Microsoft Security

零信任基本指南

領導層提升 AI 安全性的方法

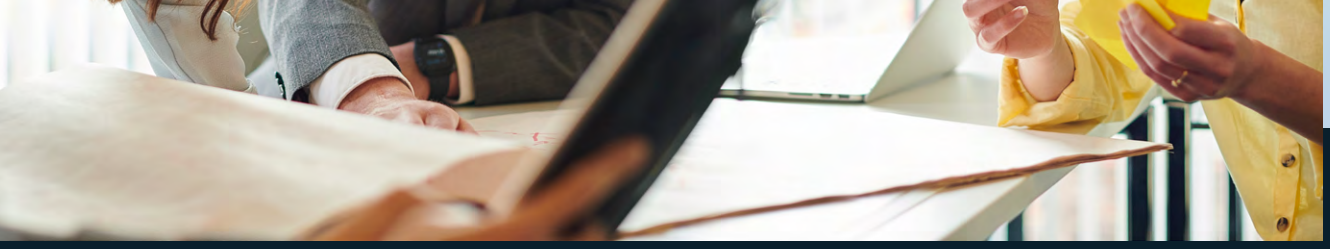
內容

您的資料存留在比以往更多的地方 — 好好保護

為了從您現今的資料中獲得具有競爭力等級的價值，不能將其隔離。必須將其連接到大量服務、合作夥伴、整合和其他資料集，以用於新流程，例如聯合學習。為了獲得 AI 的好處，您必須確保資料在網路內外都是安全的。

無論是以主要計劃的方式應用於整個系統，還是建置成小型專案，零信任都已成為關鍵的安全性策略和穩定力量。

對於防範日益複雜且昂貴的威脅、不慎資料外洩，甚至是新等級的資料移動所伴隨的法規和合規性問題，零信任理念都是中心。



在威脅格局中蓬勃發展

網路犯罪正在迅速成長，攻擊的速度、規模和複雜性亦是如此。與金融罪犯合作的國家行為體為防禦者創造了新的規模和複雜性的威脅。這些威脅執行者正在使用 AI 來降低發動攻擊所需的成本、時間和技能集。現在，藉助 AI，可以驚人的速度自動化新攻擊、惡意程式碼、深偽等，以利用弱點。

思考一下：

4,000

每天密碼攻擊次數。從 2021 年每天 579 次上升。

200%

增加的人為操作的勒索軟體攻擊數，單從 2022 到 2023 年。

9.22 兆美元

資料外洩的成本 (2024 年) 預計到了 2028 年將成長到 13.82 兆美元。

因此，零信任方法如何比傳統的周邊防禦更妥善地保護您的資料和系統抵禦這些威脅？

為了回答這個問題，我們必須首先回答另一個問題：什麼是零信任？

零信任的 3 大核心原則

零信任不是一個產品或東西；它不是技術，甚至不是工具。而且它肯定不是您需要一次全部完成的事。零信任是網路安全性的理念，它假設一切都是威脅，直到證明並非如此，在這種情況下會懷疑並且應該挑戰每項交易。

這是一個簡單的概念，但根據這種假設，零信任方法指定防禦者做出相應的行動，即使資料或個人已經知道或位於過去稱為「安全性周邊」的網域。基於這些假設，零信任安全性方法必須遵守三個原則：

1. 明確地驗證。

根據提供的所有資料點，持續驗證及授權，包括使用者身分識別、位置、裝置健康狀態、服務或工作負載、資料分類和異常。

2. 使用最低權限存取。

使用適時適度存取 (JIT/JEA)、依據風險的調適性原則和資料保護來限制使用者存取，以協助保護資料和生產力。

3. 假設入侵。

零信任不會表現得彷彿攻擊即將發生，而是將任何情形視為已經發生入侵。這不僅改善預防，而且在發生資料外洩時，還可以將影響降到最低，並有助於防止跨系統存取和進一步損失。

零信任的三項要素透過以下方式提高安全性：

- **能夠**讓您偵測網路攻擊和駭客攻擊，
- **自動封鎖**和 / 或標記有風險的行為，
- **採取保護動作**以減輕損失和橫向移動，以及
- **更妥善地管理**日益增加的網路威脅資料。

您採用零信任原則的能力，有賴於您自身的安全性挑戰、業務需求、網路能力和資源。

在我們深入探討 Microsoft 對於您在組織中使用零信任有何具體建議之前，讓我們來看一下零信任架構，該架構將為您提供策略性基礎來組織您的優先順序，並將您系統的保護視為整體，無論您是將零信任做為主要計劃，還是進行較小規模單獨應用。

Microsoft 零信任方法的元素

雖然我們並未發明零信任，但 Microsoft 已經開發了靈活的零信任方法，引導您進行考量和規劃。在思考是否及如何實施零信任時，請考慮如何處理這七個關鍵風險領域：

