



報告

2023年零信任現況調查報告

摘要

隨著分散式網路的不斷擴充以及混合辦公模式的普及，當下網路環境日益複雜且難以預測。員工通常需在企業辦公室、居家辦公或其他辦公地點之間隨時隨地存取企業網路。應用程式也同樣分散部署於本地、雲端中或以軟體即服務（SaaS）模式交付。以往，本地數據中心承載著幾乎所有關鍵數據，如今卻衍生出分佈在多個位置的多個數據中心，呈現分散化趨勢。IT 團隊的首要任務是確保所有用戶和設備均能安全可靠地存取所需關鍵資源，且無論應用程式和資產部署在何處，均能確保任意位置用戶隨時隨地進行輕鬆存取。

Fortinet《2023 年零信任現狀調查報告》著重介紹了在疫情全球肆虐引發的網路劇變下，IT 團隊在應對網路安全新常態方面取得的新進展。受大環境影響，網路邊界外的辦公用戶數量驟然增加，IT 團隊爭相忙於確保業務連續營運。然而，應急的快速修復和變通方法，進一步暴露了遠端辦公策略存在諸多薄弱環節。此外，該報告還深入剖析了將快速擴充的網路環境置於統一安全保護傘下所面臨的各項挑戰。

因安全性薄弱的居家辦公或安全經驗不足的 DevOps 團隊錯誤設置雲端解決方案引發的異常網路環境，勢必淪為網路駭客新的攻擊載體。顯而易見，許多組織中的隱式信任模型存在安全隱患。面對此類問題，多數 IT 團隊紛紛採取堆疊不同技術等傳統方式加以應對。然而不久後，新的難題又隨之湧現，即如何令孤立執行的單點解決方案實現協同執行。本報告對上述挑戰進行了充分闡釋，其中包括一些關鍵發現。

儘管不同規模組織均積極部署零信任戰略，但挑戰依舊如影隨形。

- 自 2021 年問卷調查以來，企業已部署了多種解決方案，作為其零信任戰略的組成部分。
- 企業正積極尋求覆蓋任意網路位置的全面零信任解決方案，盡可能減少違規行為或漏洞引發的負面影響。
- 儘管企業正逐步推進零信任戰略，但依然面臨不同解決方案間的協同執行、一致可見性、點到點策略進行和應用程式存取延遲等各類挑戰。
- 受訪者還表示缺乏可靠的產品資訊，幫助其選選和設計貼合企業自身需求的解決方案。

理想的解決方案應能跨本地和遠端用戶進行一致的應用程式存取策略，而現實則喜憂參半。

- 市面上的零信任網路存取（ZTNA）和安全存取服務邊緣（SASE）等諸多解決方案，通常僅支援根據雲端部署。然而，企業需確保本地和網外用戶安全存取應用程式。值得注意的是，近 40% 的組織仍將超半數應用程式部署於本地。
- 當前，任何零信任策略最大的挑戰在於，需在本地和雲端環境之間實現更廣泛的整合。
- 四分之三（75%）的受訪者過於依賴僅根據雲端的 ZTNA，而遭遇混合辦公環境防護挑戰。
- 企業部署 SASE 解決方案所關注的首要優先事項各不相同，但 58% 的受訪者均將「安全有效性」列為三大優先事項之一。

