出國報告（出國類別：開會）

參加2024年 Gartner 安全與風險管理峰會
（Gartner Security & Risk Management Summit）
出國報告書

服務機關：數位發展部資通安全署

姓名職稱：黃淇 設計師

派赴國家/地區：英國倫敦

出國期間：113年9月22日至9月27日

報告日期：113年12月24日

摘要

顧能有限公司（Gartner, Inc.）成立 40 餘年，致力於資訊科技發展、應用、市場反應等面向進行研析，並將成果透過訂閱資料庫、專家諮詢服務、高階主管會議及峰會分享與交流。為全球客戶提供趨勢分析、專家建議及決策輔助工具，並指引有需求之機關組織適應新興科技、創造價值及永續經營。

本次會議係由 Gartner 公司於 113 年 9 月 23 日假英國倫敦舉辦為期 3 天（9 月 23 日至 9 月 25 日）之安全與風險管理峰會（Security & Risk Management Summit），演講主題探討 AI、零信任、端點安全等 23 項議題，此外現場亦舉辦品牌展覽、圓桌會議、一對一諮詢等活動。本報告從生成式 AI、雲端安全及資安韌性角度，分享 Gartner 分析之觀點及解決方案，並提出與會心得及建議，作為主管機關研析資安防護措施、推動風險管理，及未來應如何面對新型資安威脅等業務之參考。

目錄

壹、 目的 1
貳、 會議經過 2
參、 會議重點摘要 3
一、 主題一：Cybersecurity Leadership（資安領導力） 3
(一) Gartner Opening Keynote：Augmented Cybersecurity: How to Thrive Amid Complexity（擴充資安：身處複雜環境如何蓬勃發展） 3
(二) Outlook for AI and Cybersecurity：The Perfect Storm for CISOs（展望 AI 與資安：CISO 正面臨雪上加霜的局面） 7
二、 主題二：Infrastructure Security（基礎建設安全） 12
(一) Cloud Security 201 — The Cloud Security Cocktail（雲端安全雞尾酒） 12
(二) Outlook for Cloud Security（展望雲端安全） 18
三、 主題三：Cyber Risk Management（網路風險管理） 24
(一) Top Trends for Cybersecurity 2024（2024 年重要資安趨勢） 24
(二) The Top Predictions of Cybersecurity for 2024（2024 年重點資安預測） 28
肆、 心得與建議事項 31
伍、 附錄一會場照片 33

圖目錄

圖 1：CYBERSECURITY CONTROLS ASSESSMENT 資安控制措施評估 4
圖 2：INVENTORY YOUR TOOLS OBJECTIVELY 如實盤點你的工具 5
圖 3：2024 TECHNOLOGY ADOPTION ROADMAP FOR SECURITY AND RISK MANAGEMENT 資安及風險管理技術採用路線圖 6
圖 4：GENERATIVE AUGMENTS 生成式擴充 7
圖 5：THE 4 IMPACTS OF GENERATIVE AI FOR CISOS　AI 對 CISO 造成的 4 種影響 8
圖 6：MANAGE CHANGE CONTINUALLY 持續管理變革過程 10
圖 7：CLOUD COCKTAIL INGREDIENTS 12
圖 8：CLOUD SECURITY ARCHITECTS 雲端安全架構師 13
圖 9：CLOUD CENTER OF EXCELLENCE 14
圖 10：CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT 14
圖 11：CLOUD ACCESS SECURITY BROKER 雲端存取資安代理 15
圖 12：CLOUD SECURITY POSTURE MANAGEMENT 雲端資安狀態管理 16
圖 13：CLOUD WORKLOAD PROTECTION PLATFORM 雲端工作負載保護平台 17
圖 14：雲端安全策略完整架構 18
圖 15：SHARED RESPONSIBILITY CHALLENGES 共享責任挑戰 19
圖 16：SAAS 層零信任部署架構 21
圖 17：IAAS 及 PAAS 零信任安全技術 23
圖 18：2024 年資安重要趨勢 24
圖 19：ODM 結果驅動型指標 25
圖 20：PIPE 框架 26
圖 21：CTEM 持續威脅暴露管理 27
圖 22：2024 年重點資安預測 30

壹、 目的

資訊科技發展日新月異，伴隨攻擊者利用新技術展開複雜且持續性的網路攻擊，導致邇來資安議題備受重視且刻不容緩，2022 年底 ChatGPT 問世，即興起生成式 AI 潮流，雖帶來業務效率提升、服務流程創新等便捷性，卻也同時產生新型攻擊手法、倫理及隱私方面的爭議。鑒於各組織日漸仰賴雲端服務，享受資料隨取隨得、資源共享、及降低成本的好處，同時可能面臨到無法掌握雲端供應商其資料儲存位置與處理過程之風險，以及未臻完善的資安管理，導致供應鏈上利害關係人資料外洩的新聞層出不窮，以上種種皆印證著資安挑戰日益嚴峻是不爭的事實，惟有不斷學習新知至關重要，方能掌握最新資安領域見解及趨勢，以制定更具前瞻及洞察性的資安策略。

本署透過參與 Gartner 國際研究機構舉辦的「安全與風險管理峰會」，由與會分析師深入探討各項資安議題背後潛藏的風險、分享最佳實踐方法及應處對策，並提供未來資安趨勢，同時借鑒業界專家傳遞實務經驗與成功案例，供主管機關往後法規或政策訂定之參考，以強化政府機關整體資安防護能力及提升組織韌性。

貳、 會議經過

一、**會議日期：**113 年 9 月 23 日至 9 月 25 日，共計 3 日

二、**會議地點：**英國倫敦 ExCeL 展覽中心

三、**參加場次：**

日期	演講名稱
9 月 23 日	Gartner Opening: Augmented Cybersecurity: How to Thrive Amid Complexity
	Outlook for Privacy, 2024-2025
	Outlook for AI and Cybersecurity: The Perfect Storm for CISOs
	Outlook for Cloud Security
9 月 24 日	Top Trends for Cybersecurity 2024
	Crossfire: XDR: Hype or Hope?
	Cloud Security 201 — The Cloud Security Cocktail
	Gartner Keynote: Cybersecurity Turbulence Report 2024: 7 Forces That Will Threaten Your Organization's Future
9 月 25 日	The Top Predictions of Cybersecurity for 2024
	Expel: Minding the (security) Gap — Connecting Cybersecurity and Risk to Build Resilience
	Improve Security Posture Using Threat Hunting Outcomes

參、 會議重點摘要

一、 主題一：Cybersecurity Leadership（資安領導力）

(一) Gartner Opening Keynote：Augmented Cybersecurity: How to Thrive Amid Complexity（擴充資安：身處複雜環境如何蓬勃發展，講者：Akif Khan, Christopher Mixter）

資訊技術發展一日千里，以致資安威脅與日俱增，行為者（Threat Actor）與組織攻擊面（Attack Surface）之間的距離越來越小，然而提升組織韌性最大的挑戰，並不是攻擊者日益猖獗或攻擊面不斷擴大，更不是因為資源短缺，而是「失效零容忍（Zero Tolerance for Failure）」思維使資安團隊早已精疲力盡。當組織崇尚「失效零容忍」思維時，一旦發生資安事故，每個人都只會如肌肉記憶般反射性回復:「這不歸我管。」以規避責任，導致沒人願意扛起責任。事實上「容錯（Fault Tolerance）」的概念無處不在，管理階層在其他方面也都能接受風險容錯，唯獨在資安方面還未能卸下心防，好比能接受因遭受詐騙導致 3%的收入損失，卻無法接受資安攻擊造成的任何負面影響。

然而現今環境中，企業及機構遭受資安攻擊是無可避免，因此我們必須摒棄「失效零容忍」的思維，取而代之的是如何提升「回應（Response）」及「復原（recovery）」等創造價值的能力，以應用在處理解決緊急事件上，這便是「擴充資安（Augmented Cybersecurity）」的概念。防護措施固然重要，它僅能讓組織在惡劣的環境中勉強生存，但讓組織在日趨複雜、瞬息萬變的局勢下，還能蓬勃發展的關鍵，便需要更加成熟的回應及復原能力。根據 Gartner「資安控制措施評估（Cybersecurity Controls Assessment）」指出「回應」及「復原」能力之重要性高於「保護」能力，惟大多數企業組織仍欠缺擴充資安兩項能力的

成熟度與輕忽其重要性，因此企業組織勢必要盡快投入更多資源於提升回應及復原能力，並與「保護」能力一樣高的水平，但這需要經過長期規劃與實踐。

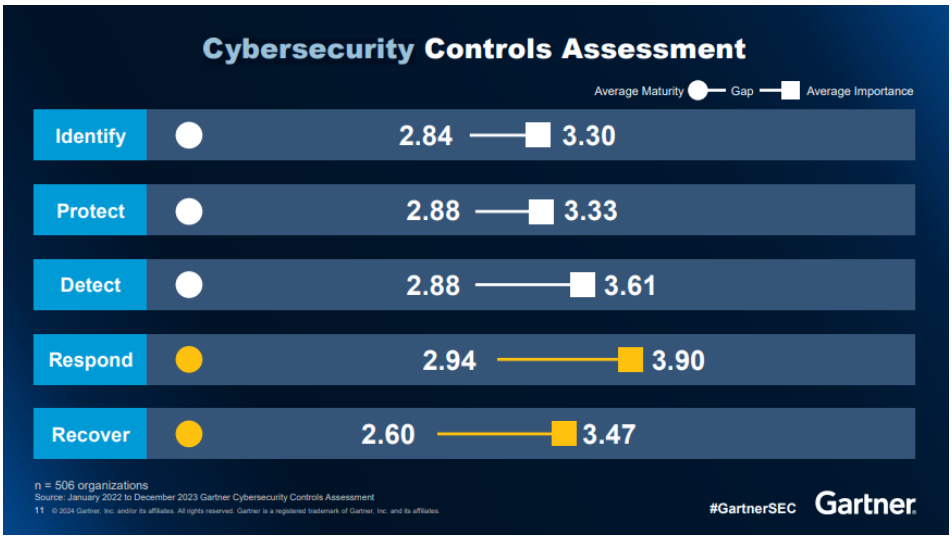

圖 1：Cybersecurity Controls Assessment 資安控制措施評估（資料來源：講者簡報）

Gartner 針對組織應如何建立容忍文化，提供下列建議：

1、 建立「容許失敗」的組織文化（Fault Tolerant Organization）

(1) 構面一：生成式人工智慧（Generative Artificial Intelligence, Gen AI）

首先需制定清晰情境手冊，假設各種攻擊模式，並據以訂定相關回應及復原措施，再進行演練，以確保資安事件發生時，內部人員皆能迅速做出應對措施，爭取將損害降到最低。

(2) 構面二：第三方（Third-party）的運用：

Gartner 發現儘管組織事前做了周密的盡職調查（Due Diligence），知悉潛在的第三方風險，仍無法抗拒其所帶來的優勢而選擇繼續使用第三方服務，因此 Gartner 建議制定正式的第三方應變處理計畫（Third-party Contingency Plan），包含退場策略、替代供應商清單及事件應變處理程序等，該措施能有效提升 43%

