CHANGING
全景軟體股份有限公司
CHANGING Information Technology Inc.

股票代號：8272

全景軟體法人說明會

2025.09.11

免責聲明

- 本簡報及同時發佈之相關訊息所提及之預測性資訊，包括營運展望、財務及業務狀況等內容，係全景軟體股份有限公司（本公司）基於內部資料及外部整體經濟發展現況所得之資訊。

- 本公司未來實際所可能產生的營運結果、財務狀況與業務成果，可能與預測性資訊有所差異。其原因可能來自各種因素，包括但不限於市場需求、價格波動、競爭態勢、各種政策法令與金融經濟現況之改變，以及其他本公司無法掌控之風險等因素。

- 本簡報中所提供之資訊，係反應本公司截至目前為止對於未來的看法，並未明示或暗示地表達或保證其具有正確性、完整性或可靠性。對於這些看法，未來若有變更或調整時，本公司並不負有更新或修正之責任。

大綱

1. 公司概況
2. 市場機會與趨勢
3. 營運及財務概況
4. 未來策略與發展方向

公司概況

成立於1998，
隸屬緯創集團，
深耕資安與認證技術

核心價值

人、事、物 安全認證
與零信任架構實踐

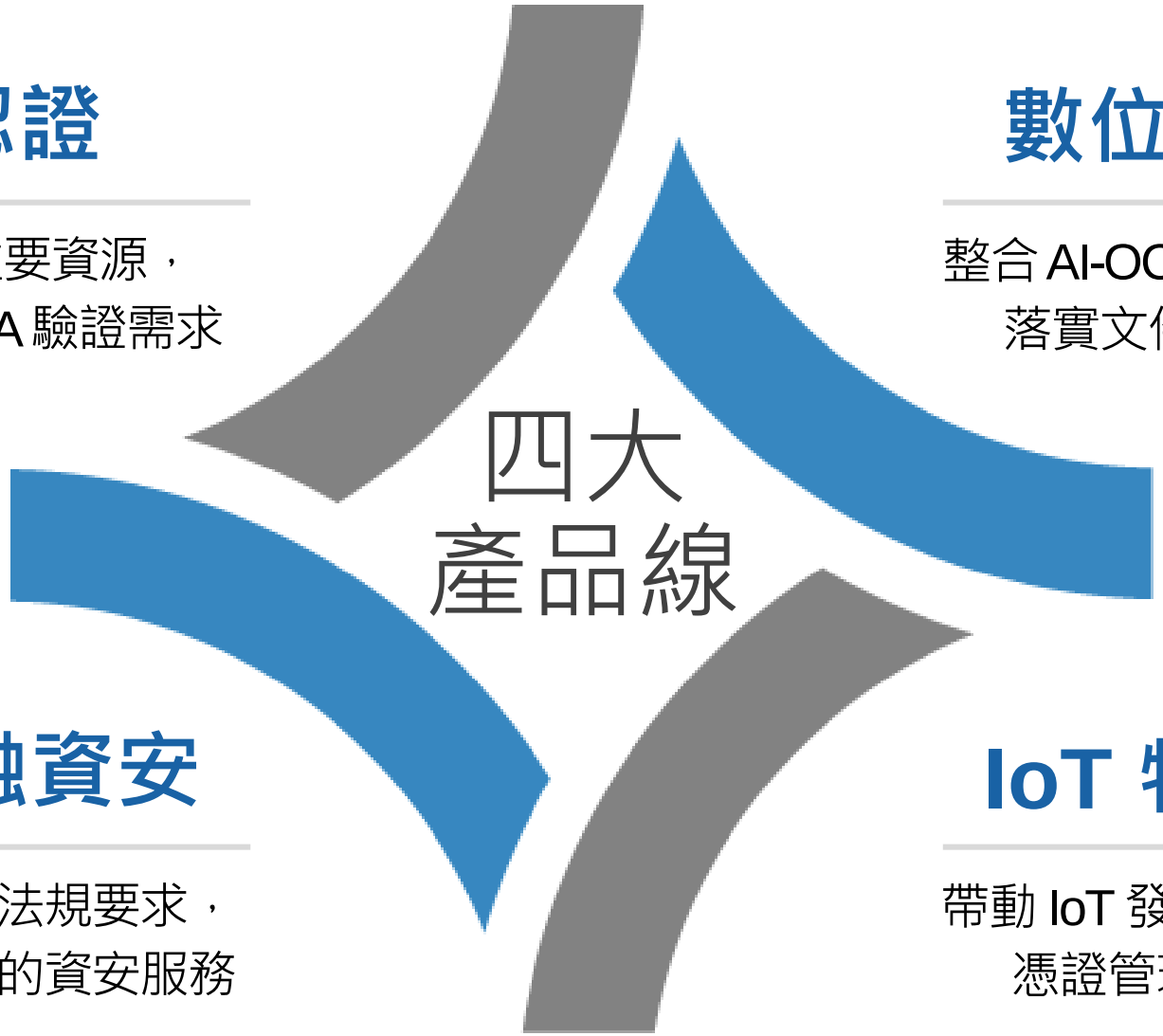
全景軟體專注於人、事、物安全認證

安全認證

無邊界保護重要資源，
完備 3 階段 ZTA 驗證需求

數位轉型應用

整合 AI-OCR、影像處理技術，
落實文件全生命週期管理



科技金融資安

滿足金融及政府法規要求，
提供高安全等級的資安服務

IoT 物聯網安全

帶動 IoT 發展，整合安全信任、
憑證管理與生態系連結

技術獲肯定，服務持續創新

預計 2025 年通過資安院
ZTA 信任推斷認證

安全認證方案 FIDO 及
OATH 認證

資安院 ZTA 零信任網路
身分鑑別/設備鑑別認證

ISO27001 認證，
由內到外推展資訊安全

fido ALLIANCE

oath CERTIFIED

afaq ISO/IEC 27001 Information Security AFNOR CERTIFICATION

數位發展部 數位產業署 Administration for Digital Industries, moda
2025年電子簽章能量登錄
2024年資服能量登錄

