商業白皮書

頂尖的 SD-WAN 和 SASE 以及零信任技術可讓數位企業如虎添翼

aruba
a Hewlett Packard Enterprise company

目錄

執行摘要

企業繼續擁抱數位轉型，目的是為了提高效率、提升客戶滿意度、尋求新的市場機會、增強獲利能力，並維持競爭優勢。將企業應用程式移轉到雲端，是任何成功的數位轉型計畫不可或缺的一部分。為什麼呢？ 如今，在雲端執行的應用程式數量已經超過在傳統企業資料中心執行的應用程式，而且其中大多數的應用程式都採用軟體即服務 (SaaS) 的形式。此外，在雲端優先的世界中，企業必須確保使用者可以隨時隨地，使用任何裝置直接且安全地存取應用程式。另外，還要確保網路可以始終如一地為員工和客戶提供最高品質的體驗。最後，企業行動裝置和 IoT 裝置數量暴增，也極大擴張了受攻擊面，使企業暴露於可能危及資料並導致網路停機的安全漏洞中。

當今的企業網路從來都不是著眼於雲端優先世界而設計的，因此無法因應數位轉型面臨的網路安全挑戰。然而，企業不僅要保護雲端的應用程式，也要保護透過廣域網路 (WAN) 連線到這些應用程式的使用者，這些都非常重要。此外，IoT 裝置數量劇增，受攻擊面大幅擴張，使組織面臨的網路安全威脅與日俱增。

因此，從策略上來說，企業有必要採用更智慧、更安全、高度自動化的軟體定義廣域網路 (SD-WAN)，因為這個網路可與雲端提供的安全性服務無縫整合，形成頂尖的安全存取服務邊緣 (SASE) 架構。SASE 必須輔以以身分為基礎的零信任安全性，以強制執行網路區隔，讓使用者和 IoT 裝置只能存取與其業務角色相符的網路目的地。

由於 WAN 和安全轉型並非一蹴而就，所以企業可能會從 WAN 或安全防護的現代化改造開始，但要實現雲端投資的真正價值，就必須同時兼顧這兩個方面。

當今的企業網路從來都不是著眼於雲端優先世界而設計的，因此無法因應數位轉型面臨的網路安全挑戰。然而，企業不僅要保護雲端的應用程式，也要保護連線到這些應用程式的使用者，這些都非常重要。此外，IoT 裝置數量劇增，受攻擊面大幅擴張，使組織面臨的網路安全威脅與日俱增

而為了避免受限於廠商，選用提供彈性和選擇自由的技術解決方案合作夥伴也同樣重要。藉由轉型網路和安全架構，企業可以及時採用新的創新來加速生產力提升、收入成長和獲利能力增長，同時控制成本。

從雲端提供應用程式 — 安全性也應該從雲端開始

傳統模式下，來自分支機構的所有應用程式流量都透過私有 MPLS 服務回傳到公司資料中心，以便進行安全檢查和驗證 (請參見圖 1)。當應用程式是完全託管於公司資料中心時，這種架構尚屬合理。但是隨著應用程式和服務移轉到雲端，這種傳統的網路架構就顯現出了短板，不僅會削弱應用程式效能，也會造成不一致的使用者體驗，因為流向網際網路的流量在到達目的地之前，都要先經過資料中心和企業防火牆。

再者，隨著越來越多的員工在公司網路之外工作並直接連線到雲端應用程式，傳統的周邊式安全已不敷使用。雲端和 SaaS 永遠地改變了使用者連線至應用程式並與之互動的方式。透過轉型 WAN 和安全架構，企業可以確保跨多雲端環境直接且安全地存取應用程式和服務，而且不管何種位置或裝置，都能存取這些內容。

