Microsoft Security

Azure 資安防禦自檢計劃與事件應變指引

台灣微軟資安團隊

Table of Contents

Part 1 春節前 Azure 資安防禦自檢重點

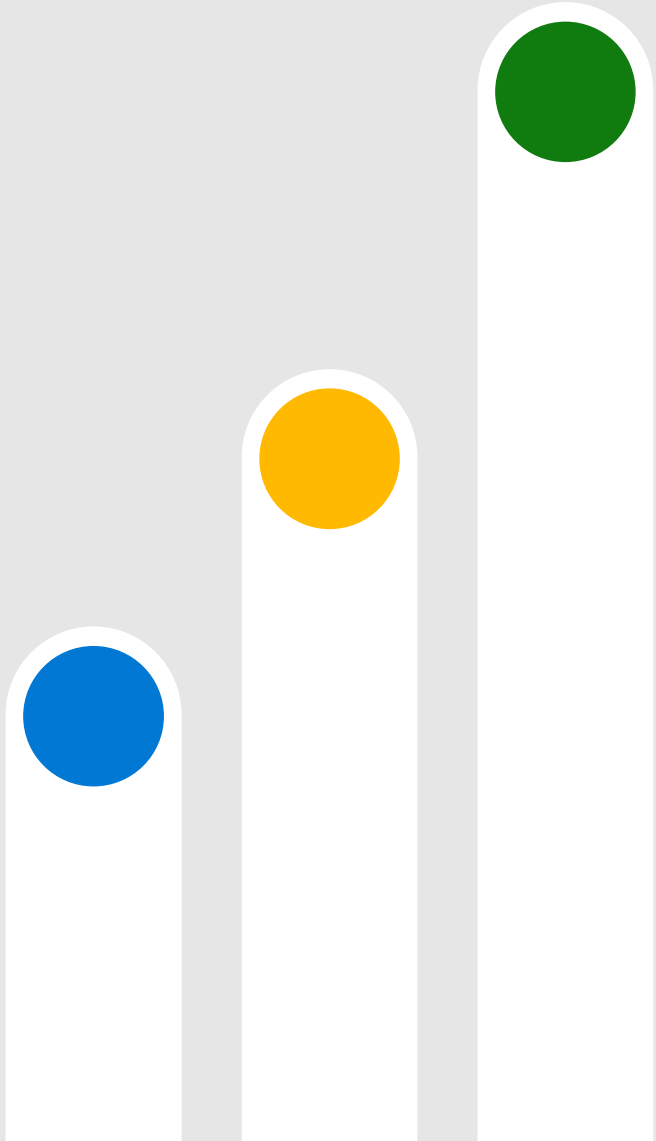
- 身分識別與存取控制
- 網路安全
- 雲端組態安全與威脅偵測
- 虛擬機器端點安全
- 應用程式安全
- 資料安全與備份
- 事件應變計劃準備

Part 2 攻擊事件應變原則

- 偵測與分析、遏制影響範圍並根除威脅

Part 3 Azure 資安持續強化指引

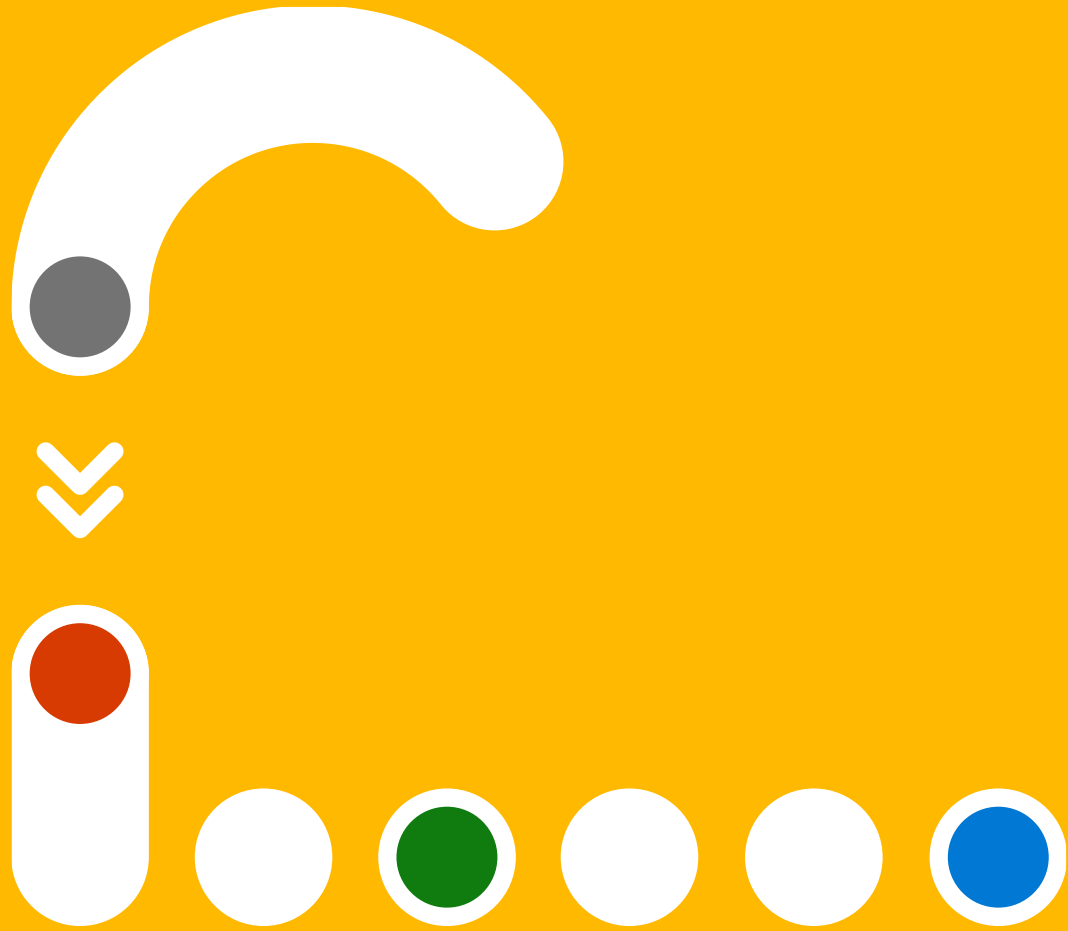
- Azure Well-Architected Framework
- Microsoft Cloud Security Benchmark
- Microsoft Defender for Cloud