「第三方資安風險管理（Third-party Cybersecurity Risk Management, TPCRM）」的效果。另 Gartner 鼓勵組織協助第三方建立更成熟的風險管理能力，將自己的勒索軟體指導手冊（ransomware playbook）、資安事件應處程序提供給第三方，由上至下、層層把關，將有效提升組織本身第三方風險管理的效果。

2、 **持續精實有效工具集（Minimum Effective Toolset）**

(1) 策略一：在有限人力及預算下，組織為抗衡龐大又複雜的攻擊面，需要更精簡且有效地管理資安工具，不幸的是大部份企業對資安工具的投資組合並不明確，且很少與資安執行團隊溝通花在管理工具的時間是否妥當，以及未能從中獲得預期效果的原因。此外「零容忍」思維容易使人陷入「沉迷器材症候群（Gear Acquisition Syndrome）」，Gartner 建議組織如實盤點所有工具，以找出哪些方面的控制措施較為欠缺，亦可發覺哪部分尚有冗餘資源。其次，可搭配 Gartner「Cybersecurity platform consolidation tool」作為參考，以決定要如何優化工具集。

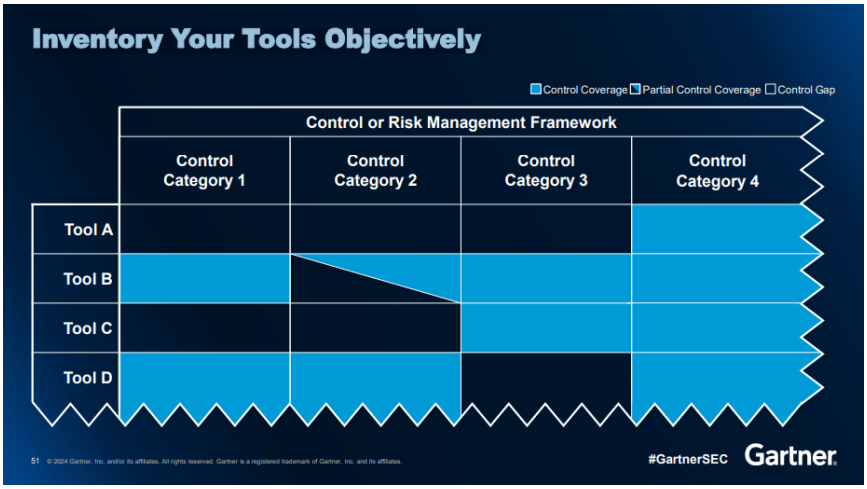

圖 2：Inventory Your Tools Objectively 如實盤點你的工具（資料來源：講者簡報）

(2) 策略二：Gartner 建議每個組織參考 Gartner 的「2024 Technology Adoption Roadmap for Security and Risk Management（如圖 O）」建

立各自的「新興科技評估表」，尤其是針對同行已經有失敗經驗的項目，並在執行概念性驗證(Proof of Concept, POC) 時，考量「資安風險（Cybersecurity Risk）」、「人才短缺（Talent Unavailability）」、「過高或不可預期的成本（High or Unpredictable Costs）」及「技術不相容（Technical Incompatibility）」等 4 個指標。

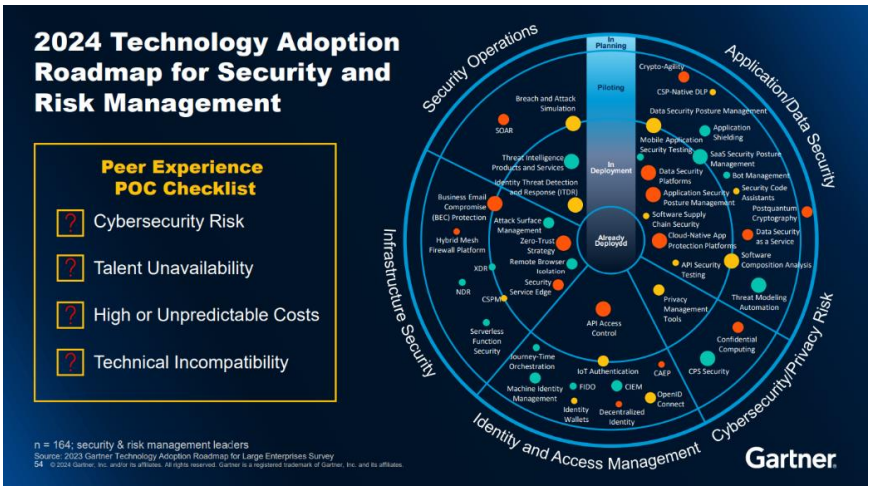

圖 3：2024 Technology Adoption Roadmap for Security and Risk Management
資安及風險管理技術採用路線圖（資料來源：講者簡報）

(3) 策略三：Gartner 建議組織開始布局 AI 策略，尤其在資安營運及應用程式安全方面，善用生成式 AI（Generative AI, Gen AI）提升效率的潛力，除了能讓資安人員透過自然語言去操作工具，以取代複雜的指令使資安團隊更有效率地達成目的，更讓無資安背景的資訊人員（如開發者）輕鬆理解及掌握資安概念及工具，Gartner 預測到 2026 年，AI 將使 SOC（Security Operation Center）效率提高至現在的 40%。

此外，同時探索 Gen AI 的擴充能力，Gartner 預測到 2028 年，生成式擴充（Generative augments）」技術將大幅縮小技能差距，從而消弭 50%的初階資安職位對專業訓練的要求。

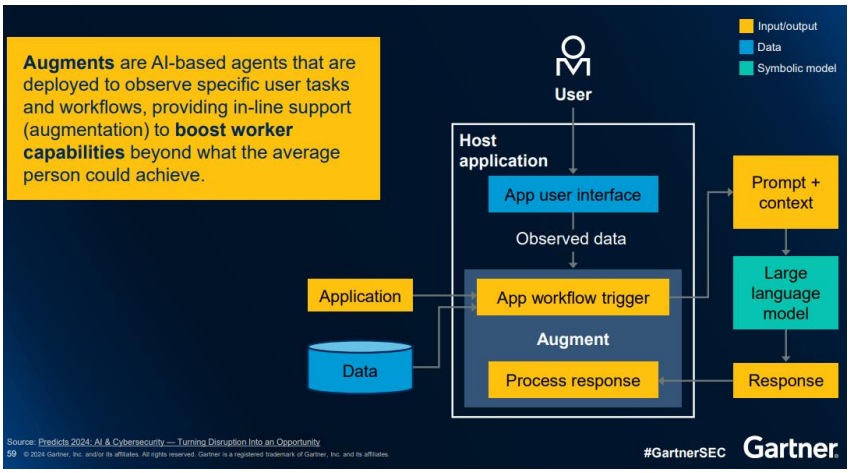

圖 4：Generative Augments 生成式擴充（資料來源：講者簡報）

3、 具韌性的網路團隊（Resilient Cyber Workforce）

首先，在工作流程中融入「自我照護（Self-care）」制度，當發生資安事故後舉辦解壓活動，或在進行工作匯報時，順帶訪談部屬的工作近況等，以建立擁有自癒能力且富有韌性的技術團隊，根據 Gartner 2022 年統計發現，參加至少一項員工福利計劃可使健康狀況提高 5%。將「韌性」視作在逆勢中茁壯成長的軟實力，給予員工足夠的支援，並深入分析員工遇到瓶頸及出現摩擦的地方，進而優化或精實工作流程，使其更快上手、容易適應。

組織應提倡拋開零容忍思維，並非所有資安措施失效皆會導致資安事故，也並非所有事故都會導致資料洩漏。相反的，所有資安事故皆是讓組織進步的難得機會。講認為面對困難、複雜或不確定性的問題，只要勇於測試或實驗，即便結果不如預期，皆是「值得讚賞的失敗經驗（Praise worthy failures）」，失敗的發生恰是因為我們正在嘗試新事物，而實驗使我們保有創新能力。

(二) Outlook for AI and Cybersecurity：The Perfect Storm for CISOs（展望 AI 與資安：CISO 正面臨雪上加霜的局面，講者：Jeremy D'Hoinne）

講者將 AI 崛起比作日蝕，不同人在不同時間點才注意到日蝕現象，在某些部落中，日蝕表示上帝對世人的警示；對一般人來說，日蝕只是一個比較罕見的天文現象，或甚至對其漠不關心；對天文學家而言，卻是觀察太陽狀態的絕佳機會，這「因人而異」的概念好比每個人對 AI 的表述及態度各不相同。Gartner 針對 AI 在資安領域的影響提出下列觀點及建議：

