VMware NSX

幫助 IT 配合業務步調前進

「技術持續以驚人的速度加快發展，因此絕對可為有能力掌握先機的企業帶來極大回報。」

Bart Van Ark 博士
The Conference Board 執行副總裁、
首席經濟學家兼策略長

VMware NSX® 是實現 VMware 雲端網路解決方案的網路虛擬化與安全性平台，可透過軟體定義的方法，將網路延伸橫跨資料中心、雲端和應用程式架構。無論應用程式是在虛擬機 (VM)、容器或是實體伺服器等任何環境上運作，NSX 都能讓應用程式享有更強大的網路與安全功能。如同虛擬機的運作模式，無論底層硬體為何，皆可佈建和管理網路。 NSX 會以軟體重建整個網路模型，並在數秒內建立和佈建任何網路拓撲，從簡單到複雜的多層級網路，都可一手包辦。使用者可依照不同需求建立多個虛擬網路，運用 NSX 或協力廠商整合的廣泛商業網路 (從新一代防火牆到效能管理解決方案) 所提供的服務組合，創造本質上更靈活安全的環境。這些服務還可延伸至雲端內及跨雲端的各種端點。

相互牴觸的需求導致妥協讓步

速度和靈活性、穩健的安全性以及應用程式的高可用性，均是 IT 部門向前邁進所須提供的極重要優先事項。企業極其倚重穩固的應用程式基礎架構，因此 IT 日益成為重要的基礎，讓企業能進行創新並成功度過數位化轉型過程。但是，飛快的變化速度以及對 IT 的期望不斷改變，都使得 IT 需要持續調整優先事項，而這往往會影響交付有效性。

IT 切身體會到，配合多方相關人員並滿足這些需求所造成的頻繁緊張狀態，因此不得不擱置其他 IT 優先事項，而先處理其中一個 IT 優先事項。舉例而言，由於安全性連帶嚴密的複雜性，所以為了保護應用程式，往往會減緩應用程式部署的速度。而為了確保應用程式在各個環境中的可用性，便會經常做出類似的妥協，因而實際上造成 IT 與範圍更廣泛的企業意見相左，反之亦然。

這種持續緊張和妥協的最終結果會對 IT 造成嚴重後果。事實上，這會導致多個職責領域出現嚴重缺失：企業無法快速滿足需求、資料中心和雲端環境存在安全弱點，以及缺乏整體靈活性。

主要優勢

- 精密的安全性 - 安全性利用工作負載層級微分段安全性原則，防止威脅在環境中橫向移動
- 速度與靈活性 - 透過自動化將網路佈建時間從數天減少至數秒，並改善營運效率
- 一致的原則和作業 - 無論資料中心、公有雲和私有雲，以及應用程式架構之間的實體網路拓撲為何，均能以一致的方式管理網路與安全性原則

發揮基礎架構的所有潛力

大多數企業已將其資料中心內的運算元件虛擬化。此外，許多企業也已決定將儲存虛擬化，其中超過 70% 的企業已採用或計畫採用軟體定義的儲存。

將功能從硬體抽象化擷取到軟體內，企業就能快速佈建應用程式元件、在資料中心之間移動虛擬系統，以及將關鍵程序自動化。不將交換、路由、負載平衡和防火牆虛擬化，就難以讓軟體定義的資料中心發揮完整價值。

事實上，網路架構深植於硬體的企業無論在速度、靈活性或安全性方面，均比不上部署虛擬化網路的企業。企業的狀態受制於網路的狀態。

資料中心網路需要一種全新的方法，也就是不再需要在速度和安全性之間或在安全性和靈活性之間做出取捨的方法。需要改寫妨礙企業發揮所有潛力的資料中心規則，讓 IT 能全力表現，不需做出任何妥協。如同數千家企業現在已明白，網路虛擬化正是所需的新方法。

