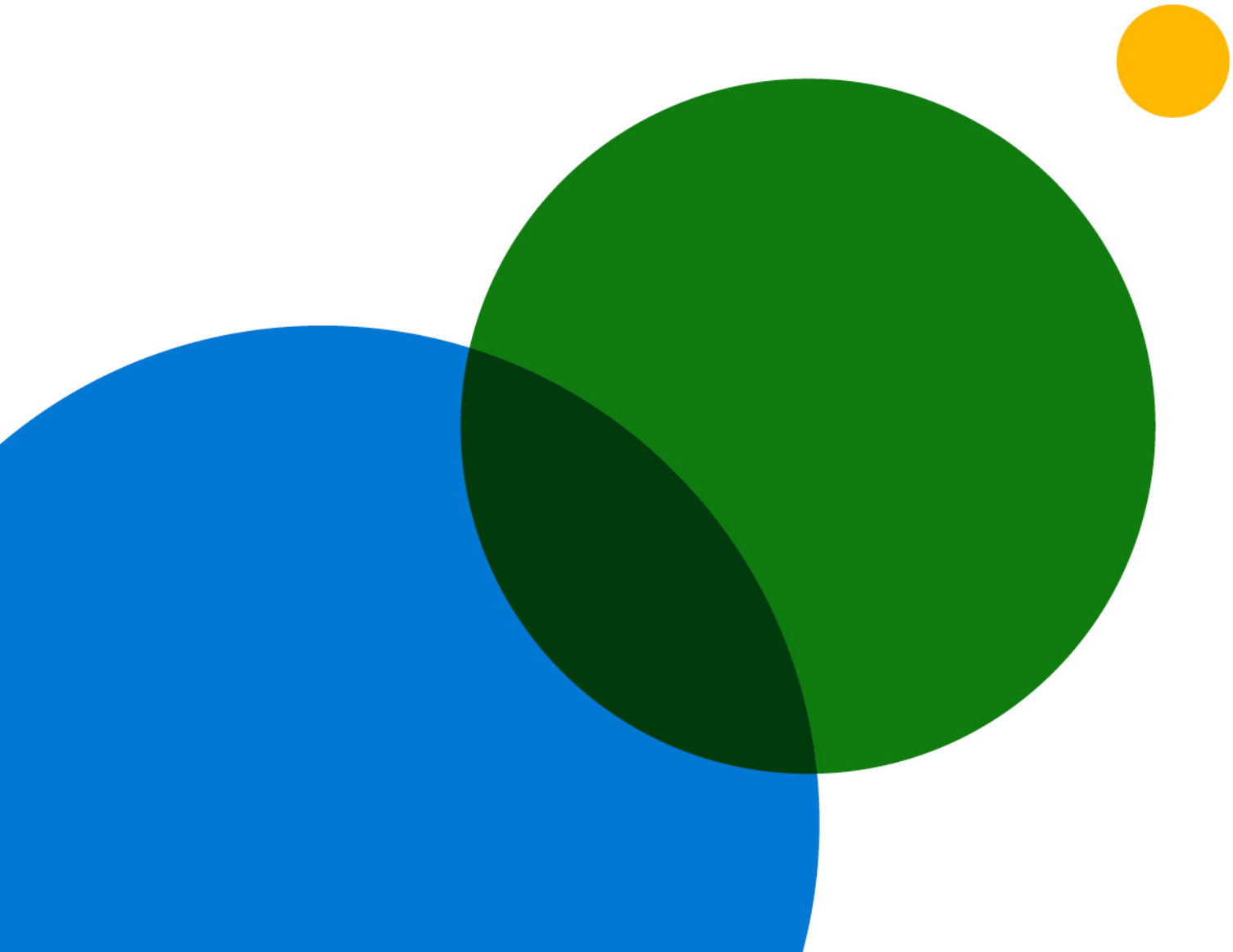
Microsoft Security

hypothesis

零信任採行報告



目錄

03
前言

06
訪談對象

04
方法

07
整體研究學習

05
採行零信任需要了解的事項

24
詳細的研究目標與招募對象

前言

Vasu Jakkal/公司副總裁，安全性、合規性和身分識別部門

過去一年，網路安全性演進有非凡的成就，零信任的興起也成為全球企業與組織的一項指導策略。

從疫情爆發的那一刻起，一夜之間，所有人幾乎都必須從遠端完成工作。這種轉變迫使許多組織快速適應，支援員工以各種方式完成工作：使用個人裝置、透過雲端服務協作，以及在公司網路疆界外共用資料。隨著各大組織逐漸適應這種轉變，他們也要面對目標定位、戰術和資源供應益趨成熟精進的網路罪犯。

混合式工作型態已成目前的現實。在此背景下，根據接受調查研究的組織所述，為因應快速變化，他們依賴零信任來提升安全性和合規性的靈活度、加快威脅偵測和補救的速度，以及提高安全性分析的簡易性和可用性。

根據明確驗證、使用最低權限存取和採行「假設存在缺口」思維等原則，在身分識別、端點、應用程式、基礎結構、網路和資料之間建立了全方位的零信任架構防護措施，同時提高可見度、自動化和協調流程。我們不僅向客戶和合作夥伴推薦這種方法，也在 Microsoft 的全球安全性和軟體發展中推行此方法。

此報告揭示了多元化市場和各行各業採行零信任的前景。我們希望此研究結果能協助您加速採行自己的零信任策略，提攜同業共同進步，並提供有關此快速發展領域未來發展的見解。

方法

Microsoft 委託 Hypothesis Group (一所提出見解、設計和策略的研究機構) 進行零信任採行報告和研究。這項研究包含美國境內突顯零信任採行趨勢和動力的兩個階段，以及在第二階段加入開展全球趨勢的其他市場。

初始研究於 2020 年 8 月展開，當時在美國進行了 15 分鐘的線上調查，合計有各行各業各企業公司 300 名負責零信任策略決策的安全性決策者 (SDM) 參與。除線上調查外，另於 2020 年 9 月對美國一些行業的 SDM 進行了五次線上深度訪談。

2021 年 4 月，針對美國、德國、日本和澳洲/紐西蘭一群類似的安全性決策者展開全球研究。900 多名參與者進行了 15 分鐘的線上調查，問題涵蓋零信任策略採行、最佳做法、優點、挑戰及未來投資方式等方面。