1、盡量減少 Gen AI 對組織的打擊

許多組織正積極導入 AI 技術，期許短期內利用 AI 代替 SOC 等資安業務，但依講者本身測試過上百件 Gen AI 產品的經驗，仍不敢斷定其在資安領域可以帶來什麼進展，現在去定義 AI 能帶來多少影響還為時過早，因為暫未出現公認的衡量標準去評估。

Gartner 將 AI 對資安長(Chief Information Security Officer, CISO) 造成的影響分為 4 面向，包含建立（Build）、使用（Consume）、防護（Defend with）、攻擊（Attacked by）。

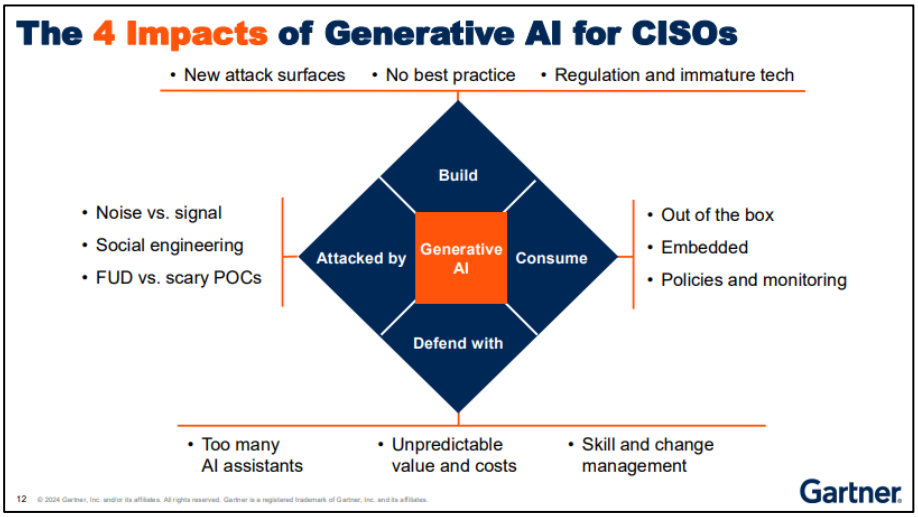

圖 5：The 4 Impacts of Generative AI for CISOs

AI 對 CISO 造成的 4 種影響（資料來源：講者簡報）

建立組織的資安計畫及持續精進控制措施，以因應 AI 應用程式擴大組織攻擊面問題，管理及監控組織應用各類型 Gen AI 之使

用情形，並使用 Gen AI 改善資安風險管理、防禦新興攻擊手法，適應不斷變化的威脅，同時降低成本支出。

2、 為「擴充資安（Augment Cybersecurity）」奠定基礎

Gartner 預測 2025 年開始，自動化的 Gen AI 技術—AI Agent 將會成為新一波的 AI 趨勢，不僅能接收 Prompt 提問或指令，亦能自動化產出並持續優化工作流程，代理人類執行繁瑣的任務，拓展在資安領域的應用範疇，下列為 Gartner 提供的指引：

(1) 建立 AI 指引、風險評估標準及素養

經 Gartner 統計 86%的人打算忽略制定 AI 資安指引，因無法不斷重新建立指引及風險評估標準，然而 AI 資安指引定位在 AI 治理中的角色及步調是很重要的，因此 Gartner 建議組織打好基礎，並透過「增強評估（Augmentative Evaluation）」概念，將原本的風險評估方式直接套用於新技術的評估方法，該理念在組織未來面對任何新興技術時，皆能更靈活地擬定相關指引。

建立 AI 素養是組織舉足輕重的課題，再精湛的 AI 模型都有可能誤會用戶提問的內容而給予錯誤的回應，甚至出現 AI 幻覺（Hallucination）現象。最近研究指出 Gen AI 的結果準確率僅有 77%，所以組織應選擇適合的衡量指標，整體性評估 AI 產品之準確率、召回率、精確度等，而非直接相信供應商宣稱及展示的效果。

(2) 持續管理變革（Change）過程

Gartner 建議組織進行改革時，應具體化改革目標以確保使用到合適的評估指標，其次於施行前，關注員工對於改革的想法，避免負面態度造成「變革疲勞（Change Fatigue）」，導致變革效果不及預期，並在改革實施後，持續蒐集及監測各項指

標，如結果指標（Outcome metrics）、體驗指標（Experience Metrics）、承諾指標（Commitment metrics）及能力指標（Capability metrics）等，以掌握變革效果及員工反饋，最終從更細微且有意義的維度加以分析，以發掘傳統上容易被粉飾的痛點。

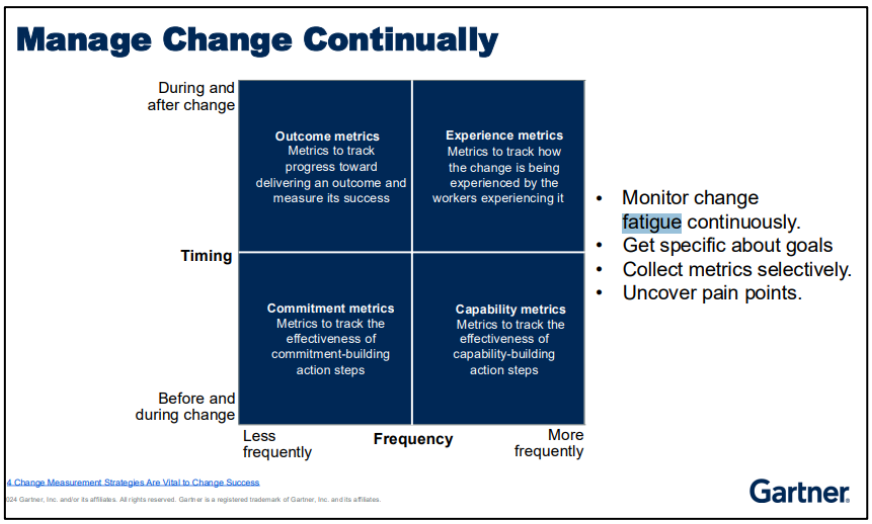

圖 6：Manage Change Continually 持續管理變革過程（資料來源：講者簡報）

(3) 培養資安團隊批判能力

培訓對組織長期發展是很重要的，Gartner 建議組織進行跨團隊知識共享，並保持資安團隊的批判思考能力，以勇於挑戰及判別 AI 推理的結果，避免過度依賴 AI 工具，一味聽從 AI 的建議及判斷。

(4) 為各式各樣的攻擊情境作準備

已有許多論文證實攻擊者具備創建自動化 AI Agent 執行網路攻擊之能力，2019 年有篇論文指出攻擊者透過強化學習（Reinforcement Learning, RL）技術，全自動化製造出各種態樣的惡意程式，且能有效躲避 VirusTotal 偵測（偵測率從 80%降至 40%以下），同時駭客組織已演化出「混淆即服務（Obfuscator as a Service）」的商業模式。Gartner 建議組織開始規劃各式各

樣的 AI 攻擊（如深度偽造、對抗式攻擊等）之情境，並落實演練作業，以應對新興攻擊、提升組織韌性。

3、 準備將 Gen AI 整合到現行的策略藍圖中

Gartner 建議直接將 Gen AI 衡量指標整合進現行的評估標準中，以結果導向評估 Gen AI 能力表現及使用者滿意度，並透過靈活的策略藍圖及足夠的實驗空間來精進評估指標。在關注 AI 為組織提升多少效率時，亦需與其耗費成本作客觀比較。另講者推薦透過「AI 可靠性、風險及安全管理（AI Trust, Risk and Security Management, TRiSM）」確保組織實施最佳的應用程式安全控制措施、資料庫存與安全性，及管理軟體供應鏈風險等，並持續監控及提升組織的 TRiSM 成熟度。

二、 主題二：Infrastructure Security（基礎建設安全）

(一) Cloud Security 201 — The Cloud Security Cocktail（雲端安全雞尾酒，講者：Charlie Winckless）

講者將雲端安全以「Cocktail（雞尾酒）」為喻，將其比擬為一杯混合著不同原料的雞尾酒，而各種雲端資安控制措施則象徵為製作這杯雞尾酒的主要材料（Ingredient）。這些防護措施如何能在同一組織中有效整合，取決於每一個組織所制定的「食譜」，也就是決策，而不同的決策導致個組織雲端安全的部署效果有著顯著差異。

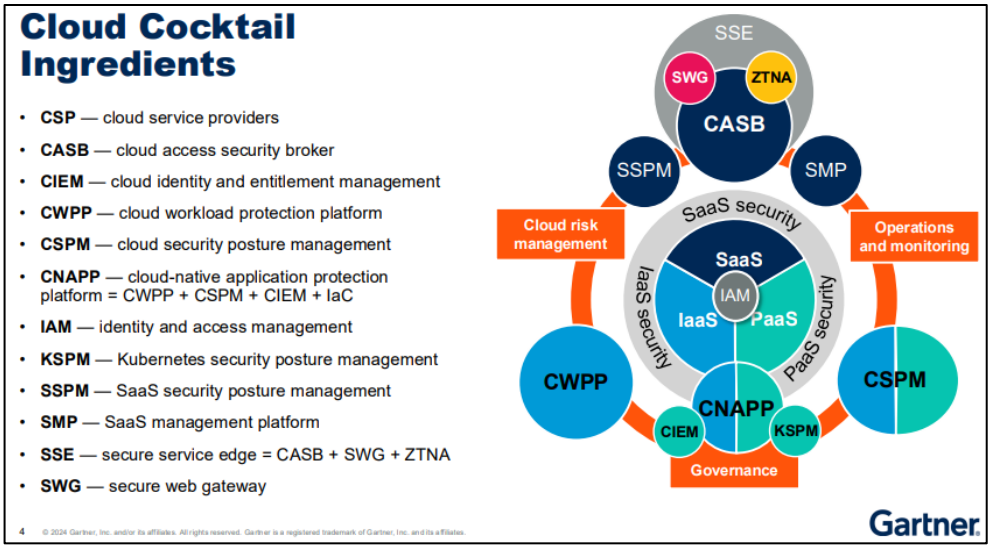

圖 7：Cloud Cocktail Ingredients（資料來源：講者簡報）

雲端安全控制措施分為六種，分別是 Governance（治理）、Identity（身分）、Controlled access（控制存取）、Managing the configurations（管理組態）、Advanced controls（進階控制）及 Convergence（融合）。下列將一一說明 Gartner 提出之觀點及建議：

