

2024 年-2025 年

身分安全層次

發揮身分安全的力量以改變網路安全價值的趨勢

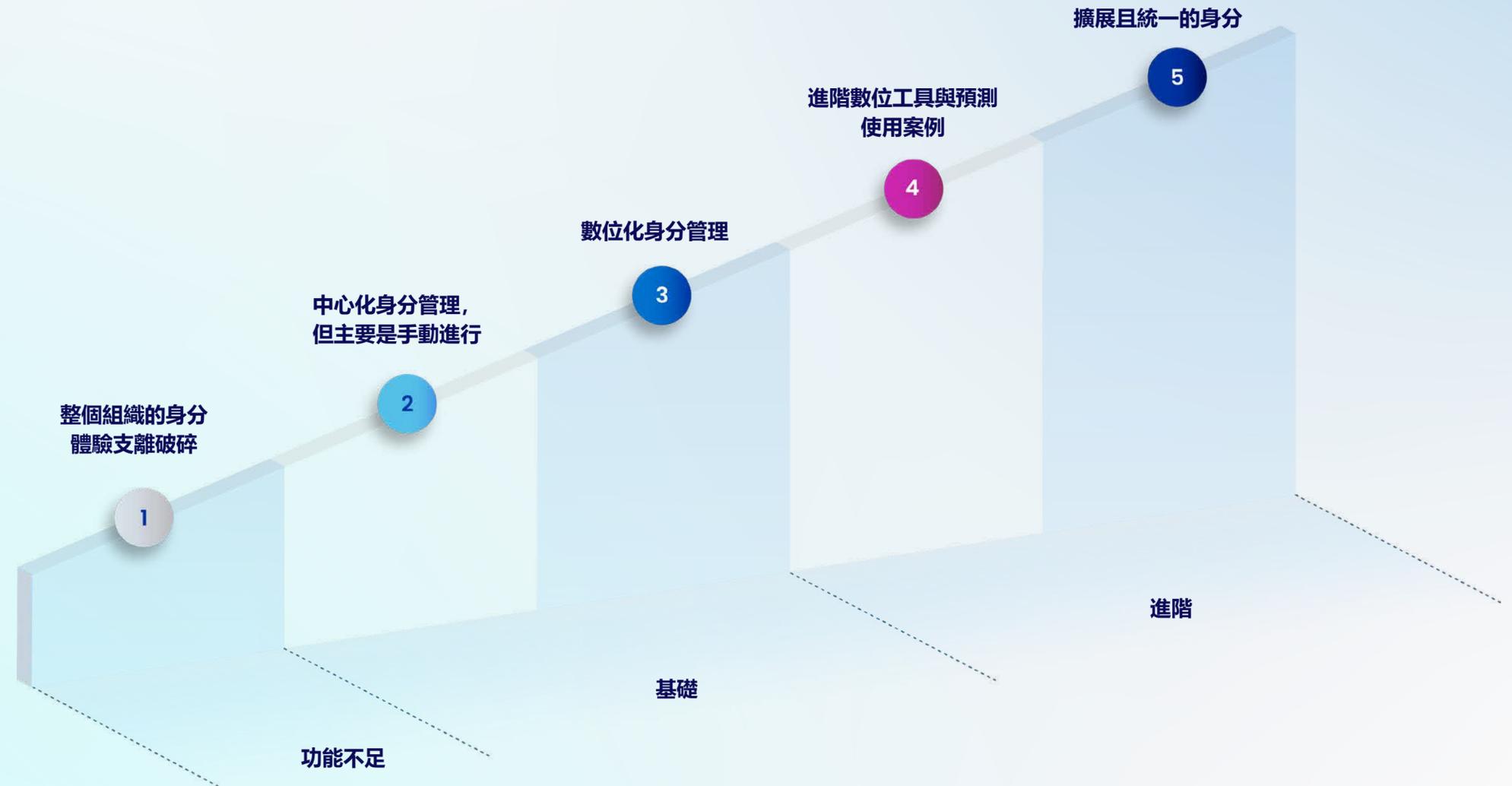
踏上提升身分安全成熟度的旅程

全球各行各業的組織正面臨雙重挑戰：他們必須對抗越來越複雜且無處不在的網路威脅，同時還要應對有限的預算和不斷大幅縮減的成本。

隨著組織的擴張，攻擊面的增加和 IT 預算的緊縮，身分安全方面的壓力尤其地沉重，而內部和外部的股東對於安全性和數位體驗有越來越高的需求。

在過去三年中，SailPoint 針對全球身分與存取管理 (IAM) 的決策者進行問卷調查，來評估他們在 5 個身分安全層次的功能表現。我們在 2024 年 7 月調查的這 350 位決策者，包含資訊科技、網路安全和風險的資深領導者，而其中超過半數任職於員工超過 10,000 人的組織，更有超過半數任職於金融或技術領域。