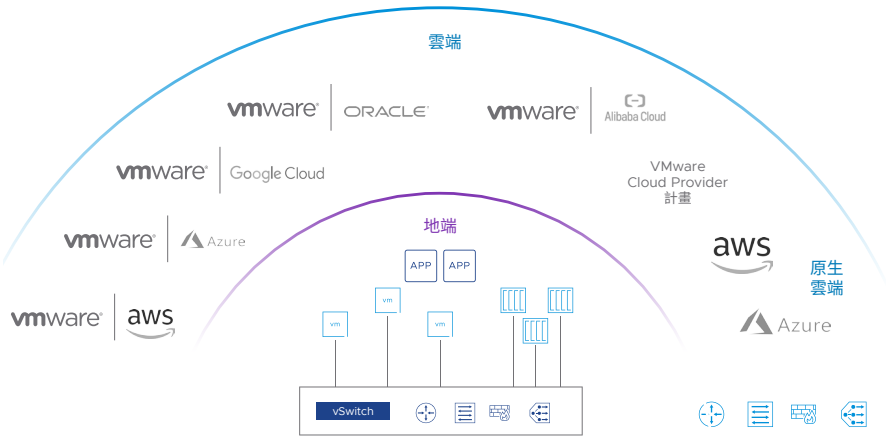

圖 1：利用 NSX 實現一致的網路與安全性

將網路與安全服務移到資料中心虛擬化層，網路虛擬化便能讓 IT 以現在建立虛擬機時所享有的相同簡便性和速度，建立、快照、儲存、移動、刪除和還原整個應用程式環境。NSX 會將通用網路與安全性原則延伸到異質環境和應用程式架構，讓這些優點能落實在資料中心、私有雲和公有雲、傳統應用程式，以及現代化應用程式之中。因此，能實現之前在營運和財務方面無法達成的安全性與效率水準。

重要功能

- 具連線狀態的分散式防火牆保護 - 實現涵蓋至第 7 層的具連線狀態防火牆保護，不僅內嵌在虛擬化管理程序核心內，還可透過直接整合到雲原生、原生公有雲和裸機主機內，分散至整個環境
- 內容感知的微分段 - 依據許多屬性和第 7 層應用程式資訊，動態建立安全性群組和原則，並自動加以更新，進而實現自調式微分段原則
- 雲端管理 - 原生整合 VMware Aria Suite、OpenStack 等項目，且完整支援 Terraform 供應商、Ansible 模組與 PowerShell Integration
- 協力廠商整合 - 透過一流的協力廠商商業網路，強化安全性與進階網路服務
- 雲原生支援 - 運用容器網路能見度，支援跨容器平台、虛擬機和裸機主機的企業級進階網路與安全性
- NSX Intelligence™ - 無須部署任何新工具或代理程式，即可減少探索、分析及施行應用程式分段原則的時間；可透過基礎架構內建的原生安全簡化安全性作業
- NSX Distributed IDS/IPS™ - 這款專門打造的進階威脅偵測引擎，可使用內建的分散式分析和精選簽名分送，偵測東西向流量上的橫向威脅移動

有了 NSX，IT 便能推動企業創新，可立即回應多方相關人員的需求，而不是將其要求視為競爭與相互排斥。現在 IT 不僅能提供前所未有的安全性水準，還能配合業務步調，同步提供如此高水準的安全性。

原生安全

VMware NSX 讓您能以獨特方式瞭解應用程式組成 (從網路通訊到個別工作負載上的流程層級行為)，這要歸功於 NSX 內建在虛擬化管理程序中的位置，以及應用程式建置於其上的其他原生控制點。由於有此能見度，所以能依據想要提供給應用程式的安全態勢，自動建立網路安全性原則。對 IT / 資訊安全以及應用程式開發團隊來說，這可減少花費在安全性審查週期上的時間。

同時，這也能將安全性原則延伸到多個資料中心和混合雲環境中強制執行，並對建置在虛擬機、容器和裸機伺服器上的應用程式，提供無所不在的控制能力。NSX Intelligence 能夠持續提供整個資料中心的能見度，以大幅簡化及自動化微分段的實際運用流程。

