trellix Network Threat Behavior Analysis 裝置。直覺式 Web 型管理介面可處理任何部署狀況，從單一裝置到廣泛分佈的業務關鍵叢集都沒問題。Trellix Network Security Manager 也可部署為 VMware ESX 伺服器上和 AWS 中的虛擬例項。

高可用性與嚴重損壞復原

Trellix Network Security Manager 可在控制站間協調，決定要將哪個控制站設為啟用或待命。當使用中的控制站變為無法使用，則待命的控制站會轉為啟用。在這種情況下，AWS 部署可獲得控制站高可用性 (HA)，提供的容錯移轉機制中，一個控制站會隨時處於運作中及可連線狀態。此外，待命的 Trellix Network Security Manager 還為 AWS 環境提供了嚴重損壞復原功能。

Trellix Virtual Network Security Platform 憑藉 Manager 嚴重損壞復原 (MDR)、控制站高可用性 (HA) 以及虛擬 IPS 偵測器的自動擴充功能，帶來了高度可用性。這使 Trellix Virtual Network Security Platform 能夠順暢運作而不中斷。MDR 解決方案提供了次要 Manager，可在主要 Manager 關閉時負責接管。在控制站 HA 配對中，其中一個控制站會隨時處於運作中及可連線狀態，因此網路不會中斷。虛擬 IPS 偵測器的自動擴充功能會在偵測器的例項關閉時，建立新的虛擬 IPS 偵測器。如此一來可在網路流量增加時執行負載平衡功能。

統一防禦架構

縝密型攻擊不會區分產品界線，而是會利用基礎架構上的任何缺口，尤其是安全性產品之間的缺口。Trellix Virtual Network Security Platform 是唯一整合不同安全性產品的 IPS，充分利用資料和工作流程來填補這些缺口，進而提

高投資報酬率，並降低整體擁有成本。其他整合的安全性產品包括：

- **Trellix ePolicy Orchestrator® (Trellix ePO™) 軟體：**全盤掌握端點的所有 IPS 事件和警示。
- **Trellix Endpoint Intelligence Agent：**結合網路與端點透視，以防止資料外洩。
- **Trellix Enterprise Security Manager：**針對 IPS 警示提供豐富的資料共用和 IPS 隔離機制。
- **Trellix Threat Intelligence Exchange：**共用不同類型裝置的學習結果。
- **Trellix Global Threat Intelligence：**全球最大型也最主動的信用評價服務。
- **Trellix Network Threat Behavior Analysis：**將可見性延伸至整個網路。
- **Trellix Virtual Advanced Threat Defense**
- **Trellix Cloud Threat Detection**
- **Trellix Management for Optimized Virtual Environments (Trellix MOVE)**
- **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

進階威脅防護

- Trellix Gateway Anti-Malware 模擬引擎。
- PDF JavaScript 模擬引擎 (輕量級沙箱)。
- Adobe Flash 行為分析引擎。
- 進階規避保護。

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) Fast Flux 回呼偵測。
- DNS Sinkholing。
- 啟發式殭屍病毒偵測。
- 多重攻擊關聯。
- 命令與控制資料庫。

進階入侵防護

- IP 重組與 TCP 資料流重組。
- Trellix、使用者定義及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 DDoS 防護。
- 閾值與啟發式偵測。
- 主機式連線限制。
- 以設定檔為基礎的自我學習型偵測。

Trellix Global Threat Intelligence

- 檔案信用評價。
- IP 信用評價。
- 以地理位置為基礎的受限制存取權。
- 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	偵測器類型 3
平台	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
虛擬 IPS 偵測器機型	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
虛擬 IPS 部署類型	獨立式	獨立式	分散式
VMware NSX 支援	無	無	有
AWS 支援	無	無	有
邏輯 CPU 核心數目[2]	3	4	3
所需記憶體[3]	4 GB	6 GB	5 GB
虛擬偵測器規格			
最高輸送量[4]	最高 500 Mbps	最高 1 Gbps	最高 500 Mbps
同時連線	200,000	600,000	200,000
每秒連線建立次數	6,000	20,000	6,000
支援的 UDP 流量	39,168	254,208	39,168
監視埠配對數目	2	3	1[5]
每個偵測器的虛擬介面數 (VIDS)	32	100	32
DoS 設定檔	100	300	100
管理連接埠	有	有	有
回應連接埠	有	有	無
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 埠檢查		VMware NSX 內置檢查

1.僅用於 VMware NSX 環境中 (以插入服務的形式)。
2.VM 資源需求可能會依各版本而有所不同。請參閱各版本的特定說明文件。
3.同上。
4.在最佳測試情況下，以 1518 位元組的 UDP 封包測得。
5.入口和出口虛擬呈現。檢查作業和 Vmware NSX 在核心層級緊密相連。

Trellix