供應商的全面整合和解決方案之間的協同執行至關重要。

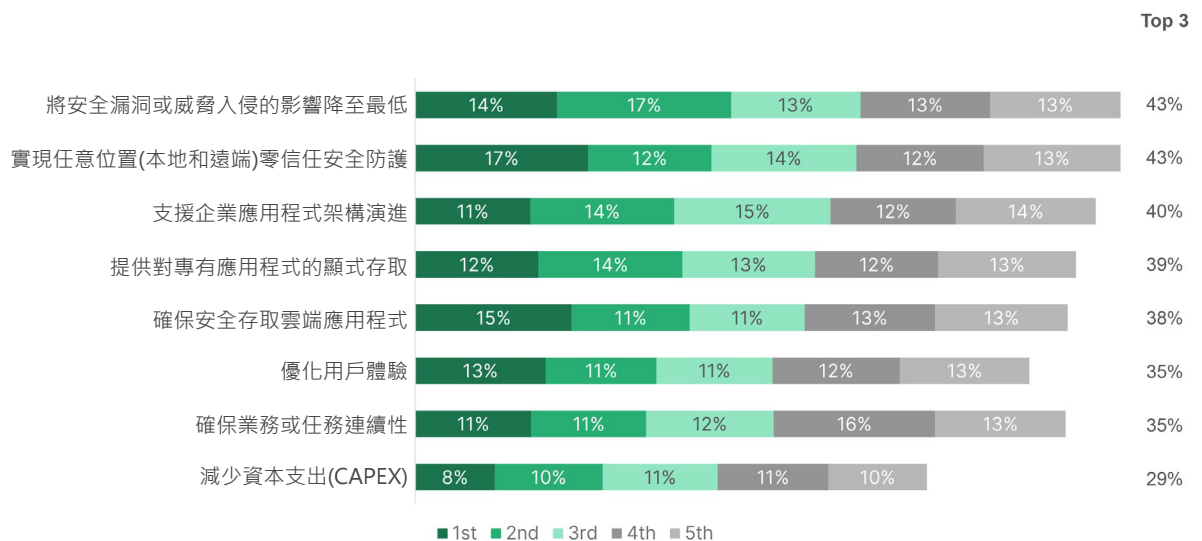
- 部署多家供應商的單點解決方案為組織帶來新的安全漏洞以及高昂營運成本等諸多挑戰。
- 大型企業正積極尋求全面整合的解決方案，以期簡化營運並降低成本。

零信任策略優先事項

受疫情影響，許多企業要求員工進行居家辦公，這一舉措推動全球企業辦公模式加速轉型。網路環境也隨之迎來巨變。幾乎一夜之間，組織需透過邊界創建對關鍵應用程式和資源的安全網路存取，而滿足這一要求通常需升級邊緣安全工具等遠端存取技術。與此同時，駭客伺機透過安全性薄弱的家庭網路劫持 VPN 隧道，進而橫向入侵企業敏感資源，傳統 VPN 技術局限性日益凸顯。有鑑於此，企業加速將應用程式遷移至雲端，以減輕網路邊界的防護壓力，並優化用戶體驗。

此前，混合辦公模式已日漸流行，網路環境也隨之悄然改變，但全球疫情肆虐顯然加速了這一進程。驟然切換至遠端辦公模式，令許多組織猝不及防，缺乏相應技術部署也令其無法進行充分防護。儘管存在諸多問題，但隨著業務發展的需要，三分之二（67%）的組織決定繼續採取混合辦公模式。相比小型企業雇主，大型企業雇主更傾向於支援員工採用遠端辦公模式。

然而，隨之而來的挑戰在於，如何為採取本地辦公+遠端辦公模式的員工，提供一致的安全存取和卓越的用戶體驗。對於部署僅根據雲端的 ZTNA 解決方案的組織（72%）而言，提供對關鍵應用程式的安全存取尤為困難。