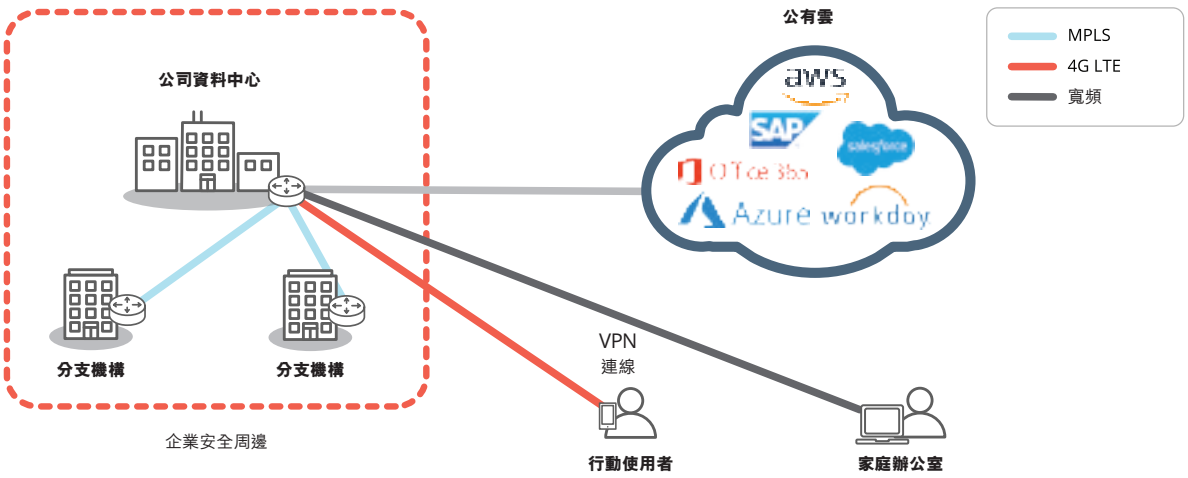

圖 1：傳統的企業 WAN 和周邊式安全方法在設計時並未考量到雲端。將所有應用程式流量從分支機構回傳到資料中心，會削弱效能並造成不一致的使用者體驗。

2019 年，Gartner 創造了 SASE (即安全存取服務邊緣) 一詞，這是用於將 SD-WAN 與雲端提供的安全性服務邊緣 (SSE) 功能相結合的架構，包含的功能有安全 Web 閘道 (SWG)、防火牆即服務 (FWaaS)、雲端存取安全代理 CASB) 和零信任網路存取 (ZTNA)。以前，這些都是獨特的專用功能，但現在可以透過雲端以統一的方式提供，如圖 2 所示。

SSE 解決方案的部分早期採用者，未能成功實作 SD-WAN，無法直接從分支機構站點套用適應性網際網路疏導機制。因此，他們無法將流量直接從分支機構站點引導到雲端。如果沒有 SD-WAN 元件，以雲端為目標的流量就仍需要回傳到資料中心，從而對應用程式效能產生負面影響。

採用安全性服務邊緣解決方案和 SD-WAN 可以消除管理多個內部部署防火牆的相關成本和複雜性，但仍需要分支機構站點的防火牆功能來阻止任何傳入的威脅。如圖 3 所示，採用進階 SD-WAN 解決方案時，企業可以使用寬頻網際網路連線，透過適應性網際網路疏導機制直接連線到雲端。辨識白名單應用程式的智慧功能，可以實現從分支機構到最近存在點 (PoP) 的在地疏導機制，藉此消除延遲，並為 Microsoft Office 365、8x8 和 RingCentral 等信任的 SaaS 和雲端應用程式提供最高品質的體驗。應用程式感知功能也可以先將其他網際網路綁定流量傳送到雲端提供的安全供應商進行進階檢查，然後再轉送到 SaaS 供應商。進階 SD-WAN 功能與雲端提供的現代安全性服務整合後，可確保對使用者、裝置、應用程式和 IoT 進行一致的原則強制執行和存取控制。如此一來，企業就能強制執行合規性、防止停機，並降低與安全漏洞相關的資料外洩風險。

