CSO

Microsoft Security

零信任安全性：
早期採用的教訓

CSO Microsoft Security

目錄

CSO Microsoft Security

簡介

過去兩年的疫情中斷已經動搖了傳統的 IT 和安全模式。因此，零信任資安防護已經從有趣的概念迅速演變為現代企業安全的基礎。

Foundry 的新研究發現，52% 的企業正在試點或已經部署了零信任架構，另外 15% 的企業正在研究零信任模式。這些採用者在報告中表示，他們的部署帶來了許多好處，包括改善了對客戶資料的保護，降低了複雜性，以及提供了對企業資源的安全防護，以及可靠的存取方式。

這本電子書將探討 Foundry 的研究結果，其中強調了零信任策略的重要性，說明如何協助 CISO 保護其組織免受來自眾多攻擊媒介的多種風險。其中還包括了指引，說明如何開始實作零信任的旅程。

關於調查

Foundry 在 2022 年 2 月和 3 月對美國企業進行了調查，探索零信任的採用現況。受訪者必須是員工人數 500 名以上的公司中的 IT 管理職員或以上職級，並在購買網路安全產品和服務方面發揮一定的作用。

這項調查有 23 個問題，共有 250 名受訪者。

CSO Microsoft Security

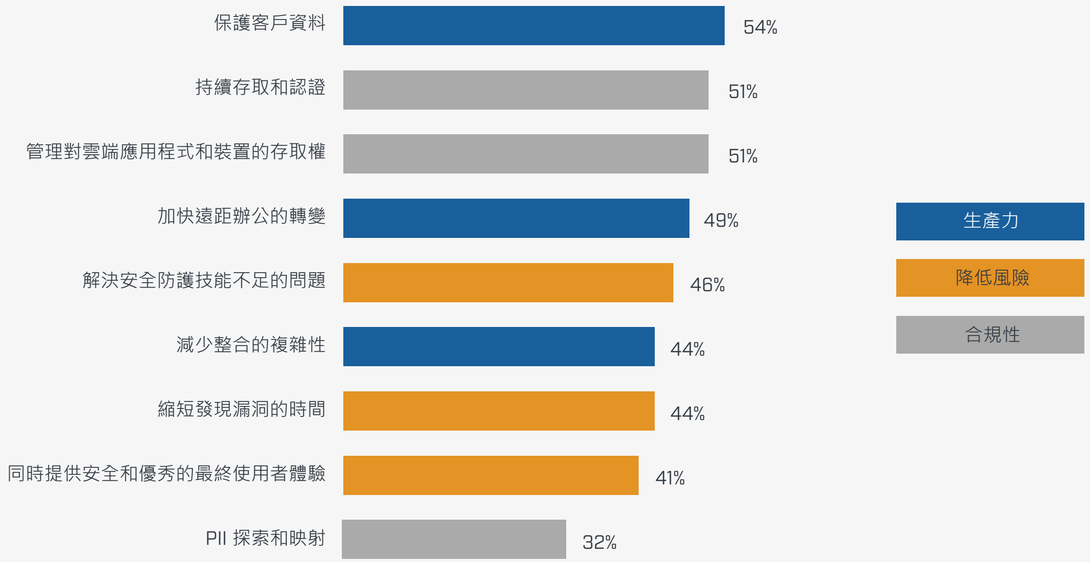
零信任的時代已然到來，並且正在提供價值

從調查結果以及對 IT 和安全執行主管的深入訪談中可以看出，零信任是大多數企業的首要考量。而部署了不同零信任元件的企業已經發揮效益。

大多數已實作零信任的受訪者 (87%) 表示，該架構在實施、採用和整合方面，達到或超過了他們最初設立的目標。

一間全球零售商的 IT 總監表示：「[零信任] 已經成為我們的標準操作程序。我不認為我們會回到以前的樣子，」[受訪者要求匿名，以換取對其安全計畫的自由討論]。

實作零信任後實現的優勢



12% 的受訪者說他們正在實現*所有*這些優勢

來源：Zero Trust Adoption Survey, March 2022, Foundry. 基礎：250

CSO Microsoft Security

約 44% 的受訪者還表示，零信任降低了實施綜合安全架構的固有複雜性。一間員工有 3500 名的呼叫中心公司 CISO 表示：「由於您只處理和使用一個架構，這確實使事情變得不那麼複雜，」