資料來源：本文件中的所有圖表均摘自《2024 年 - 2025 年身分安全層次》報告。



第1章

提升技術將能形塑 身分安全的未來。

身分安全的未來將會由 4 個 關鍵要素定義

在過去幾年間，我們的經驗和研究已證明，身分安全的未來會由整合性身分計畫所形塑。

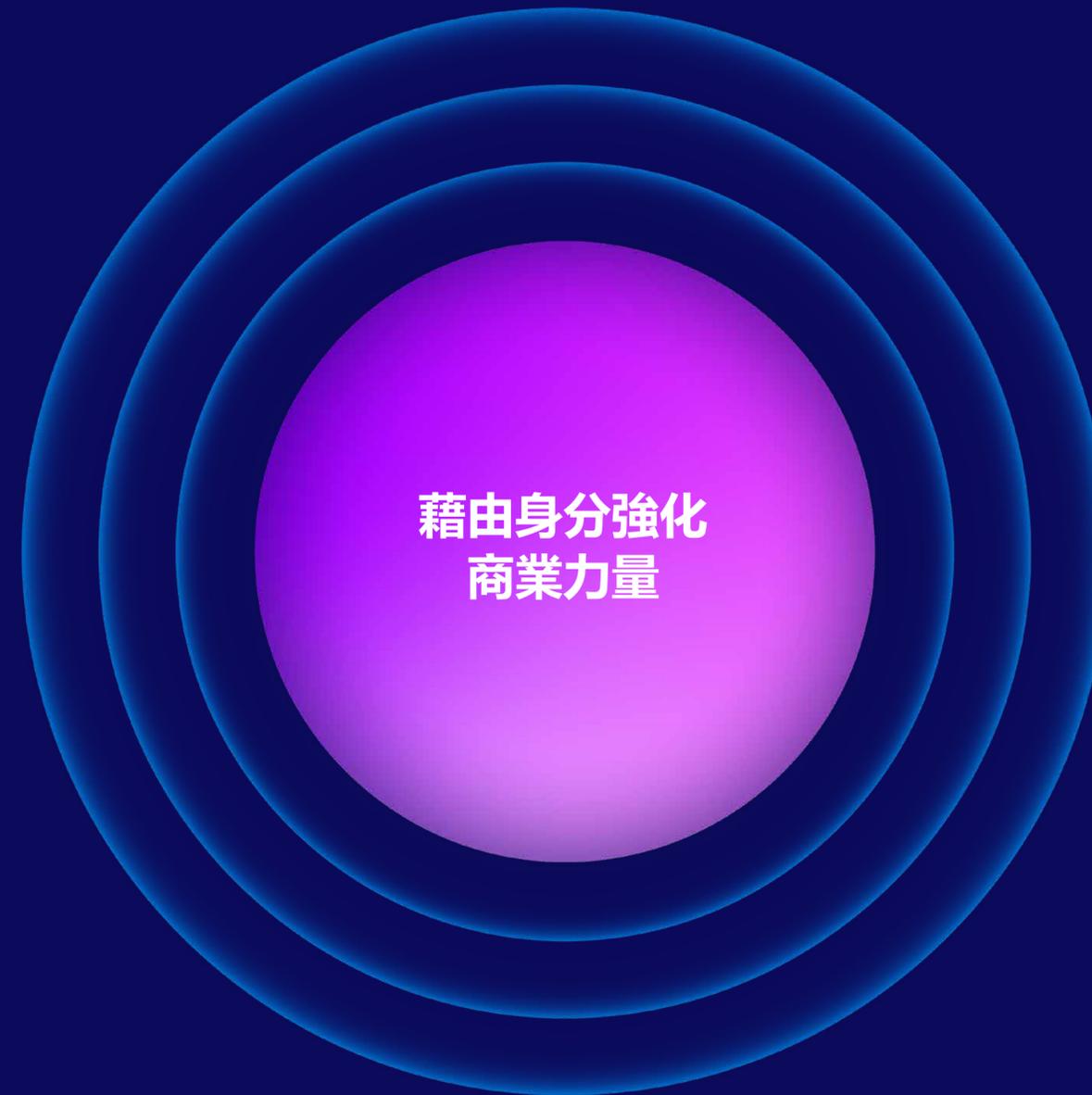
此處呈現的是關鍵要素及與之相輔相成的趨勢。

不斷演變的規章與風險態勢持續形塑這四個要素

身分安全網狀架構將成為未來安全運作的核心。

全球各地及各類產業的身分安全相關規章與產業標準激增，將提高對於身分安全方面的期望。

● 2024 年新增 ● 初創 ● 崛起 ● 主流



身分安全的未來將會由 4 個 關鍵要素定義

在過去幾年間，我們的經驗和研究已證明，身分安全的未來會由整合性身分計畫所形塑。

此處呈現的是關鍵要素及與之相輔相成的趨勢。

不斷演變的規章與風險態勢持續形塑這四個要素

身分安全網狀架構將成為未來安全運作的核心。

全球各地及各類產業的身分安全相關規章與產業標準激增，將提高對於身分安全方面的期望。

● 2024 年新增 ● 初創 ● 崛起 ● 主流

整合式身分計畫

1

- 跨 IAM 解決方案的統一存取控制
- 身分功能與安全營運整合
- 機器身分管理應對了 AI 使用案例及自動化機器人擴展
- 整合身分資料層

藉由身分強化
商業力量

身分安全的未來將會由 4 個 關鍵要素定義

在過去幾年間，我們的經驗和研究已證明，身分安全的未來會由整合性身分計畫所形塑。

此處呈現的是關鍵要素及與之相輔相成的趨勢。

不斷演變的規章與風險態勢持續形塑這四個要素

身分安全網狀架構將成為未來安全運作的核心。

全球各地及各類產業的身分安全相關規章與產業標準激增，將提高對於身分安全方面的期望。

● 2024 年新增 ● 初創 ● 崛起 ● 主流



身分安全的未來將會由 4 個 關鍵要素定義

在過去幾年間，我們的經驗和研究已證明，身分安全的未來會由整合性身分計畫所形塑。

此處呈現的是關鍵要素及與之相輔相成的趨勢。

不斷演變的規章與風險態勢持續形塑這四個要素

身分安全網狀架構將成為未來安全運作的核心。

全球各地及各類產業的身分安全相關規章與產業標準激增，將提高對於身分安全方面的期望。

● 2024 年新增 ● 初創 ● 崛起 ● 主流

藉由身分強化
商業力量

聯合身分

3

- 聯合存取正逐漸成為各身分類型的主流
- 多種身分角色，如勞動人力、商業合作夥伴及機器，正逐漸整合在身分安全控制平面下
- 去中心化身分通訊協定仍處於早期階段

身分安全的未來將會由 4 個 關鍵要素定義

在過去幾年間，我們的經驗和研究已證明，身分安全的未來會由整合性身分計畫所形塑。

此處呈現的是關鍵要素及與之相輔相成的趨勢。

不斷演變的規章與風險態勢持續形塑這四個要素

身分安全網狀架構將成為未來安全運作的核心。

全球各地及各類產業的身分安全相關規章與產業標準激增，將提高對於身分安全方面的期望。

● 2024 年新增 ● 初創 ● 崛起 ● 主流



4

無摩擦存取

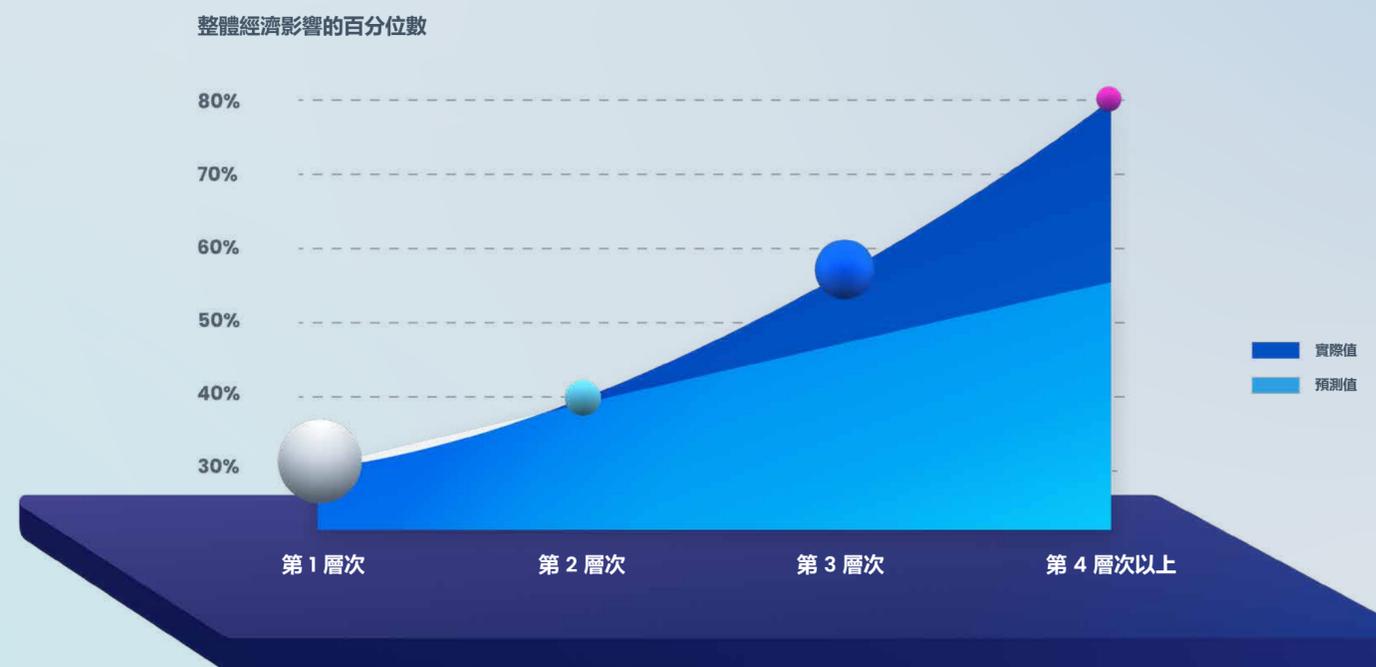
- 自動化特殊權限存取管理
- 無密碼驗證逐漸成為常態

第 2 章

投資身分安全可 「改變趨勢」。

具有成熟身分安全的組織 所花的每一分錢都能夠達成 超乎預期的高報酬

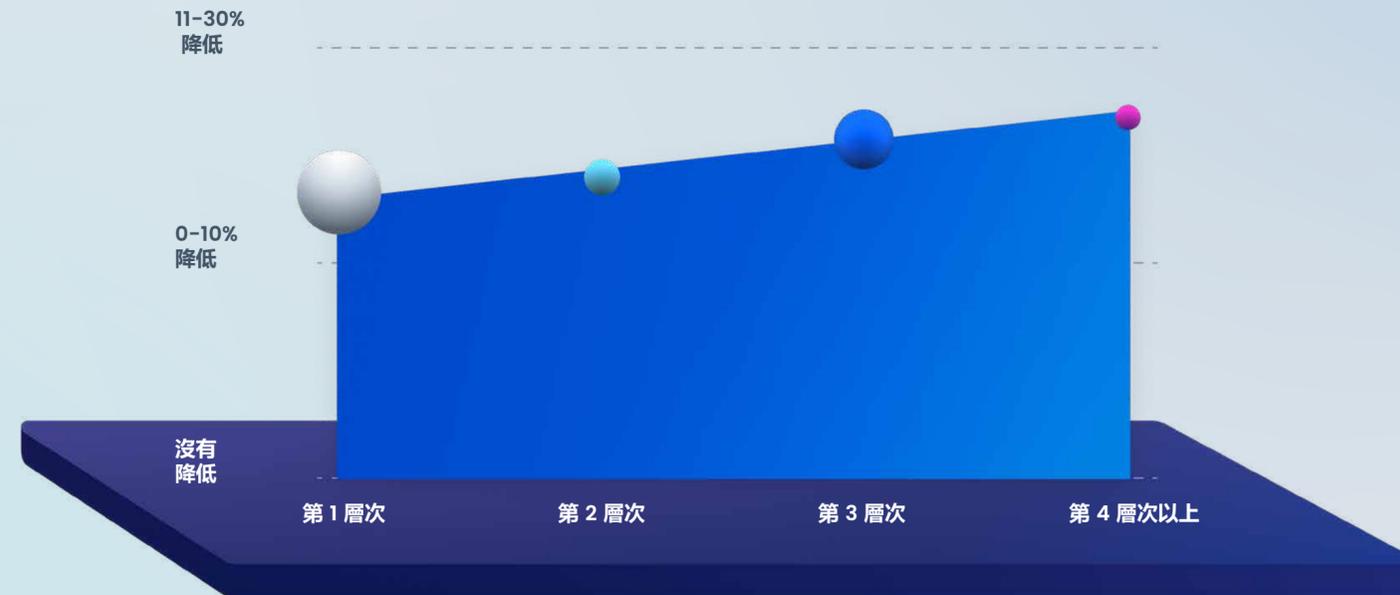
躍升至第 3 及第 4 層次會對身分安全
領域帶來極大的商業影響力，能夠以
指數形式「改變趨勢」。



*球體直徑範圍表示層次的分佈情況

突破身分安全層次縮小 潛在的漏洞攻擊面

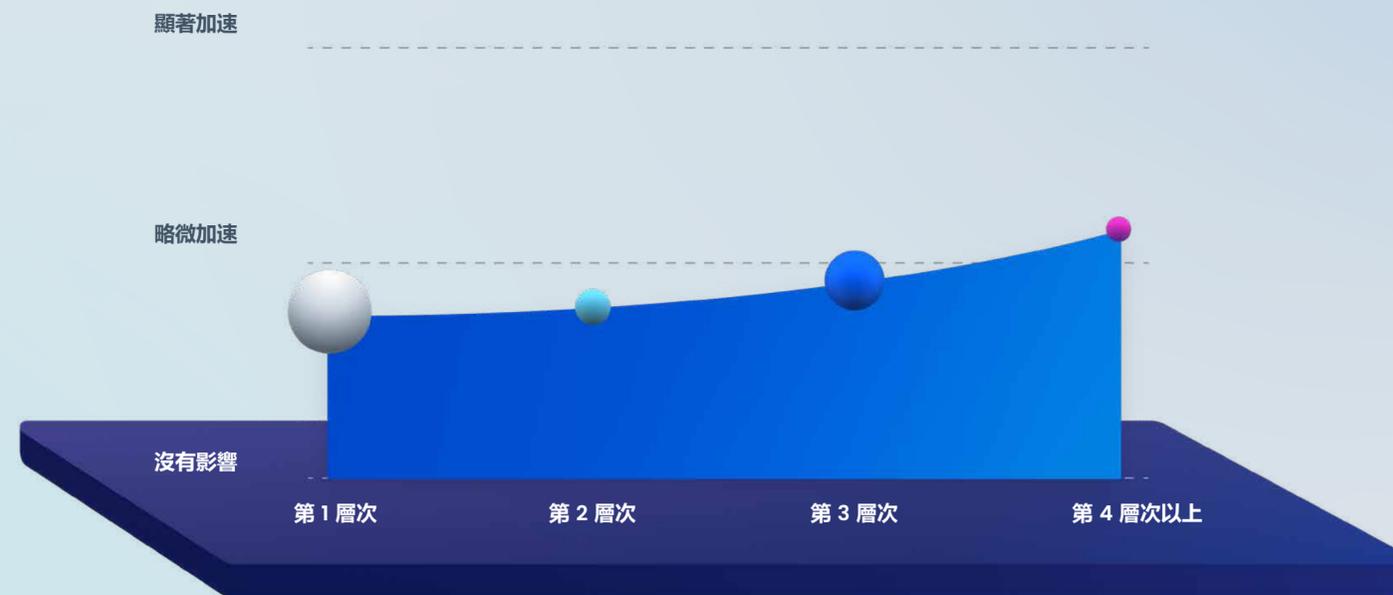
83% 的組織報告，由於 2023 年對身分安全的投資，使身分相關的安全問題有所減少。



*球體直徑範圍表示層次的分佈情況

擁有進階身分安全功能的組織， 能夠體驗更快的上市時程並減少 摩擦

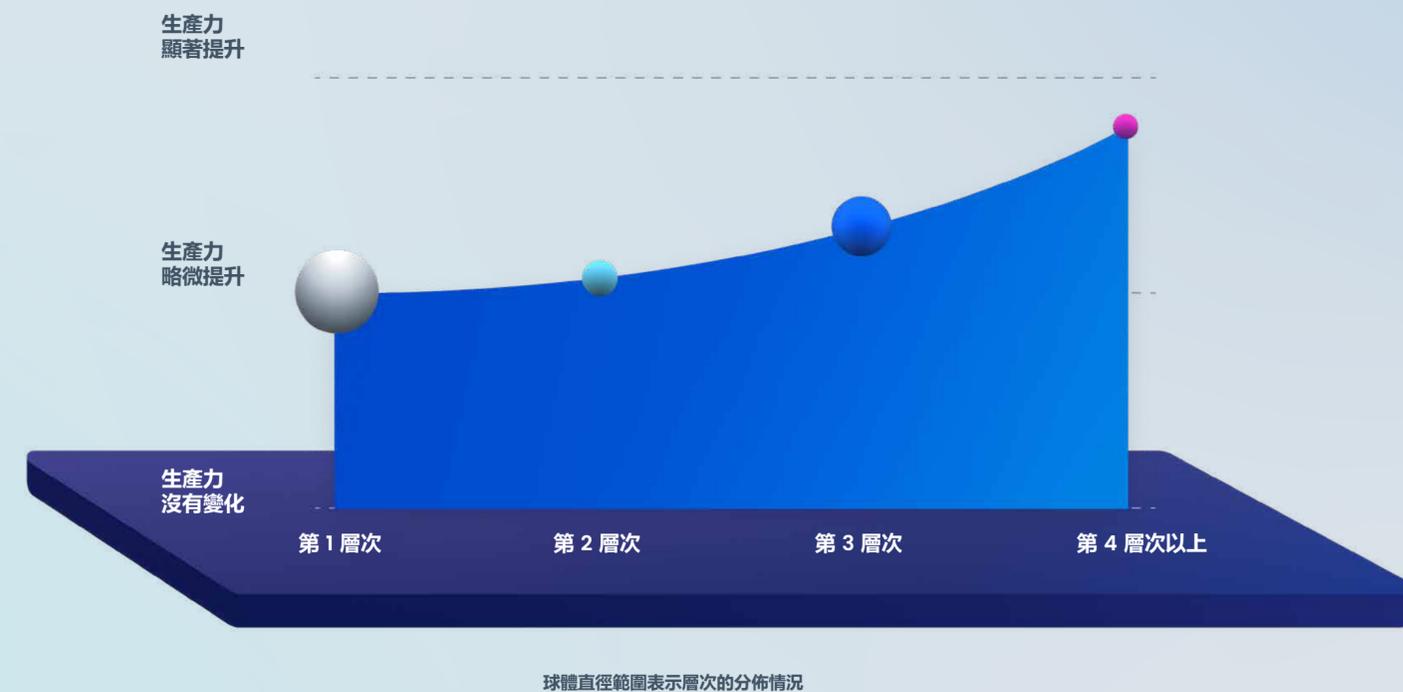
帶動整體營收：進階身分安全會加速數位轉型，達成更快速的開發循環及上市速度，並藉此提升收益。