採行零信任需要了解的事項

01 / 組織準備將零信任策略資本化，這項行動因混合式辦公的趨勢和 Covid-19 而加速

安全性決策者 (SDM) 表示，制定零信任策略為首要安全性任務，96% 的人表示這對組織取得成功至關重要。採行零信任策略的主要動機係為改善整體安全性態勢和終端使用者體驗。COVID-19 加速推動混合式辦公的趨勢，而如此趨勢也擴大了採行零信任策略的範圍：81% 的公司行號已開始走向混合式辦公，其中有 31% 的企業已全面施行混合式辦公。然而，94% 的人對轉換仍抱有疑慮，主要是擔心員工濫用、增加 IT 工作負載和網路攻擊。有鑒於此，策略的主要考量事項包括增加員工訓練和實施 Multi-Factor Authentication (MFA)，以確保順暢的使用者體驗和轉換。

02 / 零信任策略讓組織從開始實作即保有靈活性，能針對需求量身打造方法

低於 15% 的組織會在相同的安全性風險區域開始實作零信任策略。這主要是因為實作近似跨安全性架構支柱和功能的端對端流程，而不是一系列不同的獨立技術。同樣地，在安全性風險區域中實作的零信任獨立元件，其順序變化很大，因為安全性專業人員對從哪些元件最先開始實作，見解各異。

03 / 雖然零信任策略普遍獲得接受，且提高了組織管理威脅的能力，但仍有許多方面需要努力

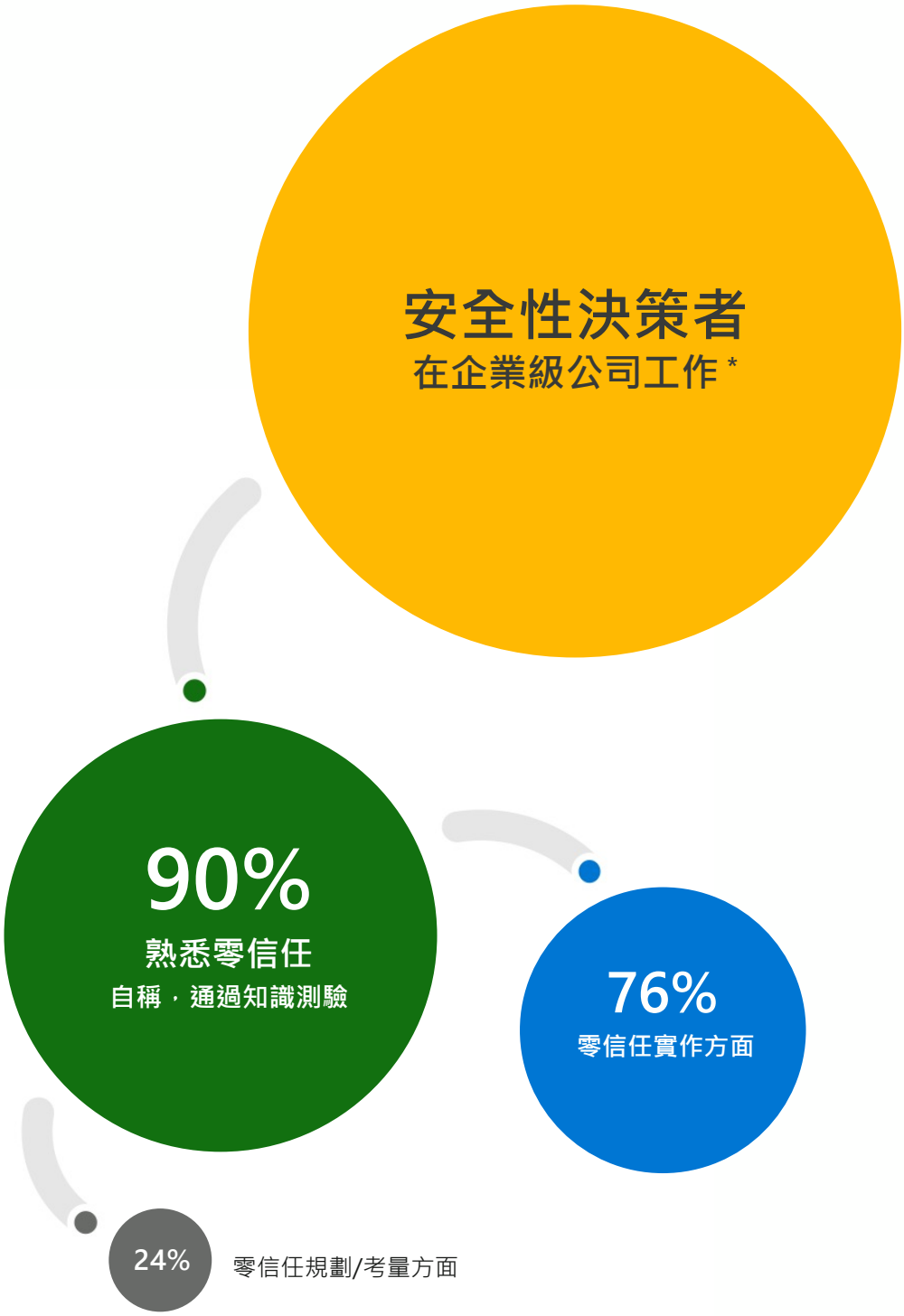
76% 的組織已開始實作零信任策略，其中有 35% 宣稱已全面實作。但宣稱已全面實作的組織承認，他們尚未就所有安全性風險區域和元件完成零信任策略實作。零信任策略因為能提高靈活度、加快偵測威脅的速度，以及提高管理物聯網 (IoT) 和操作技術 (OT) 安全性的能力，而氣勢如虹。美國境內採行零信任的比率不斷成長 (由 2020 年 8 月的 70% 增加到 2021 年 4 月的 79%)，相較於較晚開始實作零信任的其他國家/地區，美國的採行率遙遙領先，而且美國的組織宣稱預算較不受限。然而，雖有 57% 的組織宣稱先於其他組織採行零信任策略，但近半組織仍有很多工作要做，因為他們尚未對所有安全性風險區域和元件全面實作零信任。

04 / 展望未來，零信任策略仍為第一要務，在涉及員工和供應商時需要縝密決策

近兩年內，零信任策略預計仍為安全性第一要務，且組織預期會增加這方面的投資。克服來自員工的挑戰 (包括招募安全性團隊成員和取得領導層同意) 將是零信任投資翻倍的關鍵。在供應商策略方面，因為供應商選擇通常以是否具備內部專業知識為條件，所以安全性決策者在決定要與整體或綜合型供應商合作時會有傾向。一流套件方法的好處包括：提高專業知識、增加資源和提高簡易性，儘管實作的時間較長、更難整合到現有的安全架構中，並會增加可能的弱點。