一間員工有 17000 名的金融服務公司副總裁和 CISO 表示，他的公司在零信任中實施的多重要素驗證很受員工歡迎。他說：「實際上，這提高了員工的滿意度，因為現在他們不需要在公司提供的機器上使用 VPN 用戶端；他們可以從任何地方獲得資源，」

CISO 指出，最低存取特殊權限的概念也同樣得到了回報。他表示：「由於實作了特殊權限存取系統，我們的系統管理員出現災難性錯誤的情況較少，」「他們在特定的事情和特定的時間範圍內獲得授權，這代表他們不太可能犯錯。」

有鑒於網路釣魚和其他網路攻擊的日益普遍，這家零售公司的 IT 總監這樣總結零信任的優勢：「如果我們沒有這些類型的工具，我們很可能現在就身處在要用比特幣付錢的窘境。」

CSO Microsoft Security

零信任部署的動力

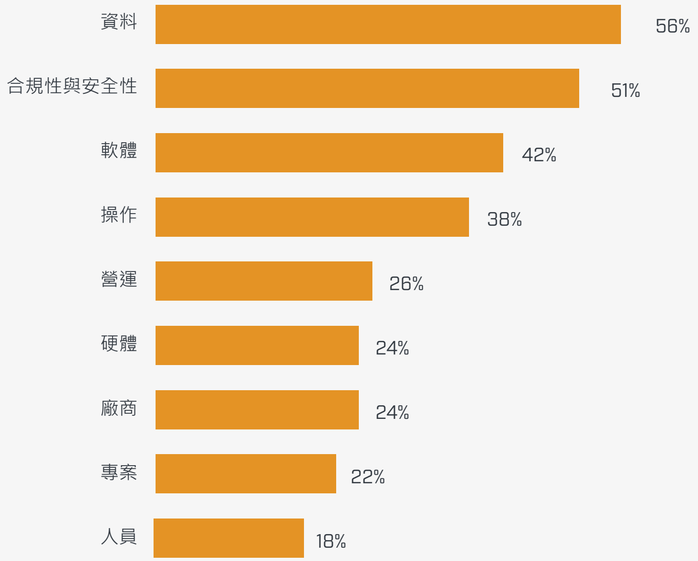
一系列事件促使企業至少考慮採用零信任架構。排在首位的是需要管理眾多資源的風險，應對眾多威脅。調查物件將多年來的安全事件歸結為若干原因，其中以協力廠商個人或組織的安全性漏洞為首。其他原因包括：

- 意外的商業風險
- 服務或系統的錯誤配置
- 惡意的、蓄意的內部攻擊
- 非惡意的使用者錯誤，包括網路釣魚受害者
- 有安全風險的身分
- 未修補的軟體
- 被盜用的憑證

這些事件帶來了各種風險，其中以資料為首。

對許多組織來說，由於疫情大流行導致的向遠距辦公的突然轉變，加速了零信任的採用計畫，因為網路周邊型傳統安全模式已經過時。許多企業在將更多的應用程式和 IT 基礎架構轉移到雲端時，已經朝著這個方向發展，但疫情大流行卻帶來了額外的衝擊。

遭受網路安全威脅的首要類別



來源：Zero Trust Adoption Survey, March 2022, Foundry. 基礎：250

CSO Microsoft Security

例如，一間員工有 1700 名的醫療技術公司資訊長表示，雲端和疫情大流行是他採用零信任的驅力，這現在為未來的任何職場模式提供了安全基礎。

他表示：「業務驅動要素是我們是一間雲端公司，需要能夠保護我們的環境，我們還必須在疫情大流行期間提供有能力的遠距勞動力。[零信任] 使我們能夠大大減少我們的資產足跡，而且我們可能會保持至少有 60% 以虛擬遠端公司的方式運作。」

CSO Microsoft Security

不缺乏威脅

合規需求也為更強大的安全模式提供驅力。一間員工有 29 萬名的金融服務公司全球資訊安全資深副總裁表示：「監管機構正在關注我們，他們希望我們能繼續改善我們的安全架構，」