*球體直徑範圍表示層次的分佈情況

第 3 及第 4 層次以上的組織 預期可取得顯著的生產力提升

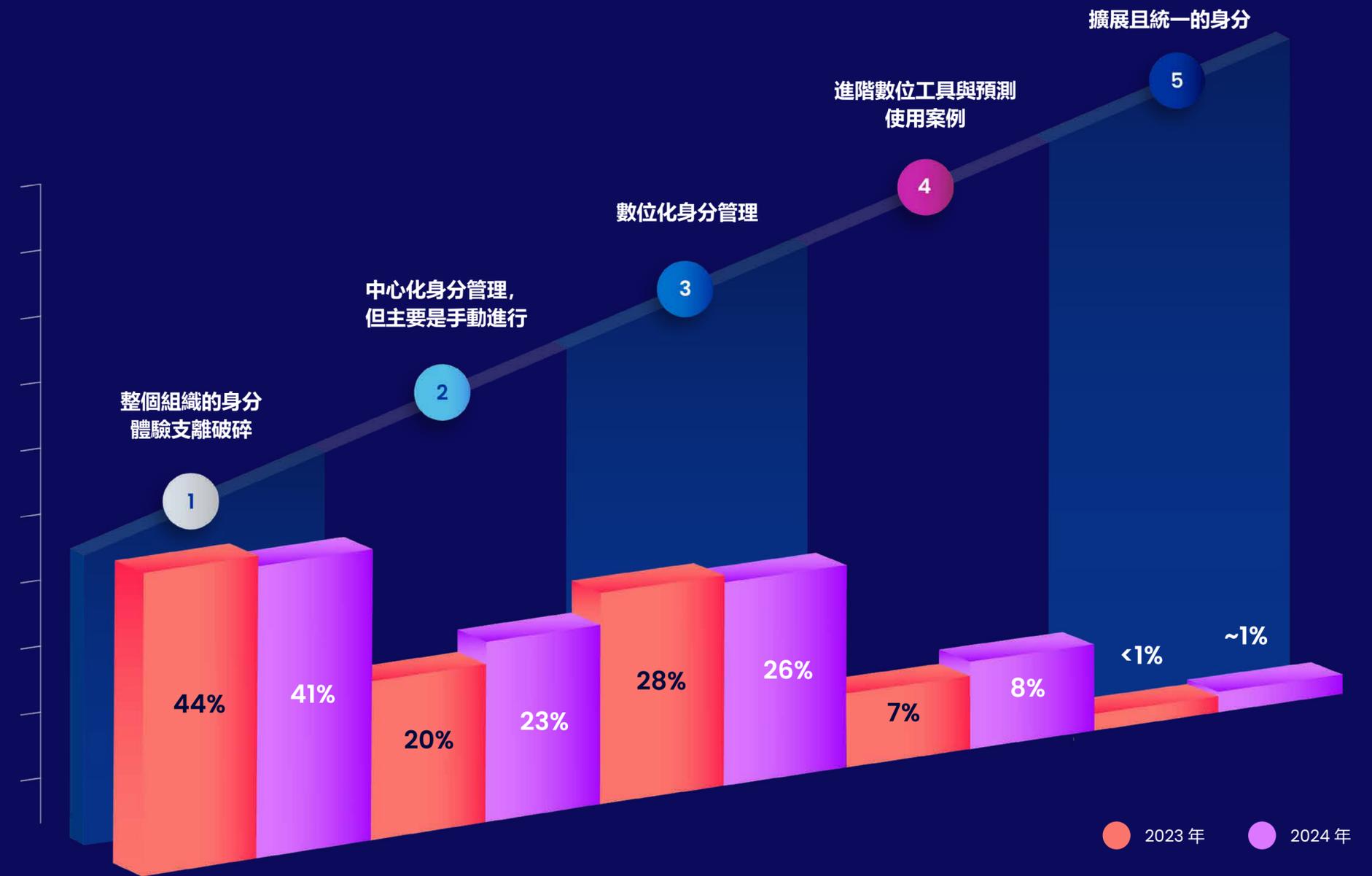
第 4 層次以上的組織藉由整合身分安全方法，並同時採納新興的使用案例，例如指引型協作助手、終端使用者服務及自動化使用者存取核准，可實現顯著的生產力提升。