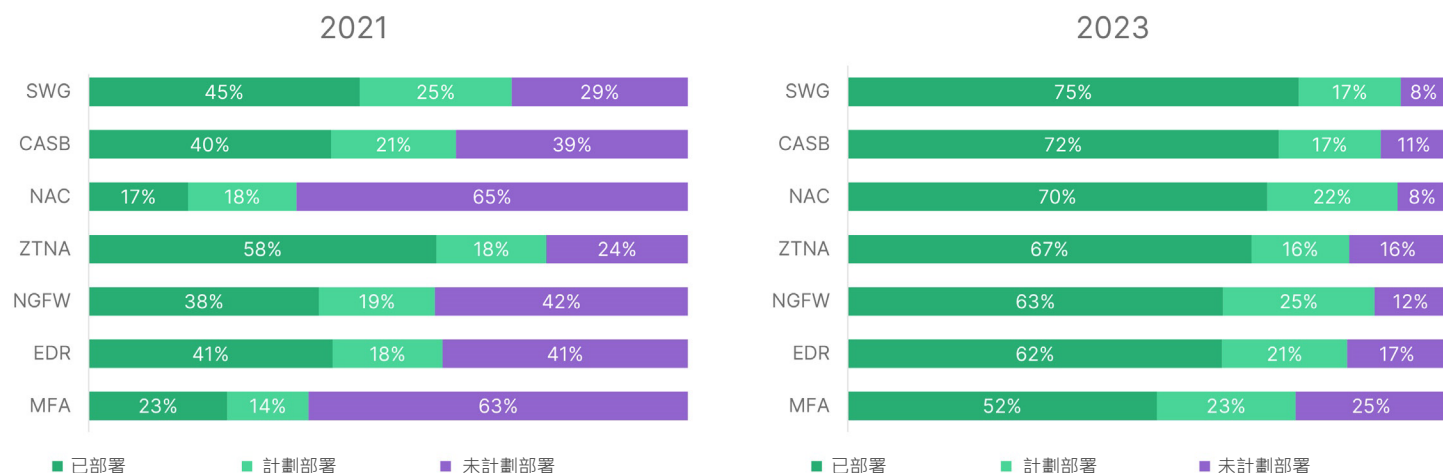


零信任策略優先級

顯然，管理和保護混合辦公用戶的最佳方法是部署零信任策略，避免根據位置的預設信任模式帶來的防護弊端，並在滿足存取需求的同時確保最低存取權限。普遍而言，部署零信任策略的原因和動機較為廣泛，但 34% 的受訪者認為，這一策略最大限度地減少了違規行為和威脅入侵引發的負面影響，29% 的受訪者則表示，實現任意位置的零信任安全防護是其主要部署動機。值得關注的是，僅有 18% 的受訪者選擇減少資本支出。儘管他們選擇零信任解決方案的首要目標（優先級為非常或極其重要）是確保應用層安全性（85%）但與本地部署和雲端環境的兼容性（82%）以及與網路和安全基礎架構其餘組件的整合（82%）同樣也非常重要。

受訪組織還表示，已部署各種解決方案支援零信任戰略，且已為支援和保護混合辦公環境做好充分準備。已部署的解決方案及佔比分別為：安全網站閘道（SWG）- 75%，雲端存取安全代理（CASB）- 72%，網路存取控制（NAC）- 70%，零信任網路存取（ZTNA）- 67%，新世代防火牆（NGFW）- 63% 以及端點偵測和響應（EDR）- 62%。令人驚訝的是，有效防範未經授權存取應用程式和其他資源的多因素身份驗證（MFA）解決方案的部署率則相對較低，僅為 52%。

那些尚未實施零信任戰略的組織表示，他們計劃投資許多相關的解決方案，作為其零信任戰略的組成部分。相比 2021 年，這些解決方案的部署佔比均大幅提升：SWG（從45%上升至75%）、CASB（從40%上升至72%）、NAC（從17%上升至70%）、ZTNA（從58%上升至67%）、本地 NGFW（從38%上升至63%）、EDR（從41%上升至63%）以及 MFA（從23%上升至52%）。



已部署或計劃作為零信任策略組成部分部署的解決方案

然而，組織在部署零信任戰略方面仍舊面臨嚴峻挑戰。近半數受訪者（48%）表示，本地和雲端中部署的零信任解決方案之間無法有效集成是當前亟待解決的最關鍵挑戰。這一關鍵發現可能是後續多項常見調查反饋的主要誘因，即無法持續對用戶和設備進行一致的身份驗證（46%）策略，無法提供一致的用戶體驗（40%），以及無法在身份驗證後持續監控用戶行為（38%）。