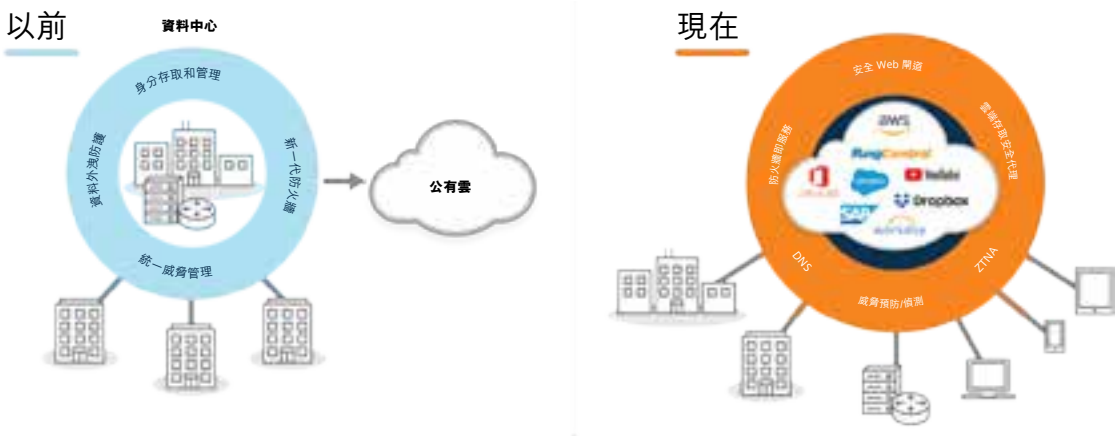

圖 2：過去，一切都是為了保護專門託管應用程式的企業資料中心。現在，應用程式已移轉到雲端並透過雲端提供，企業周邊式安全模式的效用正變得越來越微小。所以，另尋思路，將安全性移到雲端是勢在必行。

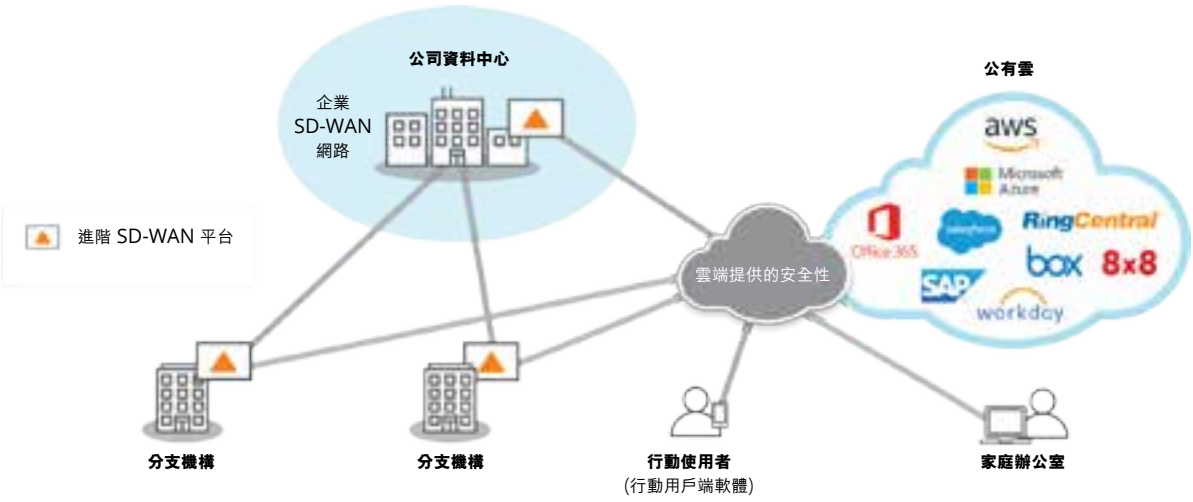

圖 3：進階 SD-WAN 為企業提供了邁入安全雲端的快捷之門。分支機構可以使用寬頻連線和適應性網際網路疏導機制，將使用者直接連線到雲端應用程式，藉此最佳化應用程式效能和使用者體驗。將進階 SD-WAN 和雲端提供的安全性相結合，可創造安全存取服務邊緣 (SASE)，確保使用者、裝置和應用程式始終安全無虞。