第 3 章

組織處於發展歷程中的哪個階段，以及成熟的組織為何能夠獲得較高的報酬。

目前有 41% 的組織仍停留在第 1 層次，這表示釋放身分安全的「完全潛力」存有重大機會



位處第 4 層次以上的組織，可藉由覆蓋範圍達 70% 的身分類型功能來降低風險，而位處第 3 層次的組織則緊隨其後

第 1 及第 2 層次的組織在身分覆蓋範圍方面有著巨大差距。下列為目前尚未受到治理的部分。

30%

員工

62%

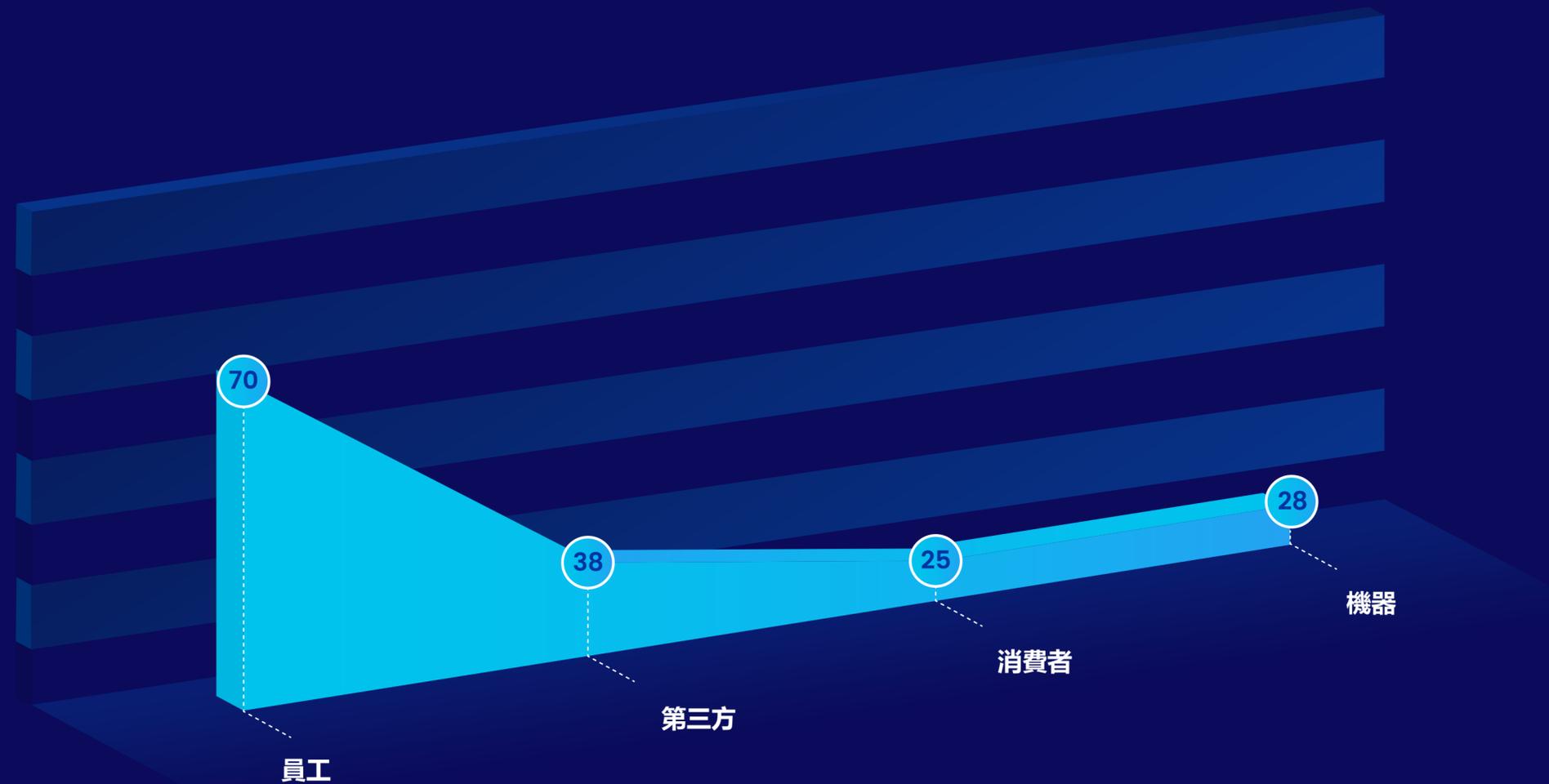
第三方

72%

機器身分

後者尤其令人擔憂，因為機器身分通常約佔整個組織總身分的 40-65%。

第 1-2 層次



位處第 4 層次以上的組織，可藉由覆蓋範圍達 70% 的身分類型功能來降低風險，而位處第 3 層次的組織則緊隨其後

第 1 及第 2 層次的組織在身分覆蓋範圍方面有著巨大差距。下列為目前尚未受到治理的部分。

30%

員工

62%

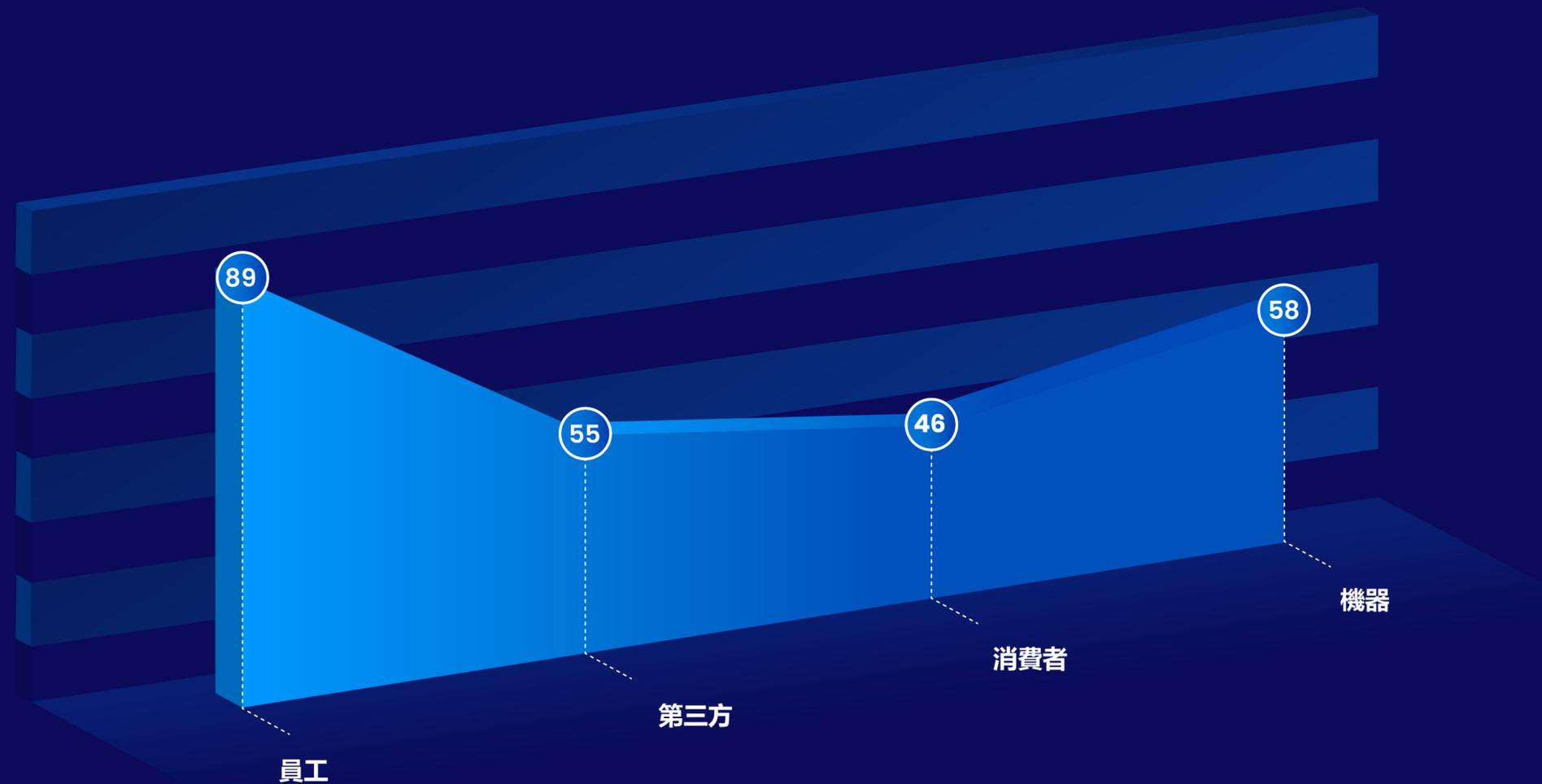
第三方

72%

機器身分

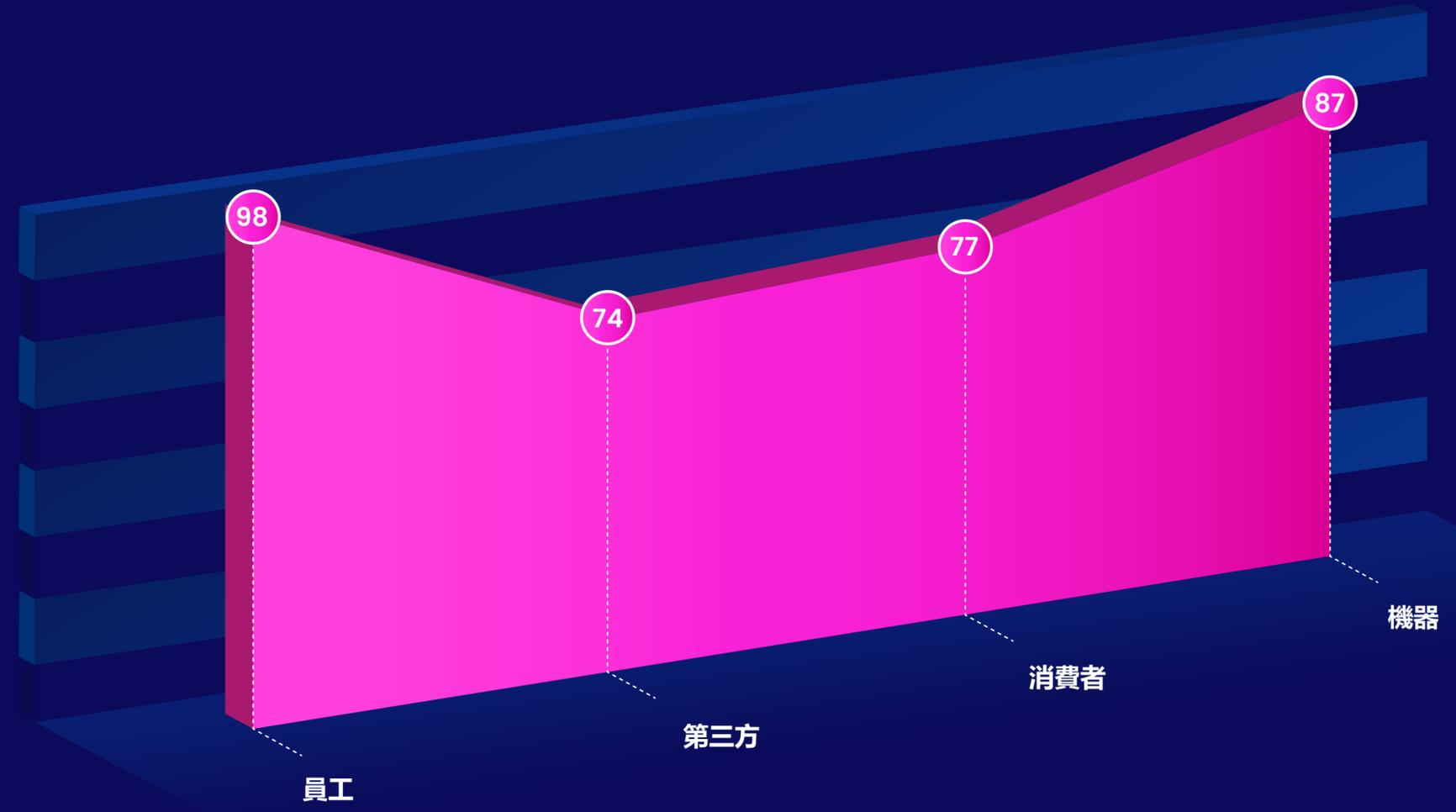
後者尤其令人擔憂，因為機器身分通常約佔整個組織總身分的 40-65%。

第 3 層次



位處第 4 層次以上的組織，可藉由覆蓋範圍達 70% 的身分類型功能來降低風險，而位處第 3 層次的組織則緊隨其後

第 4 層次以上



第 1 及第 2 層次的組織在身分覆蓋範圍方面有著巨大差距。下列為目前尚未受到治理的部分。

30%	62%	72%
員工	第三方	機器身分

後者尤其令人擔憂，因為機器身分通常約佔整個組織總身分的 40-65%。

位處第 4 層次以上的組織，可藉由覆蓋範圍達 70% 的身分類型功能來降低風險，而位處第 3 層次的組織則緊隨其後

第 1 及第 2 層次的組織在身分覆蓋範圍方面有著巨大差距。下列為目前尚未受到治理的部分。

30%

員工

62%

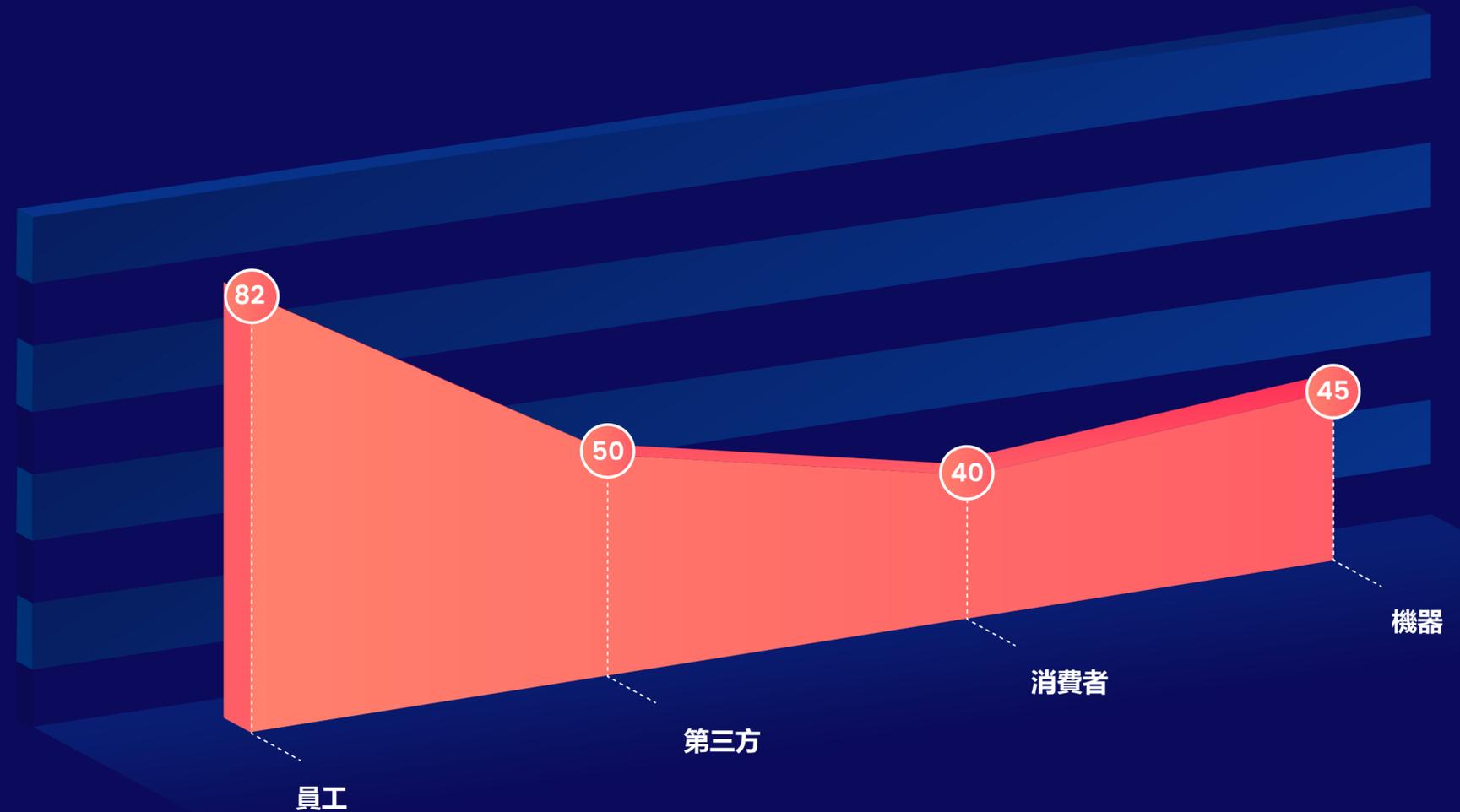
第三方

72%

機器身分

後者尤其令人擔憂，因為機器身分通常約佔整個組織總身分的 40-65%。

整體



位處第 4 層次以上的組織，可藉由覆蓋範圍達 70% 的身分類型功能來降低風險，而位處第 3 層次的組織則緊隨其後

第 1 及第 2 層次的組織在身分覆蓋範圍方面有著巨大差距。下列為目前尚未受到治理的部分。

30%

員工

62%

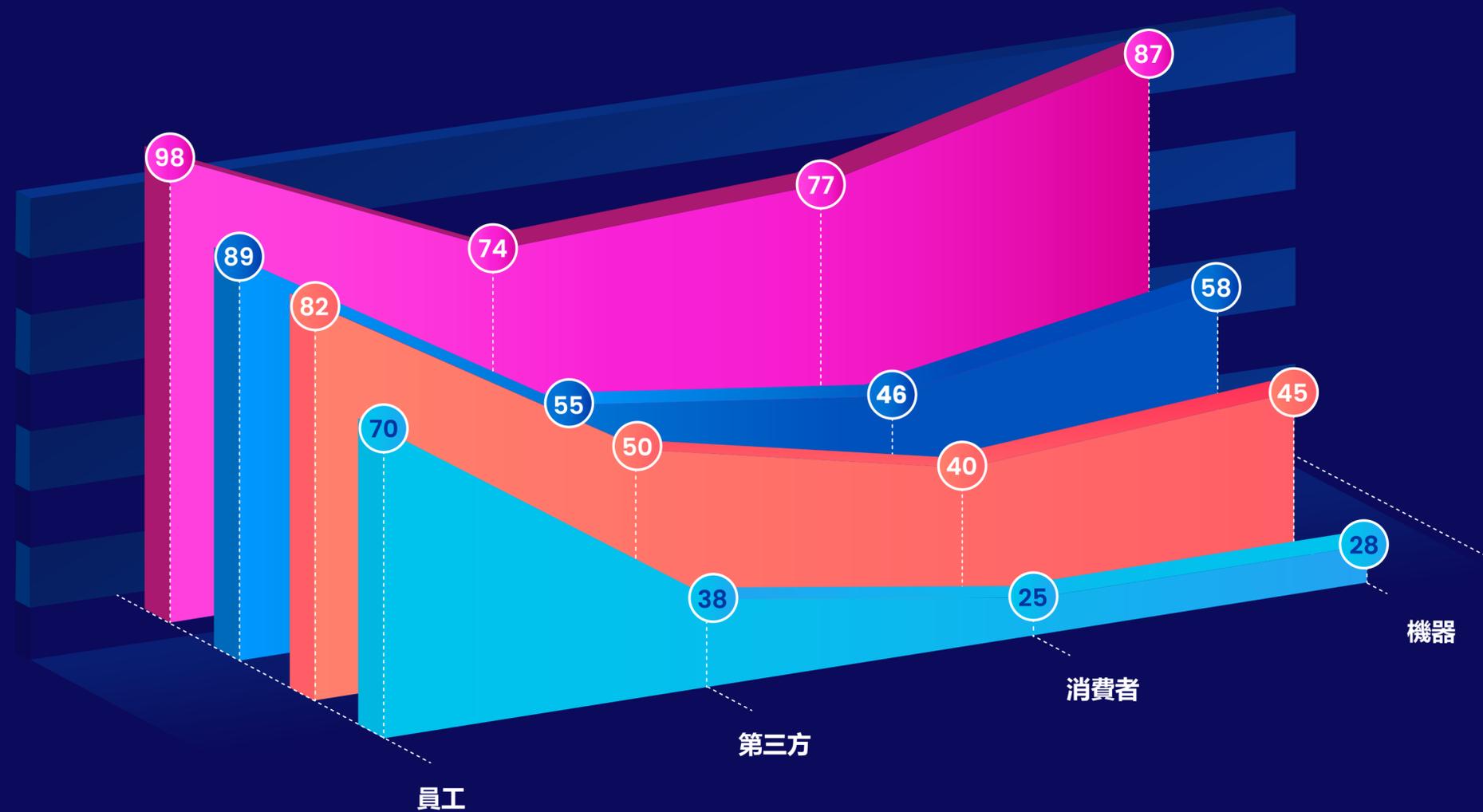
第三方

72%

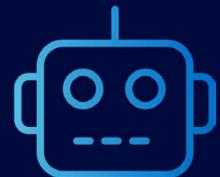
機器身分

後者尤其令人擔憂，因為機器身分通常約佔整個組織總身分的 40-65%。

● 第 1-2 層次 ● 第 3 層次 ● 第 4 層次以上 ● 整體

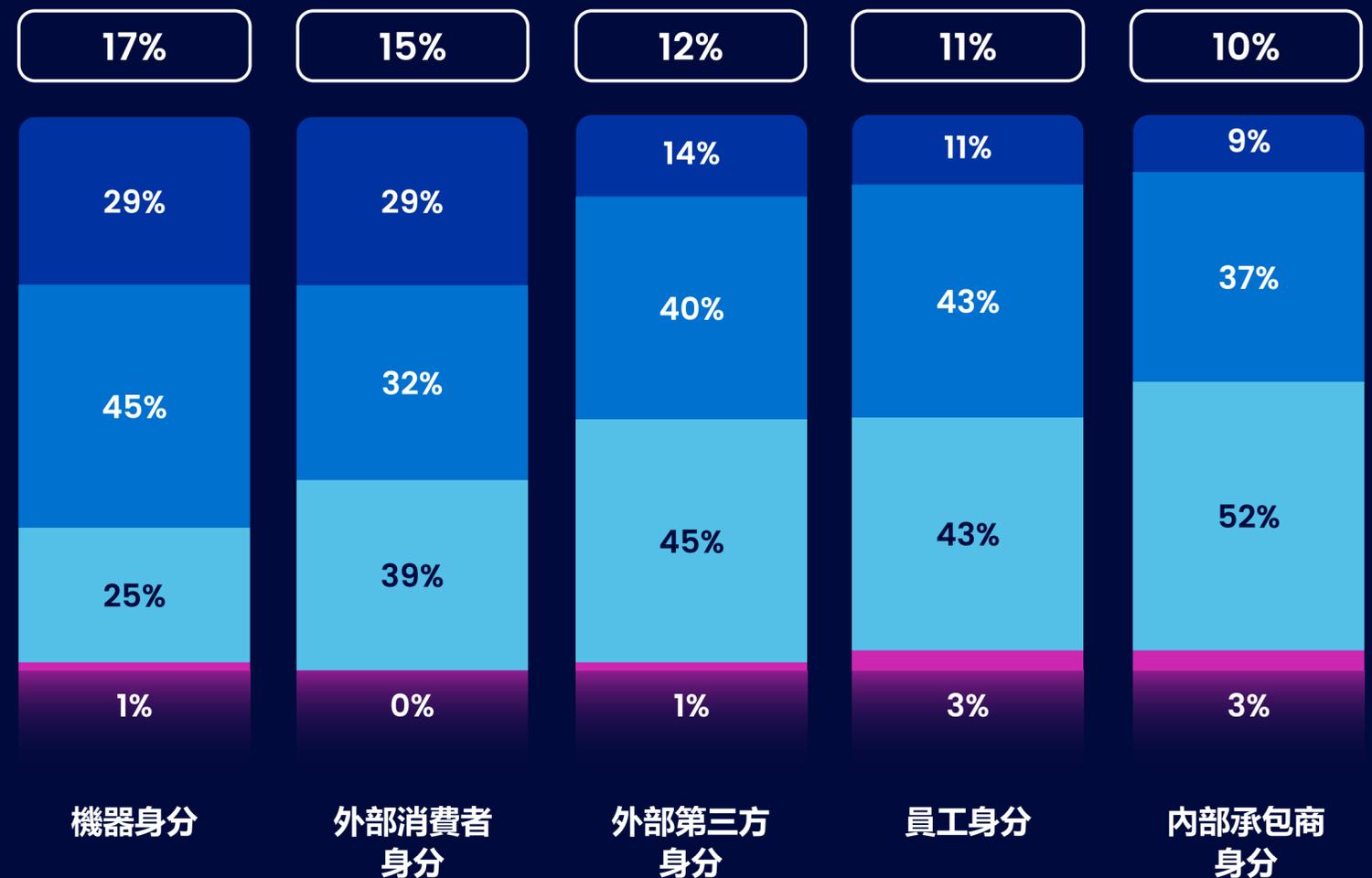


所有身分預期在未來 3-5 年內成長約 14%，而機器身分的成長最為迅速

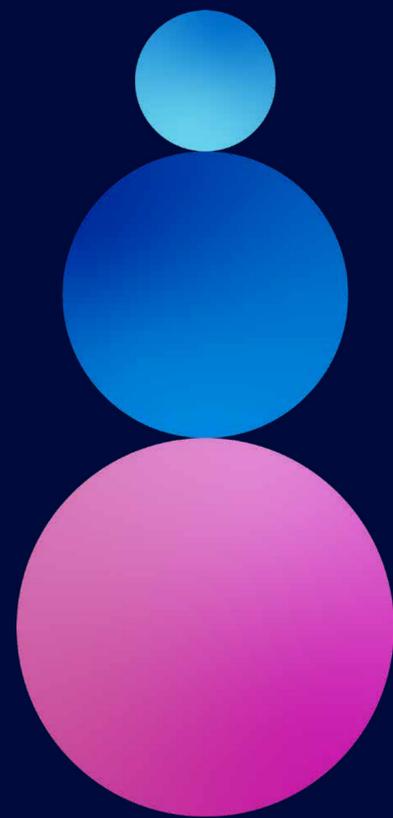


機器身分的成長速度可能會超過人類身分的增長速度。

- 增加 30% 以上
- 增加 10% - 29%
- 與現今的數量相仿 (差距不超過 10%)
- 減少 10% - 29%
- 平均預期成長率



第 4 層次以上的組織將身分資料用於可據以行動的情資以及新使用案例的機率是其他組織的兩倍



<20%