Part 1:
Azure 資安防禦自檢重點

關於 **Azure** 環境的防禦重點，我們從各個防禦面向整理出特別關鍵的部份。這份 **checklist** 引導您快速且重點式地檢視目前資安控制措施狀況，確保已建置的防護能持續有效運作，讓您面對潛在攻擊風險預先做好準備。

無恃其不來，恃吾有以待也；無恃其不攻，恃吾有所不可攻也。—《孫子兵法·九變篇》



Azure 資安防禦自檢重點 (1/4)

1.1 身分識別與存取控制

- 對 Azure 訂閱資源具有高權限的帳戶 (e.g. owner, contributor) ，應啟用 MFA 多因素認證機制以提高認證安全強度。 MFA 機制能為使用者登錄過程添加多一層保護，避免攻擊者在其他管道取得洩露的員工密碼後，可以任意存取未經授權的資源。
  - 請留意 !! 近期新聞出現多起雲端攻擊案例，起因於高權限使用者的密碼因釣魚攻擊、不當 Hard-coded 在公開程式碼儲存庫、或是共用相同密碼的第三方網站遭駭，導致攻擊者取得外洩密碼後成功冒充員工存取公司資源，啟用 MFA 將可大幅降低攻擊者成功突破的機率。
  - Reference URL: Azure AD Multi-Factor Authentication overview - Microsoft Entra | Microsoft Learn
- 使用 Azure AD 條件存取 (conditional access) 根據使用者定義的條件進行更精細的訪問控制，例如要求使用者只能在特定條件下，例如公司 IP 範圍、合規設備才能進行登入程序。
  - Reference URL: What is Conditional Access in Azure Active Directory? - Microsoft Entra | Microsoft Learn
- 檢視 Azure AD 與 Azure 資源權限指派是否遵循最小權限或 need-to-know 原則，來指派相關資源存取權限，以避免使用者持續被授予過大的存取權限所形成風險。
- 檢視 Azure AD 是否有創建緊急訪問帳戶 (Emergency Account)，防止管理員帳戶因不可預見的 MFA 機制中斷 (例如自然災害緊急情況，在此期間無法使用手機或網路完成 MFA)，造成使用者無法順利登入 Azure 環境。同時須確保緊急訪問帳戶僅限於實際緊急情況下使用。
  - Reference URL: Manage emergency access admin accounts - Azure AD - Microsoft Entra | Microsoft Learn

Azure 資安防禦自檢重點 (2/4)

1.2 網路安全

- 請確認已關閉 Azure 資源不必要的 public network access (例如 Storage Account, Database, Azure KeyVault) 設定。若資源不當允許公眾 public network 持續存取，則攻擊者有機會透過 brute-force 手法或是從其他管道取得外洩 token 執行登入存取，最終造成資料外洩。
- 請確認 Azure 資源是否有在網路層級做適當隔離措施 (e.g. NSG, Azure Firewall, VNet…)，將高度敏感數據、應用程式、資源配置在隔離的虛擬網路中，並確保相關網路流量有受監控。
- 請確認是否根據需求，對應用程式層 (layer 7) 啟用 web application firewall 以阻擋常見 OWASP top 10 攻擊例如 SQL injection / Cross-site scripting 等等；另外若企業有進階 DDoS 防護需求，請確認 Azure DDoS Protection Plan 是否以啟用 (Azure DDoS 基本版防護預設是自動啟用的)