頂尖的 SASE 提供選擇的自由度

鑒於網路安全性方法日新月異，複合式網路解決方案的構建過程也錯綜複雜，評估哪些廠商擁有備受肯定的經驗和焦點領域，並可提供頂尖的安全和網路解決方案就變得非常重要。期望單一廠商能同時在這兩個領域提供頂尖的 SASE 功能，是不切實際的想法，企業不應被迫犧牲任一領域，只屈就使用基本功能。

由於威脅的形態不斷進化，安全性成為人們心中最關心的問題，企業必須保持敏捷性，才能以快速且符合成本效益的方式採用新的安全解決方案，而不必受制於單一廠商解決方案。擁有獨立的網路解決方案，可為企業提供保證，使其根據不斷演變的業務和安全需求，安心選擇及部署最符合需求的雲端安全解決方案。

進階 SD-WAN 解決方案可與多個 SSE 廠商緊密整合，讓您可以自由選擇頂尖的廠商解決方案，以便使用自動化協調功能，統一 SD-WAN 和雲端提供的安全性。有了頂尖的 SASE，企業就可以打造一致的安全架構，封鎖網路攻擊的影響，同時提高業務敏捷性並降低複雜性。如此一來，就能協助企業從現有和正在進行中的雲端應用程式和服務投資中取得乘數效應的收益。

使用零信任方法保護企業 IOT

企業 IoT 裝置數量劇增，衍生出監控、報告、警示、自動化和最佳化業務流程的新方法 — 從生產線到自動化 HVAC 和照明節能都是。IoT 透過自動化提高企業效率，但也因為引入新技術而產生的複雜性，使得受攻擊面隨之增加。為了因應日益增加的行動裝置安全挑戰，IT 選擇部署以零信任模式為基礎的零信任網路存取 (ZTNA) 解決方案。ZTNA 解決方案會在筆記型電腦、平板電腦或手機等使用者裝置上安裝端點代理程式。

該軟體代理程式可確保先將裝置傳出的流量導向至雲端提供的安全性服務，然後再導向至 SaaS 應用程式或 IaaS 供應商。但是，與平板電腦和智慧型手機不同的是，IoT 裝置無法安裝 ZTNA 軟體代理程式，因為這些裝置採用無代理程式設計，不支援安裝協力廠商軟體代理程式。因此，企業需要為 IoT 裝置提供不同的安全解決方案，藉此保護企業網路不受潛在漏洞的威脅，進而防止網路遭到入侵或日常業務營運中斷。

支援零信任架構的進階 SD-WAN，可以動態區隔網路並套用最低權限存取原則，讓企業能在部署 IoT 裝置時降低安全漏洞相關風險。這個架構可確保使用者和裝置只能根據身分、存取權和安全狀態，與符合其角色的目的地通訊。它會協調橫跨企業 LAN-WAN-LAN 和 LAN-WAN-資料中心/雲端的端對端區隔，從而實現一致且自動化的安全性原則強制執行，同時提高網路的可見性。透過端對端區隔，企業可以為 IoT 裝置流量建立隔離的區隔。您可以為每個區隔定義獨立的安全性原則，藉此定義強制執行的裝置流量安全性原則。由於一個區隔中的流量與所有其他區隔中的流量隔離，因此可以防止任何未授權的存取。即使出現威脅，其影響也只會局限於所在的區隔內。