的第 1-2 層次組織規模化運用身分情資資料

<40%

的第 3 層次組織規模化運用身分情資資料

~50%

的第 4 層次以上組織將結構化與非結構化資料的智能指引，用於使用者存取、安全原則及存取審查

第 1-2 層次

提供使用者所需存取權限的智能指引

12

情境感知安全原則

18

智能存取審查 / 存取權限稽核

19

根據即時情境動態授權

14

根據角色指派自動建立基本存取權

20

透過分析使用者行為取得風險洞見

20

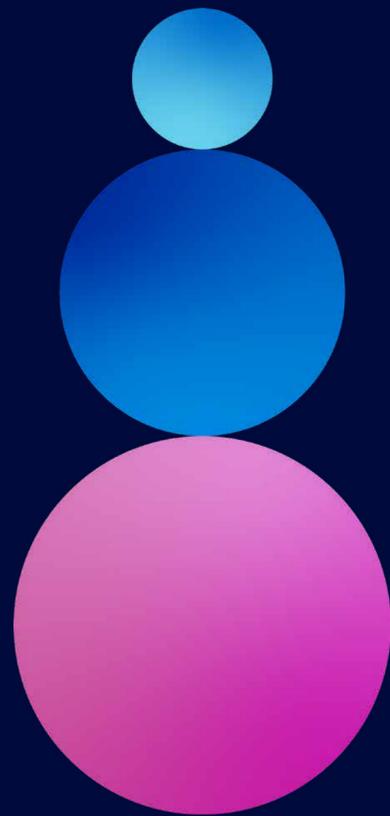
AI 驅動存取控制

5

無覆蓋 (0%)

完全覆蓋 (100%)

第 4 層次以上的組織將身分資料用於可據以行動的情資以及新使用案例的機率是其他組織的兩倍



<20%

的第 1-2 層次組織規模化運用身分情資資料

<40%

的第 3 層次組織規模化運用身分情資資料

~50%

的第 4 層次以上組織將結構化與非結構化資料的智能指引，用於使用者存取、安全原則及存取審查

第 3 層次

無覆蓋 (0%)

完全覆蓋 (100%)

提供使用者所需存取權限的智能指引

31

情境感知安全原則

35

智能存取審查 / 存取權限稽核

39

根據即時情境動態授權

24

根據角色指派自動建立基本存取權

33

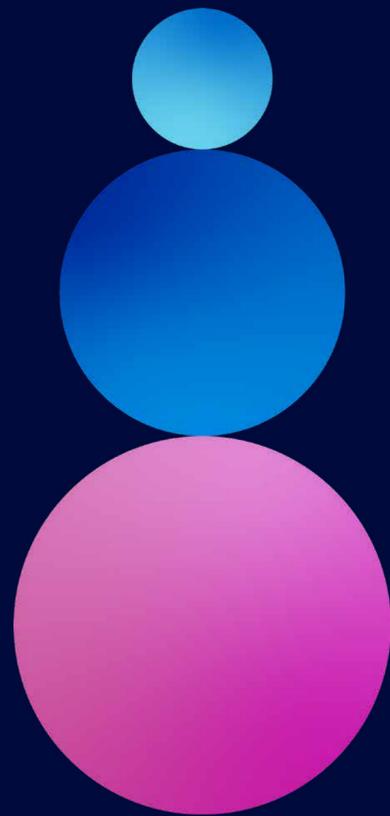
透過分析使用者行為取得風險洞見

38

AI 驅動存取控制

15

第 4 層次以上的組織將身分資料用於可據以行動的情資以及新使用案例的機率是其他組織的兩倍



< 20%

的第 1-2 層次組織規模化運用身分情資資料

< 40%

的第 3 層次組織規模化運用身分情資資料

~ 50%

的第 4 層次以上組織將結構化與非結構化資料的智能指引，用於使用者存取、安全原則及存取審查

第 4 層次以上

無覆蓋 (0%)

完全覆蓋 (100%)

提供使用者所需存取權限的智能指引

50

情境感知安全原則

50

智能存取審查 / 存取權限稽核

50

根據即時情境動態授權

42

根據角色指派自動建立基本存取權

42

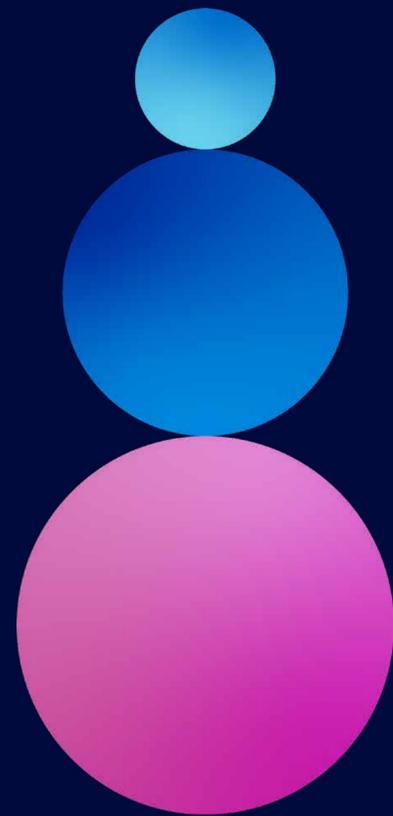
透過分析使用者行為取得風險洞見

38

AI 驅動存取控制

35

第 4 層次以上的組織將身分資料用於可據以行動的情資以及新使用案例的機率是其他組織的兩倍



<20%

的第 1-2 層次組織規模化運用身分情資資料

<40%

的第 3 層次組織規模化運用身分情資資料

~50%

的第 4 層次以上組織將結構化與非結構化資料的智能指引，用於使用者存取、安全原則及存取審查

整體

無覆蓋 (0%)

完全覆蓋 (100%)

提供使用者所需存取權限的智能指引

24

情境感知安全原則

29

智能存取審查 / 存取權限稽核

31

根據即時情境動態授權

22

根據角色指派自動建立基本存取權

28

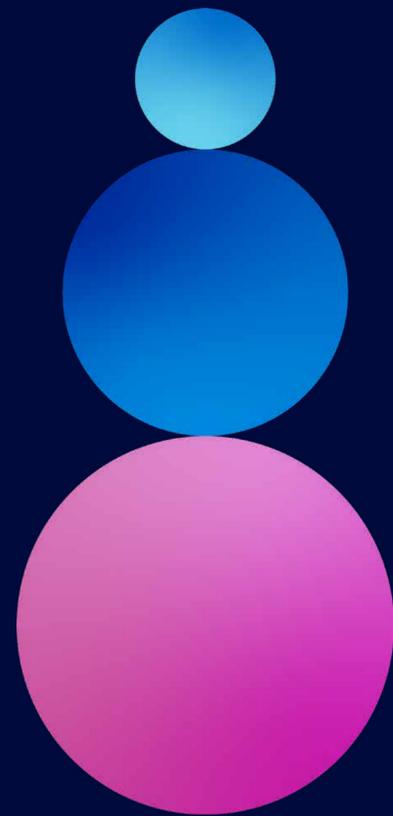
透過分析使用者行為取得風險洞見

30

AI 驅動存取控制

13

第 4 層次以上的組織將身分資料用於可據以行動的情資以及新使用案例的機率是其他組織的兩倍



<20%

的第 1-2 層次組織規模化運用身分情資資料

<40%

的第 3 層次組織規模化運用身分情資資料

~50%

的第 4 層次以上組織將結構化與非結構化資料的智能指引，用於使用者存取、安全原則及存取審查

所有資料

無覆蓋 (0%)