1、治理 Governance：建立管理體系及人員配置

組織應明確制定雲端治理的規範，以及組織內各角色之責任，

同時選擇適合的供應商至關重要，因雲端安全始於供應商的能力與承諾，然而市場上的雲端服務提供者在能力及成熟度表現參差不齊，因此組織本身應充分了解正在使用的服務內容及其具體用途，以降低第三方風險。此外，具備相關知識且執行度高的員工也是不可或缺，如「雲端安全架構師（Cloud Security Architects）」便是主導雲端安全工作的關鍵角色，培養專業人才是推進雲端安全工作的核心所在。

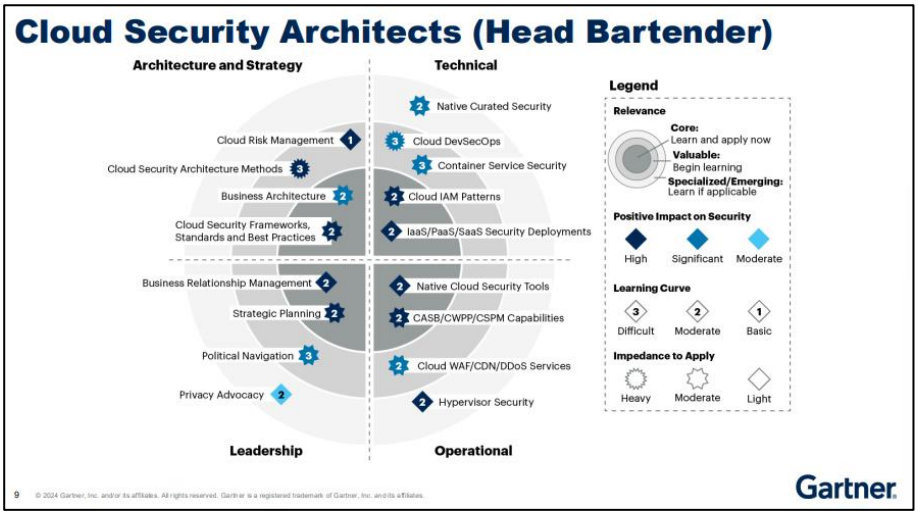

圖 8：Cloud Security Architects 雲端安全架構師（資料來源：講者簡報）

許多組織曾提出：「我擁有眾多雲端服務，應該從哪裡開始進行管理與整合？」的問題，對此，講者建議組織首先設立「雲端卓越中心（CCoE）」負責統籌治理雲端業務與資源，推動組織實施最佳實踐方案並掌握最新技術。CCoE 應囊括組織內的所有部門和管理者成員，以便在推進計畫時能夠實現高效互助與支持。此外，CCoE 還可以充當培訓平台，為團隊成員提供相關的培訓資源，以提升他們在雲端技術與安全領域的專業知識與技能。

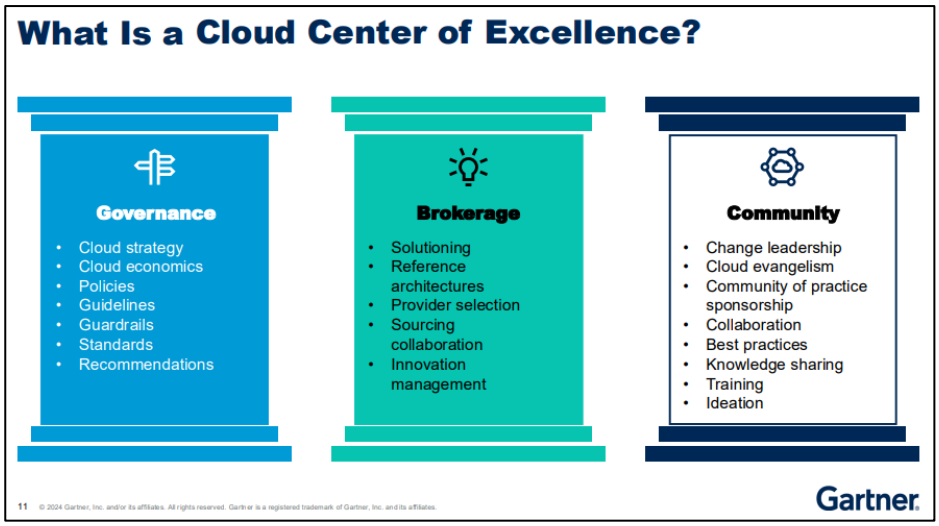

圖 9：Cloud Center of Excellence（資料來源：講者簡報）

2、身分 Identity：從「身分」開始著手

身分管理是保障雲端安全的核心，通過該措施可以有效控制人員權限及存取操作，確保敏感資料受到保護。Gartner 推薦採用「雲端基礎架構權限管理（Cloud Infrastructure Entitlement Management, CIEM）」工具，幫助組織細緻化監管雲端環境中每位用戶的身份與權限，有效地避免了權限濫用與資料洩露的風險。

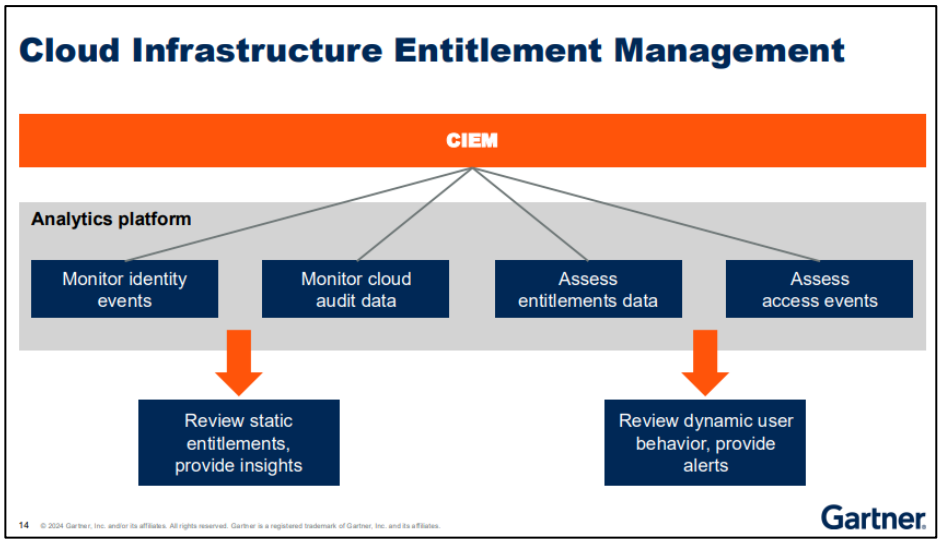

圖 10：Cloud Infrastructure Entitlement Management（資料來源：講者簡報）

3、存取控制 Controlled access

Gartner 推薦透過「雲端存取資安代理（Cloud Access Security Broker, CASB）」工具執行存取管理，該技術充當了組織與雲端服務供應商之間的中介，以保護雲端服務及應用程式的安全，負責監視、控制雲端流量並視覺化展示當前使用情況，並協助執行安全性策略。CASB 涵蓋了身份驗證、單一登入、裝置控制等多項功能，此外，還支持多種部署模式，例如 API 模式、正向代理模式以及反向代理模式等，同時採納多種部署模式，雖然可以實現更全面的安全控制，卻可能為規則設定、涵蓋範圍及效果帶來負面影響。因此，組織在整合這些工具時應更加關注實際應用場景，將重點放在成果交付，而不過於糾結於技術細節。

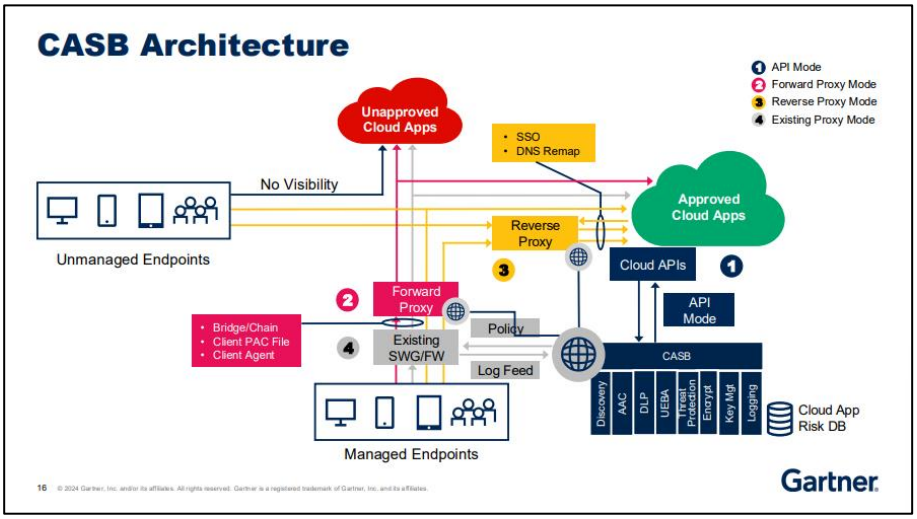

圖 11：Cloud Access Security Broker

雲端存取資安代理（資料來源：講者簡報）

4、Managing the configurations（管理組態及資源）

「完成存取身份控制後，還能做點什麼？」由於所有雲服務使用者皆共享著雲端資產及資源，為確保自身雲端安全，組織應管理雲端資產的組態及部署雲端資產的工作負載（Workload）安全性。