訪談對象

全球



*美國 1000 多名員工，德國、日本、
澳洲/紐西蘭 500 多名員工

整體研究學習

準備將零信任策略資本化的組織

零信任策略是當今各行各業的安全性第一要務，近年來有許多組織都採行零信任策略。雖然大家都很重視零信任 (53%)，但美國 (56%) 和德國的組織 (53%) 對此尤為重視。

幾乎所有的安全性專業人員 (96%) 都認為零信任策略是組織獲得成功的關鍵。(請參見圖 1) 除加強整體安全性態勢和改善使用者體驗之外，安全性專業人員還期待零信任策略能夠簡化員工的安全性程序。(請參見圖 2)

正如一位美國旅遊服務業安全性決策者所闡述：*「目標是改善整體安全性態勢，但究其實是減少終端使用者體驗在使用上的不便，讓生活更方便簡單。」*

此外，31% 的安全性專業人員視零信任策略為後疫情時代緊急轉入混合式辦公形態的重要工具，此趨勢在澳洲/紐西蘭尤為顯著 (44%)。

圖 1. 零信任至關重要

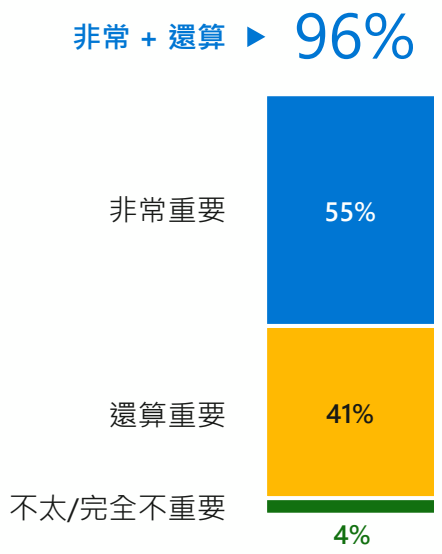


圖 2. 零信任動機

首要動機	
改善整體安全性態勢	47%
改善終端使用者體驗和生產力	44%
轉變安全性團隊共同作業的方式	38%
簡化安全性堆疊	35%
降低安全性成本	35%

轉向混合式辦公讓零信任策略更廣獲採行

81% 的組織已開始邁向混合式辦公，31% 已全面施行。話雖如此，但各個市場全面施行的比例並不一致：澳洲和紐西蘭以 37% 領先群倫，德國卻遠遠落後，只有 20% 的組織已邁向混合模式。(請參見圖 3)

雖然全球市場以不同的速率朝混合式辦公形態邁進，但絕大多數的組織 (91%) 尚未完全轉換，徹底完成預計需要五年。最重要的是，有 94% 的企業對此轉換深感憂心，員工濫用、IT 工作負載增加及網路攻擊風險增加，居於考量事項前三名。(請參見圖 4)

圖 3. 混合式辦公意向佔比

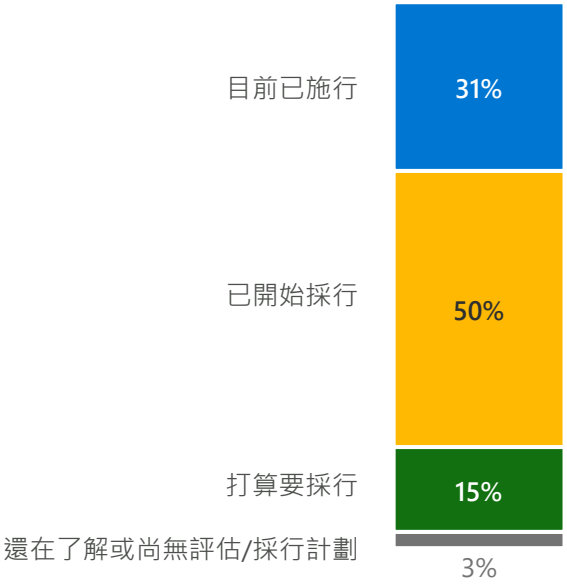
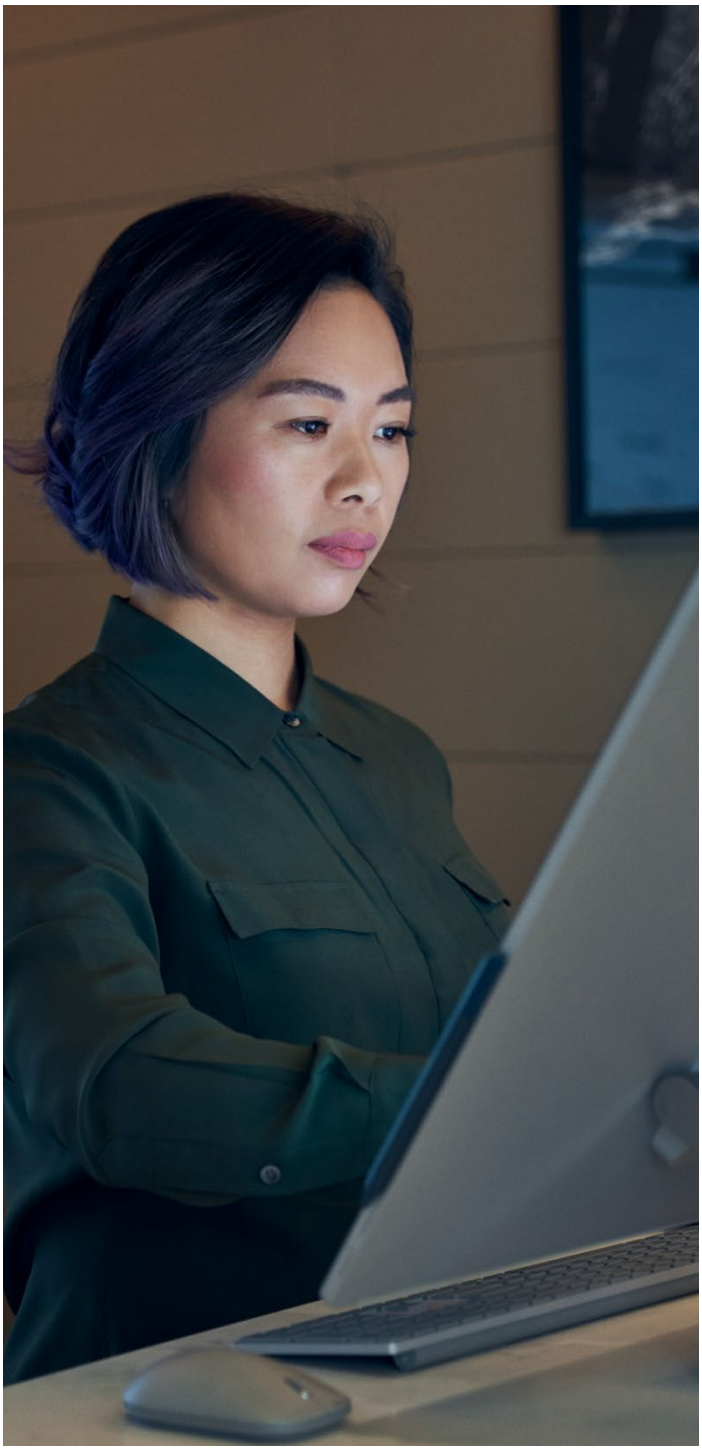