完全覆蓋 (100%)

提供使用者所需存取權限的智能指引



情境感知安全原則



智能存取審查 / 存取權限稽核



根據即時情境動態授權



根據角色指派自動建立基本存取權



透過分析使用者行為取得風險洞見



AI 驅動存取控制



● 第 1-2 層次 ● 第 3 層次 ● 第 4 層次以上 ● 整體

擁有成熟身分安全的組織，即具備投資規模化生成式 AI 驅動使用案例的基礎

第 3 層次的組織專注於工程設計可規模化解決方案，藉此增強並將身分安全規模化。同時，第 1-2 層次的組織則專注於自動化支援中心類型的重複性活動。



● 第 1-2 層次 ● 第 3 層次 ● 第 4 層次以上 ● 整體

(%) 預估對生成式 AI 的平均投資意願

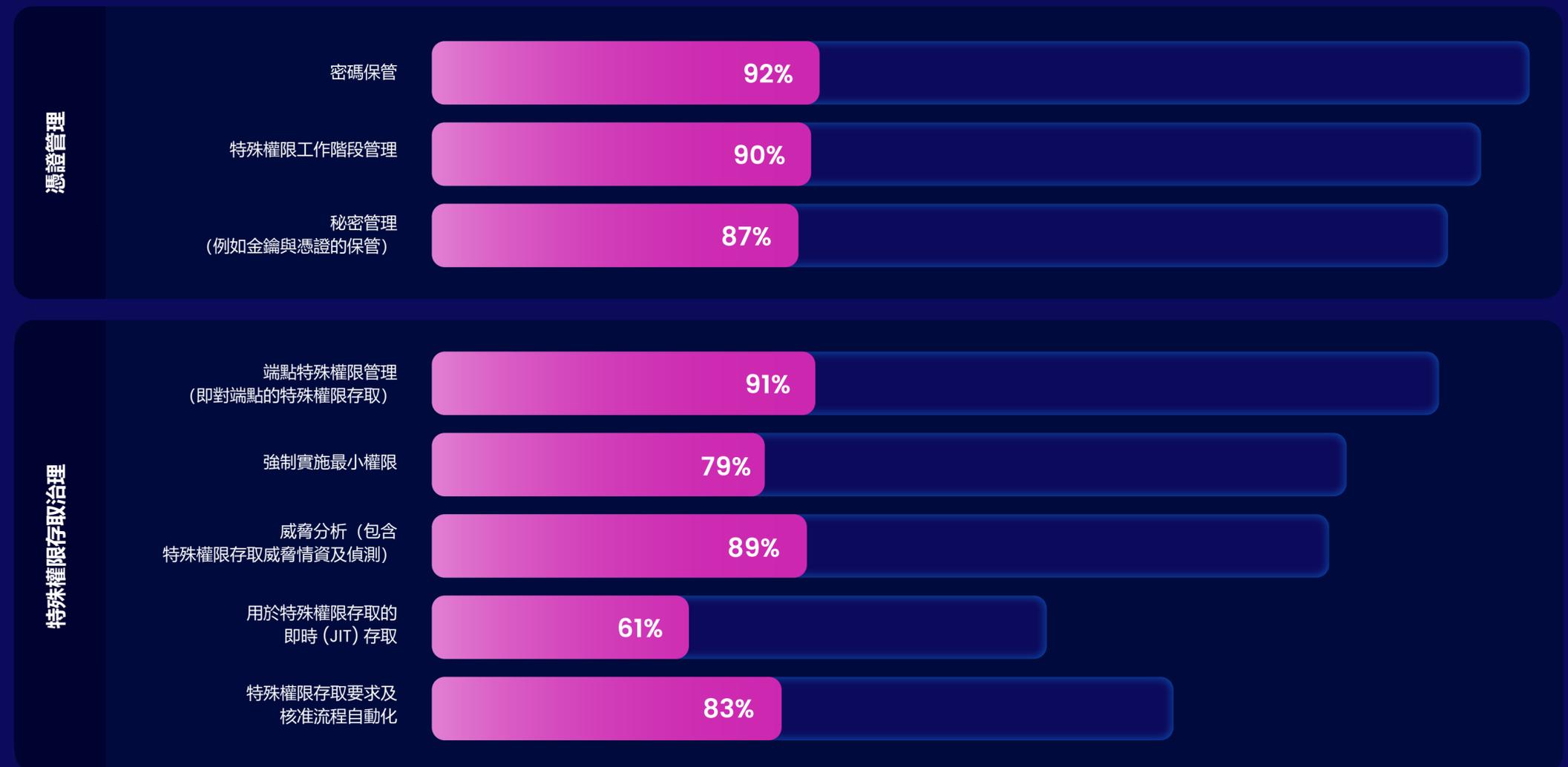


第 3 層次的組織在採用特殊權限存取治理功能方面，較第 1 及第 2 層次組織高出約 50%

投資不僅限於憑證金庫及工作階段管理的解決方案，組織便能簡化存取核准與要求，同時強化特殊權限帳戶的威脅分析。

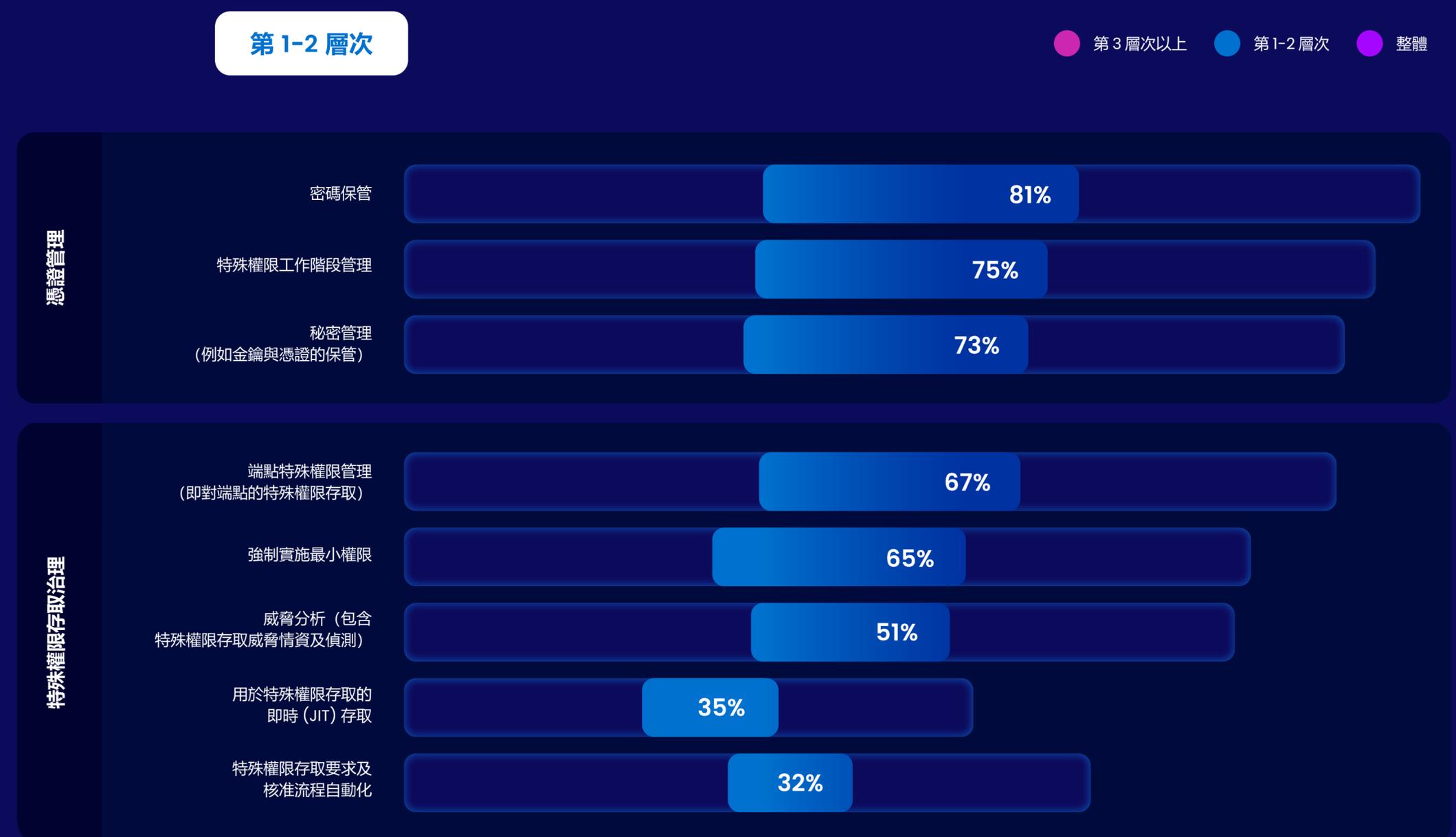
第 3 層次以上

● 第 3 層次以上 ● 第 1-2 層次 ● 整體



第 3 層次的組織在採用特殊權限存取治理功能方面，較第 1 及第 2 層次組織高出約 50%

投資不僅限於憑證金庫及工作階段管理的解決方案，組織便能簡化存取核准與要求，同時強化特殊權限帳戶的威脅分析。



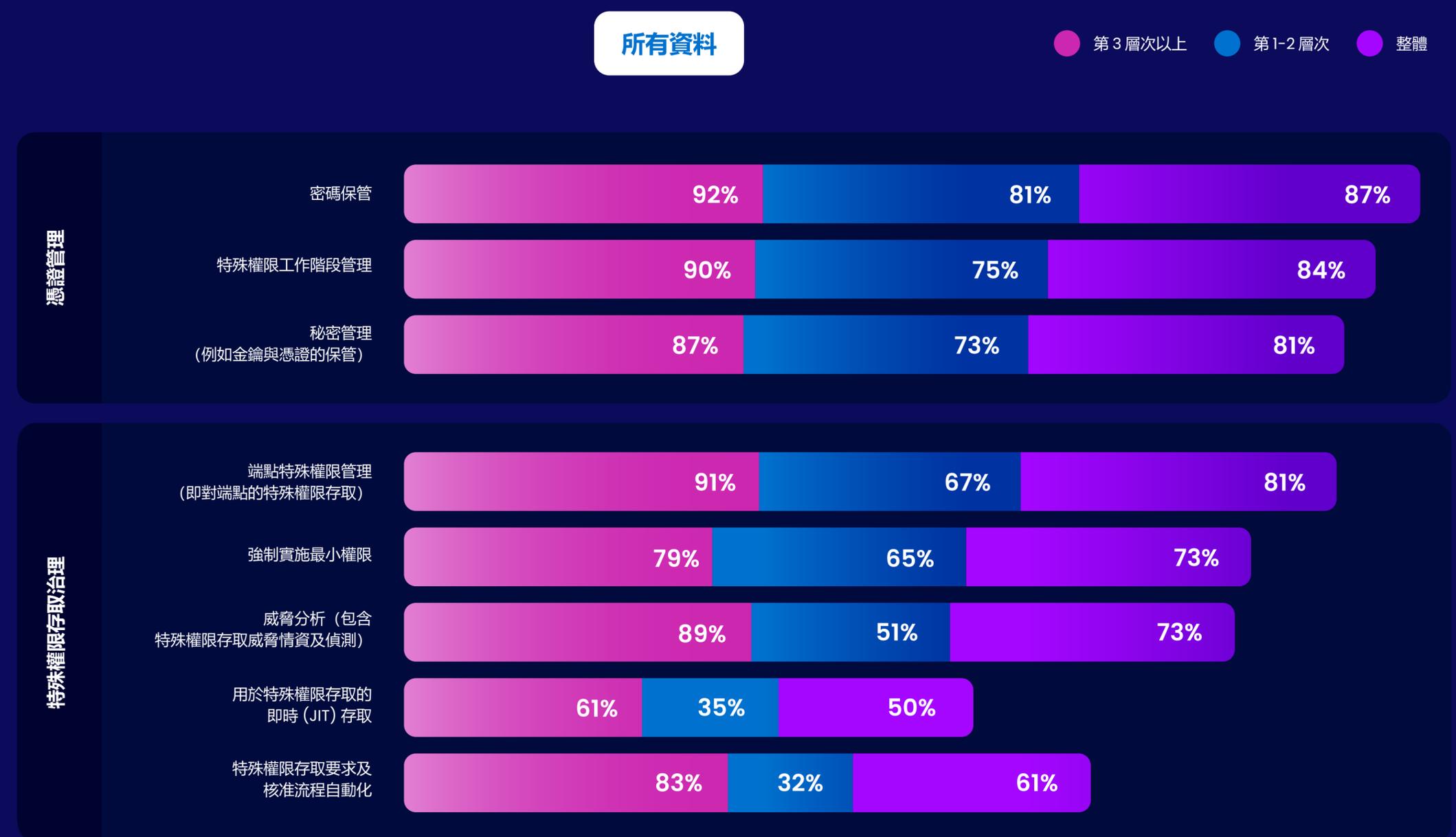
第 3 層次的組織在採用特殊權限存取治理功能方面，較第 1 及第 2 層次組織高出約 50%

