自動化軟體定義資料中心的進階安全性

VMware NSX 和 Check Point vSEC 的整合式解決方案可對所有資料中心流量的進階型威脅防禦提供動態協同互作流程

優點

- Check Point 進階型威脅防護的動態插入和協同互作流程具備最高的惡意軟體攔截率
- 在運作上可行的微分段可保護東西向的流量
- 精細區分的存取控制政策可綁定在 NSX 安全群組和虛擬機器上
- 跨虛擬和實體環境的統一式安全管理以獲得控制能力和可見度
- 數分鐘內就可佈建安全服務以進行快速的應用程式部署
- 共用安全內容以便讓各種安全控制措施能更加一致
- 隔離與修補受感染的虛擬機器

保護東西向的流量

整合式的應用程式、日益虛擬化的資料中心和動態環境，導致網路中的東西向流量，或是資料中心內部橫向的流量大幅增加。

當涉及到安全性時，重點主要是保護周邊或南北向進出資料中心的流量。只有少數控制功能可保護資料中心內東西向流量的安全。這會帶來安全上的風險，因為威脅一旦進入資料中心後就暢行無阻。解決此問題的傳統安全做法須靠人工完成，作業複雜、速度緩慢，而且無法跟上動態虛擬網路變化及虛擬應用程式佈建快速的腳步。而且單靠周邊安全性的做法會造成網路瓶頸、影響效能，並增加安全複雜性，因此造成安全團隊額外的負擔。

自動化的安全性佈建與協同互作作業

軟體定義資料中心 (SDDC) 由三大部分所定義 – 虛擬運算、虛擬儲存及虛擬網路，而 NSX 負責提供網路虛擬化元件。

VMware NSX 是領導產業的網路虛擬化平台，其優點與 VMware 提供用來運算的網路相同。NSX 等同於網路的 Hypervisor，能夠在軟體中完整重新產生所有的網路與安全性服務，包括交換器、路由器、防火牆、負載平衡等軟體。IT 部門可依需求撰寫程式管理與建立虛擬網路，因此能大幅簡化網路與安全方面的作業、快速佈建網路與安全服務，所需時間從數週縮短到數分鐘，並從根本上改善資料中心的安全。

如 Check Point vSEC 等 NSX 合作夥伴可利用 NSX 的原生安全功能、自動化及延伸性架構，在軟體定義資料中心動態插入、部署與協同互作進階的安全服務。
NSX 平台上固有的網路隔離與區段化能夠進行可實行的微分段，也就是零信任安全性模型，讓 SDDC 提供在基本上更安全的資料安全作法。政策會實施在虛擬介面上，並隨著工作負載時時提供保護。

Check Point vSEC 採用了這些 NSX 功能並整合兩者的優點，可在軟體定義資料中心環境中，提供動態部署且協同互作合作的進階資料保護。

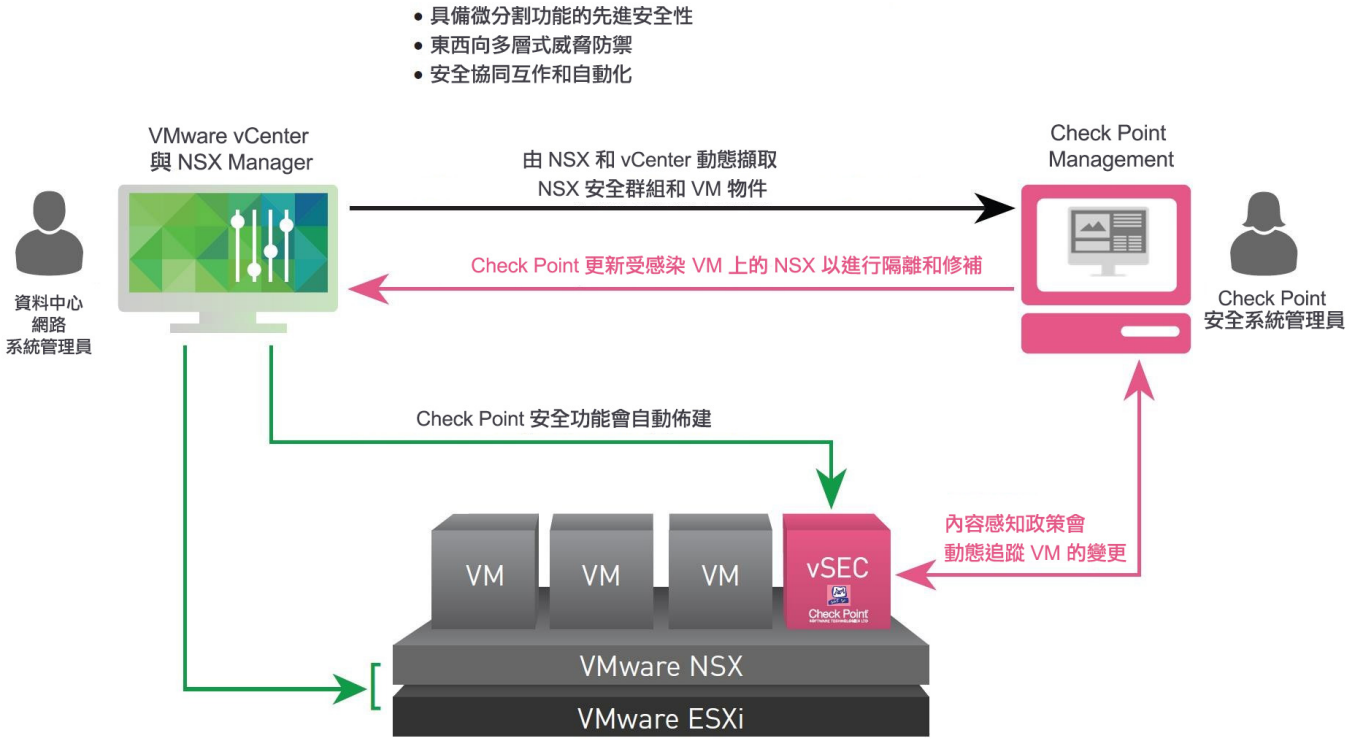
可行的微分段：固有的 NSX 網路隔離與區段化可實現資料中心微分段，無須設定 vLAN、ACL、防火牆規則、實體防火牆與路由器。安全控制可套用在最小的單位層級，以允許部署安全性最低的權限模型。 NSX 基本防火牆功能可透過 Check Point vSEC 擴充，其分層的安全政策作法能夠輕鬆地分割政策，對特定網路區段提供精細的規則定義。

