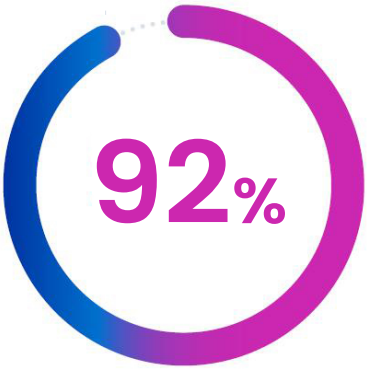
電子書

身分安全: 零信任架構策略的重要環節

面對當今網路風險以及變化多端的商業環境，我們正面臨著史無前例的挑戰。其中幾項挑戰包括:

- 遠距辦公工作者及外聘勞工的人數遞增
- 要管理及保護的系統使用者、非自然人用戶、裝置以及資料的類型，比以往大幅增加
- 需要穩定地轉移應用程式和工作負載至多樣雲端與混合基礎架構
- 雲端服務採用不同的身分模型 (例如更多繼承而來的角色和權限)

雲端運算、行動技術、物聯網、DevOps、自攜裝置上班 (BYOD)，以及在家工作等各項措施相繼出台，導致開始出現 IT 去中心化現象。行動技術和雲端技術採用率提高，表示現在有更多業務運作並非使用公司網路進行。有越來越多的使用者在各種不同的地點、使用各類不同的裝置存取應用程式和業務系統之類的資源。網路罪犯會接連不斷嘗試盜用使用者帳戶，企圖找到能夠順利入侵的破口，因此，許多組織已經將資安邊界的重心轉移到勞動力，其中員工、承包商、合作夥伴、廠商、供應商以及非自然人機器人均包括在內。這是身分安全的基礎：適度開放存取權限，同時持續保護整個企業。正是基於這個原因，許多組織將零信任架構資安計畫的根本要素放在身分安全。



的公司規劃實施零信任架構資安模型。[1]

[1]加速採用零信任架構以利管理在家工作的風險，2021 年 8 月

零信任架構不只是一套資安解決方案，更是一項策略。

零信任架構是一套資安架構，其目標除了在於支援企業的數位業務，也在於保障資料安全完整性，方法則是適度運用管理權責針對適當人選適度開放存取權限。因此，零信任架構策略要能發揮成效，身分安全是相當重要的一環。事實上，零信任架構能否發揮成效，關鍵在於身分的完整性、存取控制原則的成效和強度，以及能否在整個混合 IT 環境中持續治理身分和存取權限。

零信任架構資安保障始於身分安全

零信任架構資安保障的基礎在於「絕不信任，一律查證」以及「一律以資料外洩為假設前提」。在實務運用上，這項基礎是指絕不在不假思索的情況下信任任何一個人而同意對方存取資源，不論此人是組織內部或外部的人員都一樣。基本上，意思就是要認定每一個使用者都有嫌疑，直到證明安全無虞為止。在預設不信任一切網路流量的前提之下，以身分為基準是唯一可行的資安策略。

成功的身分零信任架構模型必須採行最小權限原則，所有使用者一律只能具備完成工作所需的最小存取權限 — 適度存取權限，不多也不少。要做到這一點，不僅要知道誰有哪些資源的存取權限，更重要的是要知道誰在什麼樣的情況下應該擁有存取權限。

根據近期的一項 IDSA 報告，幾乎所有 (97%) IT 資安專家均認同身分是零信任架構資安模型的根本要素。[2]

所以，在任何一項零信任架構計畫當中，身分安全都有著舉足輕重的地位。身分安全是指所有技術齊備，能夠自動處理身分生命週期；管理身分屬性的完整性；透過動態存取控管措施、角色型原則及職能分工 (SoD) 強制實施最小權限；以及連續評估一個範圍內的警訊，從而運用 AI/ML 之類的先進技術治理及因應。

[2] 2021 年數位身分保護措施相關趨勢。

組織若實施有強度且完整全面的身分安全計畫，就有能力管理和治理各類數位身分的存取權限，因此，您可以擬定出一套能夠依據全組織和整個威脅態勢進行系統性調整與因應的零信任架構。重要原則包括：

- **絕不信任，一律查證:** 運用以內容為準且最近期的身分資料，做出準確的存取權限決定。
- **只適時提供適度存取權限:** 運用角色和複雜的原則邏輯，強制實施最小權限。
- **連續監控、分析與調整:** 隨時更新資安措施，一出現變化及偵測到威脅，立即靈活因應。

最後，零信任架構是一套全面的資安解決方案。也就是說，零信任架構應該包含零信任網路控制（ZNTC）、特殊權限管理（PAM）和存取權限管理，以及身分安全。所有措施相輔相成，共同保護錯綜複雜的混合環境。