圖 4. 混合式辦公考量事項

員工下載不安全的應用程式	37%
IT 工作負載增加	37%
勒索軟體攻擊	36%
網路釣魚攻擊	35%
不當使用個人裝置	34%
未經授權存取資料	31%
無法管理所有裝置	30%
使用個人電子郵件帳戶	30%
不符合資料法規規範	24%

Covid-19 帶來的新考量加速了採行零信任策略的腳步



為了儘量減少可能的問題，關係人認為要偏重增加員工訓練 (54%) (尤其是日本 (61%) 和德國 (58%))，以及採行 Multi-Factor Authentication (MFA) (50%) (尤其是美國 (52%) 和德國 (56%))，以確保順暢的使用者體驗和轉換。

因為零信任策略可協助保護遠端和混合式辦公的安全，儘管市場之間出現不對稱，但 COVID-19 已促使 72% 的組織加快採行零信任策略。雖然受到疫情催化，美國 (76%)、日本 (71%) 和澳洲/紐西蘭 (69%) 近十分之七的組織採行零信任策略，但德國可能因為轉向混合式辦公的速度較慢，實作率明顯較低 (62%)。

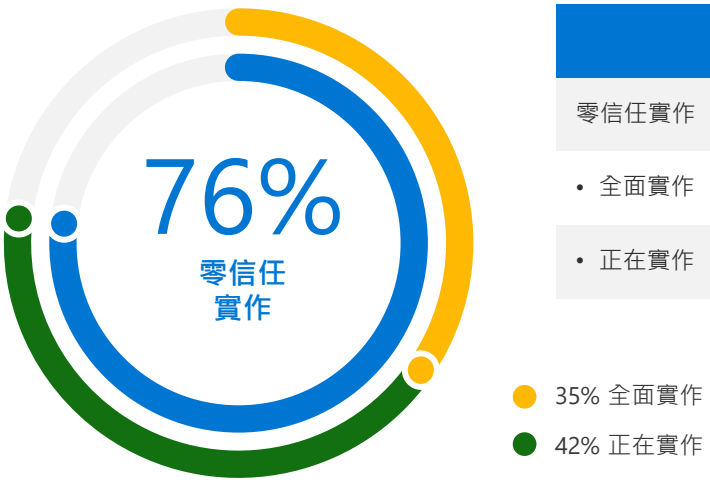
全球普遍實作零信任，美國發展勢猛

零信任不僅是流行用語，還是現實。至少已有 76% 的組織開始實作這項策略，35% 的組織認為他們已全面實作。然而這項資料描繪的前景過於樂觀，因為有許多自認已全面實作此策略的組織，承認並未在所有安全性風險區域內完成執行。目前，美國在採行零信任策略方面相對領先其他市場，且持續快速成長：與 2020 年 8 月相比，美國零信任策略實作率從 70% 增加到 79%，僅八個月就大幅增加。

(請參見圖 5)

儘管零信任策略目前在安全性領域中為主流，但其普遍性相對而言時間不長。82% 的公司是在過去三年中實作零信任策略，而有 21% 的公司是在過去 12 個月中才實作此策略。亦即，26% 的美國組織在 3 年多前才開始實作，日本為 19%、澳洲/紐西蘭為 6%，德國為 3%。美國較早實作此策略 (結合較少的預算限制)，或可解釋美國組織為何在採行零信任策略方面領先其他市場中的組織。同樣地，在德國相對新興的零信任也說明了其較低的採行率：97% 的德國組織是在過去三年才開始實作此策略。

圖 5. 零信任實作



	美國 (2020 年)	美國	德國	日本	紐澳
零信任實作	70%	79%	75%	76%	71%
• 全面實作	27%	44%	19%	32%	28%
• 正在實作	43%	35%	56%	44%	43%

零信任實作沒有萬金油方法，只要有授權，任何地方都可以是起點

沒有任何一個安全性風險區域 (身分識別、端點、應用程式、網路、基礎結構、資料、自動化和協作) 可成為零信任策略的主要起點，因為從相同安全性風險區域開始的組織不到 15%。組織可能因需求和可用的內部資源不同，而從不同的地方開始。最終企圖在所有安全性風險區域採行零信任策略，以確保針對威脅提供更多防護，因此零信任被視為是需要一段時間才能完成的端對端策略。(請參見圖 6)

除了零信任策略的安全性風險區域之外，組織必須找出每個安全性風險區域要優先實作的個別元件。就端點、應用程式、網路、資料和自動化/協作而言，沒有明確的起點；安全性專業人員各有各的最優先元件。但在身分識別方面，一般會先實作強式驗證，而在基礎結構方面，威脅偵測工具明顯優先。(請參見圖 7)

