

# VMware NSX

## 主要優勢

- 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。
- 利用微分段和進階威脅防禦，在工作負載層級以精密的安全性來保護應用程式。
- 無論資料中心和原生公有雲內部和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。
- 取得詳細的應用程式拓撲視覺化、自動化安全性原則建議與持續監控流量的能力。
- 利用內建的完全分散式威脅防禦引擎，針對東西向流量啟用進階橫向威脅防禦。

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，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。

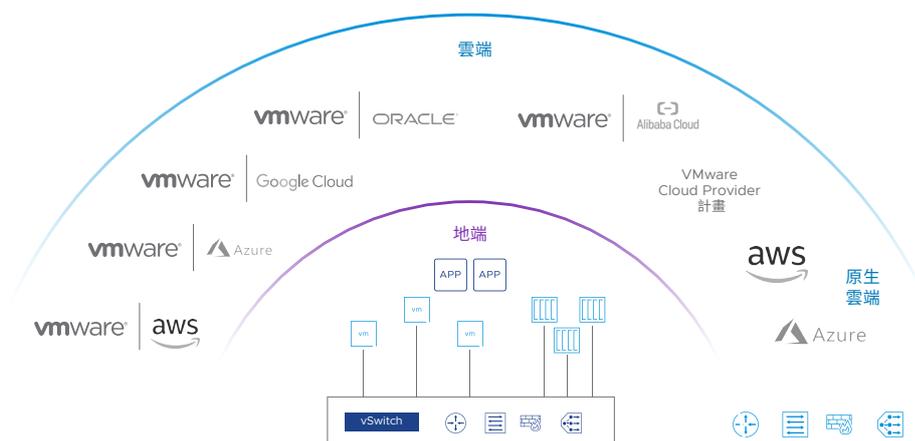


圖 1：NSX 網路虛擬化與安全性平台

## 網路全憑軟體

VMware NSX 為軟體定義的網路帶來全新的作業模式，替軟體定義的資料中心 (SDDC) 打下基礎，並延伸到雲端網路。現在，資料中心的作業人員可實現各種層級的靈活性、安全性與經濟效益，徹底擺脫過去資料中心網路完全受限於實體硬體元件的窘境。NSX 提供一套完整的邏輯網路與安全功能和服務，包含邏輯交換、路由、防火牆、負載平衡、虛擬私有網路 (VPN)、服務品質 (QoS) 與監控。可透過任何運用 NSX API 的雲端管理平台，將這些服務佈建在虛擬網路中。虛擬網路是以不中斷運作的方式部署在任何現有的網路硬體上，而且可延伸至資料中心、公有雲和私有雲、容器平台和實體伺服器。

重要功能	
交換	能夠在資料中心界限內外的路由 (第 3 層) 結構上，建立第 2 層邏輯層疊延伸。
路由	在虛擬化管理程序核心中，以分散形式執行虛擬網路之間的動態路由，並透過使用實體路由器的主動-主動容錯移轉達成水平擴充。支援靜態路由與動態路由通訊協定，包括支援 IPv6。
負載平衡 <sup>1</sup>	VMware NSX Advanced Load Balancer™ 提供企業級多雲負載平衡、全域伺服器負載平衡 (GSLB)、應用程式安全性及網頁應用程式防火牆、應用程式分析，以及從資料中心到雲端的容器流入服務。
虛擬路由和轉遞 (VRF)	利用獨立路由表、網路位址轉譯 (NAT) 和 NSX 第 0 層間道上每個 VRF 的邊緣防火牆支援，完成租戶間的資料轉發平台隔離。
分散式防火牆	第 2 層至第 7 層的具連線狀態防火牆 (包括應用程式識別、使用者識別和分散式完整網域名稱允許清單)，不僅內嵌在虛擬化管理程序核心內，還可透過集中式原則和管理分散至整個環境。此外，NSX Distributed Firewall™ 可直接整合到 Kubernetes 和 Pivotal Cloud Foundry 等雲原生平台、AWS 和 Azure 等原生公有雲，以及實體伺服器內。