ZERO TRUST 政府零信任網路
身分鑑別認證

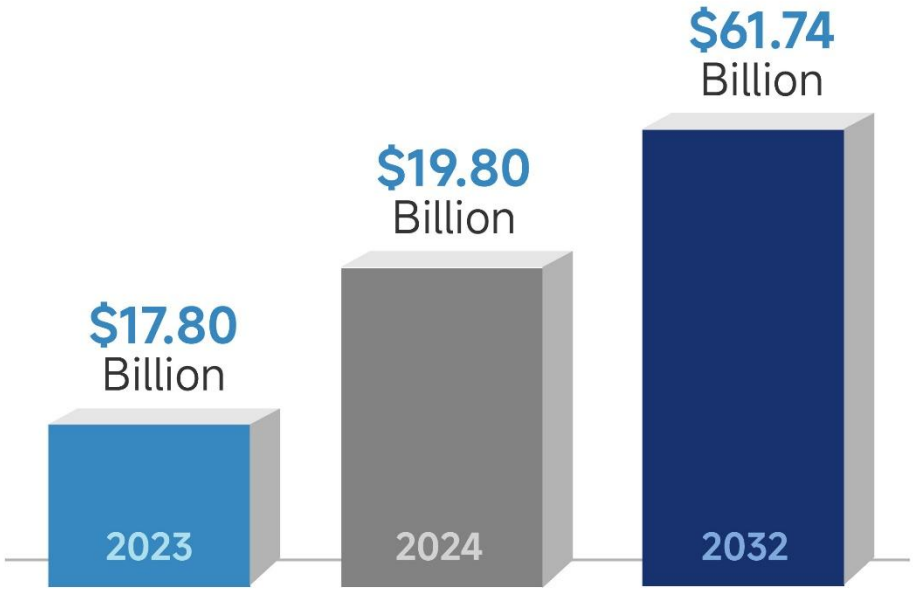
通過 政府零信任架構
設備鑑別認證

市場機會與趨勢

安全認證及管理市場在全球呈現快速增長趨勢

全球 IAM 市場規模
(Fortune Business Insights)

2024年 198億 美元 → 2032年 617.4億 美元，CAGR 15.3% 。



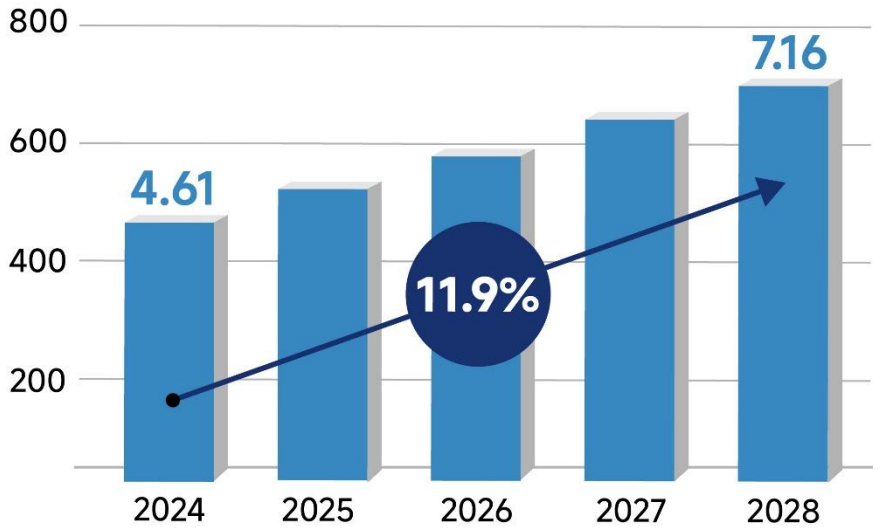
單位: 美元

Identity and Access Management Market to grow at 15.3% CAGR by 2024-2032

資料來源：Fortune Business Insights

台灣資安產品市場規模 (IDC)

2024年 4.61億 美元→ 2028年 7.16億 美元，CAGR 11.9%，其中，成長動能以軟體解決方案為主（資安軟體 CAGR 高達13.3%)。



單位: 億美元

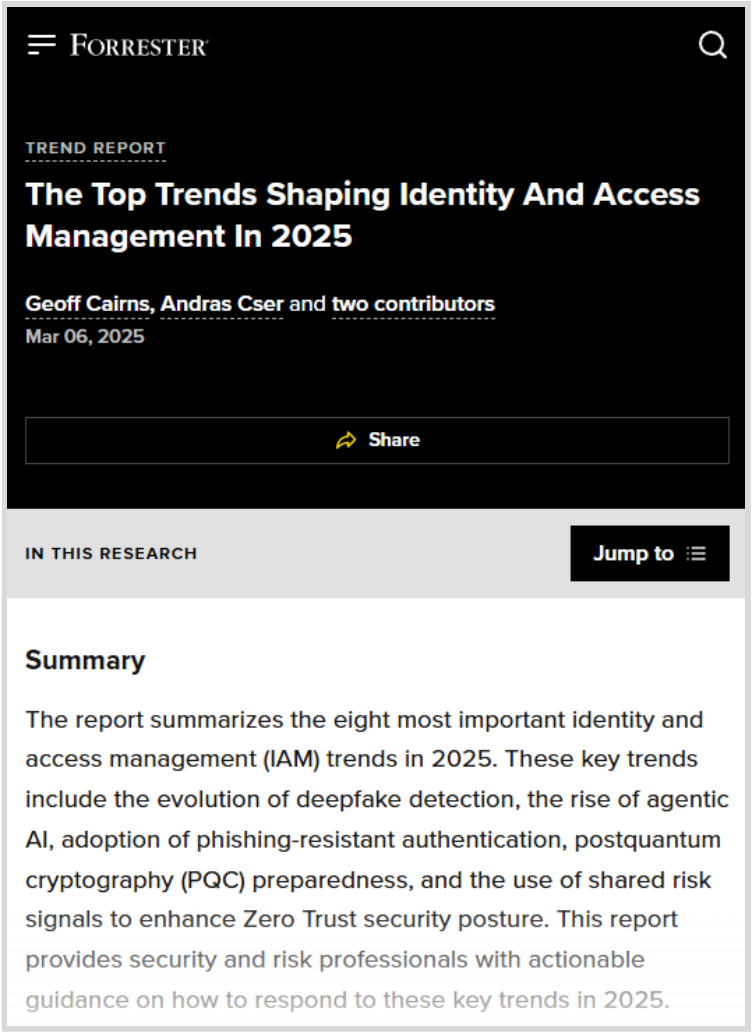
資料來源：IDC

Forrester 報告: 深偽風險與代理式 AI 攻擊為 IAM 面臨的未來挑戰

Forrester《2025 年 IAM 領域趨勢》報告 (2025 年 3 月) 總結當年度身分與存取管理領域的八大重點發展，包括：

- 深偽 (Deepfake) 身分欺騙的偵測依然困難
- 零信任架構中自主智能代理 (Agentic AI) 的興起
- 員工端採用抗網釣的強健 MFA 驟增
- 機器身分管理需求達到臨界點
- 身分驗證與身分核實成為安全核心
- 去中心化數位身分錢包生態持續碎片化
- 後量子密碼學開始影響 IAM
- 安全領域開始透過 Shared Signals 共享跨組織威脅訊息來強化身分保護