講者推薦採用「雲端資安狀態管理（Cloud Security Posture Management, CSPM）」工具，其旨在提醒管理者雲端服務中的合規風險、組態安全弱點及威脅偵測，並自動辨識及修復雲端應用程式的錯誤組態，降低未經授權的存取、資料外洩的發生。

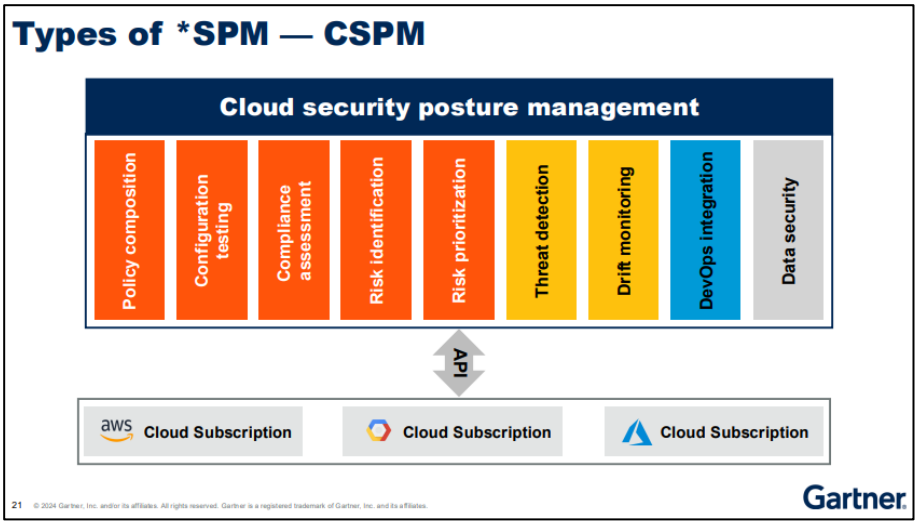

圖 12：Cloud Security Posture Management

雲端資安狀態管理（資料來源：講者簡報）

另一項講者推薦的管理工具為「雲端工作負載保護平台（Cloud Workload Protection Platform，CWPP）」，將 Agent 以 DaemonSet 或 Sidecar 模式安裝在底層端點以即時監控，保護虛擬機（Virtual Machine, VM）、容器（Container）以及無伺服器（Serverless）之雲端工作負載。CWPP 與 CSPM 的用途看似相近，實際兩者的使用目的並不相同。CSPM 主要用於監控雲端組態之正確性及合規性；CWPP 則作用於偵測雲端環境中執行軟體的弱點及威脅。

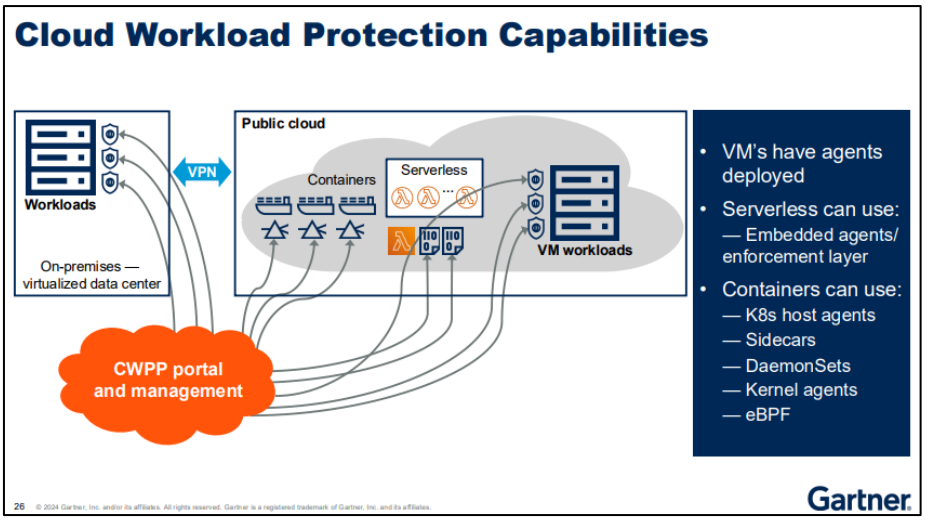

圖 13：Cloud Workload Protection Platform

雲端工作負載保護平台（資料來源：講者簡報）

5、Advanced controls（進階控制）

近年許多組織開始採取進階控制措施，例如機密計算（Confidential Compute），該技術在歐洲企業間更為流行，因歐盟對用戶隱私安全的要求十分嚴格。當要處理雲端資料時，通常需先對其解密才能執行，而機密計算技術提供一個「受信任的執行環境（Trusted Execution Environment, TEE）」，只有通過授權的應用程式能在該環境下對資料進行解密及處理，以防止攻擊者，甚至雲端服務提供者看到資料內容，因此即使本地端或供應商端遭入侵，依然能有效防止機敏資料洩漏問題。

6、Convergence（融合）

市面上如雨後春筍般出現各式資安工具，然而組織如何將所有資安產品整合為一套能協調運作的組合，並集中管理雲端組態及安全風險？Gartner 提出「雲端原生應用程式保護平台（Cloud Native Application Protection Platforms, CNAPP）」解決方案，結合前面提及的 CIEM、CSPM、CWPP 等工具，綜觀組織整體的雲端安全管理狀

態，以取代多個獨立平台，避免過度平台化，同時 Gartner 提倡「測試左移（Shift-Left Testing）」概念，鼓勵組織於盡早於開發階段考量並實踐安全措施。

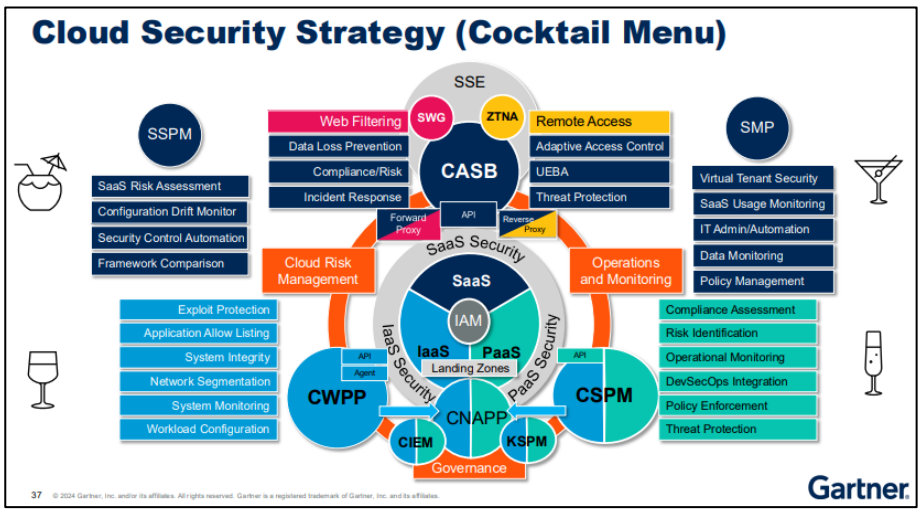

圖 14：雲端安全策略完整架構（資料來源：講者簡報）

(二) Outlook for Cloud Security（展望雲端安全，講者：Richard Bartley）

隨著越來越多組織採用雲端服務，雲端環境的安全挑戰愈加複雜且多樣化，包括治理能力不足、供應鏈安全風險、不當組態設定等，特別在「共享責任（Shared Responsibility）模型」下，使用者也需承擔部分責任，然而許多組織對該權責劃分缺乏認知，而忽視於本地端的資安防護作業。組織不僅需要面對不斷變化的攻擊面及嚴格的法規要求，還需確保雲端服務在高度風險的環境中穩定運行，並融入日常業務流程中，以下為 Gartner 針對雲端安全提出之觀點及建議：

1、 雲端安全

(1) 挑戰一：共享責任挑戰

雲端服務的安全管理依賴於服務供應商和使用者之間的協作，根據共享責任模型，不同類型的服務有著不同的責任分配。

「軟體即服務（Software as a Service, SaaS）」由供應商端承擔大部分安全管理責任，基於雙方之間不平等的可見性，組織更應監控其數據備份機制、存取控制與安全事件回應流程，並明確訂定服務水準協議（Service Level Agreement. SLA）條款，避免出現權責劃分模糊地帶。。

「基礎設施即服務（Infrastructure as a Service, IaaS）」則由客戶負擔更多安全管理責任，組織應確保對自身的資訊資產有全面掌控能力，由於不同供應商的安全設定方式各異，當企業切換供應商時，安全配置文件（Security profiles）必須重新定義，這對資安團隊是一大挑戰。

此外，各類雲端服務的共通挑戰包含合規性管理、敏感數據的可見性（Sensitive Data Visibility）、營運持續（Business Continuity）規畫及 SLA 的解讀，建議組織在導入雲端服務前，先與供應商討論上述議題之解決方案，避免履約過程中雙方出現分歧或盲點。