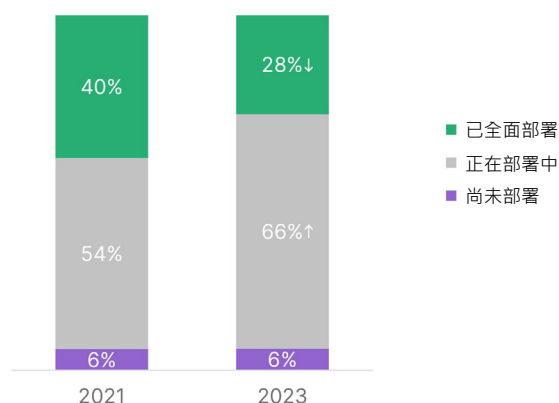
此外，另一重大發現是，近三分之一（31%）的受訪者還表示，網路延遲是其當前面臨的一項重大挑戰，近四分之一（22%）的受訪者則表示目前過度依賴傳統 VPN。顯然，部署低延遲解決方案對於成功部署 ZTNA 至關重要。

部署現狀和安全挑戰

2021 至 2023 年問卷調查期間，零信任部署現狀發生了巨大變化。2021 年，40% 的受訪者表示已全面部署零信任戰略。但 2023 年，這一比例僅為 28%。而僅有 36% 的製造企業表示已全面部署零信任戰略，這可能是因為製造業同樣亟需實現資訊技術（IT）和營運技術（OT）網路的整合。目前正在推進零信任戰略部署的受訪者數量上升至 66%，高於 2021 年的 54%。

部署現狀發生巨大轉變的背後存在以下幾大誘因：首先是零信任部署範圍得以不斷拓展。初期，企業的部署動力是確保遠端辦公用戶快速安全地存取應用程式。然而，隨著混合辦公模式的興起，用戶在本地和遠端辦公位置之間不斷切換，數據和應用程式也同樣分散部署於雲端和數據中心，主體保護範圍也隨之逐漸擴大。但是，企業要求無論何時何地均應能確保一致的數據存取體驗，這即意味著所需技

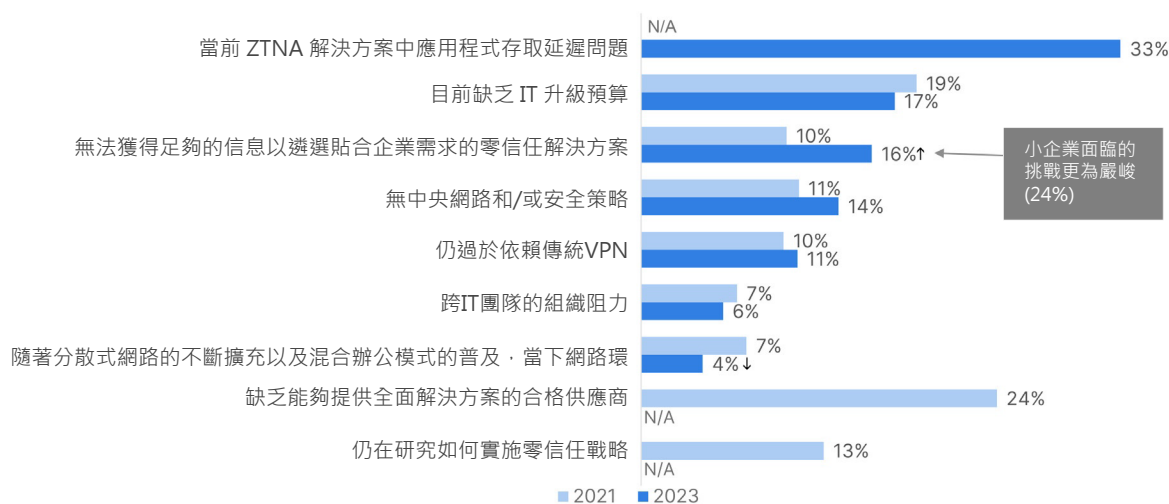
處於零信任戰略署的 哪一階段



零信任部署現狀轉變趨勢

最初人們認為，數據流只是從用戶流經應用程式再返回數據中心。如今，單筆業務的工作流通常需跨多個環境，這一改變大大增加了零信任策略部署的複雜性和規模。雲端解決方案亟需與本地網路組件無縫整合，以實現一致的點到點策略進行，有效檢測和防範威脅橫向行動。