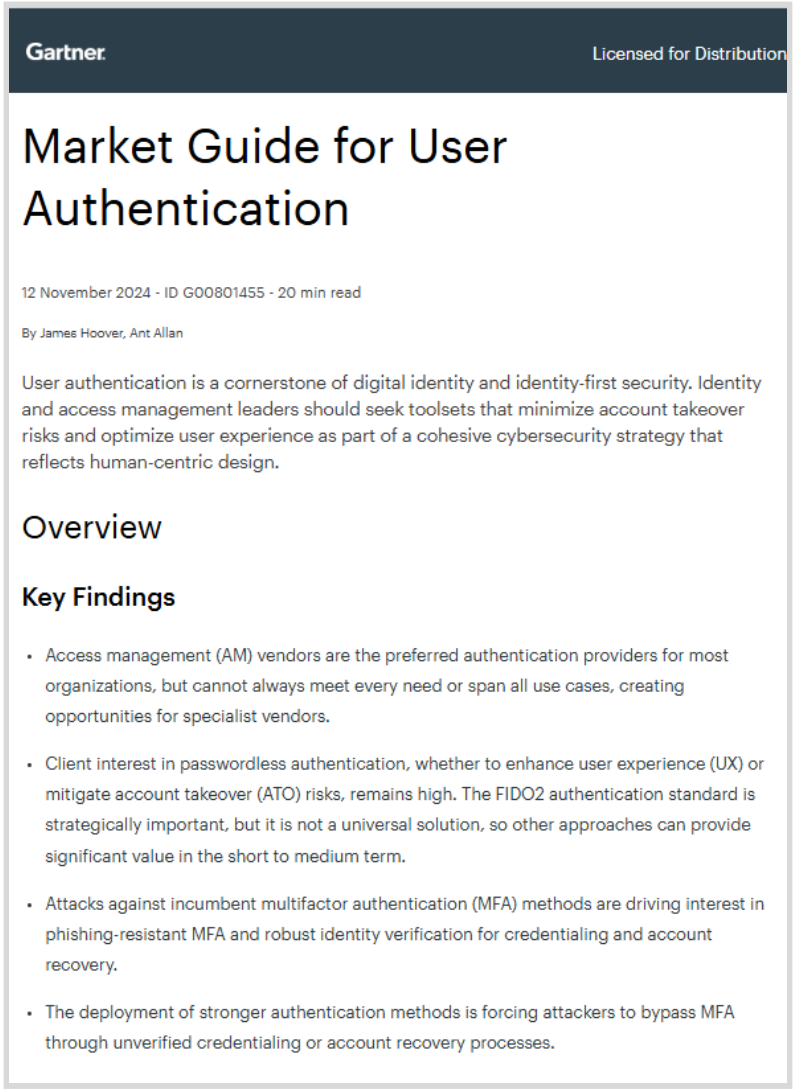
資料來源：[The Top Trends Shaping Identity And Access Management In 2025 / Forrester]



Gartner報告: 預測2027年，90%企業將全面使用IAM內建的MFA

Gartner《2025 用戶認證市場指南》聚焦身分驗證技術的發展趨勢，報告中預測到 2027 年 90% 的企業將透過存取管理工具的原生功能全面滿足遠端和雲端的 MFA 需求，並且超過 90% 採用實體載具的 MFA 驗證交易，將基於 FIDO 無密碼協議(例如 Passkey)由存取管理工具原生支援。

資料來源：2025 Market Guide for User Authentication / Gartner



Gartner Licensed for Distribution

Market Guide for User Authentication

12 November 2024 - ID G00801455 - 20 min read

By James Hoover, Ant Allan

User authentication is a cornerstone of digital identity and identity-first security. Identity and access management leaders should seek toolsets that minimize account takeover risks and optimize user experience as part of a cohesive cybersecurity strategy that reflects human-centric design.