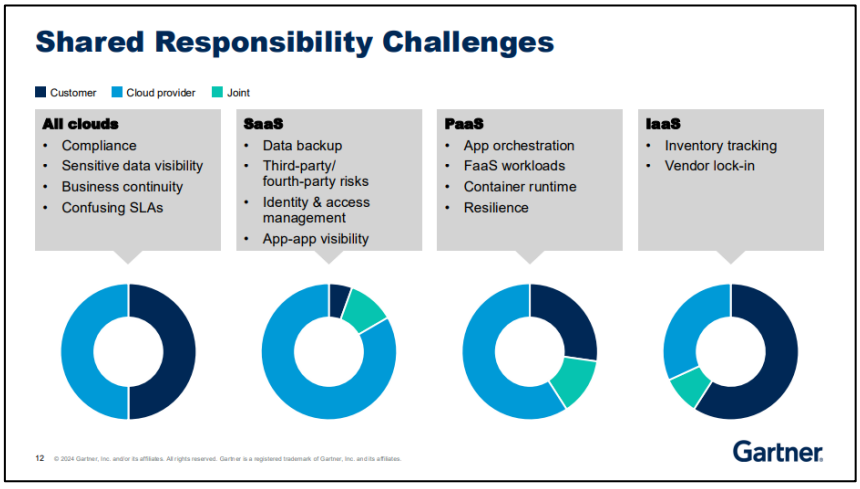

圖 15：Shared Responsibility Challenges 共享責任挑戰（資料來源：講者簡報）

(2) 挑戰二：縮小資安知識的差距

資安知識不足係為阻礙雲端安全的重要因素之一，Gartner 建

議組織建立「雲端卓越中心（Cloud Center of Excellence, CCoE）」或推動轉型專案（Transformation Project），以全面提升員工對雲端安全的認知及實踐能力。

透過基礎課程幫助無資安背景的人員了解雲端環境中的安全概念，並將雲端安全意識融入日常業務中。另為資安團隊提供專業培訓，讓其掌握安全架構設計、雲端工具操作、DevSecOps 實踐、容器及 API 安全管理，以及運用「基礎設施即程式碼（Infrastructure as Code, IaC）」與「政策即程式碼（Policy as Code, PaC）」進行自動化部署的能力。

(3) 挑戰三：安全地使用 Gen AI，並利用其保護雲端安全

生成式 AI（如聊天機器人或助理服務）逐漸成為組織生產工具的一部分，惟其帶來的風險不容小覷。Gartner 建議組織應將 AI 存取管理納入 SaaS 安全框架中，確保每次存取均經授權，並根據風險狀況評估是否可使用敏感數據，同時關注 AI 可能帶來的資料洩露、幻覺與合規性問題。

另一方面，生成式 AI 也能成為雲端安全的重要助力。它可以用於威脅偵測、風險排序、事件摘要及即時變化監測。透過結合 PaaS 層的「雲端原生應用程式防護平台（CNAPP）」及 SaaS 層的「安全服務邊緣（Security Service Edge, SSE）」，AI 技術能進一步提升漏洞檢測、合規性審查及攻擊路徑分析的效率，並將威脅建模自動套入 MITRE ATT&CK、STRIDE（Spoofing、Tampering、Repudiation、Information disclosure、Denial of service、Elevation of privilege）等框架，提升分析效率與及可信度。

2、 SaaS 層應關注之事項

(1) 部署零信任機制

建議組織在 SaaS 層實現零信任管理，確保所有存取均遵循最小權限原則，透過安全服務邊緣（SSE）工具的「零信任網路存取（Zero Trust Network Access, ZTNA）」功能管控本地端、BYOD、遠距工作用戶及第三方供應商之存取，減少過度授權與潛在威脅。同時利用 SaaS 安全態勢管理工具可輔助企業進行細化權限與授權控制，實現更接近零信任的操作模式。

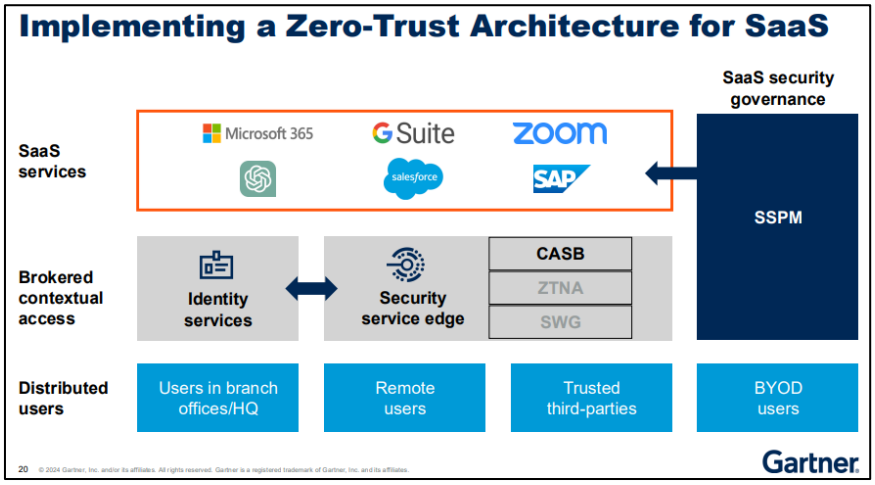

圖 16：SaaS 層零信任部署架構（資料來源：講者簡報）

(2) 其他資安建議

Gartner 建議使用安全框架，如參考美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）提出「安全雲端商業應用指引（Secure Cloud Business Applications, SCuBA）」和雲端安全聯盟（Cloud Security Alliance, CSA）的「SaaS Governance Best Practices」指引，制定適用組織本的 SaaS 安全計畫。

其次，建立並管理 SaaS 層的關鍵資產清單，避免浪費資源或成本超支，以及忽略管控「未經核准的非託管應用程式（Shadow IT）」，導致敏感資料洩露於未知的第三方工具，不完整的資產盤點使得部分雲端資源長期暴露於潛在風險之中，增加了

組織的攻擊面。

最後，制定並維護詳細的「資安事件應變處理查檢表（Security Checklists for Incident Response）」，以便有效率地完成事件回應及損害控制作業。另透過演練各式劇本（Playbook），確保組織能快速識別並應對各類 SaaS 資安事件。

3、 在 IaaS 及 PaaS 層應關注之事項

(1) 實現零信任機制

組織同樣可透過 SSE 的零信任網路存取（Zero Trust Network Access, ZTNA）功能管控存取權限，然而客戶端在 IaaS 及 PaaS 層負擔的責任更大，因此需進一步考慮如何管理並儘量減少隱性信任(implicit trust)。組織使用者透過 API 對雲端服務進行分區，如劃分處理高風險資料的高風險區域，並利用相關安全技術進行身分及存取管理。

(2) 安全技術

甲、 雲端原生應用程式保護平台（CNAPP）：

在雲端 DevSecOps 中，可於測試階段應用「基礎設施即程式碼（IaC）」工具；在雲端基礎建設安全方面，則可利用「雲端工作負載保護平台（CWPP）」切分工作負載，並針對指定分段進行回應。此外，透過「雲端偵測響應（Cloud Detection Response, CDR）」工具提供上下文資訊及偵測回應分析，保護工作負載及快速定位問題；在雲端管理層（Control Plane），採用「雲端安全狀態管理（CSPM）」以確保組態配置正確，並檢查 IaC 部署效果是否符合預期，同時利用「雲端基礎架構權限管理（Cloud Infrastructure Entitlement Management, CIEM）」 制定身分識別計畫，合

理劃分權限，減少過度授權。

乙、 應用程式安全元件 Application security component

透過「Web 應用和 API 防護（Web Application and API Protection, WAAP）」解決方案抵禦多重攻擊威脅，並利用「應用程式安全狀態管理（Application Security Posture Management. ASPM）」提供的「應用程式安全測試（AppSec testing）」功能，通過靜態（白箱）或動態（黑箱）測試發現 Web 應用程式漏洞並分析上下文。

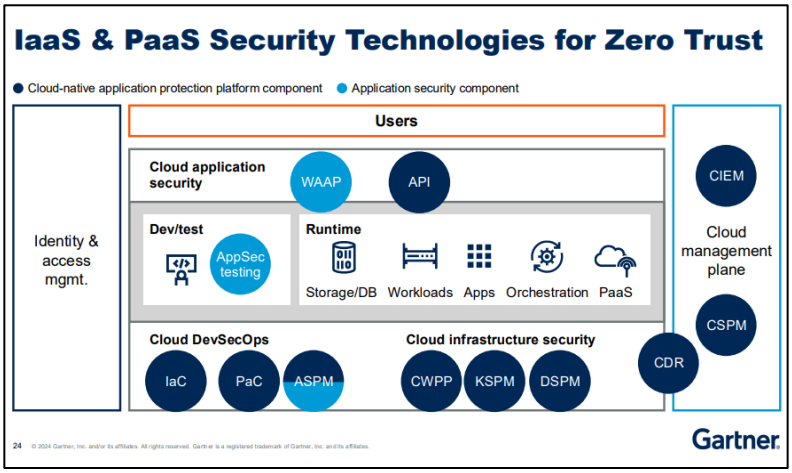

圖 17：IaaS 及 PaaS 零信任安全技術（資料來源：講者簡報）

(3) 其他資安建議

在 CCoE 中實踐 DevSecOps 機制，並重視雲端資產管理，同時結合 CNAPP 解決方案，爭取對 IaaS 和 PaaS 層的最大可見度，以確保落實安全治理，否則難以有效管理雲端安全。

充分利用雲端安全工具，以評估雲端安全漏洞及威脅，並確保資安團隊熟悉工具操作，保障日常工作流暢運行。此外，組織提升資安團隊技能時，應避免過度依賴外部招募。畢竟內部人員仍對組織環境更加熟悉，只需提供適當培訓機會，便可能快速彌補資安人力缺口。