NSX Distributed IDS/IPS 有助於輕鬆實現合規、建立虛擬安全區域，並偵測東西向流量網路上的橫向威脅移動。 NSX 也會將能見度和控制延伸到協力廠商安全服務，例如新一代防火牆、入侵防禦系統 (IPS) / 入侵偵測系統 (IDS) 解決方案和防毒工具，進而提高這些服務的效用。

NSX 會將安全性從應用程式開發生命週期的被動附加程序，轉變成生命週期中的主動整合式自動化步驟。新佈建的工作負載會自動繼承安全性原則，這些原則會在工作負載的整個生命週期中跟隨工作負載。如果工作負載遭到淘汰，其安全性原則也會隨之淘汰，這樣就能減少隨著時間增加的原則數量，並進一步簡化管理作業。

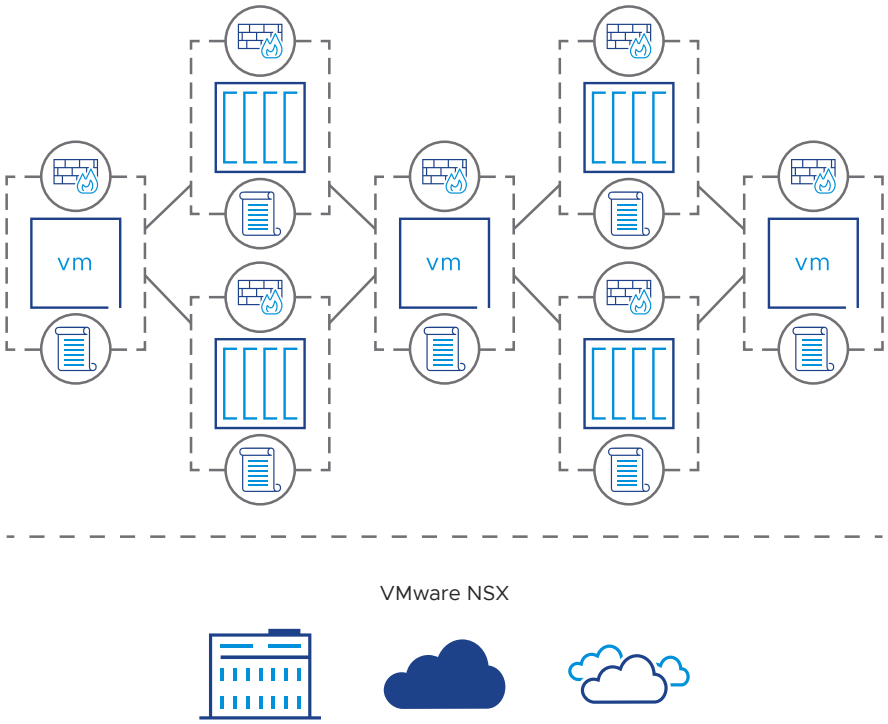

圖 2：落實資料中心內最精密等級的安全性

自動化

隨著企業的範圍和步調持續擴大和加快，將虛擬化網路與安全性自動化，可確保配合業務步調，建立和部署服務與應用程式。 透過自動化排除容易出錯的手動網路佈建工作，應用程式部署速度就會大幅加快。

VMware NSX 與雲端管理軟體 (例如 VMware Aria Automation) 搭配運作，就能從中央控制平台管理網路與安全性基礎架構和應用程式的佈建、部署、作業和淘汰作業。VMware 會使用 Terraform 和 Ansible 等工具，將網路與安全性生命週期整合至程序中，藉此讓所有的基礎架構作業自動化，而網路與安全性也不再是應用程式生命週期中的瓶頸。

將通用網路與安全性原則延伸到傳統 (虛擬機式) 與新型 (容器式) 應用程式架構，即可實現這兩類應用程式的網路與安全性自動化。此外，這也能在地端資料中心、私有雲和公有雲內，實現應用程式的自動部署、行動化和淘汰作業。