圖 6. 目前實作零信任的安全性風險區域

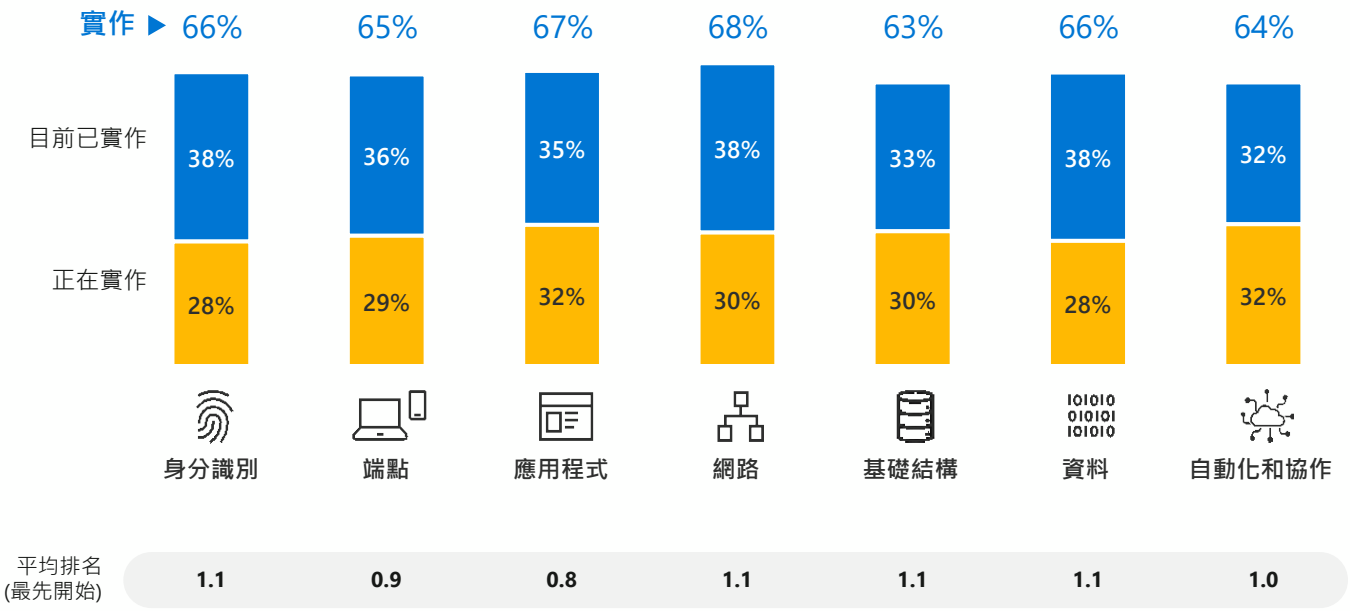


圖 7. 零信任元件實作排名第 1 位的前 3 名 (最先實作)

身分識別	
強式驗證 (即多重要素驗證、無密碼驗證)	32%
自動化風險偵測和補救	27%
控管資源存取的調適性存取原則	22%

端點	
所有非受控裝置和受控裝置的資料外洩防護原則/控制	27%
即時裝置風險評估/端點威脅偵測	26%
裝置已向身分識別提供者註冊	24%

應用程式	
持續的影子 IT 探索和風險評估	23%
對應用程式的細微存取控制 (例如有限的可見度或唯讀)	22%
對應用程式的原則式存取控制	20%

網路	
保護網路的安全存取控制	25%
使用以內容為主的訊號進行威脅防護和篩選	24%
所有流量均經過加密	20%

基礎結構	
安全性作業團隊存取威脅偵測工具	25%
跨混合式和多雲端的雲端工作負載防護	19%
所有工作負載 (虛擬機器、伺服器等等) 的細微可見度與存取控制	17%

資料	
存取權判斷由安全性原則引擎治理	21%
資料經過分類和標記	21%
最敏感的檔案會持續受到加密保護	20%

自動化和協作	
使用集中處理調查和回應的平台建立端對端可見度	29%
跨領域 (身分識別、端點、應用程式、網路、基礎結構) 收集及分析威脅資料	28%
啟用自動化調查和回應	22%

我們不僅視其為一系列的技術，還視其為處理每一位使用者資源的策略和做法，不論網內還是網外，在獲得驗證前一律不信任。”