Overview

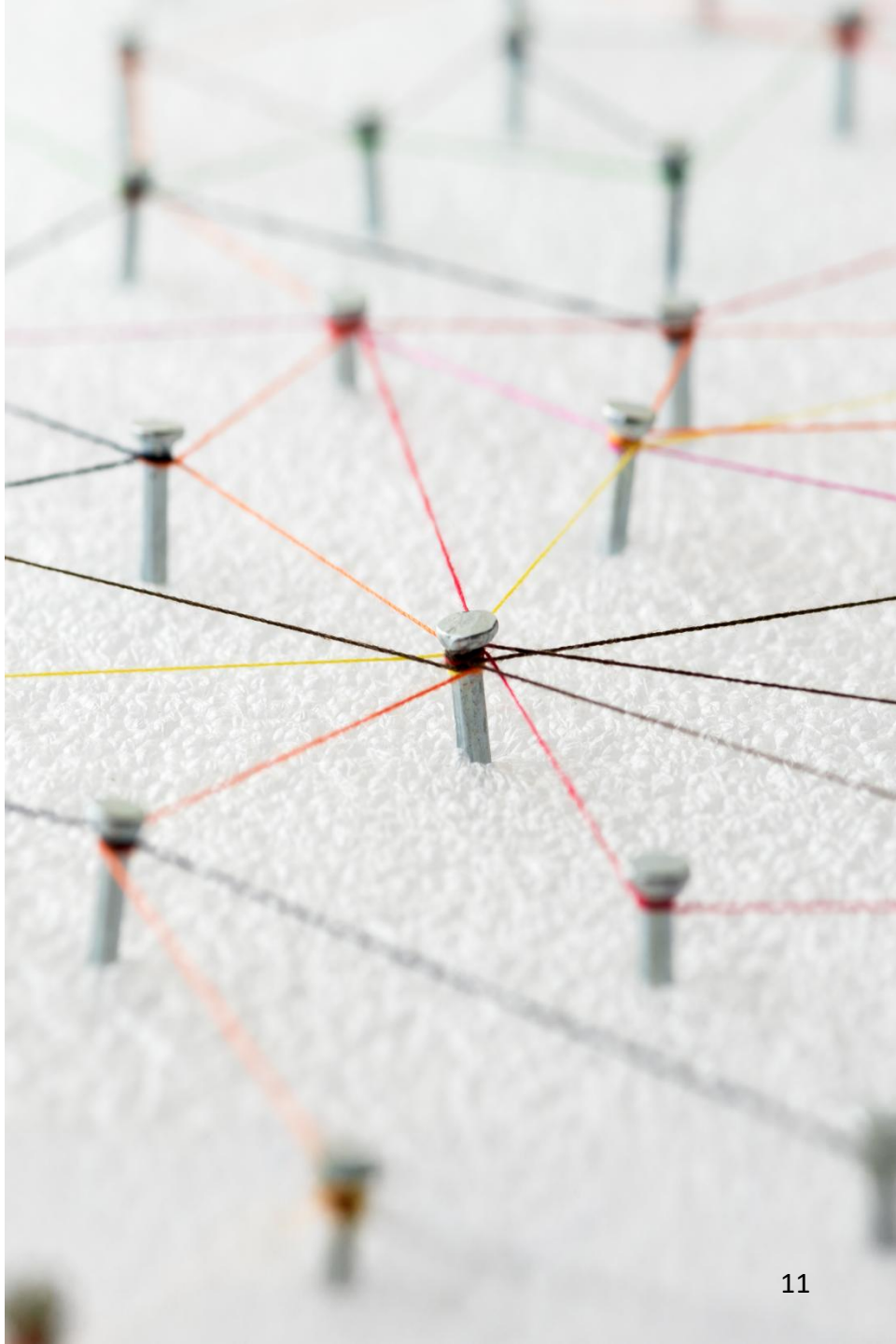
Key Findings

- Access management (AM) vendors are the preferred authentication providers for most organizations, but cannot always meet every need or span all use cases, creating opportunities for specialist vendors.
- Client interest in passwordless authentication, whether to enhance user experience (UX) or mitigate account takeover (ATO) risks, remains high. The FIDO2 authentication standard is strategically important, but it is not a universal solution, so other approaches can provide significant value in the short to medium term.
- Attacks against incumbent multifactor authentication (MFA) methods are driving interest in phishing-resistant MFA and robust identity verification for credentialing and account recovery.
- The deployment of stronger authentication methods is forcing attackers to bypass MFA through unverified credentialing or account recovery processes.

法規帶動 IoT 產業進程

無論是歐盟的CRA/NIS2，或美國的NIST IoT 框架與聯邦法案，以及國際標準如 IEC 62443 工控資安、ISO/SAE 2143 汽車網路安全等，皆指向同一趨勢：

