Microsoft

轉型零信任安全模式，強力支援遠距工作與雲端運作

網路疆界趨於模糊，難以明確區隔內外，除了持續成長的遠距工作需求，與外部夥伴及客戶的協同合作也更趨緊密。面臨可能失控的資安風險，以及無從預料的攻擊威脅，企業組織必須翻轉思維，轉型至新一代的零信任（Zero Trust）安全模式，全面防堵安全缺口，保護散布各地的人員、裝置、應用程式與資料。

隨著愈來愈多員工有遠距工作的需求，以及企業服務與應用程式的雲端化，以內網為基礎的舊式安全控管機制無法再有效保護企業組織。對許多企業組織而言似乎只有兩種選擇，一是透過緊縮的舊式網路架構來處理所有遠端傳輸，這必然大幅影響作業效能與員工生產力；另一種作法則是鬆綁，但會面臨防護、控管和可見度流失的風險。也正因為如此，愈來愈多企業組織轉而採取全新作法，以零信任安全模式為遠距工作提供更佳支援，同時也更有效地管理風險。

三大對策，嚴防錯放

料敵從寬、禦敵從嚴，任何一次錯放都可能為企業組織帶來巨大損失，零信任安全模式的概念就是預設每個存取要求可能都是安全缺口、都可能源於無法控管的網路，微軟則據此提供三大基本對策，強力落實零信任原則。

第一個對策就是明確驗證。所有可用的資料點一律都必須進行驗證和授權，包括使用者識別、位置、裝置健康情況、服務或工作負載、資料分類和異常。

第二個對策是使用最低的特殊權限存取。JIT（Just-in-time Administration）和 JEA（Just Enough Administration）權限控管模式的搭配，透過精密組合的授權規則、以風險為基礎的適性原則，在兼顧資料保護和生產力的前提之下，有效限制使用者存取。

第三個對策則是預設已有安全缺口，因此要透過對網路、使用者、裝置和應用程式的認知來分割存取權，縮小外洩的波及範圍並防止橫向移動。此外，所有驗證工作階段皆為端對端加密，並使用分析功能來取得可見度，進而驅動威脅偵測和改善防禦能力。

六大元件，缺一不可

要落實零信任安全模式，就得全面涵蓋所有數位資產，並採行預先整合的安全準則及端到端的策略，因此必須橫跨六大基礎元件進行零信任控管及相關技術的部署，相對地，每個元件也都是必須保護的重要資源，相關作法如下：

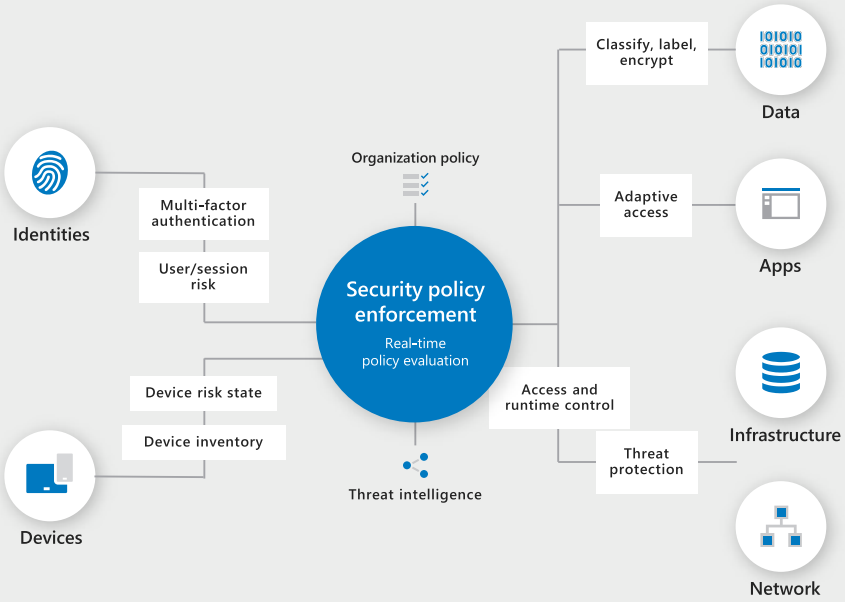
身分識別	所謂的身分不只限定於人員，還包括服務或物聯網（IoT）設定。任何身分試圖存取資源時，都必須以增強式驗證來辨明身分，以確保存取符合該身分的規則與型態，最低特殊權限存取的原則也必須落實。
裝置	一旦身分取得資源存取權後，資料可能在不同裝置之間傳輸，例如：從物聯網裝置到智慧型手機、透過自攜設備到夥伴的受管裝置，或是從內部的工作負載到運行於雲端的伺服器。這些異質裝置會衍生大量的攻擊空隙，為了確保安全存取，必須監看並落實裝置的健康狀態與合規性。
應用程式	應用程式和 API 是資料被運用之處，它們可能是內部的舊式程式、拋轉至雲端的工作負載，或是新式的 SaaS 應用。相關控管與技術要能找出影子 IT，根據即時分析確保適當的應用程式內權限，同時監看異常行為、控管使用者行動並驗證安全組態選項。
資料	企業組織的保護目標其實就是資料，無論它位於裝置、應用程式、基礎架構或網路，都必須確保安全無虞。資料必須被分類、標籤化及加密，並根據屬性來限制存取。
基礎結構	包含內部伺服器、雲端虛擬機器、容器或微服務在內，基礎結構通常是受威脅的主要目標。使用遙測來偵測攻擊和異常、自動封鎖和標記風險行為，並採取最低權限的存取原則。
網路	所有資料都是透過網路進行存取，即使裝置和使用者位於內部網路也不代表可以信任，所有內部通訊都必須進行加密、根據原則限制存取，並採用微區隔方法和即時威脅偵測。

以工具加速零信任部署

各個企業組織的不同需求、已經導入的現有技術及網路安全位階，都會影響零信任安全模式的規劃與執行。除了評估當前的整備度，進行對六大元件的強化防護，微軟也建議適時採用相關工具，確保零信任安全模式的有效實行。

增強式驗證	強化的多因素驗證和通訊會期風險偵測方案，皆可納入存取策略的骨幹，降低身分冒用的風險。
以政策為基礎的適應式存取	為資源制訂存取政策，並以一致化的安全政策引擎來落實，以因應各種變異提供治理能力和可見性。
微區隔	從以往集中式網路為基礎的邊界防護，改為透過軟體制訂微邊界，進行既全面又分散的區隔。
自動化	採用自動化警示及修復工具，縮減回應攻擊的落差時間。
智慧化與 AI	善用雲端智慧技術及所有可用信號，即時偵測及回應異常存取。
資料分類與防護	搜索、分類、保護及監控機敏資料，儘可能降低曝露於惡意行為或事件外洩的風險。

零信任安全架構



零信任安全模式不再相信防火牆之內的網路就是百分之百安全，而是如同對待開放網路一樣，每個存取要求都必須經過完整驗證、授權及加密之後，才會授與存取權。「絕不相信，一律驗證」正是零信任安全模式的運作的基本準則。

擁抱零信任安全性，實現遠距工作力

透過持續評定和以意圖為基礎的原則提供安全存取企業資源，支援您的員工進行遠距工作。
https://aka.ms/AA877io

您的組織處於零信任架構的哪個階段？

評定您的零信任成熟度階段以決定貴組織所處的位置以及如何移至下一個階段。
https://aka.ms/AA87esa