內容感知安全政策：NSX 標準標籤能夠在 VMware NSX、VMware vCenter 及 Check Point vSEC 管理平台之間進行完全內容分享，確保能夠輕鬆匯入安全群組與虛擬機器 (VM) 身分識別，並在 Check Point 安全政策中重複使用。藉此可以將安全政策的建立時間從數分鐘縮短為數秒。系統會維護這些安全群組與 VM 的內容感知能力，以自動追蹤任何變更或新增項目。如此一來，便能在虛擬應用程式上實施安全保護，無論其建立或所在的位置為何。此外，預定義的 Check Point 安全範本能夠自動處理新佈建的虛擬應用程式的安全性。Check Point 的動態安全政策能無縫因應資料中心的變更，並在虛擬與實體安全閘道之間實行。

無所不在的安全性：VMware NSX 網路 Hypervisor 位於應用程式與實體基礎結構之間的最佳位置，能夠在每一個虛擬介面上分發實施。藉由與 VMware NSX 整合，Check PointvSEC 能夠動態插入進階安全保護。Check Point 的 Advanced Threat Prevention 有多層防禦功能，並擁有業界最佳的攔截率及完整的威脅情報，可主動阻止殭屍網路、鎖定式攻擊、進階型持續威脅及零時差攻擊。VMware NSX 能夠串連不同工作負載之間的 Check Point 進階安全保護功能，並控制應用程式之間的通訊。這會減少網路複雜性，以及必須在資料中心內部使用多個 VLAN 的需求。

自動化和協同互作作業：Check Point vSEC 利用 NSX 的自動安全功能動態散布與協同 vSEC，以保護東西向流量。Check Point vSEC 會偵測被惡意軟體感染的 VM 並加上標記，也會自動更新 VMware NSX。系統會快速地阻絕威脅，並對被感染的 VM 套用適當的修補作業。在資料中心環境中，經常需要整合不同的安全工作流程管理系統。此外，還必須將重複執行的手動工作自動化，以簡化安全作業。Check Point 的安全管理 API 能精細地控制權限，將編輯權限範圍縮小到政策內的特定規則或物件，限制可使用或改變的自動化工作或整合。這個執行受信任連線的功能讓安全團隊有信心自動化及簡化整個安全工作流程。

全方位的控制力與可見度：透過集中設定與監視虛擬安全閘道，可讓安全管理作業更為簡化。系統會記錄虛擬工作負載流量，您能輕鬆地在與其他閘道記錄相同的儀表板內檢視記錄。系統會產生虛擬工作負載流量專有的安全報告，追蹤整個虛擬網路是否符合安全規定。分層式政策管理方法讓系統管理員能夠將單一政策分割成數個子政策，以便依照網路區段自訂保護功能及委派職務。這可確保在整個虛擬網路與實體網路上都會套用正確的保護等級。只要透過單一儀表板就能掌握安全管理的所有層面，例如政策管理、記錄、監視，甚至是分析與集中式報告。安全系統管理員能藉此檢視整個組織的安全態勢。



結論

此項綜合解決方案讓企業能夠快速、簡單地在軟體定義資料中心內佈建與部署 Check Point 的進階安全服務，讓客戶能夠在資料中心內擁有與 Check Point 用於周邊閘道相同層級的東西向流量安全性。安全團隊更能夠與網路團隊合作，並維持對實體與虛擬網路的完整控制權與可見度。

關於 CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) 是全球首屈一指的資訊安全供應商，提供領先業界的解決方案，並以無與倫比的惡意軟體與其他攻擊攔截率保護客戶免於網路攻擊。 Check Point 提供一個完整的安全架構，可保護企業網路到行動裝置，並具備最全方位且直覺的安全管理。Check Point 保護超過 10 萬個各種規模的組織。Check Point，保護未來。

關於 VMWARE

VMware 是雲端基礎結構與商務行動力的領導者。我們的解決方案建立在 Vmware 領導業界的虛擬技術基礎上，提供一個有彈性、迅速且更安全的新 IT 模型。客戶可以快速地開發、自動地發佈且更安全地取用任何應用程式，因此能加速創新。VMware 擁有超過 500,000 位客戶及 75,000 位合作夥伴。公司總部位在矽谷，辦事處遍佈全球，詳情請參閱 www.vmware.com。

聯絡我們

全球總部 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | 電話：972-3-753-4555 | 傳真：972-3-624-1100 | 電子郵件：info@checkpoint.com
美國總部 | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | 電話：800-429-4391; 650-628-2000 | 傳真：650-654-4233 | www.checkpoint.com