

# 機器身分安全在數位時代的重要性與日俱增

2025年7月

指數研究負責人Ilaria Sangalli

在當今快速發展的數位環境中，身分不再是人類獨有的象徵。它的主要功能已然擴大，不再局限於管理人口，而是延伸到監控成千上萬的機器。網路安全方面，機器身分安全變得越來越重要。但到底什麼是機器身分？機器身分指能核實、驗證並授權網路內各種機器（如設備、伺服器、應用程式）的數位實體。正如人類使用用戶名、密碼或其他生物辨識方式來確認身分，機器身分亦依賴數位憑證及加密金鑰進行驗證，藉此管理及確保機器之間進行互動與傳輸資料的安全性。<sup>1</sup>

機器身分的數量正在爆炸性增長，目前已遠超人類身分的數量。根據CyberArk的調查，在部分企業中，每名員工能衍生多達40個機器身分。<sup>2</sup>由於機器身分的崛起，創建強大的安全框架已成為當務之急。隨著企業對互聯設備、服務及應用程式的依賴程度加深，他們的數位存在亦明顯擴大。這當中每一個設備都需要經過身份驗證。若放任不管，這些身分可能會遭惡意行事者利用，引發嚴重的安全漏洞。

與標準的用戶帳號相比，機器身分通常會獲授更高級別的權限，故已成為網路罪犯的主要攻擊目標。此外，機器身分通常較人類身分受到更少的監視與保護。儘管企業在識別人類身分相關風險方面的技術愈發成熟，但在保護機器身分方面仍有很大的進步空間。根據CyberArk的調查報告<sup>3</sup>，在1,200名安全主任中，近42%受訪者承認他們的公司缺乏周密的機器身分安全策略。此外，在過去一年中，半數企業曾因機器身分受到攻擊而出現安全漏洞。<sup>4</sup>

機器身分是不會消失的。隨著AI解決方案變得越來越普遍，人們使用的機器身分數量只會有增無減。不少企業逐步將AI與機器學習融入日常營運，並開始採用「代理式AI」，因此對機器身分及AI系統實施完善安全管控的重要性迫在眉睫。通過優先採取對應的安全措施，企業可更好地保護敏感資料，同時降低未經授權使用AI產生的風險。

<sup>1</sup> <https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/machine-identity-management/>

<sup>2</sup> <https://www.cyberark.com/resources/machine-identity-security/ai-surge-drives-a-40-1-ratio-of-machine-to-human-identities>

<sup>3</sup> 調查範圍涵蓋美國、英國、澳洲、法國、德國及新加坡

<sup>4</sup> <https://www.cyberark.com/CyberArk-2025-state-of-machine-identity-security-report.pdf>

資料來源：納斯達克指數研究、彭博、FactSet。

免責聲明：

Nasdaq®為Nasdaq, Inc.的註冊商標。上文所載資料僅供參考及教育用途，不應詮釋為針對特定證券或整體投資策略的投資建議。Nasdaq, Inc.及其任何關聯公司均不對買賣任何證券作出任何建議，亦不對任何公司的財務狀況作出任何陳述。有關納斯達克上市公司或納斯達克專有指數的聲明並不保證未來的表現。實際結果可能與所明示或暗示的結果存在重大差異。過去的表現並不代表未來的結果。投資人在投資前應自行作出盡職調查並仔細評估公司。強烈建議投資人徵詢證券專業人士的建議。若對本譯本所提供資訊有任何疑問，請參考英文版本。

© 2025. Nasdaq, Inc. 保留所有權利。