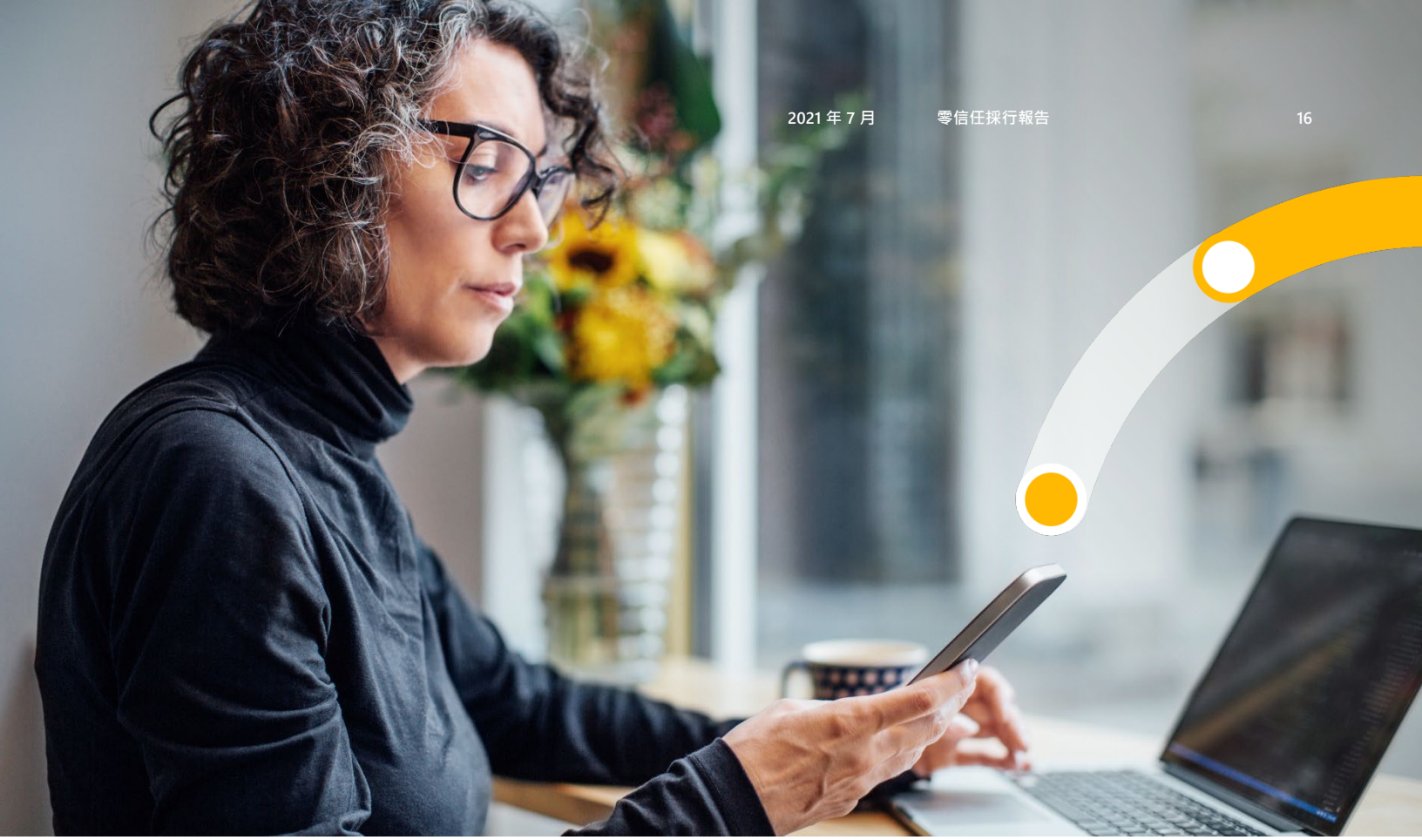
美國安全性決策者旅遊服務業

組織一開始實作零信任策略，就能立即看到提高靈活度、速度和保護等前幾項好處；但資源優勢卻不明顯

組織實作零信任策略後，即可獲得提高靈活度 (37%)、速度 (35%) 和客戶資料防護 (35%) 的優勢。(請參見圖 8) 然而，員工直接獲得的好處，包括釋出的安全性團隊人力 (27%)，以及管理基礎結構的資源需求減少 (22%) 等等，反而不那麼明顯。

重點是，組織認為零信任策略會協助他們管理大部分的環境威脅和變化，尤其是在 IoT 和 OT 安全性方面 (47%)。

圖 8. 零信任優點



組織有信心讓零信任策略發揮出最大成效

79% 的人對自己處理安全性威脅的整體能力有信心，但當威脅涉及捏造真相時，這種信心會減弱：SDM 對處理涉及合成身分識別 (20%) 和深偽技術 (10%) 的威脅最沒有信心。

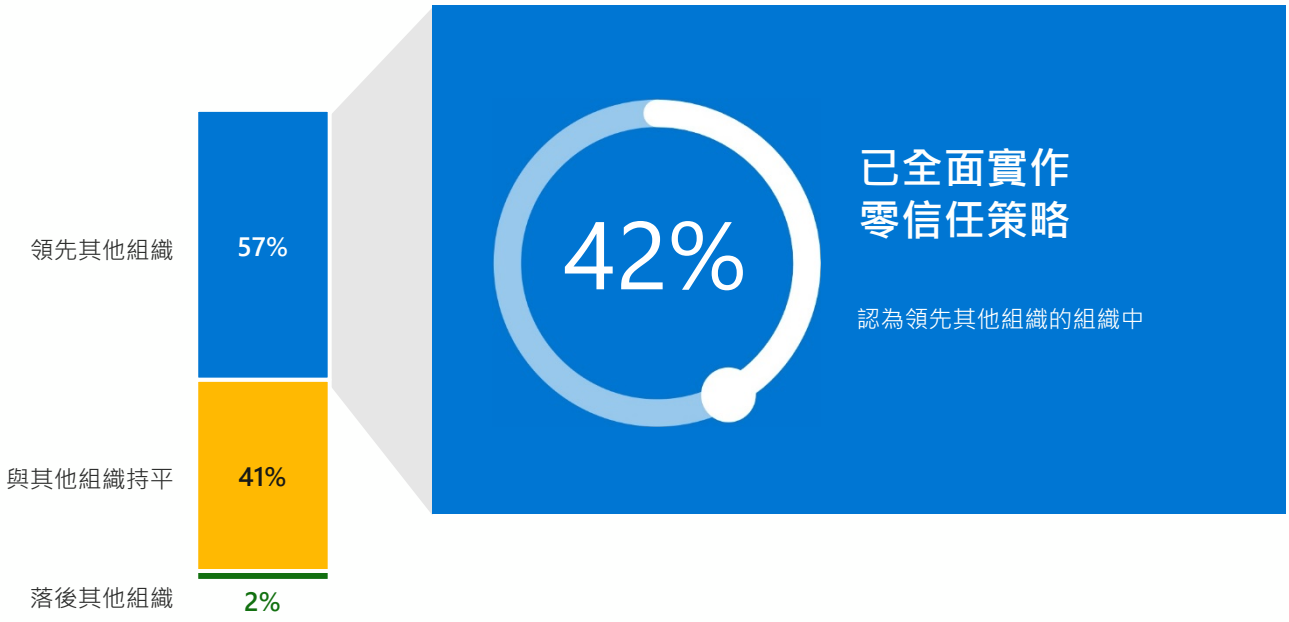
鑒於獲得的好處，人們通常對零信任有正面的聯想。在四個市場中，SDM 都認為其組織的做法兼具實用性和成功性，表示有信心 (37%) 和有效率 (31%)，以及激勵 (25%)、令人振奮 (25%) 和令人興奮 (25%)。尤其是日本的安全性專業人員將零信任描述為高要求 (27%) 和轉型 (25%)，指出零信任雖然不容易實作，但採行後的好處將影響深遠。

許多人認為他們在零信任實作方面已取得領先，但是仍有很多工作要做

雖然只有 35% 的組織已全面實作零信任策略，但有 52% 表示進度超前，57% 認為領先其他組織。認為領先其他組織的多為日本 (66%) 和澳洲/紐西蘭 (63%) 的組織。雖然各市場皆信心滿滿，但認知和現實之間似乎存在巨大分歧：在認為領先其他組織的人中，只有 42% 宣稱已全面實作零信任策略。(請參見圖 9)

雖然許多組織對自家的零信任策略深具信心，並且隨時準備要處理未來的安全威脅，但仍有大量的工作有待完成，才能在所有風險區域全面實作。例如，在認為全面實作零信任策略的組織中，目前幾乎近半未在所有安全性風險區域實作，而實作可能性最小的為基礎結構和身分識別。

圖 9. 零信任實作比較



	美國	德國	日本	紐澳
領先	59%	46%	66%	63%
持平	40%	52%	34%	32%
落後	2%	2%	0%	6%

展望未來兩年，零信任策略仍將是安全性第一要務

組織全面投入零信任策略，而決策者聲稱這項策略在接下來兩年仍然是首要安全性優先事項。預計到 2023 年，以零信任策略為安全倡議的相對重要性將計劃提高 (53% 至 58%)，因為 SDM 預測此策略對於整體成功仍至關重要 (96%)。(請參見圖 10)