絕不信任，一律查證

過去的組織只要管理密閉且相對靜態的環境。當時，只要能以恰當的登入程序驗證使用者身分，就可以認定網路上的使用者都是安全的；接下來就會自動信任使用者。不過，當網路邊界消失，組織開始採用雲端資源之後，許多新的身分類型（例如承包商和合作夥伴）開始變得越來越重要。正因如此，IT 和資安團隊必須徹底反省原本保護企業的方式。

於是，零信任架構策略的第一項要素應運而生，那就是「絕不信任」。不過，這種情況也衍生出一個疑問：倘若絕不信任存取使用公司資源的使用者，公司該如何維持運作？答案就是公司必須查證使用者的身分。對大多數組織而言，必須要有強大的存取權限管理策略和解決方案才能做到這一點。當然，單一登入（SSO）和多因子驗證（MFA）都是資安措施中不可或缺的一環，但這些方法不會對使用者的身分進行查證，因此並不能全面驗證使用者。要做到全面驗證（也讓使用者能夠進入您的信任圈），重點就是要斟酌所有屬性，具體而言，就是以內容為準且隨時更新身分資料。

要產生能據以準確做出存取權限決定的身分資訊透明度，組織應掌握以下要點：

- **完整的資訊透明度:** 要能 360 度全面綜觀所有使用者類型以及各自的相關存取權限，包括所有權限、權利、屬性以及角色。
- **單一信任來源:** 建立清楚準確的身分記錄，決定存取權限時能夠賴以為據。
- **資料完整性:** 實施身分生命週期自動管理作業，隨時更新身分資料。

雖說「絕不信任」，但組織要能維持正常運作，勢必非信任不可。倘若能夠捨棄簡易驗證決定並針對每一位使用者採用完整的身分記錄(包括權限、權利、屬性及角色)，組織就能視需要放心授予存取權限。

善用最小權限原則，只適時提供適度存取權限

若零信任架構的第一項要素是絕不在不假思索的情況下給予信任，第二項要素就是一定要預設只授予最低程度的存取權限，這就是所謂的「最小權限」。理解這個概念並不難，但若要在不斷成長與變化的商業環境中大規模實施「最小權限」，就極其困難且相當複雜。.

這個時候，角色和角色型存取控制（RBAC）就發揮相當關鍵的作用，因為這兩項措施一律會確認使用者確實具備所需的存取權限，不會對組織造成過度風險。已經清楚定義並細分存取角色的組織可以輕鬆地指派、調整以及移除存取權限，不需承擔單次使用存取權限指派作業的風險，這類風險容易忽略，而且通常從不移除。除了角色以外，要避開容易導致佈建過度甚或引發詐騙或盜用風險的不利存取組合，還必須要具備動態存取原則邏輯。例如，要確定具備採購系統存取權限的使用者在相鄰應收帳務系統內不會同時具備其他權限，否則，肆無忌憚的員工有可能會利用假造採購單的方式一點一滴挪用公司資金。

的公司仍靠人工流程調整存取權限。[1]

那麼，組織採行最小權限措施之時，該怎麼做才能只適度提供適度存取權限?

- **安全存取控管措施:** 使用角色、精細調整的屬性、權限和動態原則，授予剛好夠用的存取權限。
- **自動存取:** 建立新使用者或變更角色時，會根據存取原則自動授予及更新存取權限。為減輕曝險程度，會自動解除未使用的存取權限以及無活動的帳戶。
- **長期防護及職能分工:** 偵測並預防不利的存取組合，防範可能發生的詐騙或盜用情事。

連續監控、分析與調整

許多組織得以順利採行「絕不信任」和「最小權限」等原則，但棘手之處在於確定其零信任架構模型不會偏離重點，而且能夠接納網路內外發生的所有變化。組織往往習慣於「設定後，即疏忽」，疏於主動監控、治理以及調整存取原則與控管措施。之所以會如此，通常是因為組織無力應對這類措施所產生的大量身分資料，內部也欠缺妥善維持零信任架構策略所需的專業知識。

身分資料是零信任架構中不可或缺的一環，因為這類資料包含重要資訊，例如身分屬性、存取權限、存取權利、行為資料，以及角色和群組成員資格。不過，由於身分資料過於龐大，根本無法靠人力手動整理所有資訊。分析大量身分相關資料時，為了因應組織變化而調整以及做出正確的存取決定，就必須運用以人工智慧和機器學習為主的工具，還要整合其他能夠支援其零信任架構策略的資安系統。使用身分資料的組織能夠運用強大的策略，因此得以隨時更新資安措施，一出現變化及偵測到威脅就能立即靈活因應：