投資不僅限於憑證金庫及工作階段管理的解決方案，組織便能簡化存取核准與要求，同時強化特殊權限帳戶的威脅分析。



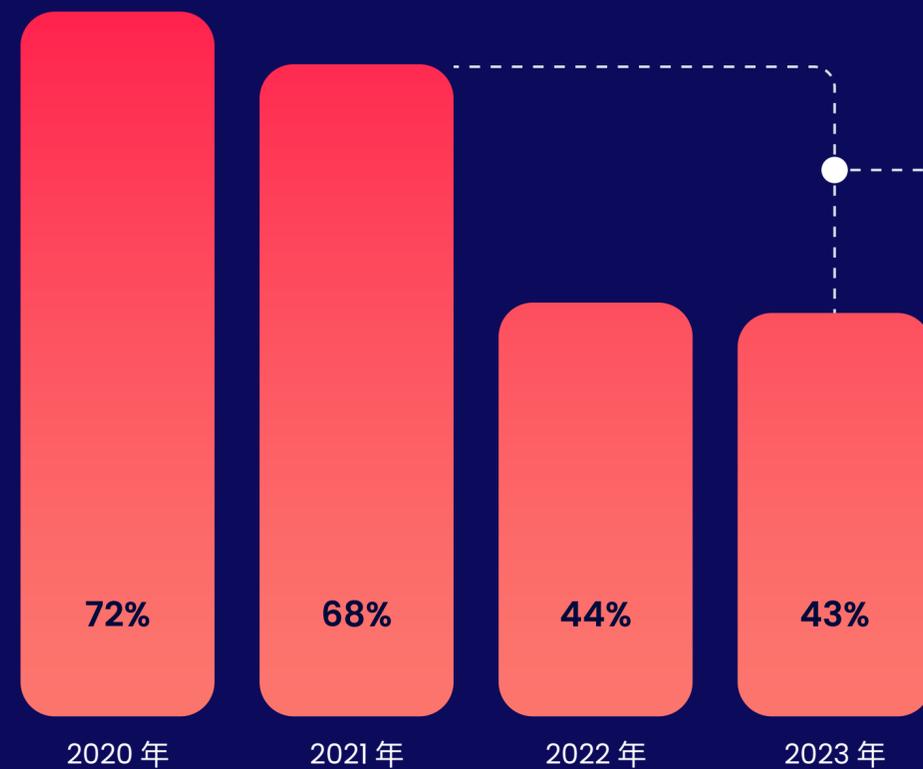
第 3 層次的組織在採用特殊權限存取治理功能方面，較第 1 及第 2 層次組織高出約 50%

投資不僅限於憑證金庫及工作階段管理的解決方案，組織便能簡化存取核准與要求，同時強化特殊權限帳戶的威脅分析。



隨著網路保險公司開發出更成熟的網路風險管理評估方法， 網路保險費用也隨之上漲

網路保險公司已降低其損失比率，且在風險評估與管理方面
變得更加成熟.....