讓我們看一個例子。在安裝了 PoS 和 HVAC 系統等無代理程式 IoT 裝置的遠端站點中 (下圖 4)，進階 SD-WAN 平台能以獨特方式識別裝置使用的應用程式。有一個系統原則會攔截 PoS 流量，並將其導向到託管信用卡交易處理應用程式的公司資料中心。在本例中，我們套用了部署在資料中心的現有防火牆安全性服務。另一方面，HVAC 系統原則會對 HVAC 流量進行區隔，並將其導向至雲端提供的安全性服務，以進行額外的安全檢查，之後再傳送到託管在公有雲的 IoT 控制中心。由於 IoT 流量是根據業務原則進行隔離，因此 HVAC 區隔中的安全漏洞不會危及 PoS 區隔中的信用卡和個人資料或使其面臨風險。網路區隔也有助於組織滿足業務的 PCI (或其他) 合規性要求。如本例所示，採用進階 SD-WAN 平台的全方位安全部署可以更好地保護當今動態變化中的企業，讓他們在轉型過程中，既能擁抱 IoT 的優勢，也能確保自身安全。

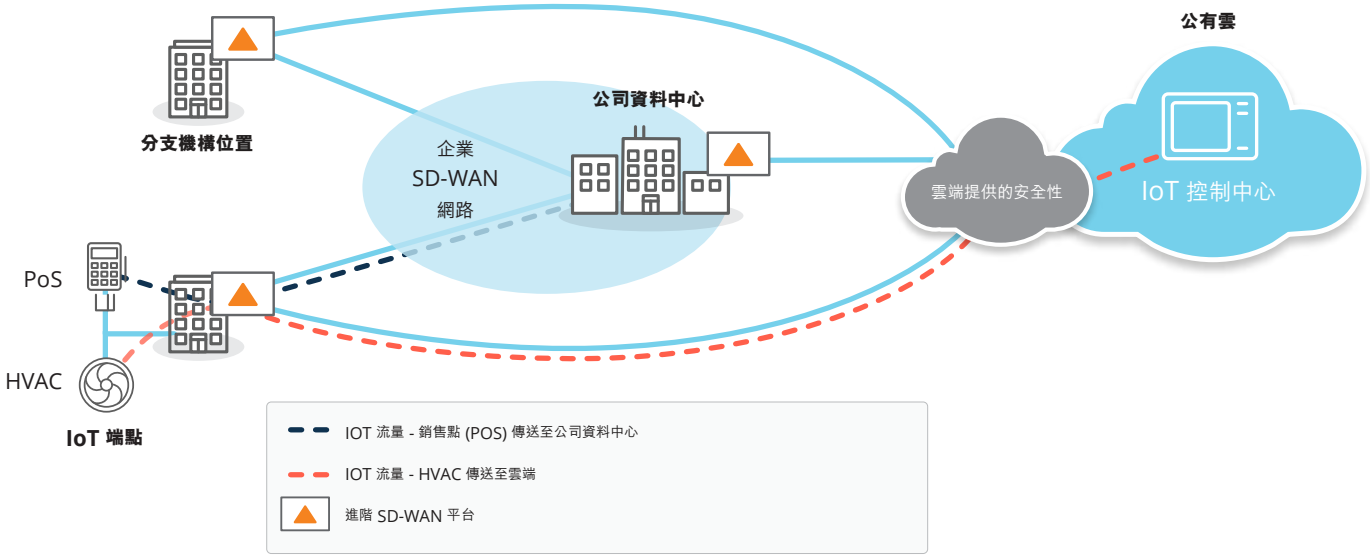

圖 4：IoT 端點數量倍增，也帶來新的安全漏洞風險。利用進階 SD-WAN 平台，企業可以實作零信任架構來保護 IoT 裝置，並隨需動態區隔網路。如圖所示，來自分支機構的所有 PoS 交易資料都會傳到企業資料中心，而 HVAC 流量則會路由到雲端的 IoT 控制中心。