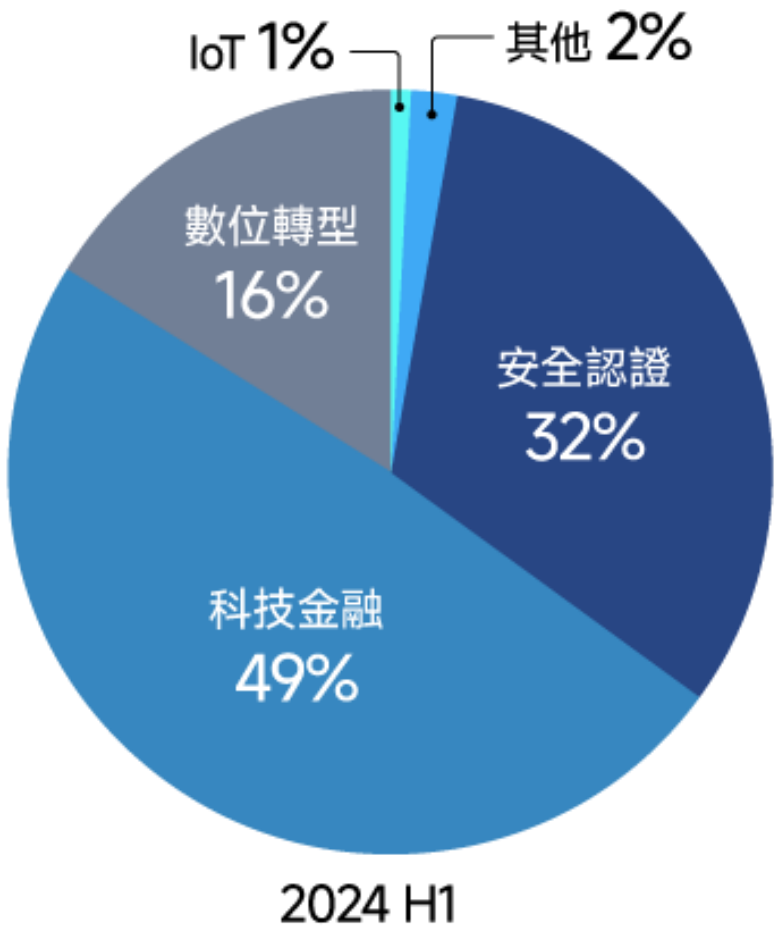
資安合規已成為供應鏈的敲門磚

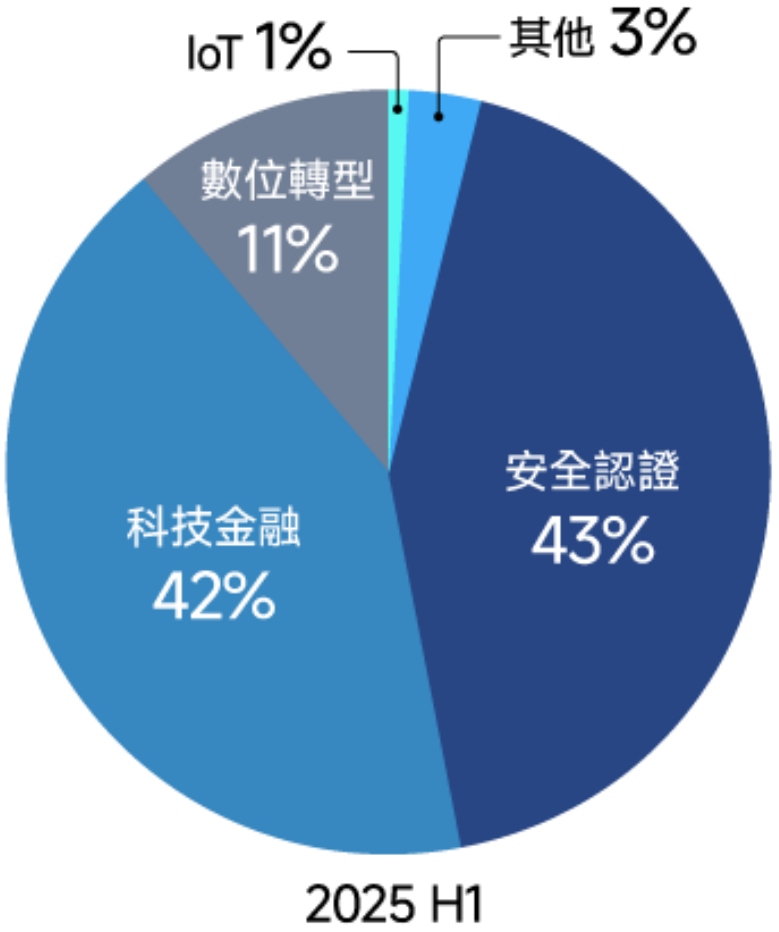


營運及財務概況

四大產品線營收佔比

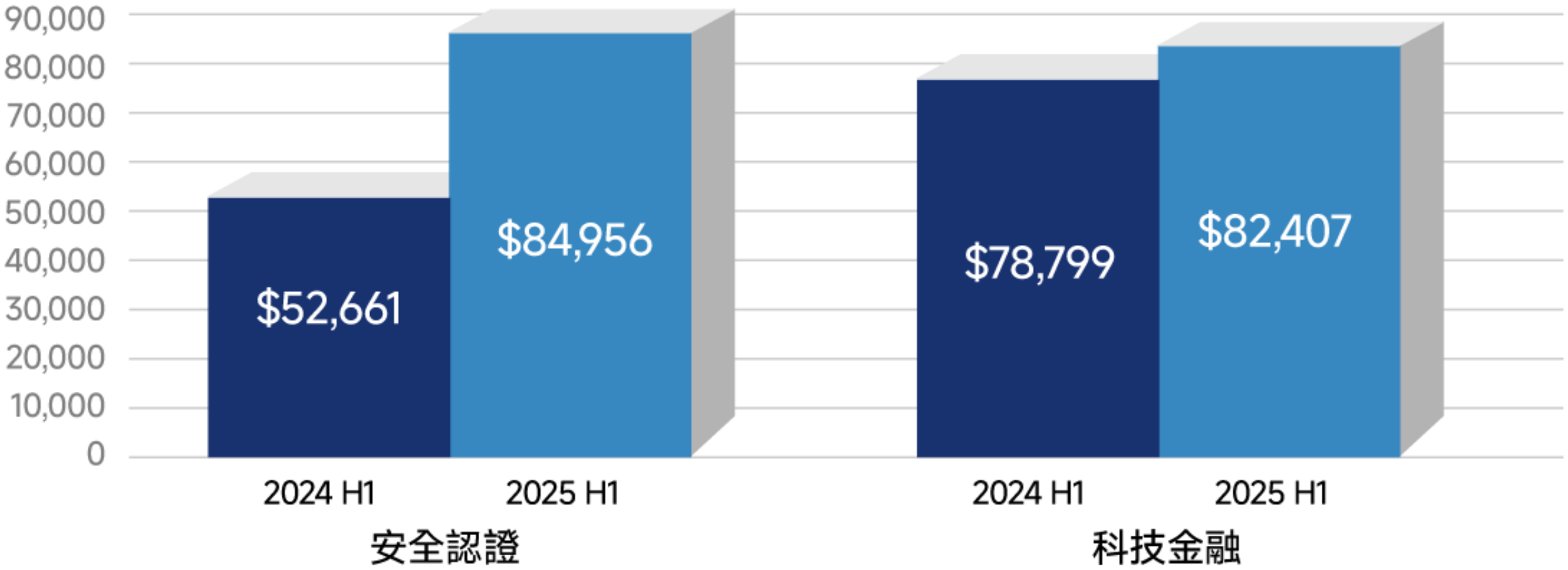
安全認證及零信任專案穩定成長





安全證認營收年增61%；科技金融營收年增5%

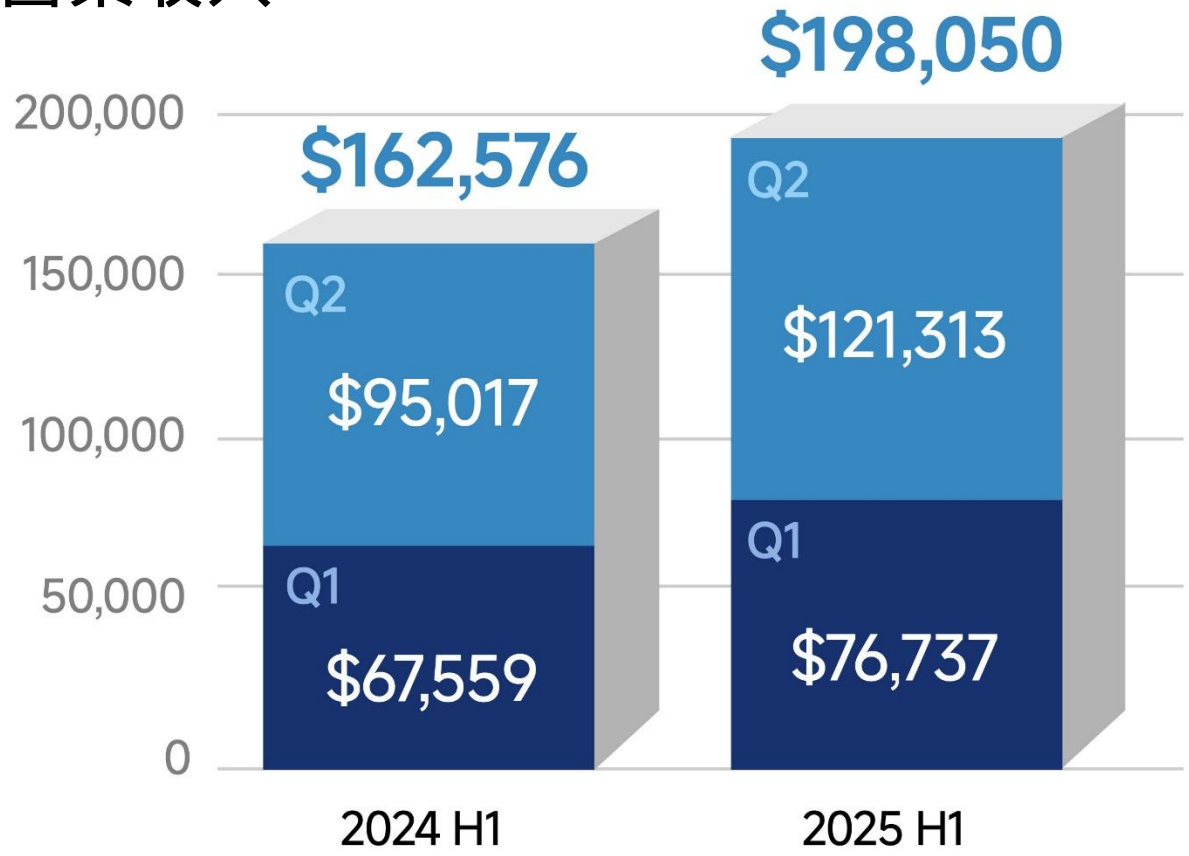
營業收入



單位：千元

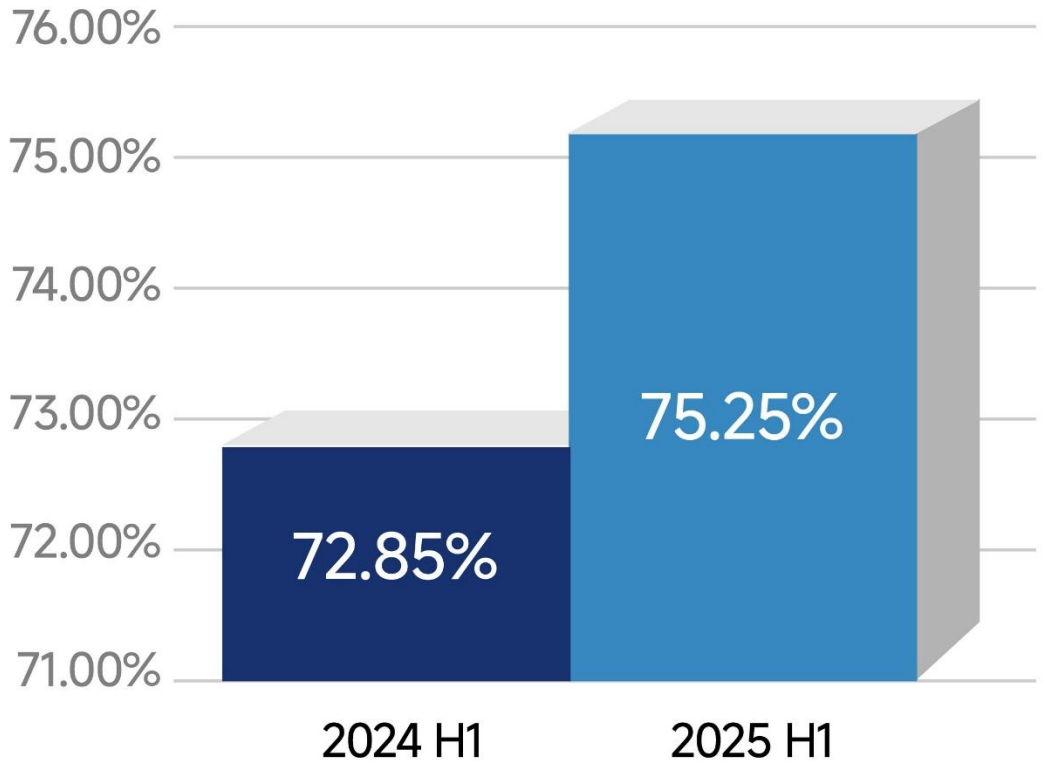
營收年增21.8%；毛利率年增3.3%