1.3 雲端組態設定安全與動態威脅偵測

- Defender for Cloud - CSPM 可根據一組預設的安全最佳作法、或是指派的產業合規評估基準，來自動評估目前雲端環境資源的組態設定是否合乎建議的設定值，並將評估結果匯整成一個量化的分數與相關建議供您參考。若要提高安全性，請查看 Defender for Cloud 的安全建議頁面，並實行建議的修正措施來保護每個攻擊面。
  - 請注意! 常見的組態設定疏失可以藉由 Defender for Cloud 及早找出並修補 (e.g. 高權限帳號未啟用 MFA, 網路 RDP port 3389/ SSH 22持續對公眾 Internet 開放存取、資料傳輸時未啟用 https 加密…)
  - Reference URL: Security posture for Microsoft Defender for Cloud | Microsoft Learn
- Defender for Cloud – CWP 能協助您持續監控 vm server 與 PaaS 服務是否有攻擊或是威脅行為正在發生，並產生安全警報通知對應人員，您可以根據環境中所用到的 workload (例如 Defender for Server, Defender for App Service, Defender for DNS, Defender for Storage, Defender for Container…) 啟用對應的進階防護措施 。
  - Reference URL: Enable Microsoft Defender for Cloud's integrated workload protections - Microsoft Defender for Cloud | Microsoft Learn

Azure 資安防禦自檢重點 (3/4)

1.4 虛擬機器端點安全

- ☐ 請確認 VM server 已安裝了作業系統與第三方軟體的相關安全性更新。
- ☐ 請確認 VM server 已安裝防毒軟體與並更新至最新的病毒碼 (virus pattern)。
- ☐ 請確認 VM server 已安裝相關 EDR 解決方案 (e.g. Defender for server)，持續偵測端點所發生的異常行為。
- ☐ 儘可能最小化 VM server 所對外開放的網路 port ，因為攻擊者或常見勒索軟體通常會利用這些對外曝露的服務和開放的 port (e.g. RDP:3389, SSH:22, SMB:445) 在網路中執行或傳播攻擊。除了確認其開放的必要性外，也應確認試圖存取這些服務的對象為可信任的來源。
- ☐ 若您在 Azure 環境上有佈置具有「派送功能」伺服器，例如 Domain Controller 、防毒軟體中控平台、資產管理系統等具有軟體派送功能的伺服器。也需注意安全性更新，並密切觀察其群組原則或工作排程是否不正常異動。針對 AD 可疑活動的偵測，您可選擇使用 Microsoft Defender for Identity 做監控分析。

1.5 應用程式安全

- ☐ 若您的的應用程式程式碼內容包含機敏資訊 (e.g. encryption key、database connection string、API token…) ，請務必做好妥善存取控管，避免未經授權人員可以存取到這些資訊。
  - ✓ 短期強化措施：確保程式碼未不當公開在 public repository、並審核可存取的人員權限。
  - ✓ 長期強化措施：以 Azure KeyVault 存放這些機敏資訊以強化存取控管，降低 hard-coded 所造成的資料外洩風險。
- ☐ 請確認應用程式所引用的函式庫與未包含已知 CVE 安全漏洞 (e.g. Apache log4j 漏洞)。
- ☐ 請確認應用程式上線前執行弱點掃瞄 (SAST/DAST) 所找到弱點已完成修復。
- ☐ 請確認容器使用的 docker image 已執行安全掃瞄 (e.g. 啟用 Defender for Container 強化容器與 AKS 安全)

Azure 資安防禦自檢重點 (4/4)

1.6 資料安全與備份

- 確認高機密性或重要的資料儲存時有做加密保護，確保這些機敏資料萬一遭竊取，攻擊者將很難利用它們。
- 確認敏感資料在傳輸過程中使用加密機制保護 (e.g. 儲存體帳戶, Azure App Service)，以避免中間人竊聽攻擊，避免攻擊者能輕讀取或修改數據。此外應選用到有高強度的 TLS 1.2 或更新版本的傳輸層安全性協定。
- 重要資料必須要事前做備份，對於 Azure Backup 服務所支援的雲端資源 (e.g. Azure VM, SQL server, Azure storage…) 應啟用 Azure 備份，並根據所需的頻率與保留期來配置備份設定；另外對於其他相關程式碼、application artifact、license 也需要做好備份保護。
- 確認備份資料有經定期執行的資料恢復測試，以驗證備份配置和備份資料的可用性能夠正確滿足 RTO (恢復時間目標) 和 RPO (恢復點目標) 中所定義的恢復需求。