預期關鍵性在日本組織中尤為高，有 70% 的安全性決策者表示零信任策略在未來兩年將會非常重要，整體平均值為 56%。零信任策略預算預計也會成長，預計有 73% 的組織會增加預算。雖然德國的數值略低 (67%)，但仍有 31% 預期預算會維持不變。(請參見圖 11)

圖 10. 預期未來兩年零信任的關鍵性

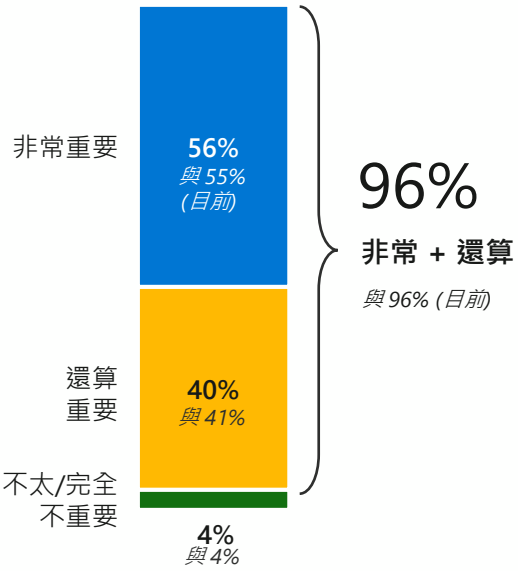
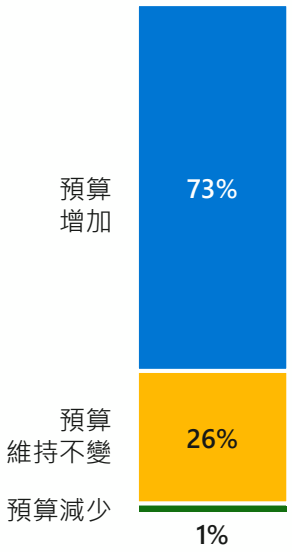
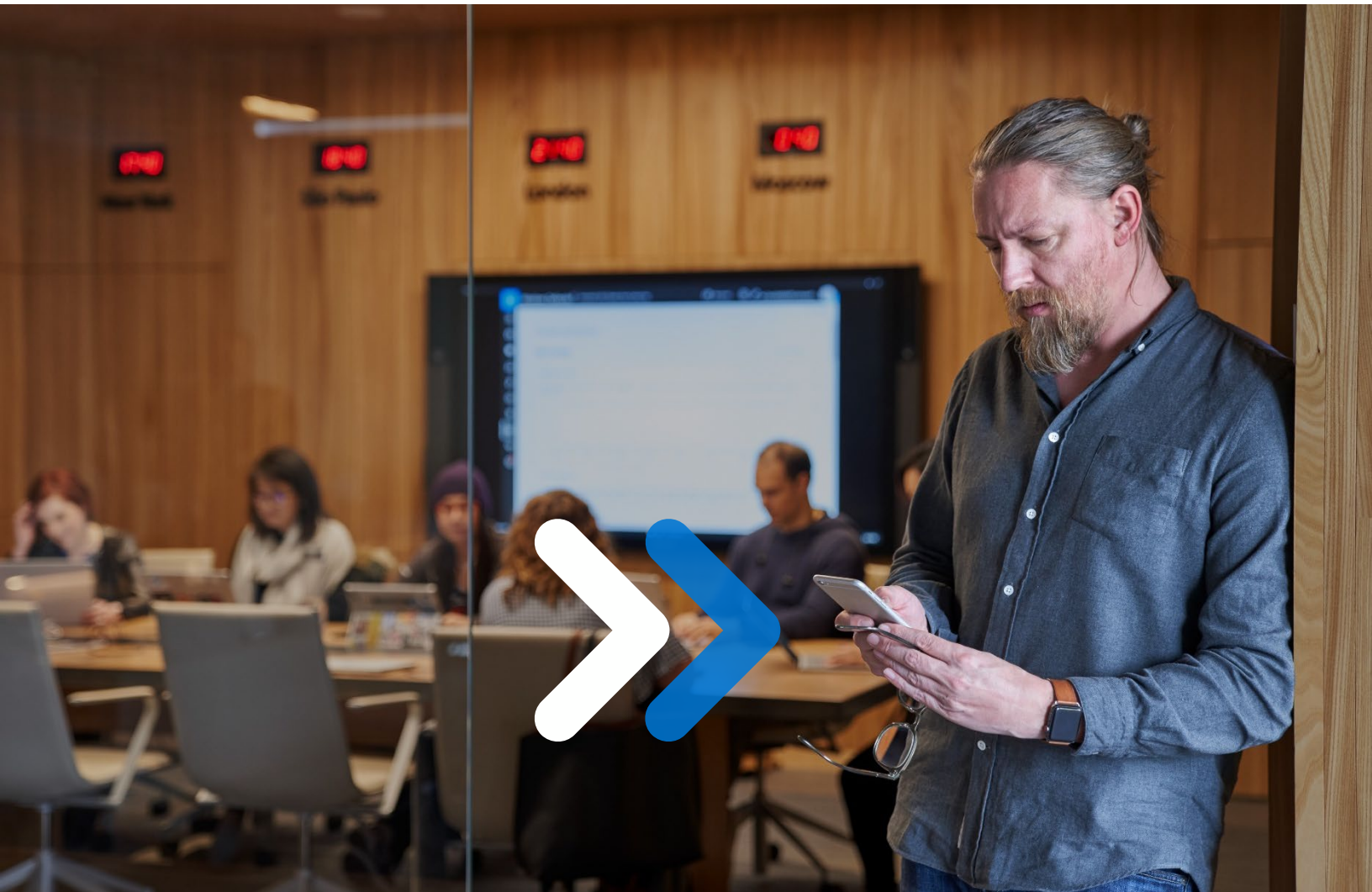


圖 11. 預期未來兩年的零信任預算



證明零信任策略成功可刺激進一步投資

完全接受零信任的組織預計未來兩年將加倍投資，而尚未開始採行此策略的組織將面臨更加落後的風險。這些組織將零信任列為安全計劃第一優先 (42% 與 66%) 並預計增加預算 (66% 與 72%) 時，不僅會追蹤全面實作的對手，還會明顯感到對未來管理 IoT 和 OT 安全性不是那麼有把握 (40% 與 53%)。