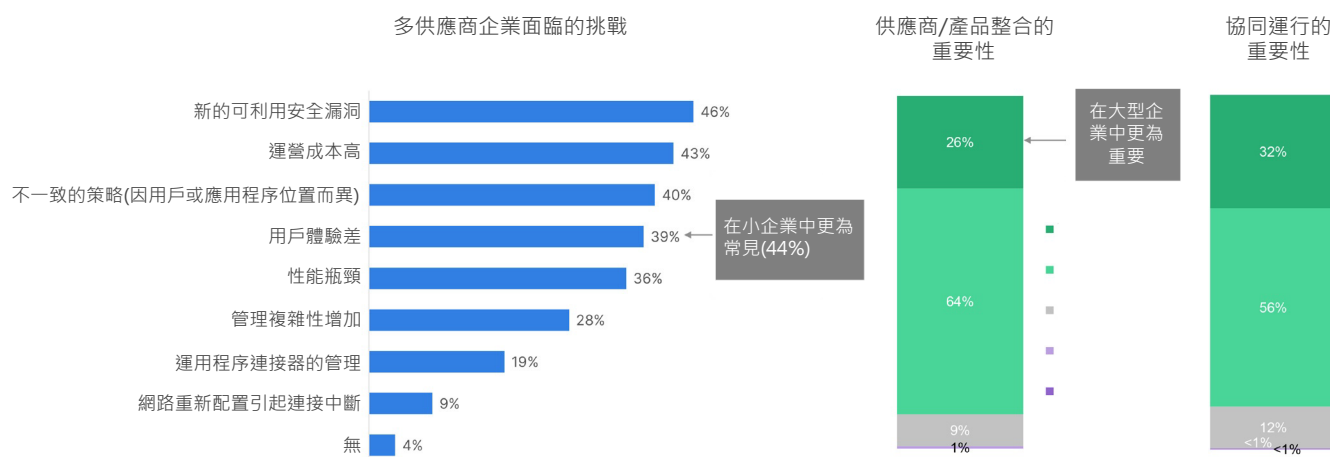
部署趨勢發生變化的另一大原因是，一些解決方案已部署就位後，某些問題才隨之顯現，此外，安全孤島中的單點解決方案之間的連動難題同樣亟待解決。眾所周知，孤立執行的單點解決方案想要實現協同執行困難重重，故障排除時的暫行解決方法可能會消耗大量 IT 資源。目前，企業面臨的兩大阻礙是：16% 的受訪組織（小型企業為24%）表示無法獲得足夠的產品資訊，以選擇貼合企業自身需求的零信任解決方案，四分之一（24%）的受訪者表示，缺乏能夠提供全面解決方案的合格供應商，權宜之計，只能自行拼湊或疊加部署單點解決方案。僅有4%的受訪者表示面臨人力資源短缺難題（低於7%）。一旦混合辦公模式實現常態化，企業便亟需部署更一致和可靠的解決方案，且