- **持續監控存取情形:** 透過 AI 導向的見解，組織可以深入洞悉並瞭解所有使用者的存取情形，包括趨勢、角色、離群值以及關係。
- **一致的治理方式:** 衡量應用程式、資料和雲端資源存取控管措施的效益，有助於確保各項權限一律遵守原則。
- **協調流程:** 持續監控數位生態系統發出的風險警訊，並且與零信任架構閘道保持通訊，有助於確保能即時強制實施資安原則。
- **擴充能力:** 組織若能善用自訂工作流程、API 以及事件觸發程序，就能在其他網路安全與存取系統全面自動處理身分安全計畫。

67% 的受訪者認為使用自動化及先進技術可增進企業預防網路攻擊的能力。[3]

[3] Ponemon Institute: 執行網路安全生命週期防護措施的經濟價值 (The Economic Value of Prevention in the Cybersecurity Lifecycle)。

零信任架構必須採用全面的方法

前幾節的內容提過零信任架構策略必須依賴不同的系統相輔相成。這套全面的資安方法對所有零信任架構部署均非常重要。

身分定義安全聯盟 (Identity Defined Security Alliance, IDSA) 是由身分和資安廠商組成的協會，這個聯盟擬定了一個參考架構 (圖 1)，協助人們瞭解身分定義安全的不同要素。

不同類型的「使用者」(圖左) 需要申請目標資源 (資料，圖右) 的存取權限。除了身分管理和治理以外的各種身分和資安控管措施 (以不連續的方塊顯示，圖中)，全都是在各類裝置、網路、基礎架構、應用程式以及資料中保護使用者存取權限的重要機制。

身分安全解決方案需輔助並整合能夠相輔相成的身分和資安技術，才能提供完整的零信任架構資安解決方案。

圖 1.身分定義資安參考架構 [1]

[1] IDSA: 身分定義資安指南 (The Guide to Identity Defined Security)

您的零信任架構策略是否符合身分安全方法?

這項核對清單可以協助您確認零信任架構策略是否符合身分安全策略，能夠隨著您的業務和資安需求變化而靈活調整。

- ☐ **部署身分倉儲:** 建立身分資料集中存放庫，讓每一位使用者、非人類對象、裝置以及資料來源 (包括影子 IT) 的身分完全透明且清楚易懂。
- ☐ **採行強大的存取控管措施:** 運用角色和存取原則管理，只因應需要指派資料和應用程式資源管理權限，並且設定 SoD 原則，避免可能出現不利的存取權限組合。
- ☐ **遵循最小權限原則:** 持續檢討並調整使用者的身分權利和角色，確保使用者確實只具備適度存取權限，能夠適時存取他們確實需要的資源。
- ☐ **監控活動資料:** 將使用者運用組織資源存取權限進行的活動全數記錄下來，並且監控相關記錄並找出可疑的行為。
- ☐ **活動資料相關警示:** 標註可疑的存取活動或權利變更，並且提醒相關管理員注意。
- ☐ **移除未使用的存取權限:** 對於不再需要的存取權限，自動進行解除部署。
- ☐ **自動處理事件回應:** 根據使用者屬性或位置的變更情形，自動修改或終止其存取權限。
- ☐ **協調事件回應方式:** 整合您的資安系統和身分系統，讓您能夠全面綜觀可能代表潛在威脅的資安事件。偵測到高風險活動時，自動執行補救措施。

採行後續措施

SailPoint 身分安全是能讓零信任架構策略奏效的基石。零信任架構能否發揮成效，關鍵在於身分的完整性、存取控制原則的成效和強度，以及能否在整個混合 IT 環境中持續治理身分和存取權限。SailPoint 是身分市場領域的頂尖廠商，提供的身分安全技術能夠自動處理身分生命週期；管理身分屬性的完整性；透過動態存取控制、角色型原則及職能分工強制實施最小權限；以及運用 AI/ML 對存取進行連續評估、治理及因應存取風險。

如欲深入瞭解，請上網瀏覽 **sailpoint.com/solutions/zero-trust**

關於 SailPoint

SailPoint 是現代企業身分安全治理的領導廠商。企業安全管理範圍從身分存取開始至結束，現單憑人力已無法協助企業有效治理和保護身分安全。SailPoint身分安全治理平台以人工智慧與機器學習為基礎，協助企業於適當的時機向對的身分和技術資源開放必要的存取權限，以滿足當今以雲端發展為主的企業對規模調度、速度與環保等各方面的需求。SailPoint智慧、自主與整合的解決方案以身分安全治理作為管理數位業務的核心，支持全球組織架構複雜的企業打造以身分安全治理為基準的策略，以應對現今嚴峻的安全威脅。

sailpoint.com

EB2160-2208

FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市前鎮區一心二路128號9樓之1