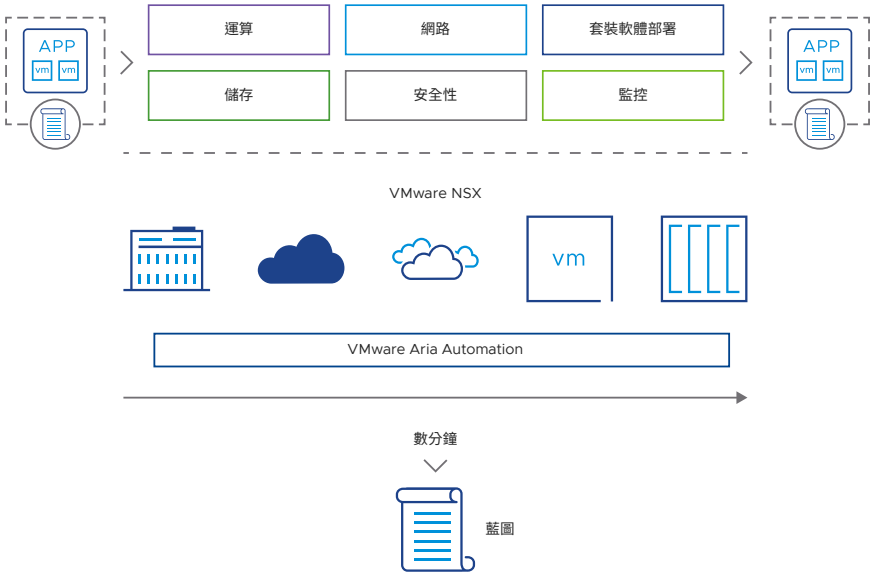

圖 3：透過自動化網路與安全性實現快速且可重複的部署

多雲網路

NSX 和 NSX Cloud™ 提供一個跨站點的統一網路與安全性模式，因此不再需要手動設定網路，並可透過網路自動化實現高營運效率。網路與安全性原則會在個別工作負載的整個生命週期當中跟隨工作負載，因此能簡化混合雲和多雲環境中的原則與管理。NSX 同盟可集中管理不同地點 (地端和雲端) 的原則，藉此提供作業簡便性，並跨越多個雲端實現一致的執行作業。

這也讓企業能將虛擬機或整個資料中心從一個位置移轉到另一個位置，而且極少或不會造成應用程式停止運作。因此，企業能在計畫性移轉和意外停擺期間，加快復原速度。由於網路與安全性跨越異質環境，因此企業也能運用不同實體資料中心內的資源，將其視為單一私有雲運作。這種主動-主動式資料中心資源集區化形式，稱為多資料中心集區化或城域集區化。

這些技術共同提供安全且順暢的應用程式行動化，能輕易移轉到雲端或從中移出，或是在實體站點之間移轉。針對 IT 部門在基礎架構上使用的同一個虛擬化網路與安全性平台，NSX 和 NSX Cloud 可將其延伸至雲端或其他站點，提供一個快速且低接觸的移轉程序。

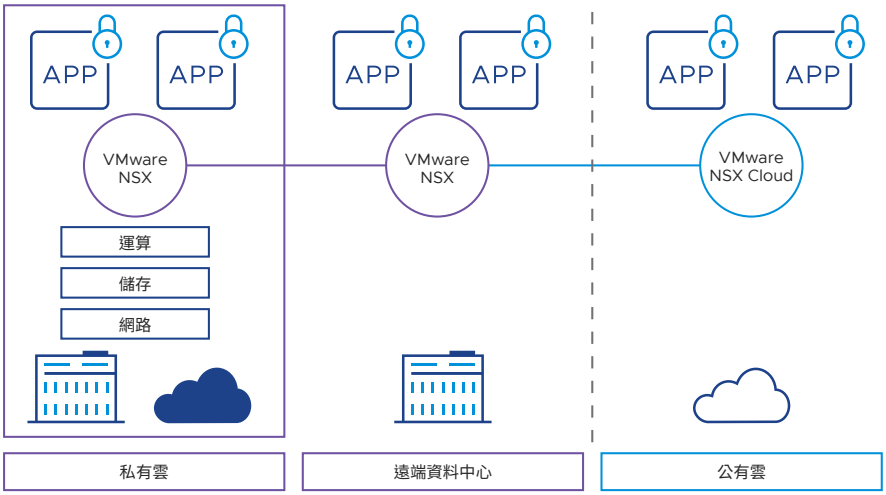

圖 4：在各個站點與雲端環境獲得一致的網路與安全性，同時減少停擺的影響

現代化應用程式的網路與安全性

VMware NSX 與新型應用程式平台整合，以提供網路與安全功能 (例如負載平衡、防火牆保護、交換和路由)，整個過程完全在軟體中進行，而且可透過基礎架構即程式碼、API 導向方式使用。