重要功能	
情境感知的微分段技術	可依據屬性 (不僅止於 IP 位址、連接埠和通訊協定) 動態建立並自動更新安全性群組和原則，以包含機器名稱與標籤、作業系統類型和第 7 層應用程式資訊等項目，進而實現自調式微分段原則。依據從 Active Directory 和其他來源取得之身分識別資訊所建立的原則，能達到使用者層級的安全性，深入遠端桌面服務和虛擬桌面基礎架構 (VDI) 環境內的個別使用者工作階段層級。
VMware NSX Intelligence™	針對每個網路流量獲得自動化安全性原則建議與持續的監控和視覺化能力，進而提升能見度，實現可輕鬆進行高度稽核的安全態勢。NSX Intelligence 與 VMware NSX 共用相同的使用者介面，能為網路與資安團隊提供單一介面。
NSX 閘道	為設定在實體網路和 NSX 層疊網路上的 VLAN 之間提供橋接支援，以便順暢連接虛擬與實體工作負載。
閘道防火牆	功能完善的企業級網路防火牆，運用完整的第 4 層至第 7 層具連線狀態防火牆提供保護。這包括第 7 層應用程式識別、使用者識別、NAT 等功能。
VPN	針對雲端閘道服務提供未受管理的站點對站點 VPN。
NSX 的分散式與閘道進階安全功能 <sup>2</sup>	<p>搭配安全性附加元件的 NSX 可提供數種進階安全功能，當中包括：</p> <ul style="list-style-type: none"> <li>• 分散式安全性： <ul style="list-style-type: none"> <li>– 分散式入侵偵測和防禦系統 (IDPS)</li> <li>– 分散式惡意軟體防禦</li> <li>– 分散式網路流量分析 (NTA)</li> <li>– 網路偵測與回應</li> </ul> </li> <li>• 閘道安全性 – 根據網頁類別和信譽篩選 URL</li> <li>• 惡意軟體偵測</li> </ul>
DPU-based Acceleration for NSX	提供在連接至應用程式主機的 DPUs <sup>3</sup> 上實作的高效能網路與安全服務。將 NSX Services 自虛擬化管理程序卸載至 DPU，可釋放主機運算資源，並加快交換和路由、實現高效能安全性，以及強化可觀察性，同時保留現有的 NSX 使用者體驗。

重要功能	
同盟	從單一介面對多個位置進行集中式原則設定及強制執行，針對整個網路啟用一致的原則，以簡化作業與災難復原架構。
多雲網路與安全性	無論底層實體拓撲或雲端平台為何，均能在各個資料中心站點以及跨私有雲和公有雲界限，實現一致的網路與安全性。
容器網路與安全性	<p>VMware NSX Container Plugin 提供適用於 VMware Tanzu® Kubernetes Grid™、VMware Tanzu Application Service™、VMware vSphere® with Tanzu、Red Hat OpenShift 和上游 Kubernetes 的容器網路。</p> <p>VMware Container Networking™ with Antrea™ 提供叢集內網路和 Kubernetes 網路原則，且具備商業支援和已簽署的二進位檔。與 NSX 整合後，可透過 NSX 管理平台的 Traceflow 提供多叢集網路原則管理，並集中化進行連線的疑難排解。</p>
NSX API	採用 JSON 技術的 RESTful API，方便與雲端管理平台、開發營運自動化工具和自訂自動化整合。
作業	提供原生化作業功能，例如中央指令行介面、Traceflow、層疊邏輯 SPAN 與 IPFIX，可進行疑難排解和主動監控虛擬網路基礎架構。與 VMware Aria Operations™ for Logs (前身為 VMware vRealize® Log Insight™) 和 VMware Aria Operations for Networks (前身為 VMware vRealize Network Insight™) 等工具整合，前者能達成可高度延展的日誌記錄管理，後者能進行進階分析和疑難排解。
自動化與雲端管理	能與 VMware Aria Automation™ (前身為 VMware vRealize Automation™/vRealize Automation Cloud™) 等進行原生整合。完整支援 Ansible 模組、完整支援 Terraform 供應商及 PowerShell Integration。
協力廠商合作夥伴整合	支援與協力廠商合作夥伴在各種不同類別上的管理、控制平台和資料轉發平台整合，例如新一代防火牆、入侵偵測系統 / 入侵防禦系統 (IDS/IPS)、無代理程式的防毒保護、交換、作業與能見度、進階安全性等等。

## 使用情境

### 安全性

透過 NSX，即可在私有雲和公有雲環境中，有效率地實際運用應用程式的零信任安全性。無論目標是要鎖定關鍵應用程式、在軟體中建立邏輯緩衝區域 (DMZ)，還是縮小虛擬桌面環境中的攻擊範圍，NSX 都能實現微分段，以定義並施行個別工作負載層級的網路安全性原則。

### 多雲網路

NSX 帶來一套網路虛擬化解決方案，能在各個異質站點提供一致的網路與安全性，進而簡化多雲維運。因此，從順暢的資料中心延伸、多資料中心建立集區，到快速工作負載行動化等多雲使用情境，NSX 都能配合。

### 自動化

透過網路與安全服務的虛擬化，NSX 成功免除手動管理網路與安全服務和原則所面臨的瓶頸，進而加速推動完整堆疊應用程式的佈建與部署作業。NSX 能原生整合雲端管理平台和其他自動化工具 (例如 VMware Aria Automation、Terraform、Ansible 等)，協助開發人員和 IT 團隊按照業務所需的步調來佈建、部署和管理應用程式。

### 雲原生應用程式的網路與安全性

NSX 為容器化應用程式和微服務提供整合式完整堆疊的網路與安全性，進而在開發新應用程式期間提供以個別容器為基礎的精密原則。如此一來，傳統與新應用程式皆能享有原生的容器對容器第 3 層網路、適用於微服務的微分段，以及網路與安全性原則的端對端能見度。