身分識別

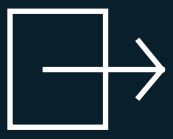
- 自動化風險偵測和修復，讓適當的人員能夠適當存取適當的資料類型。
- 跨整個數位資產利用諸如多重要素驗證 (MFA) 和單一登入 (SSO) 等健全措施，以保護資源的存取。

資料

- 跨雲端和內部部署環境來分類、標記和保護資料，以防不當的分享並降低內部風險。
- 當資料在網路內部待用或移動時加以保護。
- 在資料用於資料共用 (如聯合學習) 時，保持資料安全。

應用程式

- 盡可能簡化員工對雲端和行動應用程式，以及對內部部署企業資源的安全存取。



端點

- 了解存取資料的端點類型，以及如何有效地管理每個端點。
- 專注於減少受攻擊面的大小，以及減少需要具彈性、整合式管理和安全性方法的裝置和端點數量。

網路

- 減少以周邊為主的安全性弱點，例如 VPN。
- 提高安全性應用程式的可擴縮性，跟上雲端和混合環境的多變性。

基礎結構

- 確保您的內部部署、雲端和混合基礎結構以有效率且自動的方式受到保護和管理。

AI

- 利用 AI 的力量更快地找出威脅和風險，並即時調適，以便動態地調整安全性原則和控制。

這些都是完整安全性方法的組成部分，可因應不斷變化的安全性環境。當您考慮當中各個領域時，請記住，沒有單一的正確答案；根據您的目前形勢、每個領域的需求，以及您所面臨的威脅，您的組織將具有獨特的優先順序。

採取行動並不意味著一次全部完成

現在對零信任有清楚的了解後，來看看您可以開始應用零信任以獲得最大好處的一些方法。請記住，這並二選一的建議。您不用為了從零信任中獲益，而顛覆安全性：從您目前及合理的地方開始著手。

查看您的業務優先順序；與領導階層的同儕討論零信任。最佳的方法是從上述七個風險領域的簡單速贏或較小型計劃開始，看看符合您的業務目標的好處。請記住，Microsoft 擁有資源、工具和解決方案，可在整個過程滿足您的需要。