隨著越來越多的應用程式採用容器和微服務架構，能夠在細至個別工作負載的情形下連接並保護這些新型應用程式，就變得很必要。NSX 將容器和微服務視為一級物件，就如同任何其他工作負載或端點，包括執行第 3 層網路的能力。其也能以原生方式執行容器對容器網路，以及進行細至個別容器層級的微分段，因此能為微服務進行微分段；而在工作負載佈建、變更、移動和淘汰的過程中，原則也會跟隨工作負載。

NSX 可與多種應用程式與容器協調作業平台、虛擬化管理程序和公有雲環境整合，也可整合到不同應用程式平台上，隨著新型應用程式開發完成，能為應用程式提供固有且靈活的網路與安全性。

深入瞭解

如需詳細資訊，請參閱下列資源：

- VMware NSX 產品頁面
- VMware NSX 規格說明
- VMware NSX Intelligence 解決方案概觀
- VMware NSX Distributed IDS/IPS 產品頁面

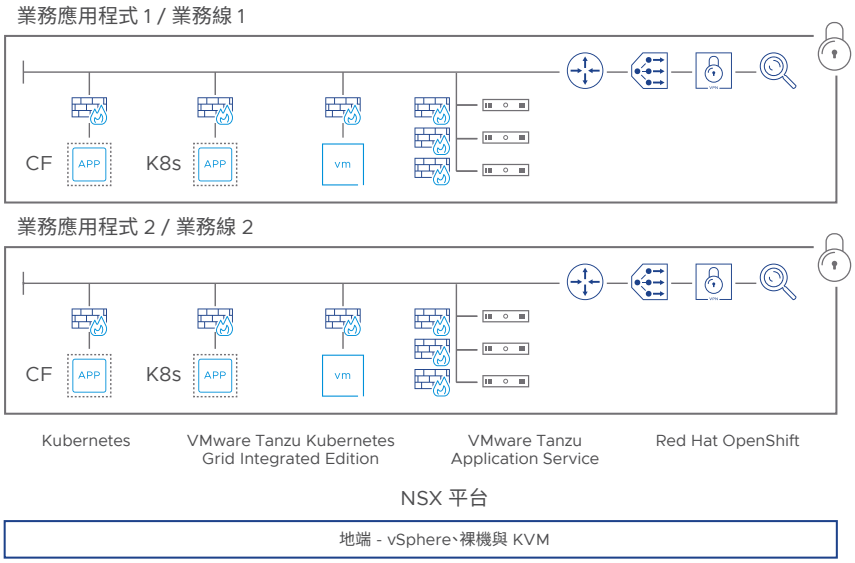

圖 5：為不同應用程式架構、平台、站點和雲端上的容器化工作負載，帶來進階網路與安全性

加快實現現今的商業價值，並為未來奠定基礎

已部署 NSX 的企業發現，這款解決方案正快速成為 IT 部門成功與否的決定性因素，而且是資料中心基礎架構和多雲策略的基礎部分。目前有數以千計的 NSX 客戶正加速為其企業提供價值，以便能在快速、靈活且安全的虛擬網路之上，以傳統硬體式網路所無法實現的方式，交付一些最敏感且最關鍵的應用程式。

網路與安全性的進展，讓 NSX 客戶能獲得顯著且立即的效益，且能免除之前佔用企業如此多頻寬的耗時、繁重工作。這讓企業在規劃未來發展以及 IT 支援該願景所需具備的功能時，有餘裕思考更好的企業策略。

文件編號：1356650aq-so-nsx-a4_TW 10/23