獨立網路保險損失比率，作為理賠支付的保險費用比例



40%

網路保險公司損失的降低，顯示其在
網路風險管理方面有所改善

.....並上調保險費用來配合加劇的風險
概況



77%

的組織報告過去 3 年保險費用有所
上漲



“

保險公司如今更加深入瞭解一家公司擁有哪些安全控制措施.....他們可能會提供折扣來激勵您實施新的安全控制措施。

大型經紀公司中的網路保險專業人員

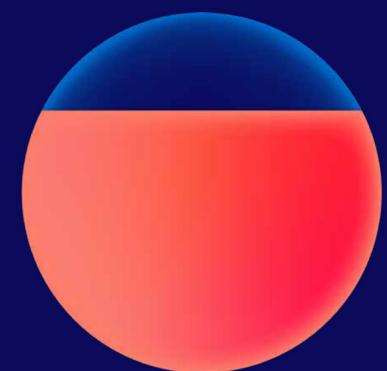
網路保險客戶反映，身分安全功能對保險評估影響最為顯著

影響網路保險評估的主要網路安全功能，選擇該功能為最具影響力的受訪者百分比



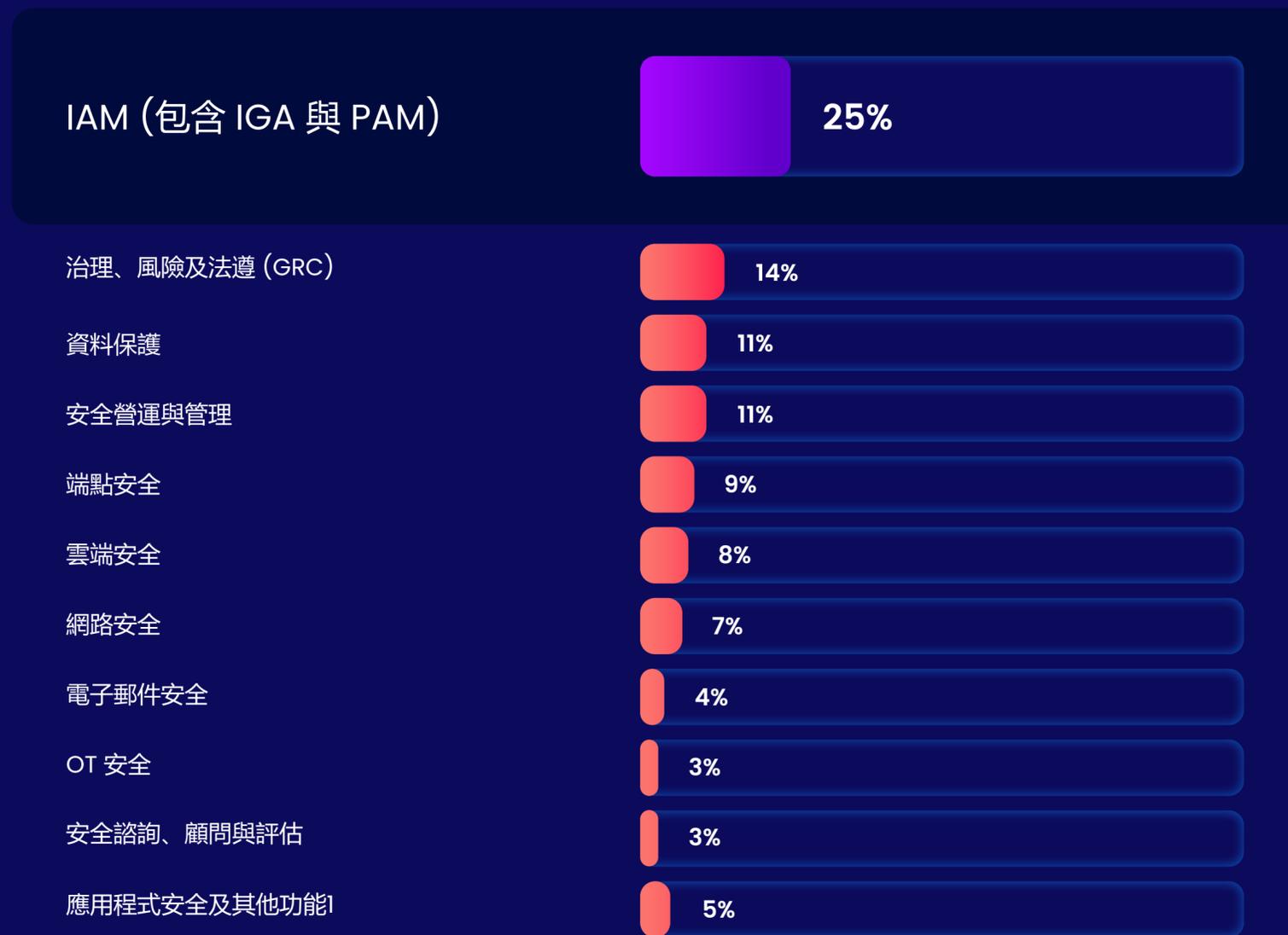
25%

的受訪者認為 IAM 是網路保險評估中最關鍵的要素，其佔比最高



73%

的網路保險客戶認為 IAM 功能是影響保險評估的前三大功能



包含 Web 安全及 MSSP / 外包服務

自 2010 年以來，與身分相關的規章在各地區及產業中已增加七倍之多

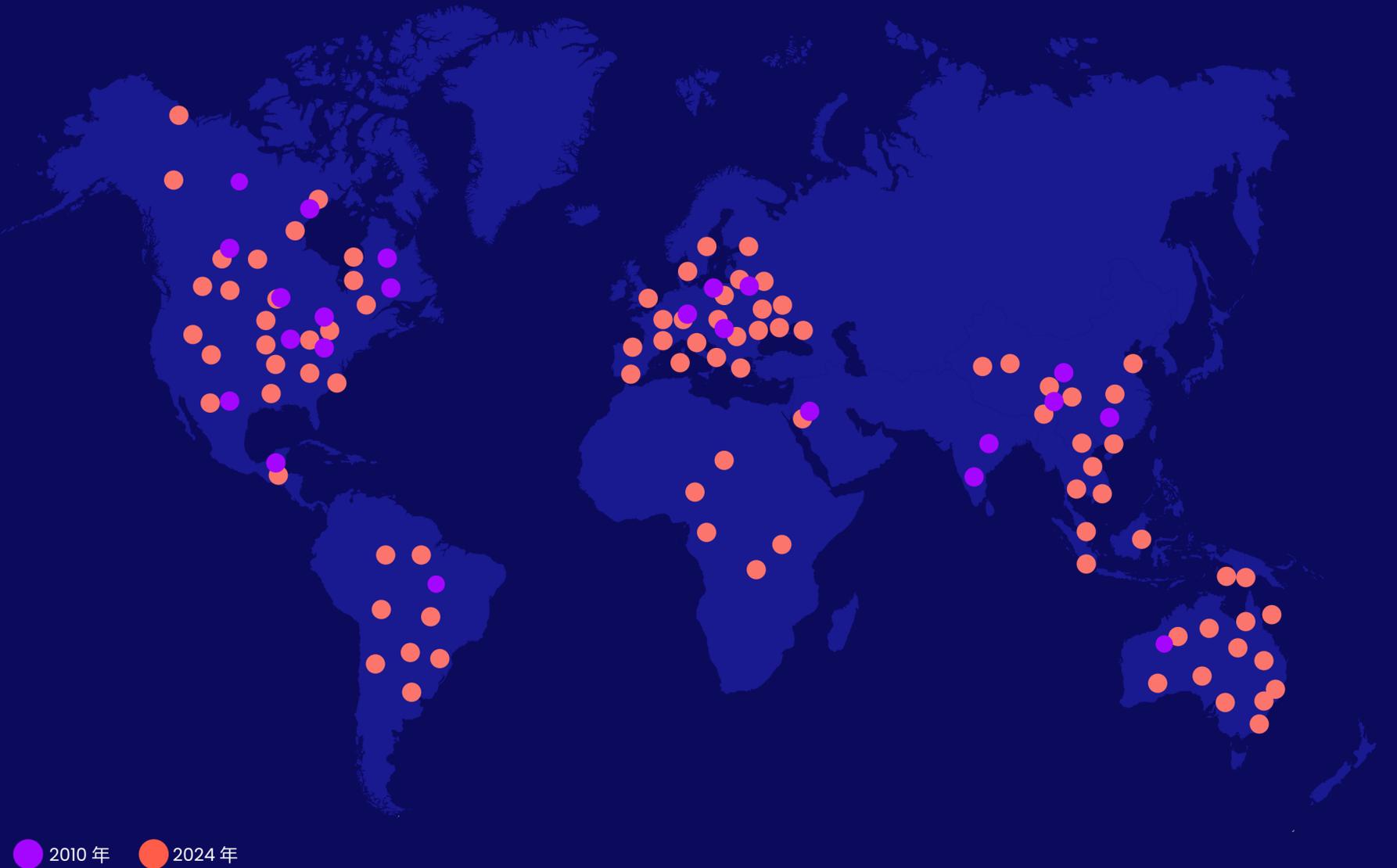
全部

增加 5 倍以上

就金融與醫療保健以外產業的規章而言

增加 13 倍以上

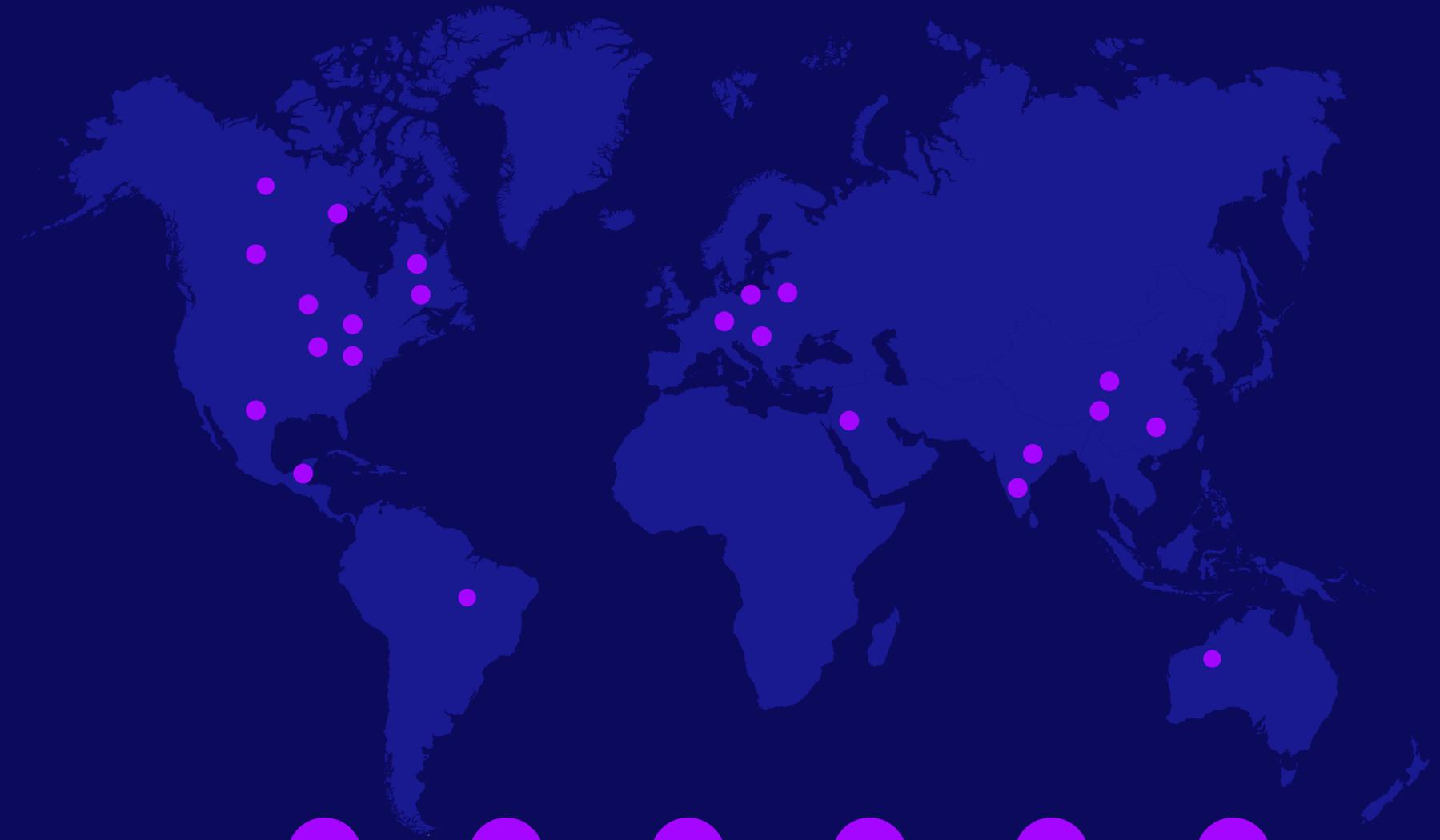
就北美、亞太地區及歐洲以外地區的規章而言



● 2010 年 ● 2024 年

自 2010 年以來，與身分相關的規章在各地區及產業中已增加七倍之多

2010 年



約有 25

項總體規章與框架，著重於成熟地區及特定產業
(2010 年)

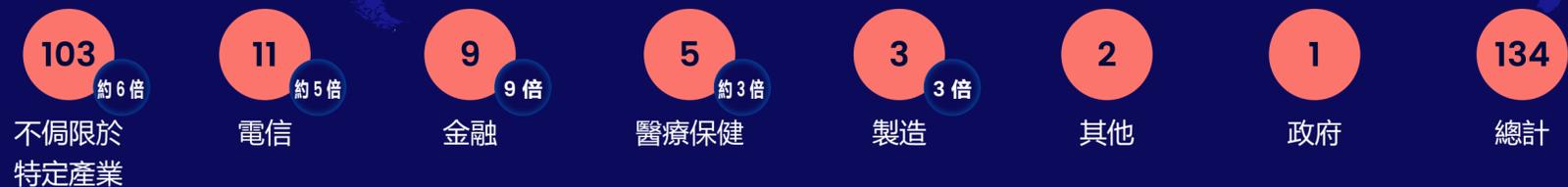
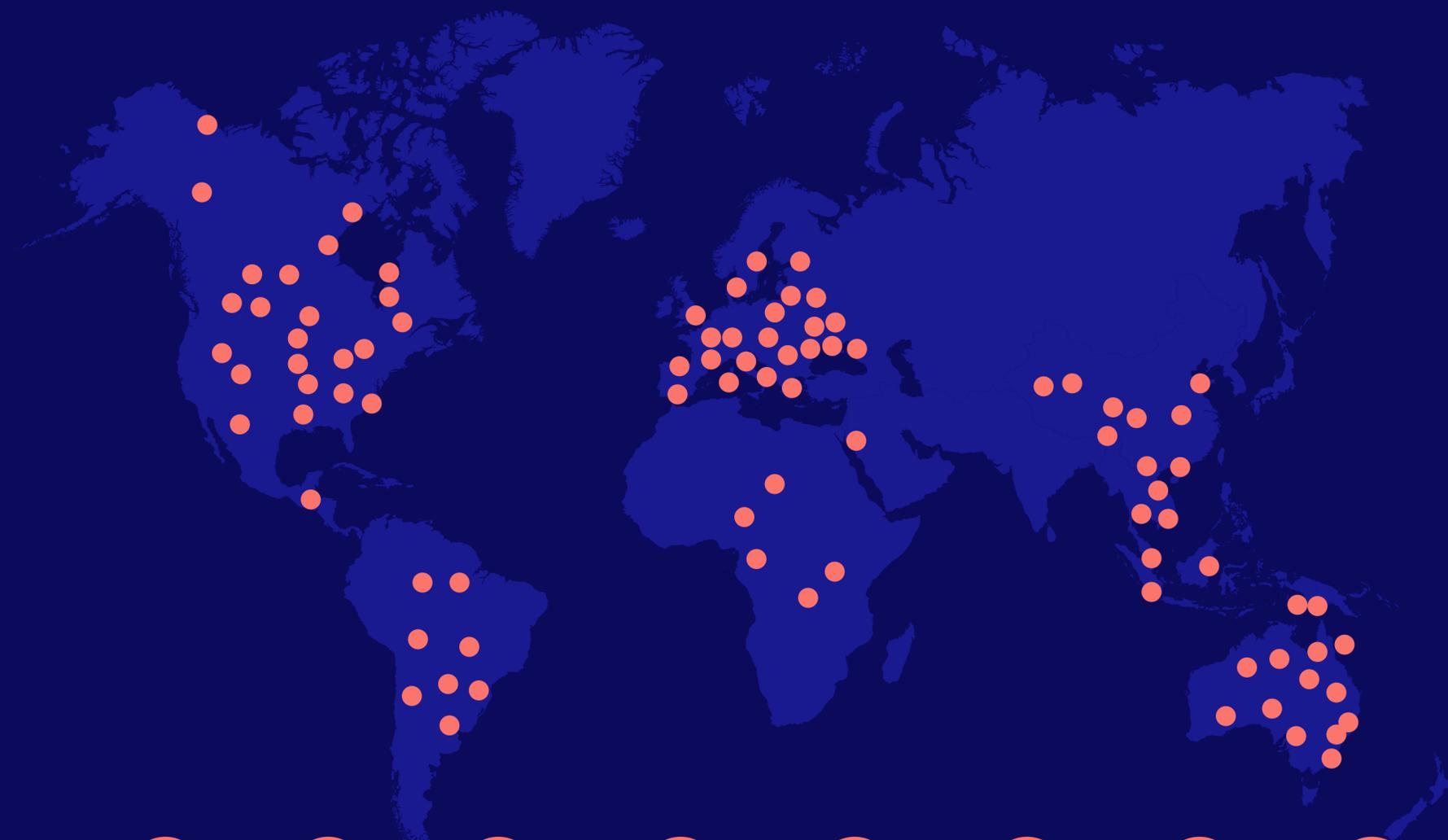


自 2010 年以來，與身分相關的規章在各地區及產業中已增加七倍之多

2024 年

約有 135

項規章與框架，在所有地區及產業均有顯著增長
(2024 年)



第 4 章

位居領先的組織如何 改變趨勢。

組織個案研究

世界各行各業首屈一指的組織正投資於身分安全來改變網路安全價值趨勢，從而在法遵、營運效率、使用者生產力及安全方面獲得超乎尋常的回報。



目標： 降低網路風險並提高生產力

BNP Paribas Bank Polska 將手動 IAM 任務大規模自動化來提升生產力。

經歷一系列併購後，該銀行需要管理 10,000 名使用者及約 1,000 個應用程式，但採用的卻是各自獨立的 IAM 計畫。若無自動化，IT 團隊便無法應對龐大的使用者要求及 IAM 任務。如今自動化後，所有驗證活動僅需由兩名員工管理，且每名員工僅需分配約自身 15% 的工作時間來處理相關事宜。



4 萬

每月執行的自動化身分任務數量



90%

自動執行的存取要求百分比



4 千

每月自動重設及變更密碼的次數

目標： 生產力

一家業界領先的製藥公司，擁有 72,000 名員工，其透過自動化 IAM 任務來強化生產力與效率。

該公司希望擁有可規模化且基於雲端的系統，來取代過時的內部部署身分解決方案（需要大量手動維護作業）。全新且基於雲端的系統上線後，該公司得以簡化規章遵循事宜，並顯著減少存取審查及等待存取所需的時間。



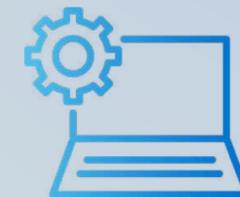
40%

在存取審查方面
所減少的時間



20%

在等待存取方面所
減少的時間



30%

為 IT 營運人員
減少的手動作
業負擔量



目標： 提升商業價值

Absa 是一家泛非金融機構，擁有超過 35,000 名員工，其透過精簡登錄流程與第三方身分管理來降低成本。

為遵循 GDPR 與 POPIA，該銀行部署了基於 AI 的風險管理工具，具備即時佈建及第三方身分標準化驗證功能。這種基於風險的存取模式降低了營運開銷，並簡化了承包商與非員工的身分治理。



\$300

每個身分登錄所節省的金額



15

為第三方身分登錄所縮短的天數



1.2萬

具備安全身分的非員工人數



目標： 降低網路風險

Currys 是一家總部位於英國的科技零售商，擁有超過 800 家門市，其透過強化身分治理及自動化身分安全來降低風險。

Currys 是一家總部位於英國的科技零售商，擁有超過 800 家門市，其透過強化身分治理及自動化身分安全來降低風險。該公司先前的方法是使用基於 Excel 的手動流程，加上員工經常變動，從而導致過度佈建與法遵風險。現在自動化能夠提供完整的稽核線索，將法遵挑戰及未執行權限最小化，同時增強整體的安全態勢。



3 倍

為約 6,000 個帳戶
設定適當特殊權限
而降低的風險



210

每年節省的手動作
業時數



2.4 萬

受管身分

Aboitiz 這家全球科技集團在 24 個月的時間內，憑藉「鉅變」計畫直接從第 1 層次躍升至第 3 層次以上

將游標暫留在各區塊上方來查看採取的行動

- 第 1 層次 (2020 年)
- 第 3 層次以上 (2022 年)



“

我們的起點是零，但這也給了我們透過科技實現層次躍升的機會……我們決定將時間與精力投入到組織最寶貴的資產：身分。

Aboitiz Equity Ventures 資安長 (CISO)

aboitiz

第 5 章

邁向下個層次的道路。

邁向下個層次的道路



**深入瞭解身分安全成熟度
及貴組織的層次。**