營業收入



單位：千元

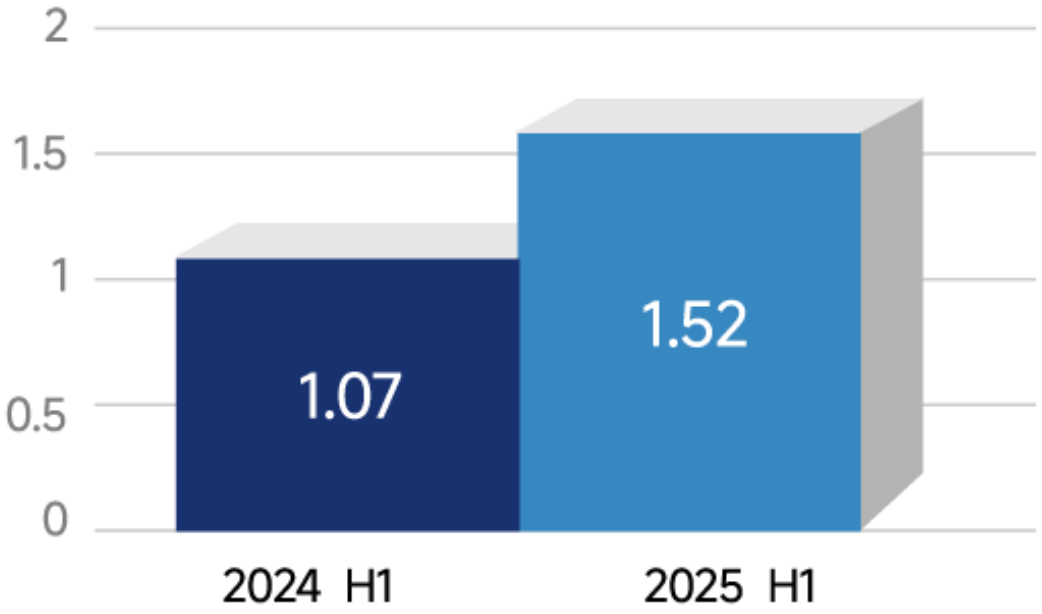
毛利率



單位：%

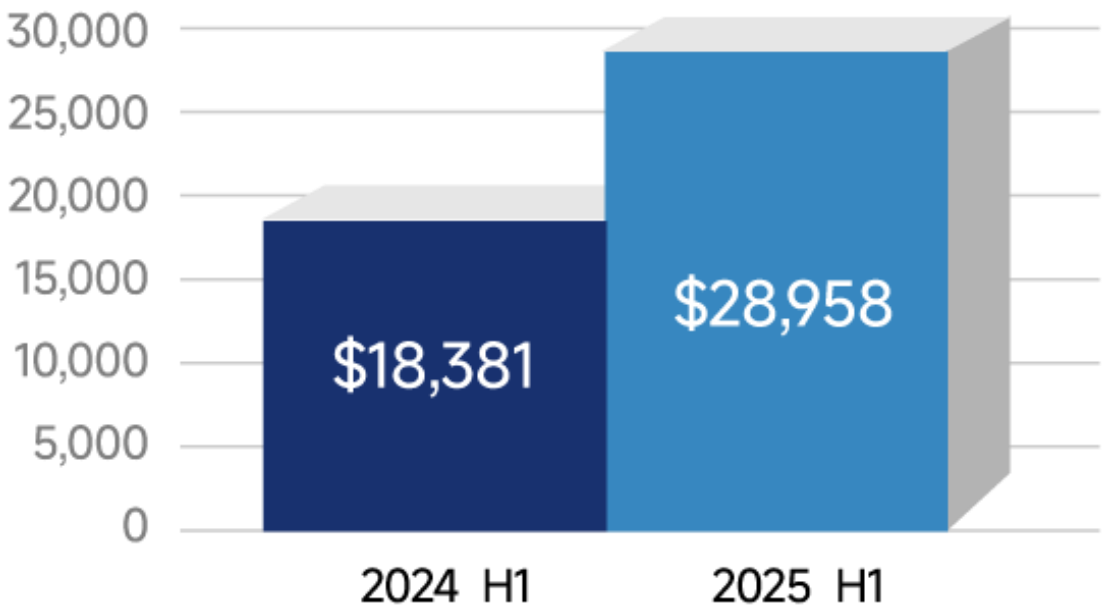
每股盈餘年增42.1%；獲利年增57.5%

EPS



單位：元

淨利



單位：千元

未來策略與發展方向

未來策略與發展方向

- 零信任專案長期深耕
- 安全認證 SaaS 服務
- IoT 安全串連產業生態系
- 擴展研發投入

零信任專案長期深耕

台灣金管會於2024年7月發布「金融業導入零信任架構參考指引」，不斷耕耘金融業者

政府機關深廣同步推展

- 中央政府持續深化，推動零信任進入第 2、3 階段落實。