有些企業已積極主動地採取實現零信任的措施，以避免高調的漏洞使他們犯錯而成為鎂光燈下的焦點。一間員工有 3500 名的高等教育機構資訊長表示：「這是關於主動出擊並試圖遠離新聞版面的問題，」「有些真實發生的可怕案例，其他與我們規模差不多的地方機構，都癱瘓了很長時間。」

其他人經歷了嚴重的網路安全事件，促使他們迅速重新審視自己的安全防護策略。一間員工有 6000 名的保險公司遭受了勒索軟體的攻擊，使公司網路關閉了兩個星期，執行長直接下達了採用零信任的命令。該公司的 IT 發展副總裁表示：「我們加快了實作的速度，一開始肯定是使用最佳做法，然後在我們被勒索軟體攻擊之後，就真的更加快速了。」

雲端催化劑

一間大型金融服務公司的副總裁暨資訊長表示，他的團隊幾年前就認為需要有新的安全架構，因為團隊已開始採用更雲端型資源，使用者變得更具行動力。

他表示：「我們意識到，過去所依賴的城堡式傳統安全架構並不能保護我們在未來免受攻擊。

這樣的實際情況在 2020 年初變得清晰可見，當時該公司發現在前一年的某個時候，已有個攻擊者滲透到網路周邊，並在環境中橫向移動而沒有被發現。「我們需要新的架構來保護和驗證這些資源的使用，無論其所在位置為何，而零信任就是旨在實現此目標的架構。」

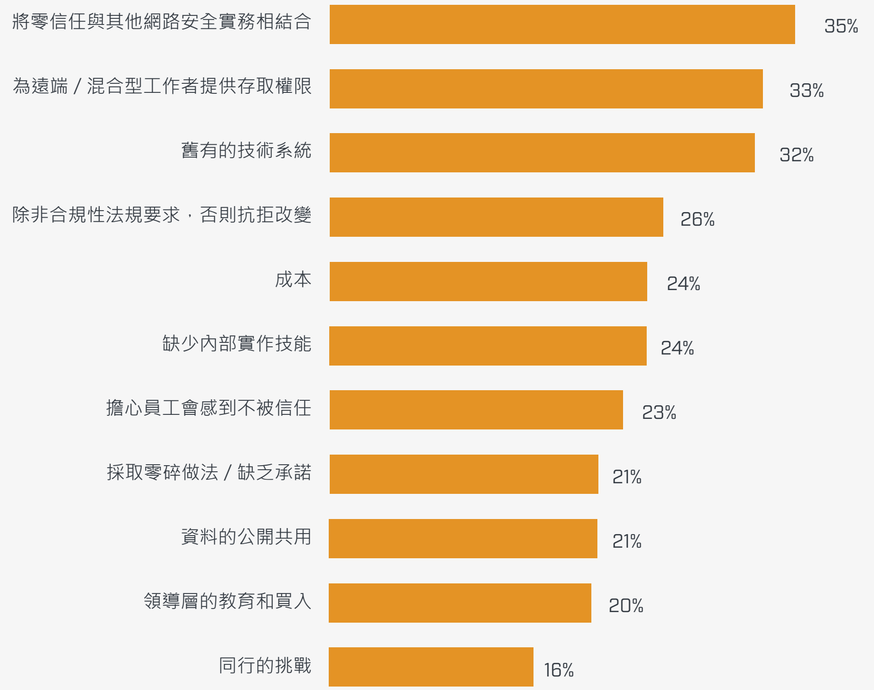
CSO Microsoft Security

採用零信任的障礙

對許多組織來說，零信任代表著安全結構、流程和思維方式的徹底轉變，這也解釋了他們在採用零信任之前必須克服的一些障礙。

呼叫中心的 CISO 指出：「我們在組織內部有許多不同的孤島，」他在解釋中提到，伺服器、網路和資料庫團隊都有自己的網路服務器和工具的分隊。「這使我們陷入困境，因為每個人都有不同的想法，不知道該到哪裡去，也不知道該怎麼做。」

是什麼阻礙了零信任的採用？



來源：Zero Trust Adoption Survey, March 2022, Foundry. 基礎：250

CSO Microsoft Security

Microsoft 零信任資深產品行銷經理 Anthony Mocny 表示，發現這樣的問題，其實可以成為零信任的正面副作用。他表示：「作為一個架構，Zero Trust 旨在打破生活在技術支柱中安全團隊的孤島，並幫助團隊團結一致地工作。他說：「就團隊合作的方式而言，它可能也代表文化的改變。」