## VMware NSX 版本

### Professional

適合需要敏捷和自動化網路，外加微分段功能，且可能有公有雲端點的組織。

### Advanced

適合需要 Professional 版本功能，外加進階網路與安全服務，並與廣大商業網路整合，且可能有多個站點的組織。

### Enterprise Plus

適合需要最進階的 NSX 功能，外加 VMware Aria Operations for Networks 的網路作業、VMware HCX® 的混合雲行動化，以及 NSX Intelligence 的流量能見度與安全性作業的組織。

## Remote Office Branch Office (ROBO)

適合需要在遠端辦公室或分公司，將應用程式的網路與安全性虛擬化的組織。

	Professional	Advanced	Enterprise Plus	ROBO
網路 <sup>4</sup>				
分散式交換與路由	•	•	•	• <sup>5</sup>
軟體第 2 層橋接到實體環境	•	•	•	
透過 ECMP (主動-主動) 的動態路由	•	•	•	•
具備靜態路由的 IPv6 及靜態 IPv6 配置	•	•	•	
具備動態路由的 IPv6、動態 IPv6 配置及服務		•	•	
雙協定 (IPv4/IPv6) 外部管理		•	•	
VRF (第 0 層閘道 VRF)		•	•	
乙太網路 VPN (EVPN)			•	
分散式安全性				
為在實體伺服器上運作的虛擬機和工作負載提供分散式防火牆保護	•	•	•	•
情境感知的微分段技術 (第 7 層應用程式識別、RDSH、通訊協定分析器)		•	•	
分散式完整網域名稱允許清單		•	•	
分散式進階安全功能	NSX 安全性附加元件授權可提供額外的分散式安全功能。請參閱 <a href="#">NSX Distributed Firewall 規格說明</a> 。			
閘道安全性				
NSX Gateway Firewall™ (具連線狀態)	•	•	•	•
NSX 閘道 NAT	•	•	•	•
VPN (第 2 層與第 3 層)	•	•	•	•
閘道進階安全功能	NSX 安全性附加元件授權可提供額外的閘道安全功能。請參閱 <a href="#">NSX 安全性規格說明</a> 。			

其他資源

[VMware NSX Distributed Firewall 規格說明](#)

[VMware NSX Gateway Firewall 規格說明](#)

[VMware Container Networking with Antrea 規格說明](#)

	Professional	Advanced	Enterprise Plus	ROBO
現代化應用程式				
容器網路與安全性		•	•	
多站點				
多 vCenter® 網路與安全性		•	•	
同盟			•	
作業				
原則 API、中央指令行介面、Traceflow、層疊邏輯 SPAN 與 IPFIX	•	•	•	•
整合				
DPU-based Acceleration for NSX <sup>6</sup>			•	
與雲端管理平台整合 <sup>7</sup>	•	•	•	•
與分散式防火牆整合 (Active Directory、VMware AirWatch®、端點保護與協力廠商服務增強)		•	•	•

	Professional	Advanced	Enterprise Plus	ROBO
<b>相關產品</b>				
VMware Aria Operations for Logs for NSX <sup>8</sup>	•	•	•	•
VMware Aria Operations for Networks Advanced <sup>9</sup>			•	
VMware HCX Advanced <sup>9</sup>			•	
VMware NSX Advanced Load Balancer – Basic Edition <sup>1</sup> (具備 SSL 卸載和直通技術的第 4 層至第 7 層負載平衡、伺服器運作狀況檢查、提供程式編寫能力的應用程式規則，以及透過 GUI 或 API 操控流量)		•	•	•
VMware NSX Intelligence (虛擬機對虛擬機流量分析、防火牆能見度、自動化安全性原則、規則和群組建議分析)			•	

- VMware 建議客戶使用 NSX Advanced Load Balancer 來進行負載平衡。NSX Advanced Load Balancer – Basic Edition 包含在 NSX Advanced 和 Enterprise Plus 版本內。NSX Advanced Load Balancer 的進階功能會以附加元件授權的形式提供。如需詳細資訊，請造訪 [NSX Advanced Load Balancer 產品頁面](#)。
- 若要瞭解進階安全功能，請參閱 [NSX Distributed Firewall 規格說明](#)。
- 支援數家主流 DPU / 網路卡和伺服器 OEM 廠商。如需詳細資訊，請聯絡您的 VMware 代表。
- VMware NSX 使用授權包含有權使用 VMware Workspace ONE® Access™ 功能，但僅限特定功能。如需詳細功能說明，請參閱有關 NSX Data Center for vSphere 功能及 NSX 功能的知識庫文章，包括 [NSX 4.0.x 產品方案](#) 文章，以取得最新資訊。
- 僅支援基於 VLAN 的交換功能。
- DPU-based Acceleration for NSX 於 Enterprise Plus 中提供，按核心訂閱授權。
- 只與第 2 層、第 3 層和 NSX 閘道整合。不會使用安全性群組。
- 如需詳細資訊，請參閱 [VMware Aria Operations for Logs 規格說明](#)。
- NSX Enterprise Plus 包含完整版 VMware Aria Operations for Networks Advanced 與 VMware HCX Advanced。如需詳細資訊，請參見 [VMware Aria Operations for Networks 規格說明](#) 和 [VMware HCX 規格說明](#)。