- 導入版圖擴展至地方政府與國防等單位，拓展更多應用場域。

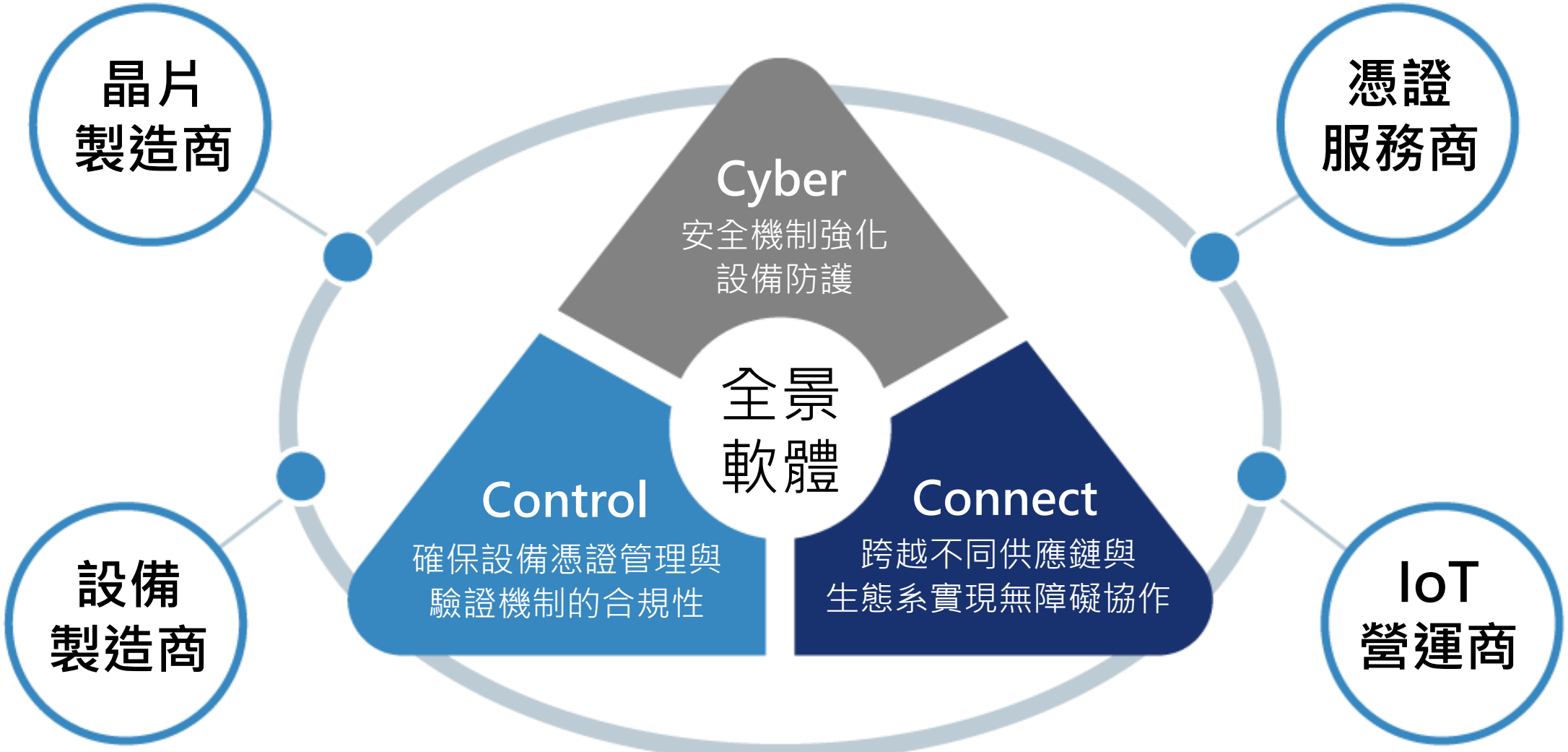
安全認證 SaaS 服務

聚焦中小與成長型企業，
需求核心在雲端彈性與快速導入

全雲架構上線應用，
採 K8s 流程自動化、彈性擴充

中長期目標，發展雲地
合一 IDExpert Hybrid 架構

IoT 安全推動產業生態系的連結



IoT 安全發展的完整方案

因應供應鏈安全需求

HSM + KMS

硬體安全模組與金鑰管理系統

金鑰生成、存放與管理全程防護

由人的身分驗證延伸至設備

DAC + CLM

裝置身分憑證與生命週期管理