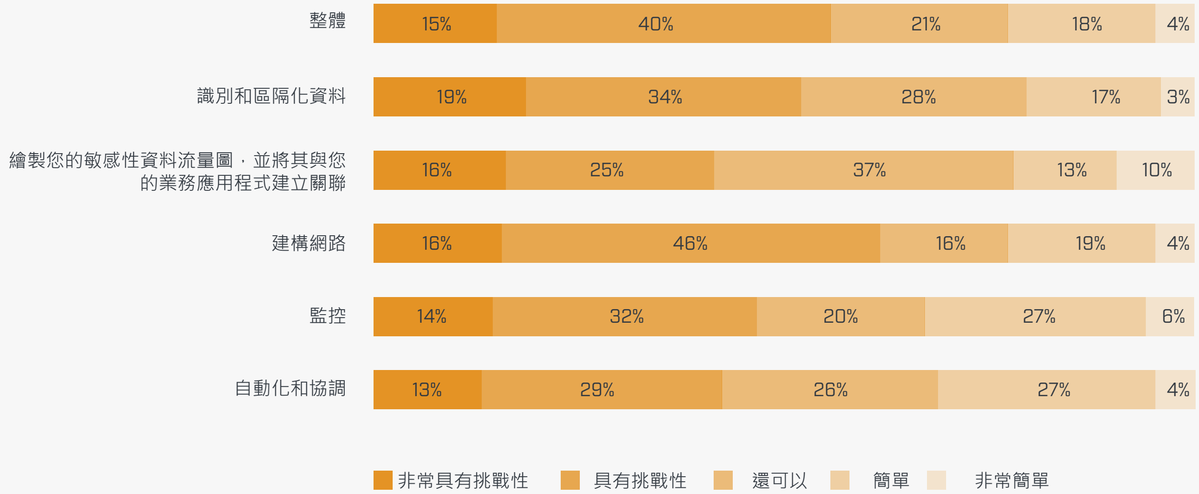
對於這位金融服務副總裁 /CISO 來說，傳統的應用程式是通往零信任道路上需要克服的障礙。他表示：「這些架構必須用現代認證技術加以改造，」「有鑑於他們已存在許久，這可能不是一件很容易做到的事情。」

CSO Microsoft Security

部署的挑戰

一旦公司踏上邁向零信任的旅程，各種實作挑戰也會相繼浮現。超過一半的受訪者 (56%) 承認，實作零信任架構具有挑戰性或非常具有挑戰性。具體特色如下：

實作零信任架構的挑戰性有多大？



來源：Zero Trust Adoption Survey, March 2022, Foundry. 基礎：168

CSO Microsoft Security

在深入訪談中，經常出現與區隔和微區隔相關的挑戰。

金融服務副總裁 /CISO 表示：「您正在將您的網路區隔細分到各個主機，這就像在內部網路的每部主機間設置了一個小防火牆，這樣就可以看到所有的流量，並控制到每台機器的流量。這有巨大的安全優勢，但實作起來卻超級困難，因為現在您必須實際管理數萬個防火牆。」

繪製流量圖表可能又是個耗時數月的程序。對於一間員工有 5000 名的出版和媒體公司技術長來說，在定義了他們需要保護的關鍵資料、應用程式和網路服務之後，他表示：「我們繪製了網路上的交易流程，並試圖將它們理解為一組資訊，」他表示：「[我們隨後] 對這些資訊的部分進行了區隔，以及其實際穿越網路的方式，甚至細分到單一封包的程度。」在這一點上，該公司將零信任政策套用到每種流量類型。「我們還建立了新的能力來監控和維護我們的網路。」

儘管存在挑戰，許多受訪者認為零信任最終簡化了日常營運。對於傳統技術，負責全球資訊安全的金融服務資深副總裁表示：「需要幾天的時間來進行修改；您必須在所有的硬體和軟體元件中推送，我們為此使用了大量的資源，當我們看待零信任時，從長遠來看，它確實最大限度地減少了架構的複雜性，並減少了我們做相同類型工作所需的員工數量。」