1.7 事件應變計劃準備

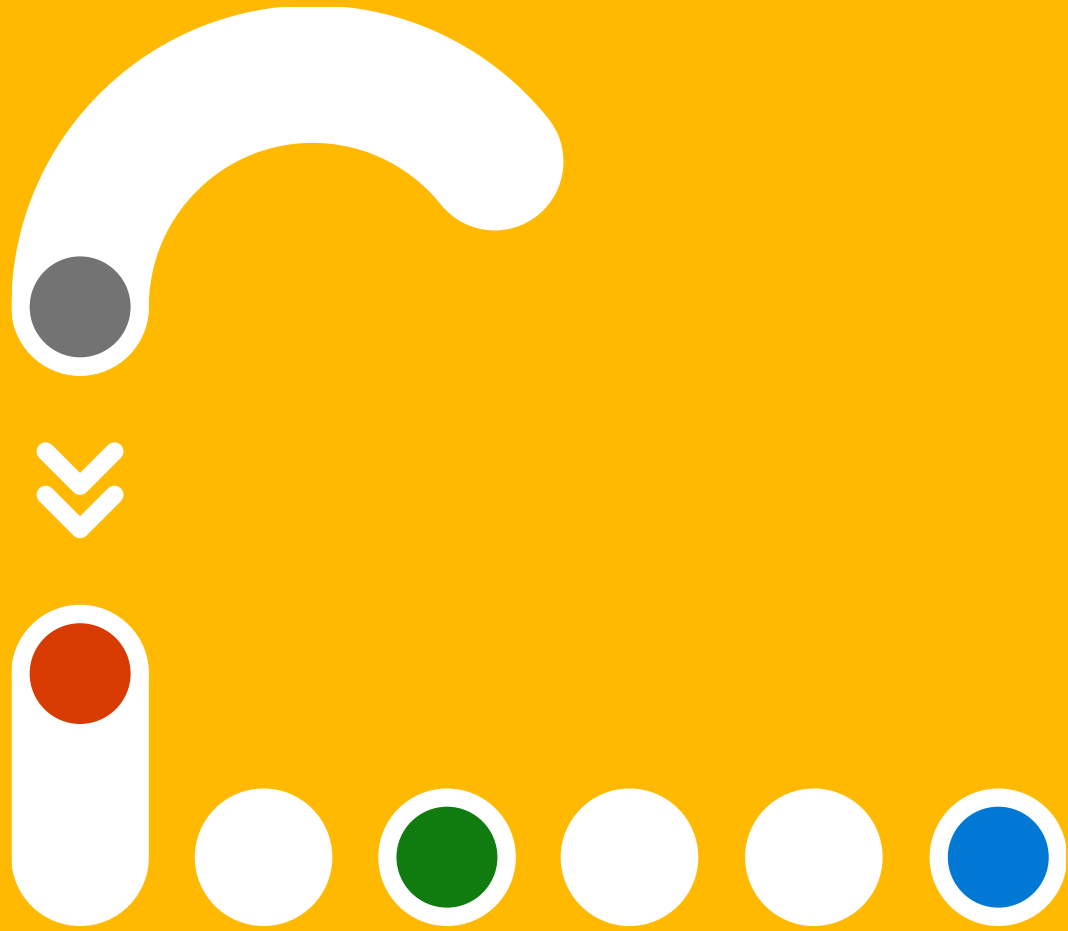
- 確認存在可偵測攻擊的警報機制：面對可能發生的攻擊風險，必須確保攻擊發生的時候，能夠針對遭入侵的雲端資源，產生出高精確度的 alert 警報來提醒管理者與資安團隊，例如前面章節 1.3 所提到可針對特定 workload 來啟用對應的動態防禦措施。
- 確認資安團隊在調查潛在事件時，可以透過 SIEM 平台 (e.g. Microsoft Sentinel) 來查詢到各種關鍵來源日誌 (e.g. Windows Security Event, Network Log)，全面瞭解環境中的事件情況，並追蹤攻擊者在整個狙殺鏈中的活動。
- 確認資安應變計劃已預先建立，並定義好相關 1/2/3 線負責人員及通報流程。另外，資安事件的類別與嚴重層級也要事先定義清楚，當真正有影響的資安事件發生時，能呼叫聯絡人並啟動事件應變程序。

Part 2:
攻擊事件應變原則

如果您的組織成為攻擊的受害者，建議您參考本篇指引原則來做快速因應，從事件調查分析、確定事件的優先緩急順序、到遏制影響範圍並根除威脅，最大程度降低損害。

知己知彼，百戰不殆；不知彼而知己，一勝一負；不知彼不知己，每戰必殆。

—《孫子兵法·謀攻篇》



攻擊事件應變原則 (1/3)

事件調查分析

- 先確定哪些系統或資源受到影響，並立即隔離它們！
- 安全運營團隊在調查潛在事件時，可從 SIEM 平台 (e.g. Microsoft Sentinel) 分析各種數據源，以全面瞭解所發生的情況，並根據來自不同來源的資料關聯出更精確的攻擊事件軌跡，例如:
  - Azure AD sign-in logs & audit Logs
  - Workload access logs (OS level, application level)
  - Network data (NSG flow log, Azure Network Watcher