讓我們來看一下零信任和 Microsoft 可以幫您實現的目標。

零信任如何加強安全性態勢

降低風險和複雜性，同時透過擴大對數位環境的可見度、依據風險的存取控制和自動化原則，實現數位轉型。

簡化安全性，驗證每項交易、強制最低權限存取，以及套用進階偵測和回應威脅。

跨環境保護資料，無論是在多平台、多雲端或其他環境中。

簡化和降低成本，使用零信任橫跨整個組織部署單一控制項，而不是多個未整合的安全性控制。

提升和簡化員工和管理員的體驗，與 Microsoft 或其他公司的資源和技術整合。

探索 Microsoft 零信任解決方案

- Security Copilot
- Entra Copilot
- 條件式存取
- 信任結構
- Entra Suite
- 依據風險的條件式存取

零信任如何改善合規性和治理

保護您最關鍵的資產與資料，即使它們移出您的網路之外用於 AI 功能也一樣。

提高業界安全性標準的合規性，例如 NIST，透過全面策略無縫地保護、管理和控管資料。

自動化原則強制執行和控制，以確保遵守法規要求。

改善客戶關係和信任，支援整個組織的合規性計劃。

實現彈性部署，對雲端和容器環境進行細微控制。

提高組織的敏捷性，跨越組織不斷變化的身分識別、端點、應用程式、基礎結構、網路、資料和 AI，抵禦不斷改變的安全性威脅。

探索 Microsoft 零信任合規性方案

- Azure
- Microsoft 365
- Dynamics 365
- Power Platform

零信任如何協助實現 AI 未來

自信地部署生成式 AI，同時管理風險，以協助實現 AI 承諾的業務成果。

獲得支援 AI 的工具和資源所增強的力量，來偵測異常並在風險和威脅影響您之前「看出」端倪。

在貴組織中創新和實現 AI，以創造更安全的環境，使 AI 模型和資料受到保護。

即時調適和回應，以更快的速度查看威脅和風險，使用 AI 來推動洞察力並動態調整安全性措施。

設計存取、資料和應用程式安全性控制，保護您寶貴的商務資料，同時享有 AI 支援的應用程式優勢。

零信任如何協助實現 AI 未來

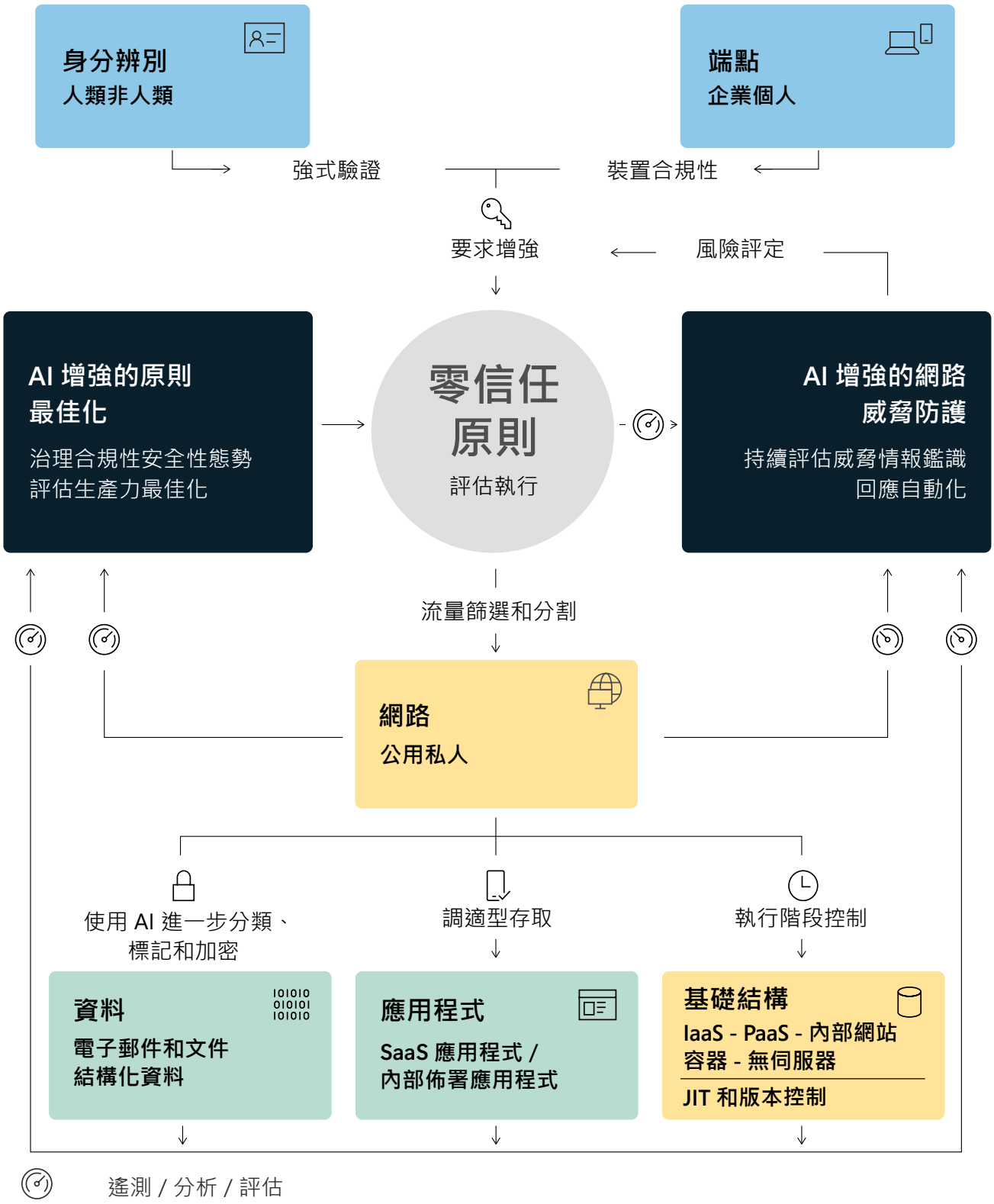
- Microsoft Security Copilot
- 適用於 DevOps 的 GitHub Copilot
- 適用於 AI 的 Purview
- Microsoft Security Copilot 及第一方嵌入式解決方案：Entra、Intune、Purview、Defender、適用於雲端的 Defender

視覺化您自己的零信任架構

在您考慮通往零信任的路徑以及如何開始著手時，請考慮您的整個組織，不只是網路，還有定義、傳遞和使用它的人、實體、端點、原則、資料、應用程式和基礎結構。雖然您不必在整個組織中一次全部實施零信任，但當您計劃和進展時，不妨以大局著想。

為了協助將一切視覺化，請使用此架構開始塑造您的零信任方法。

Microsoft 零信任架構



開始以零信任架構為基礎建置

有了最新的威脅情報和全方位的零信任方法（工具、架構和產品），Microsoft 就可以成為現代化安全性方法的基礎。了解它如何能協助您降低風險，並藉助易於理解、實作為和管理的架構來減輕攻擊的影響。零信任敏捷安全性方法還有助於有效管理 AI 安全性風險，同時加速組織的零信任旅程。

深入了解 Microsoft 零信任