部署零信任解決方案的最大挑戰

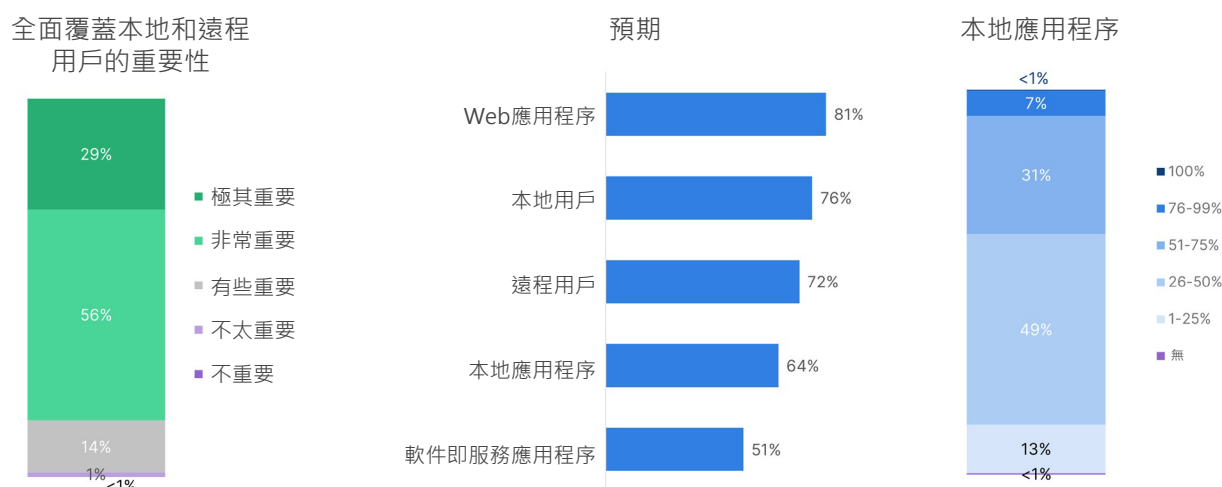
本報告的另一個關鍵要點是，部署多家供應商解決方案為組織帶來各類新的挑戰，包括因供應商和解決方案疊加而無意間引發的安全漏洞和高昂營運成本。據調查顯示，當前，90% 的組織將供應商和解決方案全面整合列為極其重要或非常重要事項，88% 的組織同樣極為關注解決方案間的協同執行。與前一次調查相比，這種認知方面的變化使得許多以往認為自身已全面部署零信任解決方案的組織，開始重新審視這一結論。顯而易見，實現供應商和產品的全面整合和協同執行對於成功部署零信任戰略而言至關重要。

近半數受訪者（46%）表示，當前最棘手的問題莫過於單點解決方案之間無法實現互聯互通，以及因此產生的新可利用漏洞和入侵風險。40% 的受訪者還表示，當前無法實現一致的策略部署和進行。與這些發現息息相關的現狀是，試圖確保安全孤島中單點解決方案正常執行的高昂成本，43% 的受訪者認為這一難題是其當前面臨的最大挑戰。其他相關挑戰包括用戶體驗差（39%），效能瓶頸（36%）和管理複雜性增加（28%）。



為何全面整合和互操作性至關重要

儘管聲稱一切都在向雲端中遷移，但多數組織仍沿用應用程式和數據的混合部署策略。令人驚訝的是，38% 的組織仍然將超半數應用程序部署在本地。另有 49% 的受訪者將 26% 至 50% 的應用程式部署在本地。鑑於此，85% 的受訪者將部署覆蓋本地和遠端用戶的 ZTNA 解決方案列為非常重要或極其重要事項。受訪者一致認為 ZTNA 應能覆蓋任意位置提供全面保護，無論應用程式和用戶位於何處，混合 ZTNA 策略的主要防護領域應涵蓋 Web 應用程式（81%）、本地用戶（76%）、遠端用戶（72%）、本地應用程式（64%）和硬體即服務（SaaS）應用程式（51%）。