確定事件的優先順序

- 根據組織事件回應計劃中定義的警報嚴重性和資產敏感度，向安全運營團隊提供相關資訊，幫助他們確定應首先關注哪些事件。例如從 Defender for Cloud 或 Microsoft Sentinel 所產生的每個事件警報都會有嚴重等級，可協助判斷出應首先進行調查的優先順序。
- 對受影響的系統或資源進行分類以進行恢復正常運作，並根據系統重要性來排序恢復的優先序。
- 與您的團隊協商討論，對所發生事件記錄下初步了解與分析結果
- 通報您的內外部團隊及利益相關者，並了解他們可以提供什麼協助來減輕、響應攻擊並從事件中恢復。

攻擊事件應變原則 (2/3)

遏制影響範圍並根除威脅

- 當緩解措施尚未施行前，從受影響的 VM Server，取得磁碟與記憶體的 Snapshot Image。此外，儘可能收集相關日誌檔以及任何可疑的惡意軟體執行檔、攻擊徵兆 (例如，可疑的系統命令、 IP 地址、可疑登錄檔、或其他相關偵測到的檔案)。
  - 注意要把證據保存在安全的地方，以防止遺失或遭到篡改(例如，系統記體 dump 內容、Windows 安全日誌、防火牆日誌資料)
- 參考相關受信任的資安指南 (例如政府單位發佈的指引、MS-ISAC、信譽良好的安全供應商等)，對於特定的勒索軟體種類採取對應的建議措施，以遏制攻擊持續從遭受感染的系統或網路擴散。
- 識別出攻擊初期所涉及的相關系統與帳號 (可能也包括電子郵件帳號)
- SD根據已確認的攻擊結果與受影響的細節，進一步保護任何可能被攻擊者繼續橫向移動的主機。通常攻擊會伴隨大量的 credential/密碼的洩露，因此需要保護相關網絡的連接來源 (例如 VPN, remote access server, single sing-on resources…)，避免這類 credential 盜用登入行為能成功執行。
- 檢驗組織內其他現有的資安偵測防禦系統 (防毒軟體、EDR、IDS、IPS 等) 和相關日誌，這樣做可以找尋到其他系統相關受攻擊證據，或是找到攻擊早期階段所利用的惡意軟體。

攻擊事件應變原則 (3/3)

- 根據系統/服務的關鍵程度做先排順序，以決定重建系統的優先順序 (例如健康、安全、營收相關系統通常具高優先性)，若可能，儘量使用 pre-configured standard image 來做復原重建系統，並從備份回復資料。
- 一旦環境已淨化並完成重建 (包括移除所有攻擊者拿來做持久化攻擊的跳版工具)，接下來對有受攻擊事件影響的系統發出密碼重置要求，並確保任何相關的漏洞和 security control的不足之處都完成修補。這些程序可能包括更新 OS / Application / Library patch、升級軟體套件、或是採取其他先前未採取的資安預防措施。

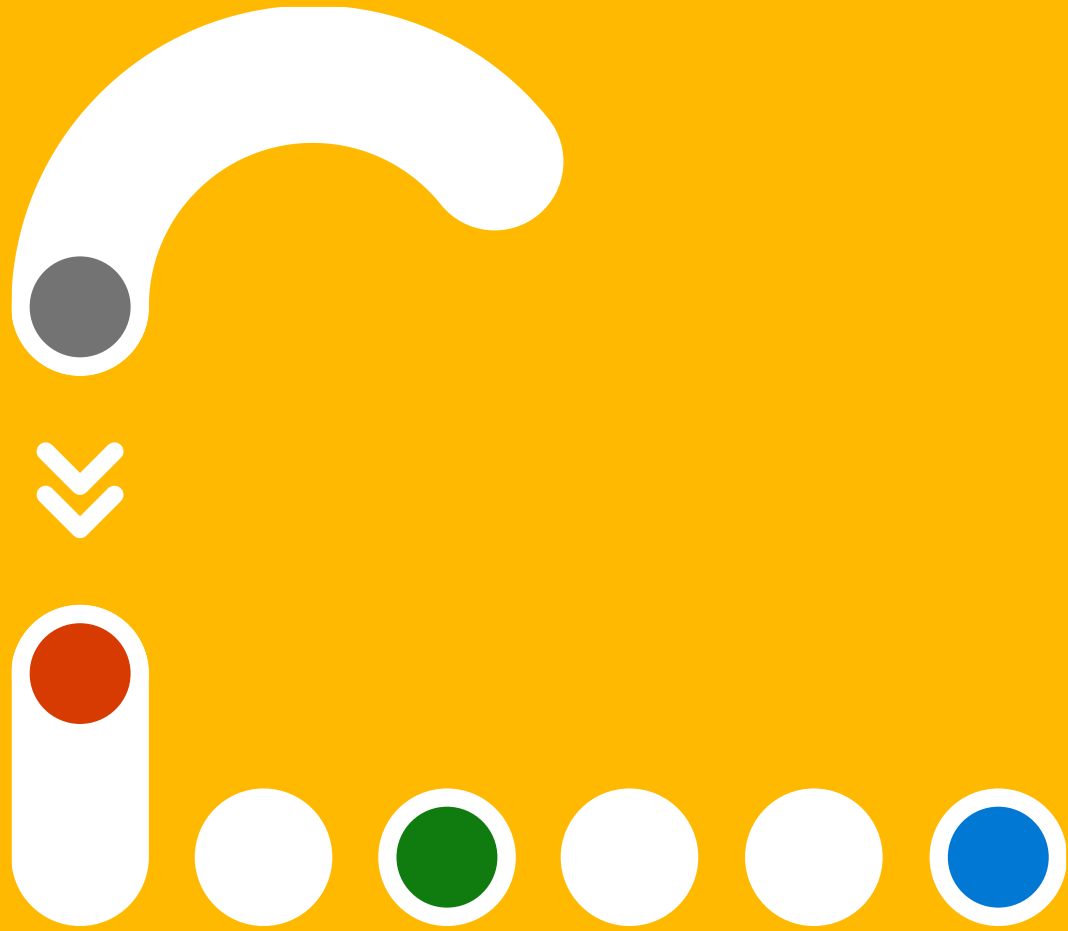
相關攻擊應變參考措施:

