SailPoint

# 掌握先機，防範網路風險

**身分安全成熟度如何促進韌性提升**

身分的數量與類型不斷擴增，這不僅會加劇安全漏洞，還會加重法規遵循壓力並提高網路保險成本。

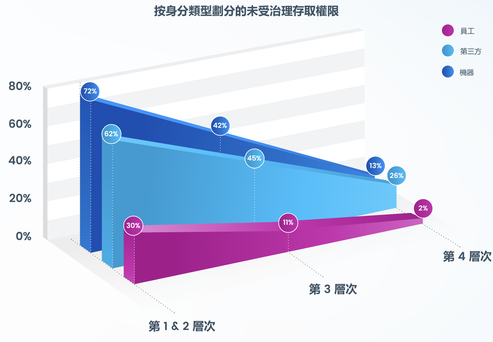
**↑30+%**
未來 3 到 5 年內，機器身分的增長幅度

**↑14%**
未來 3 到 5 年內，數位身分的增長幅度

**↑77%**
3 年來，網路保險費用的上漲幅度

**↑7x**
自 2010 年起，身分相關規章的增加幅度

## 最近一項針對約 350 名身分與存取管理 (IAM) 及安全決策者的調查顯示，未受治理的存取權限仍然是 2024 年的重大議題。




**第 1 & 2 層次**
手動作業：基本的身分處理流程為手動管理，這樣通常會導致效率低下並產生安全漏洞。

**第 3 層次**
數位化：將帳戶佈建自動化，藉此提升準確度並降低手動工作量。

**第 4 層次**
進階工具與預測型使用案例：實施由人工智慧 (AI) 驅動的解決方案，實現智慧決策與主動式身分管理。

## 機器身分代表著最大的安全風險，其數量通常是人類身分的 10 倍以上

機器需要專業的管理，以防止安全風險及未符法規遵循的問題。

**66%**
的公司表示管理機器身分**需要更多的手動作業***

**60%**
的公司表示他們管因機器身分而**遭遇稽核問題***

**72%**
的公司表示他們**有意保留閒置狀態的機器身分***

*機器身分危機：手動流程的挑戰與暗藏的風險

## 保護每個身分。管理所有存取權限。獲得回報。

透過更具策略性的 IAM 投資，組織可有效降低身分相關的安全問題及事件的波及範圍，同時改善其整體網路韌性。

**約 40%**
得益於 AI, 第 4 層次及以上組織偵測及回應網路攻擊的加速幅度

**83%**
的組織因投資身分安全，而回報其 2023 年身分相關安全問題有所降低

**40%**
網路保險公司的損失降低幅度，彰顯出網路風險管理成效有所改善

## 按數字呈現的風險降低成功案例

**3 倍**
**網路風險降低幅度，**為約 6,000 個帳戶設定適當權限所達成

**12 萬**
**的非員工擁有安全身分**

**14.4 萬**
**自動化帳戶修改與驗證的次數，**降低潛在的安全威脅

**>300 萬美元以上**
**防止勒索病毒付款而節省的金額，此為透過健全的身分安全所達成**

## 評估貴組織目前的狀況並提升網路韌性。

探索身分安全層次的框架與評估方法，瞭解成熟的組織如何提升安全保障、簡化營運並達成法規遵循。

探索調查結果


本文件中的所有資料點均摘自《身分安全層次》報告，除非另有說明。

SailPoint



sailpoint.com/zh-hant

IN2636-2504