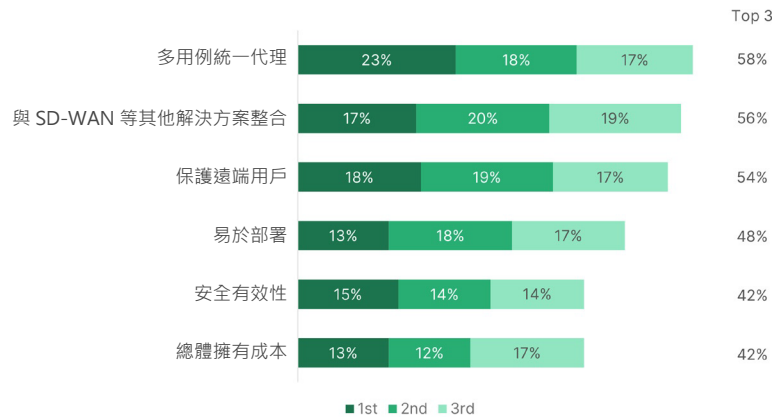
ZTNA 解決方案需全面覆蓋用戶和應用程式，無論其位於何處

值得注意的是，四分之三的受訪者表示，因過於依賴僅根據雲端的 ZTNA 而面臨混合辦公環境防護挑戰，因而亟需部署一款通用 ZTNA 解決方案，為其提供一致的功能和策略，全方位保護跨雲端和本地部署的應用程式，與此同時，該解決方案還應支援每用戶授權模型，以便隨時隨地辦公（WFA）用戶在居家和本地辦公室之間切換時，安全防護（和授權證）可隨之無縫。

SASE 整合

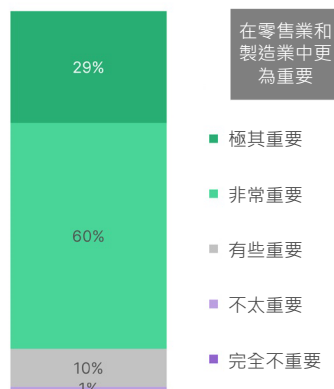
任何零信任策略的一大關鍵要素在於能夠提供一種簡便無縫的防護機制，為遠端和居家辦公用戶提供一致安全性。眾所周知，在向混合辦公模式過渡的早期階段，高效保護安全性薄弱的居家辦公是企業面臨的最重要挑戰。然而，將企業級安全性擴充至這些環境既耗費高額成本又會佔用大量資源，因此 SASE 解決方案應運而生，迅速成為確保遠端辦公用戶安全高效存取根據雲端應用程式的不二之選。

然而，新的挑戰再次出現，多數 SASE 解決方案無法與物理網路實現無縫連動。連接、策略和監控等必備功能需另行透過某種經設計和管理的機制進行交付。因此，儘管安全有效性是 SASE 解決方案的重中之重（58%），但 56% 的受訪者還希望擁有一個支援多個用例的統一代理，54% 的受訪者希望 SASE 能夠與 SD-WAN 等其他解決方案實現協同執行，42% 的受訪者希望 SASE 解決方案應易於部署且總體擁有成本可控。



SASE 解決方案優先事項

89% 的受訪者認為，SASE 與本地解決方案的無縫整合非常重要或極其重要。這一整合優勢的價值在於，能夠持續加強用戶體驗、透過整合任務簡化營運、全面進行一致的零信任策略以及安全存取雲端應用程式。這充分錶明，SASE 整合解決方案可將網路和安全融合功能覆蓋至位於分佈式環境的所有用戶和設備提供，許多組織可從單一供應商 SASE 解決方案中獲益。



SASE 與網路其餘組件全面整合的重要性

結論

隨著混合辦公模式的常態化以及本地、多雲和雲端服務（如SaaS）等應用程式部署模式的不斷演進，持續推動組織加速從隱式信任模型過渡至零信任架構。無論何時何地，均能確保可靠的應用程式存取、一致的安全性和優化的用戶體驗，成為這一轉變的關鍵驅動因素。然而，挑戰在於，多數網路環境複雜且瞬息萬變，應用程式分散部署於雲端和本地數據中心，而用戶辦公地點也在居家環境和企業辦公室之間不斷切換。因此，部署零信任戰略比許多組織最初預想得要複雜且困難得多。組織通常很少或根本無法從供應商處獲得可靠的技術指導，且許多供應商僅提供根據雲端部署的安全解決方案。

隨著零信任細分市場的不斷成熟，已開始實施零信任戰略的組織必須全面整合其供應商及其解決方案，以打造跨多個環境，且支援將網路與安全性及高效存取融合至單一整合架構的解決方案。透過這種解決方案，組織可將零信任策略無縫擴充至位於網路任意位置的所有用戶和應用程式，同時保持廣泛的點到點可見性和控制能力。唯有如此，組織才能充分利用當今混合戰略優勢，不斷開創新的商機，立於不敗之地。



www.fortinet.com/tw