- ✓ Microsoft Security Best Practices: Microsoft DART ransomware approach and best practices | Microsoft Learn
- ✓ 台灣電腦網路危機處理暨協調中心: TWCERT/CC 勒索軟體威脅防護專區 (antiransom.tw)
- ✓ US CISA (Cybersecurity & Infrastructure Security Agency): Ransomware Guide | CISA

Part 3:
Azure 資安持續強化指引

資訊安全是複雜的主題，攻擊方的入侵手法不斷變化演進，試圖找到各種可利用的漏洞或錯誤的組態設定。因此，防禦方在佈建雲端環境時，更要依循實證過的資安 **Best Practice** (例如 **Azure Well-Architected Framework**) 來實作，並善用雲原生工具持續評估並監控安全狀態。

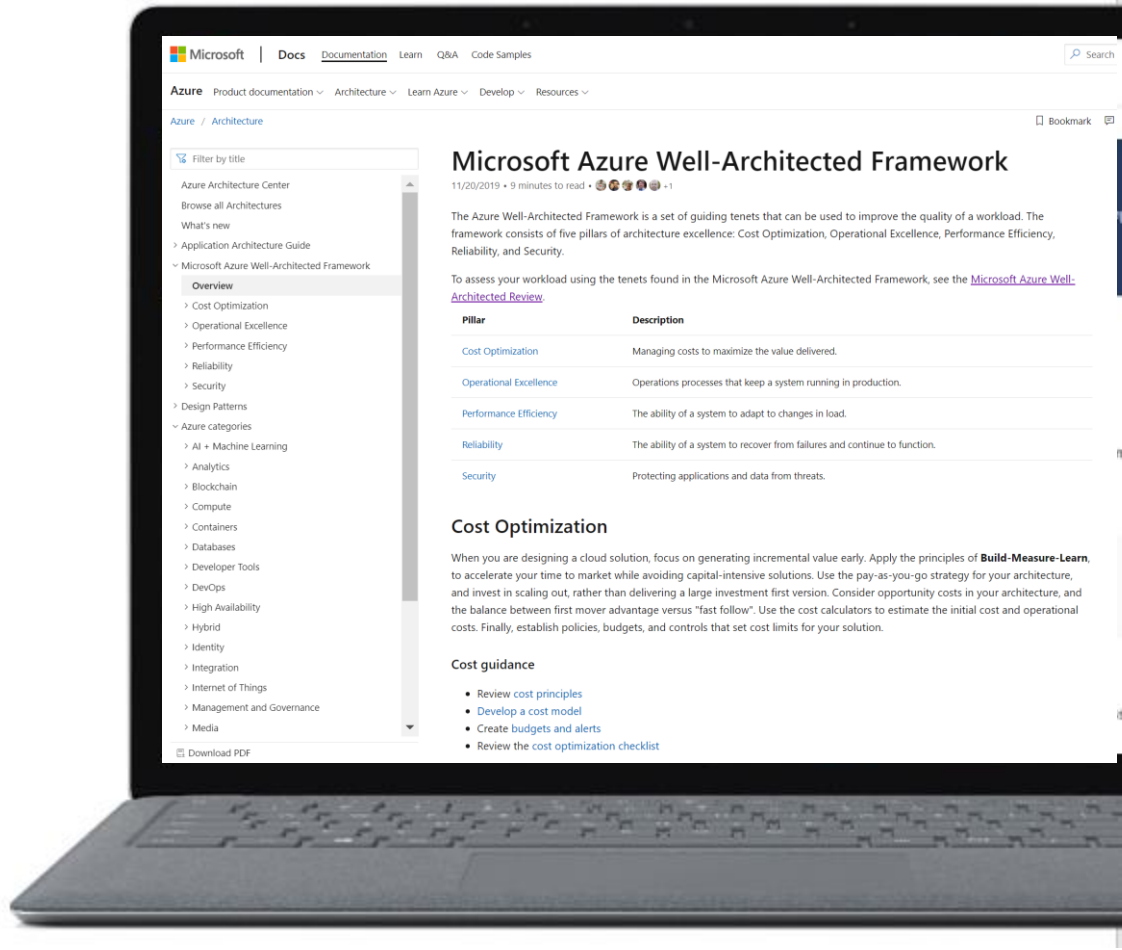
凡戰者，以正合，以奇勝。—《孫子兵法．勢篇》



Azure 資安持續強化指引 (1/3)

Azure Well-Architected Framework

Azure Well-Architected Framework 是一組指導原則，可以用來改善雲端 workload 的品質。此框架包含五大構成要素：可靠性、安全性、成本最佳化、卓越營運、效能。特別是其中安全性的部份，可引導您在設計安全架構上的時候，須考量哪些風險、建議的設計原則，以及如何實作在 Azure 環境上。

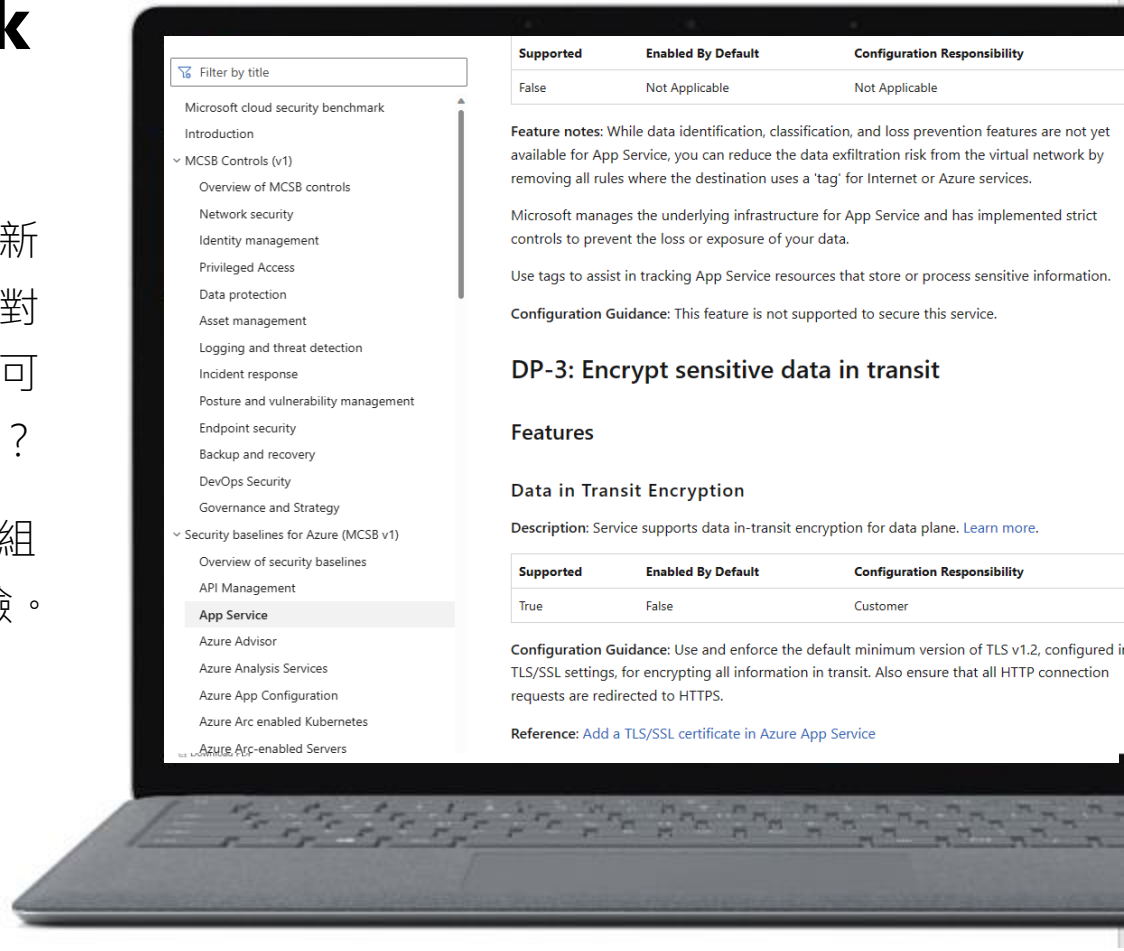


https://aka.ms/wellarchitected/framework

Azure 資安持續強化指引 (2/3)

Microsoft Cloud Security Benchmark (MCSB)