實作零信任的最佳做法

隨著越來越多的公司實作零信任架構，他們正在開發路線圖和最佳做法，供其他人學習。以下是部署計畫時的五個注意事項。

不要一開始就進行太多的任務

如果只從大角度來看，您會認為零信任策略就是必須要修改網路、資料、應用程式、身分識別、端點和基礎架構的政策和保護措施，這可能令人怯步。這位受過高等教育的資訊長表示：「一開始，當您只看到有這麼多要做的事時，會不禁懷疑是否真的能做到這一點，您只需要逐步進行即可。」

這位資訊長和他們的團隊最終採取了「跟錢走」的方法，優先將財務和工資應用程式區隔到一個單獨的網路中。

Mocny 表示，確定要保護的最關鍵資產是一種健全的方法。他說：「首先要考慮到您實作零信任的原因，」

當有疑問時，就從多重要素驗證開始

在確定安全堆疊的優先次序時，許多 CISO 和安全供應商建議首先關注認證和其他身分識別的保護措施。Mocny 表示：「如果您不知道從何做起，多重要素驗證會是個好的起點，」Microsoft 估計，多重要素驗證可以防止 90% 以上的身分識別型攻擊。

金融服務副總裁 /CISO 同意這個觀點。「身分驗證是實作零信任架構的一個基本要素。如果不能驗證終端使用者的身分，則其他元件都無法發揮作用，所以我們從這裡開始。」

接下來，這位金融服務副總裁 /CISO 處理了網路元件，這為支援遠端工作人員帶來了直接益處。該團隊將微區隔留到了後期進行，因為廣大企業不容易察覺到這方面的益處。他表示：「完成後，您的安全層級明顯提高了，但沒有人知道其中的區別，」

CSO Microsoft Security

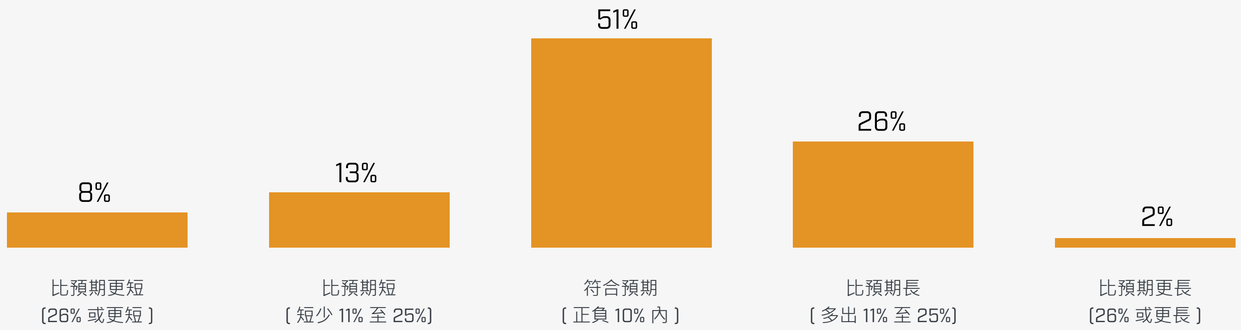
要有實際可行的時間表

重要的是，CISO 要對零信任的部署設定實際可行的期望。這位金融服務副總裁 /CISO 表示：「實作零信任架構是計畫而非專案，這是一個巨大的變化。進行實惠涉及許多專案，而且很可能持續數年；實作零信任架構不可能快速又簡單。」