克服來自員工的挑戰將是零信任投資翻倍的關鍵

儘管採行零信任策略已取得快速進展，但組織在實作方面若要再更進一步，就必須克服無數挑戰。(請參見圖 12) 最常見的挑戰來自資源和領導層。實作零信任策略需要的時間和欠缺最高管理層的支持，名列障礙清單前幾名，後者在澳洲/紐西蘭尤為顯著 (65%)。

此外，預算限制 (45% 的組織認為這是障礙) 在資源和領導層挑戰中可能也佔一席之地。

例如，21% 的 SDM 認為，證明零信任投資的 ROI 為實作障礙困難重重，這是阻礙最高管理層同意的挑戰。因為美國以外的市場更可能出現預算限制 (日本 60% 的組織、德國 57% 的組織、澳洲/紐西蘭 57% 的組織)，所以可能出現漣波效應，造成日本、德國和澳洲/紐西蘭在零信任策略實作方面，較美國低迷遲緩。

圖 12. 零信任障礙

資源挑戰 60%	領導層 53%	技術面 46%	供應商 46%	預算限制 45%
20% 實作時間太長	20% 欠缺最高管理層的普遍支持	21% 難以整合安全性解決方案	21% 需要供應商提供實作支援	21% 實作零信任策略的成本
19% 缺乏內部變更管理	19% 欠缺關係人的支持	19% 與舊版系統不相容	21% 難以找到合適的供應商	21% 難以證明 ROI
18% 需要更多教育資料	19% 需要協助以提供令人信服的商業案例	19% 難以在全組織中擴縮	17% 找不到富有創新精神的合作夥伴	14% 預算不足
17% 我們這種規模的組織不需要	18% 缺乏組織同意			
16% 沒有合適的人才可妥當實作				

“最初讓大家同意極富挑戰性，但達成共識成為關係人後，大家一致同意投資此專案，每個人都是團隊的一分子。”

美國安全性決策者金融科技

安全性決策者較偏向提供整體或綜合型服務的提供者

在零信任供應商策略方面，組織要在最佳套件或一流提供者間取捨。前一項策略是向提供整體或綜合型服務的提供者購買整套完整的零信任架構產品，SDM 認為這種解決方案能為內部資源匱乏的人員提供更多的專業知識、資源和簡便性。但是，這種方法有弱點增加和缺乏彈性等問題。(請參見圖 13)

後一項策略 (一流提供者) 涉及從專業供應商處取得獨立的零信任技術元件。此策略和最佳套件不同，依賴專精於不同領域的提供者，提供更大的彈性，能與組織策略更密切地配合。雖說如此，安全性專業人員認為一流提供者策略成本更高、需要更多資源，而且有礙可見度，而這些缺點最終會造成供應商及預算方面的挑戰。(請參見圖 14)

雖然組織的看法大致兩分，但偏多數的 SDM (55%) 偏好與提供整體服務 (最佳套件) 的提供者合作。(然而，澳洲/紐西蘭的組織偏向反方向，52% 的組織偏好與一流提供者合作)。

圖 13. 前 2 名的最佳套件優點和障礙

⊕ 最佳套件優點	
供應商在所有解決方案中提供業界專屬的專業知識	24%
更多可用資源可協助規劃零信任策略	23%
簡化了安全性堆疊	22%

⊖ 最佳套件缺點	
依賴單一供應商會增加弱點	34%
需要與舊版架構進行更複雜的整合	33%
無法彈性提供專業功能	29%

圖 14. 前 2 名的一流提供者優點和障礙

⊕ 一流提供者優點	
可彈性追求任一零信任策略元件的最佳方案	33%
解決方案可與組織的架構或策略密切配合	30%
提高與不同供應商創新發想的機會	26%

⊖ 一流提供者缺點	
成本增加	29%
無法跨不同解決方案共用資料	26%
內部團隊需接受和管理大量解決方案	26%

總結

當安全性風險日益頻繁且更加險惡，各市場和各行業的組織都選擇「絕不相信，一律驗證」的零信任策略。對旨在改善整體安全性態勢、使用者體驗和生產力、簡化員工安全性程序及降低成本的組織而言，零信任策略是第一要務。然而，儘管零信任策略的優點歷歷在目，但有限的資源和領導層抱持的懷疑態度，仍阻礙普遍性的實作。

過去三年中，零信任策略的採行速度加快，部分係受到 COVID-19 疫情的影響。重要的是，遠端和混合式辦公趨勢讓大眾更普遍接受零信任方法，承諾即使員工離站存取系統和資料 (有時使用個人裝置)，也會保護系統和資料的安全。因為 COVID 而加速採行零信任方法，是整體零信任整備程度的良好預測指標，在疫病大流行期間採行此策略的組織，比對手在更多安全性風險區域實作此策略。

儘管如此，即使是最先進的零信任策略採行者，也還有許多未竟之事，而組織對其零信任成熟度的錯誤認知，可能遺留一些他們自己都不知道的弱點。

不同市場中有大多數組織認為，零信任策略的關鍵性只會與時俱進，期望預算會因此而增加。這種對優先順序轉移的預期心理在非美國市場尤為重要，因為在這些市場，預算問題是採行此策略的重大障礙。努力達成全面實作可能無法抵抗財務和邏輯方面的壓力，但是零信任方法的好處不容置疑；當這些組織開始這項發展迅猛的新興事業時，Microsoft 會為其提供指導和支援。

若要深入了解零信任並評估組織的零信任成熟度，請瀏覽

aka.ms/zerotrust

詳細的研究目標與招募對象

研究目標包括：

1. 了解零信任方法的目前狀態
2. 發掘採行零信任方法的觀念、最佳做法、優點和挑戰
3. 探索零信任方法的未來
4. 說明零信任方法的創新和趨勢

為符合篩檢標準，安全性決策者必須是：

組織安全性事務的負責人，包括網路安全性、安全性作業、威脅防護、身分識別管理、風險管理、應用程式安全性、數位鑑識和事件回應

企業級公司的全職員工 (員工人數標準：美國 1000+，德國/日本/紐澳 500+)

25-75 歲

熟悉零信任

參與零信任策略制定/實作決策

在 2021 年 4 月接受研究浪潮訪談的 911 安全性決策者：

美國受訪的 SDM 為 477 名

德國受訪的 SDM 為 201 名

澳洲/紐西蘭受訪的 SDM 為 126 名

日本受訪的 SDM 為 107 名

注意：研究進行時正值 COVID-19 全球大流行，處於擴散/抑止的不同階段

© Hypothesis Group 2021. © Microsoft 2021.
著作權所有，並保留一切權利。07/21