運用 VMware AppDefense 保護虛擬化和雲端環境內的應用程式

雖然全球投注在 IT 安全性的花費持續攀升，但是組織成為資料外洩受害者的機率卻依然上升至四分之一。[1] 儘管市面上有數千種安全性產品，而且有龐大的預算來購買這類產品，但是資料並未變得更安全。這對於必須保護日益動態的分散式 IT 環境內應用程式和資料的資訊安全長 (CISO) 而言，無疑是巨大挑戰。隨著更多組織採用靈活的現代化應用程式開發模式，配合業務的速度落實安全性的難題就變得更加棘手 — 安全性常被視為進步的阻礙。

資訊安全長和其團隊在努力保護其資料和應用程式時，面臨兩個主要挑戰：

未偵測到的威脅和誤報警報
現有端點安全性解決方案會觸發無數的誤報警報，導致安全作業團隊浪費時間和人力在調查不存在的威脅上面。更糟的是，安全作業團隊甚至可能完全未察覺真正存在的威脅。

變化快速的動態環境
現有安全性解決方案不是專為因應現代化應用程式開發和部署的速度所設計，也就是說隨著新應用程式的推出和更新，安全性無法同步跟進。

透過虛擬化進行安全性轉型

VMware AppDefense 具備獨特的優勢，可化解上述兩個挑戰。AppDefense 是一套資料中心端點安全性產品，可將威脅偵測與回應功能直接內嵌於應用程式和資料所在的虛擬化層中。AppDefense 運用 VMware vSphere®，提供現有端點安全性解決方案未提供的三個重要優勢：

可靠的應用程式目標狀態知識 – 當您知道哪些部分運作良好，便能偵測出哪些部分運作不佳
由於 AppDefense 位在 vSphere Hypervisor 內，所以對於資料中心端點應有的運作效能具備可靠的瞭解，出現變更時，會率先得知該變動。具備此情境智慧，就不再只能憑猜測判斷哪些變更為合理，以及哪些異動是真正威脅。

自動化且精確的威脅回應 – 適時做出適切回應
偵測到威脅時，AppDefense 能觸發 vSphere 和 VMware NSX®，協調做出對威脅的適切回應，而不需人工介入。例如，AppDefense 能自動：

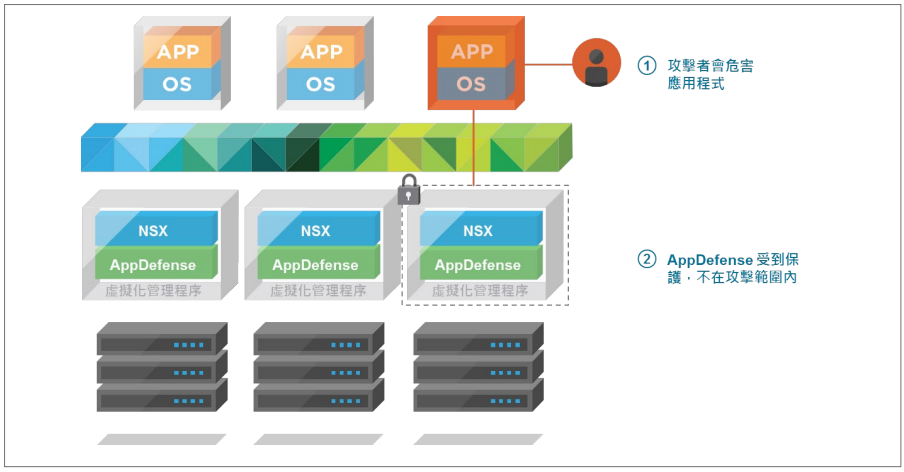
- 封鎖程序通訊
- 產生端點快照，供驗證分析
- 暫停端點
- 關閉端點

概觀
VMware AppDefense™ 是資料中心端點安全性產品，可保護在虛擬化環境中執行的應用程式。不同於現有端點安全性解決方案是追逐威脅，AppDefense 著重於監控應用程式是否維持在其目標狀態，也就是發揮應有效能，並且在應用程式偏離其目標狀態，即出現威脅時，自動做出回應。這會讓安全作業達到最高效率和成效，並且精簡應用程式安全性就緒度的審查程序。

關鍵焦點
- 簡化資料中心端點安全性
- 提高 SOC 內的威脅偵測能力
- 自動化執行事件回應程序
- 精簡應用程式安全性審查

與攻擊範圍隔離 – 防護更上一層樓

大多數惡意軟體變體在侵入端點時，第一步就是讓防毒軟體和其他採用代理程式的端點安全性解決方案停擺。虛擬化管理程序提供一個受保護的位置，讓 AppDefense 能從中運作，因此即使端點遭受入侵，還是能確保 AppDefense 本身受到保護。



AppDefense 的運作方式

AppDefense 是一項基礎安全性產品，會對組織的安全策略產生深遠影響。

為安全性作業中心 (SOC) 提供以應用程式為中心的警示功能

AppDefense 不會產生大量警示，所以當其發出警報時，聽從警報立即因應會是明智之舉。AppDefense 發出的可靠警示會連帶自動化回應功能，讓安全性管理員能專心找出並根除環境中的威脅，不必逐一過濾干擾的資料，而調查不存在的威脅。

進行應用程式安全性就緒度審查轉型

在現代化應用程式開發環境中，應用程式的發行、變更和除役速度極為迅速。等到安全團隊知道有新的應用程式推出時，該應用程式往往早已有變更。AppDefense 會建立應用程式團隊和安全團隊之間通用的資料來源，進而簡化安全性審查程序。

VMware 提供以應用程式為中心的安全性

VMware 藉由網路虛擬化平台 VMware NSX，以及此平台能進行資料中心微分段的能力，讓網路安全性完全改觀。NSX 會將網路與安全服務（例如防火牆保護）直接架構到虛擬化管理程序內，因此能實現網路的最低權限模式。結果就是網路安全團隊能遏止威脅在其環境內橫向移動。

深入瞭解

如需更多資訊或購買 VMware AppDefense，請造訪 http://www.vmware.com/tw/appdefense，並且到我們的 Hands-On Lab 試用此產品。

AppDefense 會將威脅偵測和回應功能分層到基礎架構的另一個核心區域，因此能實現資料中心端點的最低權限模式。萬一有威脅侵入端點，AppDefense 會立即偵測到此威脅，並自動精準回應此威脅。NSX 和 AppDefense 共同提供一套穩健的解決方案，能保護應用程式基礎架構，因此一併保護其中的應用程式和資料。

[1] Ponemon Institute，2017 年 6 月，《2017 年資料外洩成本研究：全球概觀》(2017 Cost of a Data Breach Study: Global Overview)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
台北市 110 信義路五段七號台北 101 大樓 57 樓 C 室 電話 +886-2-8758-2804 傳真 +886-2-8758-2708 www.vmware.com/tw

文件編號：vmw53313-sb-securing-app-cloud-env-app-defense-en-US-a4-101 8/17