他的同事金融高級副總裁同意這一點。他表示：「我不認為我們會完成任務，因為總是有新的技術、新的惡意軟體或新的威脅出現，」

大多數調查對象 (72%) 表示，他們的部署時間表正在按計畫進行或提前進行，其餘表示實作時間比預期要長。

零信任是否符合您時間表中的目標？



來源：Zero Trust Adoption Survey, March 2022, Foundry. 基礎：168

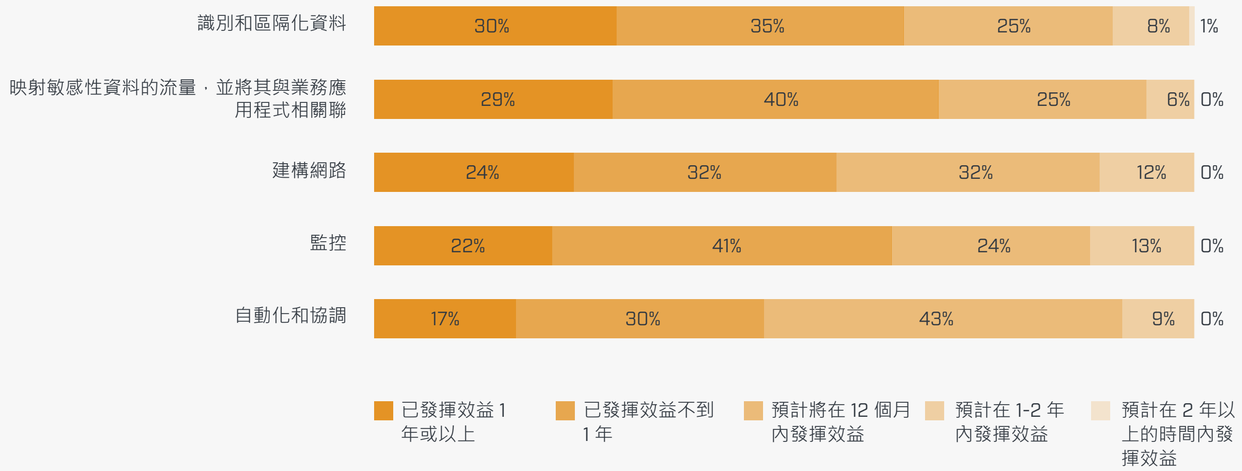
CSO Microsoft Security

邊做邊測

雖然零信任部署是持續進行的過程，但 CISO 可以也應該在這一過程中建立里程碑來衡量進展。好消息是，大約三分之二的調查對象表示，一年內就從專案中的大部分方面發揮效益，另外四分之一或更多的人預計在 12 個月內會發揮效益，包括身分識別和區隔資料、繪製流量圖和建構網路等關鍵活動。

Mocny 表示：「零信任是個旅程，因為您需要不斷評估，以抵禦不斷變化的攻擊性質，要隨時注意改進。」

實現零信任優勢的時間表



來源：Zero Trust Adoption Survey, March 2022, Foundry. 基礎：103

CSO Microsoft Security

不只是技術，也要專注在人員身上

零信任安全模式的廣泛影響到每位員工，包括負責部署該模式的 IT 和安全團隊。這就是為什麼與任何大型技術專案一樣，必須確保部署工作與新流程和變革管理實踐同步，以確保順利和成功地推出。

Mocny 表示：「除了技術上的變化，還有文化上的變化，」「如果已有多個團隊處理安全問題（包括網路架構師或身分識別專家），您還需要改變這些團隊的合作方式。您需要打破孤島，以確保技術都能凝聚在一起。」

消除孤島涉及讓所有這些學科的團隊密切參與試點和概念驗證 (POC) 專案。一間員工有約 2000 名的電信公司 IT 系統主管在部署過程中遇到了幾個單點故障，包括服務無法認證和突然「不受信任」，導致自家系統和有些系統都無法使用，之後他記取了這個教訓。

他表示：「部署一個服務可能會產生骨牌效應，使其他服務癱瘓，」展望未來，「我們將在部署前更加謹慎，花費更多的 POC 時間並進行審查，與更多主題專家一起審驗架構。」

零信任投資報酬率

2021 年委託 Forrester Consulting 進行的 Total Economic Impact™ 研究量化了 Microsoft 零信任解決方案的成本撙節和商業利益。根據 Forrester 採訪的五間企業，一間複合組織透過實作 Microsoft 的零信任架構，實現了 92% 的三年投資報酬率。

透過消除對零信任下變得多餘的安全工具的需求（端點管理、防病毒和反惡意軟體解決方案），這間複合組織平均在每個員工身上每月節省 20 美元。

CSO Microsoft Security

您位於實現零信任的哪個階段？

如調查所示，零信任安全模式的好處顯然超過了 CISO 及其安全團隊所面臨的一些部署挑戰。以周詳計畫來應對這些挑戰，有助於貴組織迅速改善保護措施、降低風險，並開始為整個企業提供價值。

要評估貴組織的零信任成熟度，並看到更多實用的部署資源，請參加 Microsoft 的**零信任成熟度模型評估**。