三、 主題三：Cyber Risk Management（網路風險管理）

(一) Top Trends for Cybersecurity 2024（2024 年重要資安趨勢，講者：Alex Michaels）

2024 年各組織為優化資安韌性及效能，實施各項控制措施並努力尋找應用 Gen AI 能力的機會，以因應 AI 興起、資安人才短缺、對雲服務過度依賴、嚴格的法規要求及不斷演化的威脅攻勢等挑戰，Gartner 提出在 2024 年資安領域上影響深遠的六大趨勢：

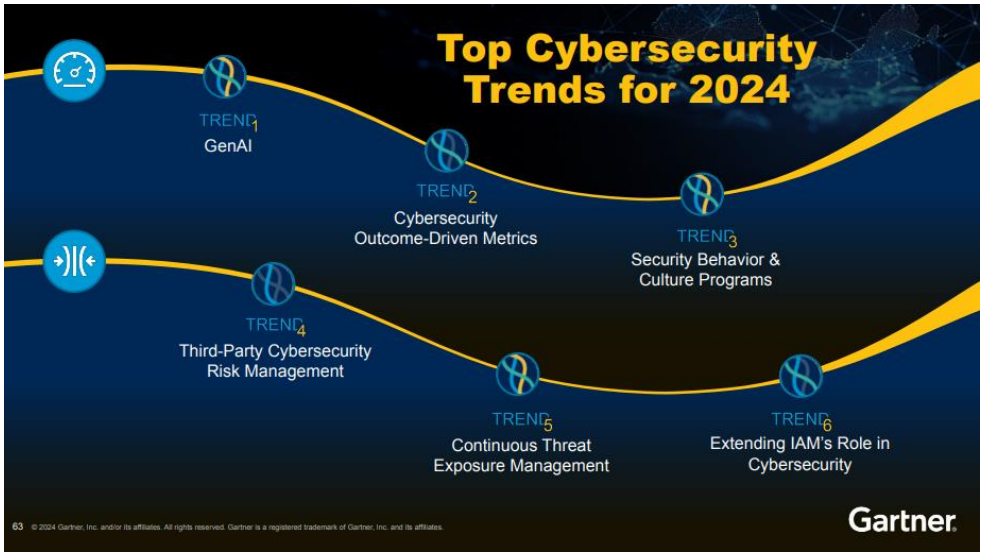

圖 18：2024 年資安重要趨勢（資料來源：講者簡報）

1、 短期而言，組織仍對 Gen AI 保有疑慮；長期來看，Gen AI 將帶領組織開創嶄新未來。

隨著技術演進及市場發展，Gen AI 應用程式架構日新月異，Gartner 建議 CISO 持續吸收新的 AI 知識及技術，並不斷評估及精進現行保護措施，以滿足組織需求。此外，AI 惡意軟體將成為未來的惡意軟體的主流，其與 SolarWinds、WANNACRY 攻擊截然不同，之前或許還有偵測、通報的空間供組織回應及處理，惟 AI 攻擊將不再施予轉圜餘地，因此 CISO 應致力於減少風險暴露，並持續監

控及評估威脅情勢，並確保組織具有足夠的韌性。

2、 建立與董事會之間溝通的橋梁，以減少意見分歧。

許多 CISO 正在使用「結果驅動型指標（Outcome-driven Metrics, ODM）」，視覺化呈現投入成本後達到的資安防護效果，幫助董事會、高階領導者及職能部門（Functional counterparts）了解 CISO 為組織帶來的資安價值，進而做出可行的最佳風險決策，是執行定性（qualitative）及定量（quantitative）風險評估之間很好的分析工具。

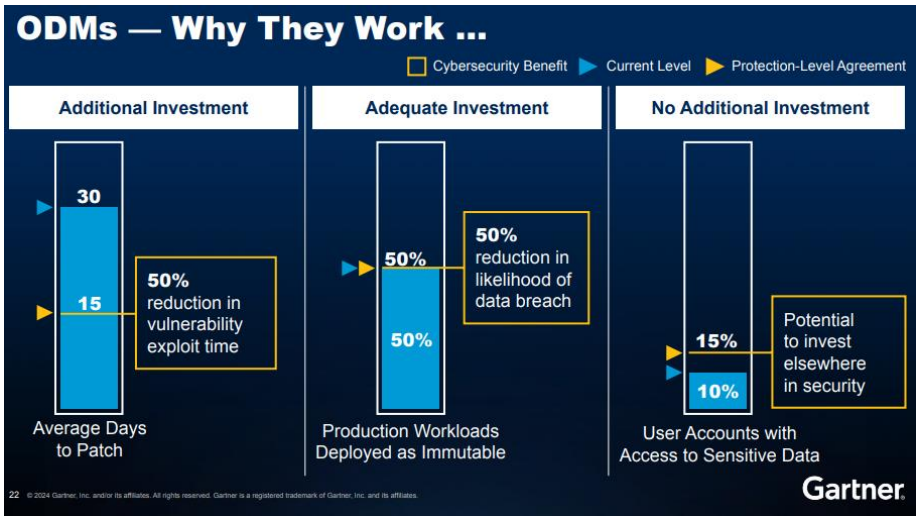

圖 19：ODM 結果驅動型指標（資料來源：講者簡報）

3、 安全行為與文化計畫（Security Behavior & Culture Programs, SBCP）：有效減少人為的資安風險而越來越受歡迎。

許多 CISO 正在使用 SBCP 概念作為推動資安目標的工具，旨在於培養創新思維，以激發新的安全工作流程，並將其深入於組織的安全意識及企業文化。舉例來說，透過事件日誌紀錄，找出員工最常犯且高風險的違規行為，並將對應的改善措施融入工作流程，這便是展現 SBCP 的精神。另 Gartner 建議參考 PIPE （Practices, Influences, Platforms , 5E）框架協助 SBCP 的推動，並透過結果驅動型指標（ODM）來評估 SBCP 成效，以爭取高階主管的支持。

圖 20：PIPE 框架（資料來源：講者簡報）

4、第三方的資安風險管理（Third-Party Cybersecurity Risk Management, TPCRM）：以韌性為導向、高效使用資源

Gartner 調查發現近 2 年 65%的資安管理者投入更多資金、76%的受訪者投入更多時間在第三方資安風險管理上。CISO 及資安管理者就像變色龍一樣需適應變化萬千的環境，在有限資源下提升組織的韌性便是首要任務，傳統上許多 CISO 會在前期投入周密的盡職調查，然而再多的盡職調查也無法發現所有第三方帶來的風險，因此 Gartner 建議組織建立「資安營運持續計畫（Cybersecurity Contingency Plan）」，為最壞的情況做好準備，並讓供應商參與該項計畫，同時改善與第三方的合作關係。如開場演講所說，向涉及組織重要資產的第三方分享降低風險的最佳實踐方法，以與他們建立互惠互利的關係。

5、持續威脅暴露管理（Continuous Threat Exposure Management, CTEM）：勢頭日益增強

僅透過漏洞管理（Vulnerability Management, VM）早以無法抵禦強勢的惡意威脅，Gartner 建議採用 CTEM，以結構化方法持續評估、

排序、驗證及修復資安風險。首先擴大評估攻擊面範圍，包含設備、應用程式、社群軟體及供應鏈等超出傳統執行 VM 的資產範疇，再根據業務影響度識別出構成風險的破口，並依「漏洞利用率」及「資產價值影響程度」對風險進行排序，其次執行驗證工作，以證明該風險確實會影響到組織運作，以及驗證組織實際的偵測及回應能力。除資安團隊外，亦需動員相關部門共同協作資安策略及實施控制措施。

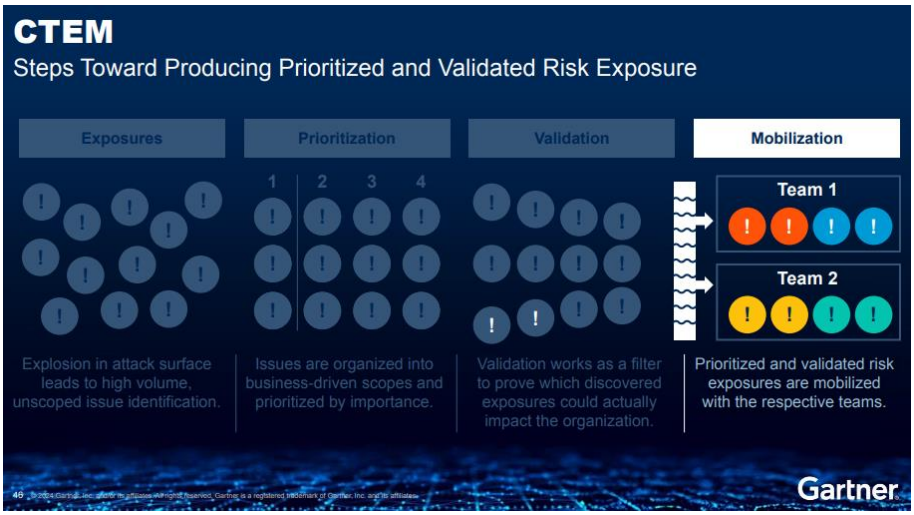

圖 21：CTEM 持續威脅暴露管理（資料來源：講者簡報）

6、擴展身份識別與存取管理（IAM）：擴大發展 IAM 以改善資安防護效果

遠端工作模式讓「身份識別」在資安防護上占有一席之地，許多 CISO 將 IAM 作為組織的核心策略，實施並增進組織「身分威脅偵測及回應（Identity Threat Detection and Response, ITDR）」能力，並將組織的身分基礎架構發展為支援不同身分識別服務的「身分識網（identity fabric）」，提供更全面且靈活的身分管理模式。另依 Gartner 研究顯示，三分之二的受訪者將在明年增加對 IAM 的投資，然而組織應同時考量低效 IAM 技術累積的技術債（Technical Debt）及迭