使用進階 SD-WAN 保護分支機構免遭外部威脅

隨著企業的數位化，過去十年，網路攻擊風險顯著增加。在傳統的路由器型網路環境中，分支機構堆積了大量的網路和安全設備，但這些設備難以進行配置、維護，無法及時跟上最新的威脅趨勢。遠端站點也欠缺經驗豐富的 IT 人員，因而暴露於潛在的安全漏洞中。

除了使用頂尖的 SASE 保護雲端營運外，進階 SD-WAN 解決方案也可以保護分支機構免於惡意威脅。這個解決方案採用新一代防火牆打造而成，內建威脅防禦功能，例如入侵偵測和預防 (IDS/IPS) 以及 DDoS 等，可有效保護分支機構免於惡意威脅。

以特徵為基礎的 IDS 系統，通常會監控網路流量以找出與特定攻擊特徵相符的模式。當偵測到入侵時，感應器會提供捨棄、檢查及允許流量等處理動作。入侵防禦系統可以在嚴格模式或高效能模式下執行。在嚴格模式下，流量會經過感應器，因此在發生入侵時，就會立即封鎖流量。在高效能模式下，系統會傳送流量副本進行分析，藉此提供更高的效率，而不影響網路效能。一旦偵測到入侵，就會立即封鎖。組織可以根據自己的安全需求，在嚴格模式或高效能模式之間進行選擇。

進階 SD-WAN 還可以動態偵測 DDoS 攻擊，例如通訊協定攻擊、ICMP 洪水攻擊、SYN 洪水攻擊和 IP 詐騙攻擊。在偵測到異常的網路行為後，這個解決方案會使用快速老化、捨棄過多數量、封鎖來源等處理動作，來限制要求的數量。此外，萬一遭到 DDoS 攻擊，也可以透過不受影響的網路連結來路由流量，確保業務永續性。

透過將進階網路與安全功能 (例如路由、WAN 最佳化和新一代防火牆) 整合到一個單一 SD-WAN 解決方案中，組織將可以大大簡化分支機構的網路營運。此外，安全性原則可以透過零接觸配置，從中央位置自動推送到分支機構，藉此協助進行網路和安全性原則的配置。新分支機構的設定既快速又輕鬆，安全性原則變更可在幾分鐘內自動散發到數百或數千個分支機構，同時還能將錯誤降至最低。

WAN 轉型對於數位轉型的成功至關重要

除了移轉到雲端提供的現代安全架構的所有好處之外，當今的雲端優先企業推動 WAN 轉型也有極大的價值。傳統以路由器為中心的 WAN，從來都不是著眼於雲端而設計的。企業必須對其 WAN 架構進行現代化改造，並重新思考如何以最好的方式架構分支機構網路，以提高雲端應用程式的效能和安全性。企業對於雲端和 SaaS 的使用日益增加，其目的重在為使用者提供最高品質的體驗。

WAN 轉型包括在使用者和雲端之間提供更有效的路徑和更好的體驗。如前所述，直接從分支機構位置對雲端託管的應用程式和 SaaS 應用程式採用適應性網際網路疏導機制，不僅可以最佳化可用頻寬，還可以減少任何可能對使用者生產力產生負面影響的延遲。

許多組織都在開展網路邊緣的轉型，並擁抱 SD-WAN 以使用寬頻網際網路連線來連接分支機構。SD-WAN 會根據集中定義的原則，跨越多個 WAN 連結 (MPLS、寬頻網際網路、LTE 等) 提供應用程式導向型智慧路徑選擇。SD-WAN 的優勢包括：

- 提供具有成本效益的業務應用程式交付
- 改善應用程式效能、可用性和終端使用者體驗品質
- 滿足現代分支機構/遠端站點或位置的需求
- 可適應 SaaS 和雲端型應用程式和服務
- 透過自動化服務佈建，提高分支機構的 IT 效率

