IBM Resiliency Orchestration 與 Cyber Incident Recovery

以特別設計的功能保護資料和平台設定，遭受網路攻擊時可迅速復原，方法靈活可靠

產品特色

- 利用無法更動的氣隙隔離模式儲存資料和平台設定檔
- 可迅速偵測 Windows 或 Linux 系統設定中的異常情形，包括 Windows 登錄檔、應用程式設定和裝置設定
- 經過精心設計的資料和平台設定復原機制，作業迅速，有助於減少網路攻擊導致的中斷，或任何其他中斷情形所造成的影響
- 自動化的測試和驗證平台，可在不影響企業系統的情況下頻繁執行測試
- 一目瞭然的流程和報表，有助於因應合規需求

無論是何種規模的企業組織，都不斷受到網路攻擊的嚴重威脅。儘管 IT 安全性團隊防範網路攻擊的能力持續提升，但問題仍在於這類攻擊發生的「時機」（如果尚未發生），而不是發生的「可能性」。網路攻擊所造成的業務中斷會毀損您的關鍵資料和系統設定，而這類中斷事件也和資料竊取或全面 IT 中斷一樣，會對企業組織的財務健康狀況和商譽造成傷害。

每當網路攻擊牽涉到資料加密或特別鎖定資料備份的惡意軟體時，上述傷害便格外顯著。若網路持續曝露於備份與災難復原 (DR) 位置，惡意軟體就能趁機毀損或加密這份資料，讓主要和備份資料都無法使用，進而大幅延誤恢復上線營運的速度。

一般來說，這類損害發生的原因在於現有的 DR 解決方案在設計時並未考量資安事件復原，或者持續受到 DR 功能相關問題困擾：過度依賴人工流程、過時的 Runbook 和測試不足。而最後的結果就是復原作業所花的時間過長、資料復原時間點過舊，或者復原作業本身便失敗。

以功能為考量：專為網路防護所打造

Cyber Incident Recovery 採用 IBM® Resiliency Orchestration 技術且經過精心設計，能夠在網路中斷事件發生時，迅速復原資料和平台設定。Cyber Incident Recovery 專為資安事件復原所打造，可提供下列優勢：

- 在不影響生產環境的情況下輕鬆測試功能
- 加速偵測出資料毀損並迅速因應，縮短停機時間
- 高效率的時間點復原，可最佳化復原點目標 (RPO)
- 無比的擴充能力，可在數分鐘內處理大規模的站台層級偵測與復原作業
- 精簡的能見度和報表功能，有助於因應法規要求

Cyber Incident Recovery 功能是由各種技術架構區塊所組成，這些區塊可提供一個橫跨生產和 DR 環境運算與資料層的平台，進而實現靈活的網路災難復原方式。這個架構涵蓋下列項目：

固定式儲存空間。將不變儲存技術運用在設定資料或應用程式資料的單點多讀 (WORM) 儲存空間上，備份資料儲存後即無法更動，有助於避免毀損並確保可復原性。就應用程式資料而言，這種方式僅能寫入時間點累加變更的新副本，也有助於降低儲存成本。

氣隙隔離防護。對於內有受保護的遠端或 DR 站台備份資料的 WORM 儲存空間而言，網路隔離能夠讓生產環境與 WORM 儲存空間個別獨立。WORM 儲存空間也能限制為只有在資料可供備份時才能存取。這種結合固定式儲存的方法，有助於避免受保護的資料因可周遊網路或專門鎖定備份資料的惡意軟體而毀損。

設定資料驗證。這個元件可協助確保受保護的設定或資料內容完整無瑕且能夠復原。這項流程內建在 Resiliency Orchestration 中，能夠自動偵測系統設定遭到修改，以及與「最佳」版本相左的時間。Resiliency Orchestration 也能夠與客戶提供的應用程式驗證指令碼整合，提供應用程式和資料層級測試。

自動化和協調流程。Resiliency Orchestration 能夠將資料、應用程式、切換和運算基礎架構的端對端復原流程自動化，藉此迅速還原您的 IT 環境。Resiliency Orchestration 可取代傳統人工流程和經過測試及確認的預決工作流程，讓您只要按下按鈕，就能夠復原整個業務流程、應用程式、資料庫或離散系統。這些工作流程會協調復原互連系統和資料所需的多個步驟，控管人為疏失。Resiliency Orchestration 也能夠運用內含 450 多種預設模式且可整併建立工作流程的現有資料庫，加速解決方案實作。

將 Cyber Incident Recovery 用於平台設定

想要全天候經營業務，就必需持續提供以業務關鍵應用程式為根基的 IT 基礎架構：實體伺服器、VM 執行個體、儲存系統和網路裝置。網路攻擊者會破壞這些平台的設定資料，導致業務停擺。