- 雲端服務不斷有新的功能在演進，開發人員正利用它們快速發佈出新的應用程式，且攻擊者也在不斷尋找組態配置錯誤的漏洞。當人員對雲服務相關組態知識不熟悉，或是粗心大意執行錯誤設定，都很有可能埋下一顆不定時炸彈，我們如何知道哪些安全組態要設？怎麼設？
- MCSB 包含了一系列的組態安全建議，透過它您可以更有效的配置組態設定 security baseline，參考最佳實踐以有效降低雲端環境的風險。



[Microsoft cloud security benchmark | Microsoft Learn]

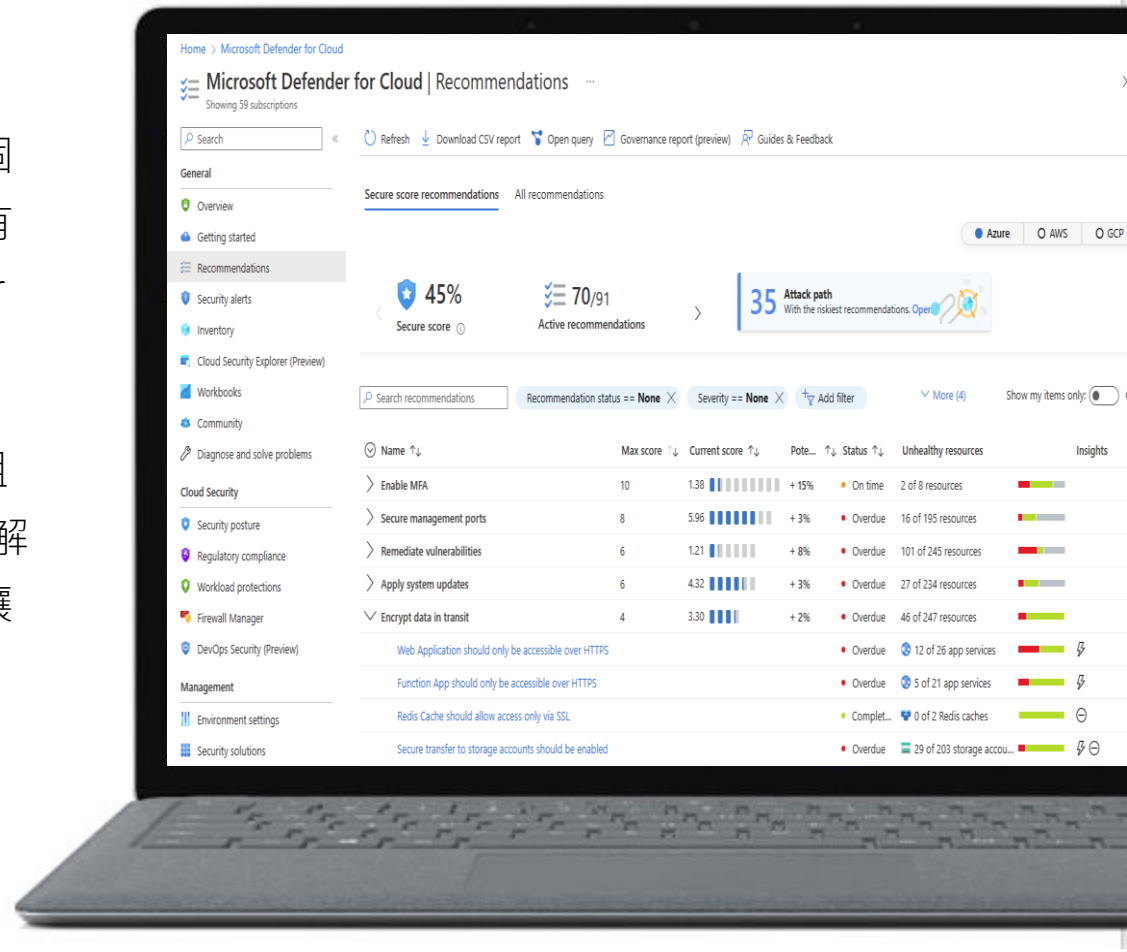
Azure 資安持續強化指引 (3/3)

Microsoft Defender for Cloud

- 當您正苦惱要從什麼地方開始著手強化雲端資料的旅程、能不能有個自動化的工具能幫助您找出雲端組態設定的弱點、甚至直接告訴您有哪些高風險的組態要改? 改在哪些雲端資源上? 怎麼改? Defender for Cloud 絕對是您的最佳武器，協助您在資安強化上取得 Quick Win!

- Defender for Cloud 可以自動且持續地評估您 Azure 訂閱中的資源組態設定，當發現有不當的組態設定時，會協助您 prioritize 出須優先解決的風險並提供實際改善建議，並且將評估結果量化成一個分數，讓讓您一目瞭然地了解當前環境的安全狀況。

[What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud | Microsoft Learn]



Microsoft Security

即刻聯繫微軟團隊
協助您的企業建構資安韌性