滿足應用程式 SLA 的要求

這會直接促成企業生產力和業務敏捷性的改善。企業需要一個高效能網路，這個網路必須建立在高度可用的基礎上，能可靠地支援關鍵業務應用程式。面對安全，絕對不可抱持亡羊補牢的想法。微區隔功能和精細的原則強制實施，讓企業能保護 WAN 的安全、符合合規要求，並防禦安全漏洞。

企業需要敏捷性來快速啟動新的分支機構，也需要動態調整原則和安全規則。傳播原則內容的能力，是分支機構自動化的關鍵需求。因此，進階 SD-WAN 解決方案的概念極具吸引力，因為可以讓企業不再需要執行專用安全功能的多個裝置，進而簡化及整併 (或「精簡」) 分支機構的 WAN 邊緣架構。進階 SD-WAN 邊緣平台讓企業能透過單一集中管理平台，統一 SD-WAN、路由、WAN 最佳化、區隔和分支機構的安全性，進而實現 WAN 轉型。

集中式 SD-WAN 協調和特定於應用程式的方法，可確保網路的行為模式始終反映業務的優先事項。將網路和安全性原則的協調統一，也能確保 QoS 和安全性始終如一地套用於應用程式 (或應用程式類別) 並強制實施，無論以何種方式或在何處存取應用程式。應用程式效能和安全性可透過由上而下的業務原則來設定，而不受到由下而上的技術約束。進階 SD-WAN 會持續監控網路和應用程式的狀態，偵測不斷改變的狀況，並立即觸發自動化的即時回應，以免斷電、停電和安全威脅等事件的影響。再者，透過應用程式可程式化介面 (API) 的整合，將雲端平台連線功能自動化，也可以簡化 IT 營運，讓企業可以及時存取雲端提供的安全性服務、IaaS 和 SaaS。當今的網路需要端對端的可見性、程式化能力和自動化，藉此動態保障多雲端環境所需的效能、安全性和最高體驗品質。採用頂尖 SD-WAN 和雲端提供安全性解決方案架構的智慧型 WAN，可推進數位轉型措施，讓企業能在不限制其生產力和成長的情況下，及時演進及擁抱新的創新技術，同時將安全風險降至最低。

結語

隨著現代雲端優先企業不斷將應用程式從資料中心移轉到雲端，他們必須擁抱 WAN 和安全轉型，才能實現雲端投資的最大報酬。SASE，也就是安全存取服務邊緣，將會帶動整個產業轉往新方向。如圖 5 所示，企業在架構安全存取服務邊緣以實現無縫體驗時，必須同時考量 WAN 和安全轉型。

進階 SD-WAN 平台可以無縫連線到各種頂尖的雲端安全性服務，從而提供頂尖的 SASE 架構。歸根結底，沒有任何一家 SASE 廠商能真正透過單一平台同時提供頂尖的網路和安全技術。隨著威脅的型態不斷進化，企業必須要保持敏捷，才能以快速且具成本效益的方式採用新的安全解決方案。企業可以獲得更好的服務，在評估不同的平台後自由選擇最合適的那一個，用來整合頂尖的 SASE。這樣，就可以避免受制於專有的單一廠商解決方案，或是避免屈就於基本特色和功能。