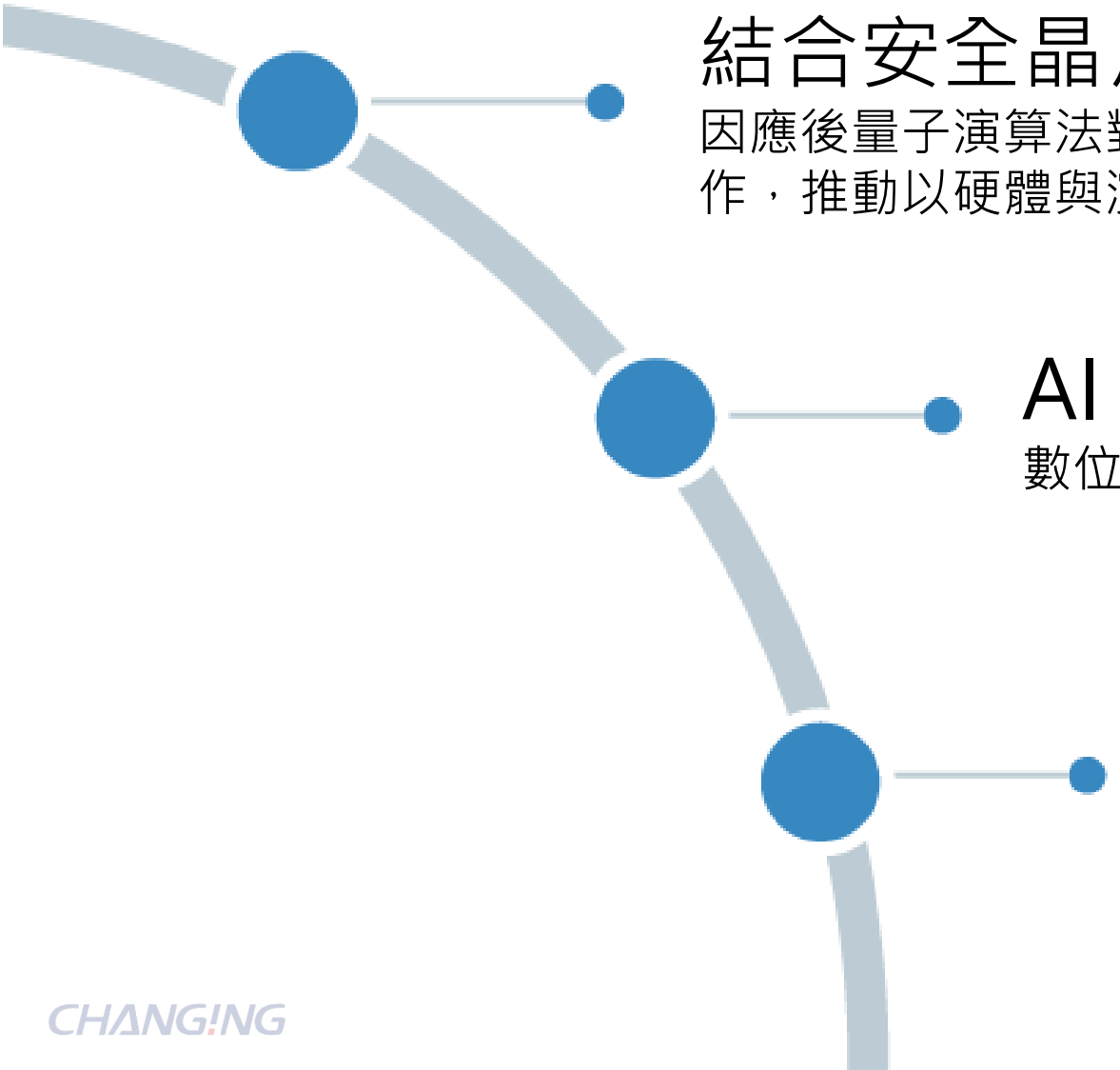
設備身分的建立與全階段管理

應對智慧家庭標準化趨勢

Matter 通訊模組

提供跨品牌互通與安全連線基礎

擴展研發投入：量子資安、AI 自動化、ESG 加值



結合安全晶片，打造裝置原生的防護機制

因應後量子演算法對運算與儲存的挑戰，全景軟體與安全晶片廠商合作，推動以硬體與演算法深度整合的資安架構。

AI 自動化

數位資料進件及資料分析服務導入AI應用。

ESG 加值

- 數位轉型方案協助企業落實 ESG，將節能減碳成果轉化為可量化數據，直接納入永續報告。
- IoT 安全提供智慧能源的安全連線基礎，推動智慧電網發展，進而實現綠色供應鏈。

CHANGING

THANK YOU