代更新 IAM 基礎設施造成的額外成本、不易維護、減緩軟體開發速度等問題。

(二) The Top Predictions of Cybersecurity for 2024（2024 年重點資安預測，講者：Craig Porter）

CISO 的目標是「時刻保持清晰的大局觀，以幫助組織解決資安問題」，然而未來充斥著「波動性、不確定性、複雜性及模糊性（Volatility, Uncertainty, Complexity and Ambiguity, VUCA）」，意味著組織不能再僅關注自身，須從更多角度去規劃戰略。Gartner 預測未來組織發展資安計畫時可能會面臨的八大情境，講者強調這些情境並非獨立或順序性地發生，是會並行且遍佈在各個時間點上，不僅影響資訊科技領域，甚至對組織的商業活動及人員皆會產生影響。

1、**到 2027 年，全球每 100 家組織中，有三分之二的組織會將個人法律風險納入考量，向資安領導者提供董監事及重要職員（Directors & Officers, D&O）責任保險。**此外，組織需明確定義 CISO 角色及責任歸屬，以保護其不會被迫承擔義務以外的責任。歐盟規範的《於歐盟實施高度共通程度之資安措施指令（NIC2）》及《數位營運韌性法（Digital Operational Resilience Act, DORA）》皆越來越重視這個概念。

2、**到 2028 年，企業用於打擊惡意資訊的支出將超過 5 千億美元，占用了一半的行銷及資安預算。**Gartner 定義惡意資訊為將事實經過演算法修飾後產出的錯誤資訊（Misinformation）或不實資訊（disinformation），旨在影響大眾心理並誤導其做出其他決定，大規模的惡意資訊可能導致 AI 幻覺的發生，建議持續培養組織員工及利害關係人對惡意資訊的高度警惕，並投入資源及工具來檢測並處

理此類威脅與攻擊。

3、**到 2028 年，Gen AI 的應用將減少技能差距，使 50%的初階資安職位不再需要專業訓練。**Gartner 發現日常使用的辦公室生產力工具出現了許多 AI 生成式擴充功能，提供智能助理服務。建議組織利用跟上這波趨勢，將 Gen AI 擴充於資安工具上，如使用大型語言模型（large language model，LLM）自動產生主題性的上下文劇本及威脅模型，從而改善組織的事件應處能力。

4、延續去年針對零信任的大量預測，**到 2026 年，75%的組織將從其零信任策略中排除非託管、汰舊和虛實整合系統。**Gartner 建議組織對非 IT 環境應用零信任基礎概念，並要求零信任服務供應商充分展示在組織環境中，可以降低哪些風險以及如何實踐。

5、 **到 2026 年，能在安全行為與文化計畫中，將 GenAI 功能與「平台式架構（Platform-based Architecture）」相結合的企業**，因能即時掌握並回應員工行為，**將減少 40%因內部人員疏失造成的資安事件。**

6、 **到 2026 年，40%的領導者的核心職責包含偵測及回應「身分識別與存取管理（IAM）」相關的違規行為。**特殊權限濫用及憑證竊取仍是當前最大威脅，惟部分 CISO 和管理階層對 IAM 的了解有限，因此 Gartner 建議組織應促進董事會參與，將 IAM 作為資安「保護等級協議（Protection-Level Agreement, PLA）」的目標，以引導董事們意識到該風險並優先投資相關防護計畫。

7、**到 2027 年，70%的組織將「預防資料遺失」、「內部風險管理規則」與 IAM 環境結合，以更有效地識別可疑行為。**分散式管控的「資料外洩防護（Data Loss Prevention, DLP）」技術僅識別特定的資料特徵，防止未經授權的移動及使用稽敏資料，惟容易造成 SOC 人員警報疲勞。隨著資料安全市場發展日漸成熟，傳統「以資料安全為中心」

解決方案越來越不合時宜，而主張集中管理的「以身分為中心」的解決方案將嶄露頭角，將移動及使用機敏資料之操作行為關聯到使用者行為，並產出風險模型，讓領導者更全面地了解資料安全管理情況。

8、**到 2027 年，30%的資安團隊將重建應用程式安全，讓非資安專業開發或 IT 人員的直接管理應用程式安全。**專門負責應用程式安全的人力難以負荷組織內成千上萬應用程式及軟體安全的管理工作，為填補這項差距，Gartner 建議組織提供內部人員輔導及訓練資源，並發展「低度程式碼或無程式碼（low code/no code）」的開發方法，讓非技術專業人員不需編碼，便能輕易上手視覺化、拖放工具來建立應用程式及網站。

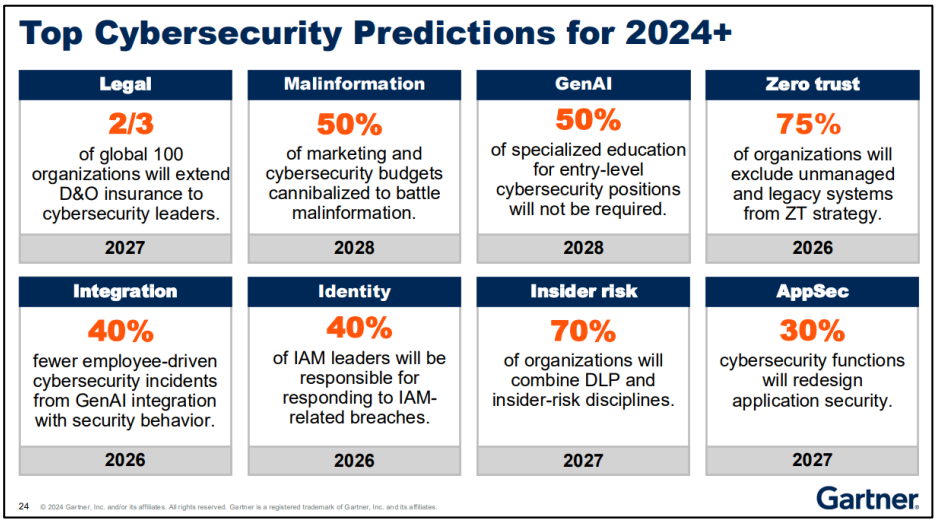

圖 22：2024 年重點資安預測（資料來源：講者簡報）

肆、 心得與建議事項

政府機關擁有大量涉及國家機密、人民隱私，及維運重要民生系統資料庫等機敏資料，容易成為駭客組織攻擊的目標，然一旦遭遇資安事故，將導致資料外洩、營運中斷等情事，危及國家及人民生命財產安全，影響民眾對政府的信任度，嚴重斲傷政府形象。從雲端安全到 Gen AI 的應用，資安風險不僅來自於傳統的攻擊面，還包括供應鏈風險、新型威脅以及資安意識與維安技能的不足。同時，許多單位仍因陷於「失效零容忍」思維而削弱了組織的韌性，也導致資安團隊壓力過大，且回應、復原能力與防護能力資源分配失衡的困境，難以有效應面對現實中不可避免的資安事件。

本次會議以「擴充資安」為主軸，將資安從被動防禦轉變為創造價值的積極策略，Gartner 分析師於會中提出利用生成式 AI 提升效率、加強第三方風險管理、強化身分驗證及存取管理機制，以及推動韌性文化等議題之具體建議，鼓勵企業組織接受風險並將新興科技控制措施融入現行組織政策，採用更靈活的資安策略，始能在快速變化且日趨複雜的環境中，保持韌性之餘還能蓬勃發展。以下從本次會議提出值得參考之建議及精進方向：

一、管理面

(一) 建立容許失敗且富有韌性的組織文化

摒棄「零容忍」思維，將失效行為及資安事件視為進步的契機，並正向鼓勵員工知錯能改、敢於創新的勇氣。同時重視「回應」與「復原」能力，透過制定清晰的資安事件應處手冊，並定期模擬演練，有效提升組織韌性。

(二) 加強第三方風險管理

鑒於雲端共享責任之特性，機關應明確界定與供應商之間的責任歸屬，面對供應鏈風險，建議針對第三方制訂完整的應變處理計

畫，包括替代供應商清單、退場策略及應處流程等，以降低損害程度，並與其共享資安管理竅門及實踐指南，奠定穩健的供應鏈生態。

二、技術面

(一) 善用生成式 AI 技術及強化雲端安全

應用生成式 AI 於威脅分析、事件摘要與自動化應對，以提升資安防護效率，並對新型攻擊手法進行模擬演練，使員工熟悉應處程序，同時考慮於雲端環境中部署 AI 功能，協助預測攻擊行為並即時回應，如自動隔離受感染的工作負載或調整權限設置。

(二) 整合資安工具，以集中式管理

建議機關應透過 CNAPP（雲端原生應用程式保護平台）整合 CSPM、CWPP、CIEM 等工具，實現集中化管理，以減少資源分散及平台重疊問題。另建議「左移」資安測試，在軟體開發生命周期之初便考量安全性，提早發現弱點並即時修正，降低整體修復成本。

三、人員認知及培訓

(一) 提升內部技術團隊的專業能力

針對資安技術人員提供如威脅偵測、滲透測試、生成式 AI 應用及雲端安全工具（CSPM、CWPP 等）實作課程，並確保技術團隊保持解決複雜問題的能力。另提供實踐 DevSecOps 之機會，培訓開發人員在建置初期融入安全性原則。

(二) 建立友善工作環境及溝通橋梁

為資安團隊提供紓壓活動，透過「自我照護」機制保持團隊成員的身心健康，並定期審視工作瓶頸與摩擦情況，以優化及精實工作流程。此外，資安長可善用視覺化工具，如結果驅動型指標，向高階管理層傳達資安工作的價值與需求，爭取資源投入及政策支持。

附錄一會場照片

照片 1：開幕主題演講

照片 2：主題演講

照片 3：廠商 DEMO 場域

照片 4：一對一專家諮詢會議室

照片 5：Gartner Showcase 主辦方展示攤位

照片 6：各品牌展示攤位