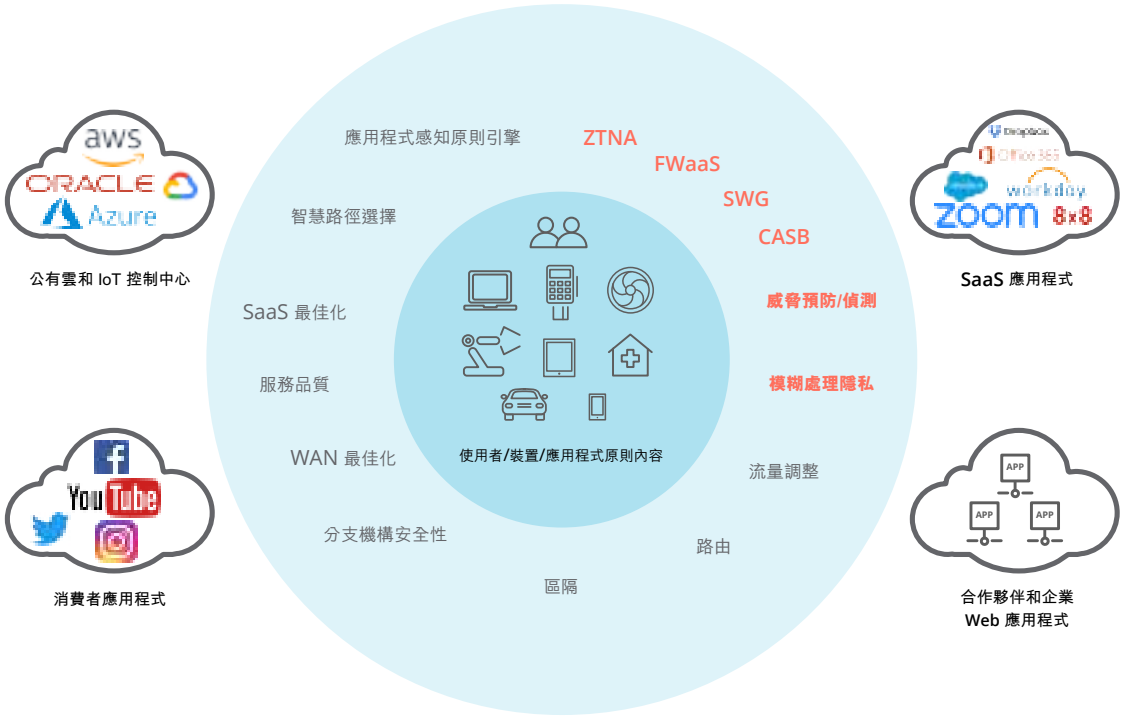

圖 5：需要安全的存取服務邊緣來支援企業的數位轉型措施，即雲端優先策略和員工行動性需求。在強大的 SASE 架構中，全方位的 WAN 功能必須與全方位的網路安全功能相結合，才能支援數位企業針對使用者、裝置和應用程式的動態、安全存取需求。

此外，隨著 IoT 裝置數量激增，SASE 必須輔以零信任安全架構，以便根據身分動態區隔流量，使使用者和 IoT 裝置只能存取與其業務角色相符的網路目的地。

進階 SD-WAN 可將新一代防火牆與 IDS/IPS 功能相互整合，以支援分支機構所需的基本安全功能，也可與雲端提供的安全性互補，從而在整個企業中無縫強制實施端對端安全性原則。如此一來，企業就能簡化自己的網路基礎架構，並有機會按照自己的步調轉換到現代的雲端優先安全 WAN 架構，而不需要有所妥協。

最後，有的企業可能還沒有準備好淘汰分支機構防火牆，無法完全轉向雲端提供的安全模式，但重要的是找到一個可提供選擇自由度的進階 SD-WAN 平台，以便支援業界領先的協力廠商統一威脅管理 (UTM) 軟體解決方案，同時在分支機構將這些解決方案當成一個整合式解決方案來執行。如此，不僅可消除使用個別專用防火牆時往往會產生的額外成本和管理複雜性，還可以為企業提供部署頂尖解決方案的彈性，終而協助企業順暢移轉到雲端提供的安全模式。

隨著企業繼續在雲端方面進行大筆投資，必須兼顧 WAN 和安全轉型的需求終究會讓企業走上正確的道路，從而為使用者提供最高品質的體驗，同時因應當今的網路安全挑戰。經過深思熟慮後踏上毫不妥協的 WAN 和安全轉型之旅，最終將使企業有能力保護自己的數位資產，並從現有和持續的雲端投資中，獲得乘數效應的收益。

aruba
a Hewlett Packard Enterprise company

BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932zht

聯絡我們：www.arubanetworks.com/contact