Cyber Incident Recovery 的平台設定功能（如圖 1 所示），能夠將伺服器和裝置設定資料的「最佳副本」，複製到雲端物件儲存空間或 IBM 資料中心內採取氣隙隔離防護的固定式儲存空間，藉此迅速還原服務。生產裝置也會經過檢查，以便偵測設定資料異動。系統會分析異動情況，確認異動是否有效，並且在偵測到可疑的設定資料變更時發出通知。這類通知也可提供來自變更控制管理軟體的相關問題單。

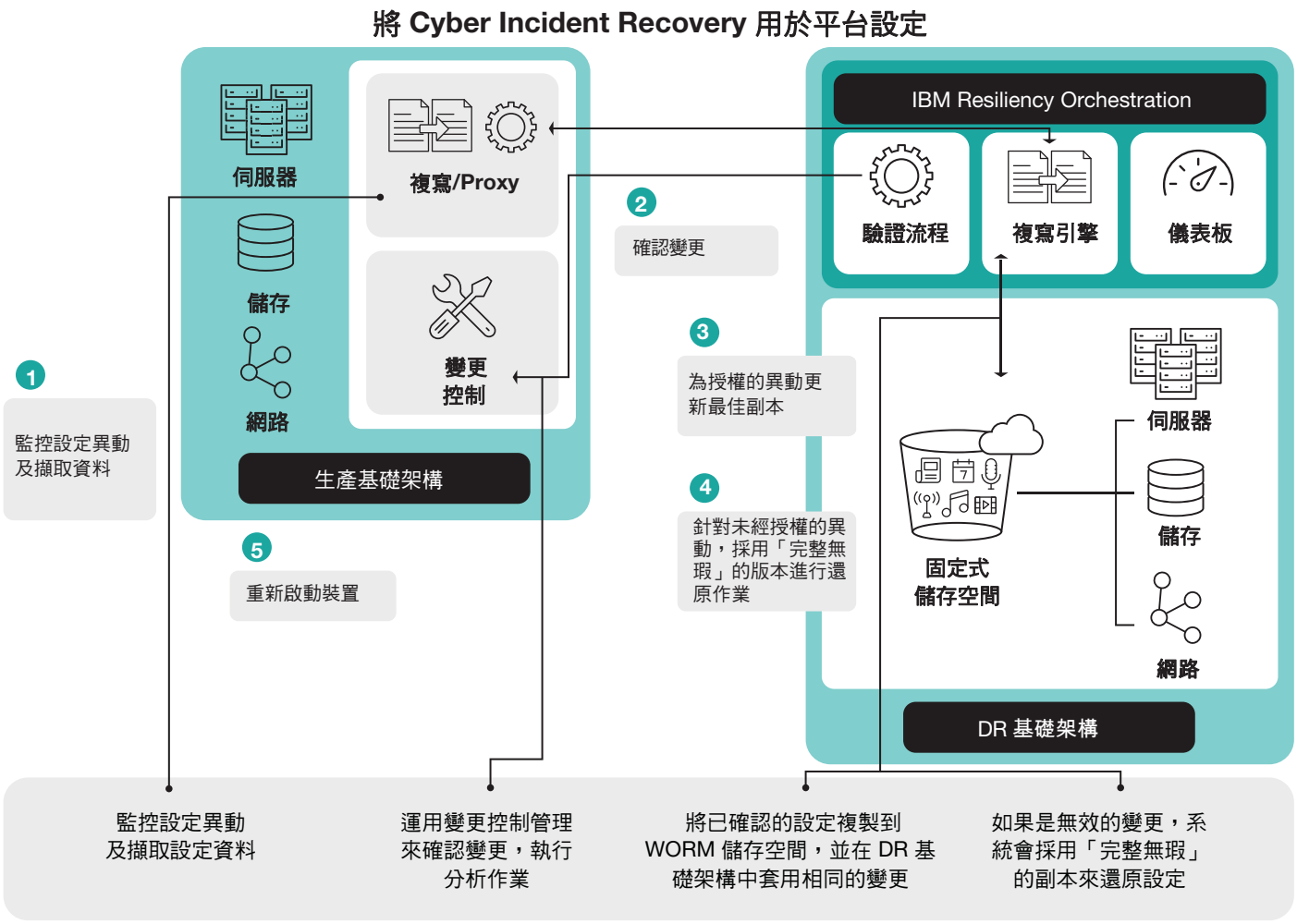

圖 1. 將 Cyber Incident Recovery 用於平台設定，有助於保護實體和虛擬伺服器，以及儲存和網路裝置的設定資料。

在變更確認有效時，系統會將新產生的「最佳副本」複寫到固定式儲存空間中，藉此妥善保護設定資料。如果發現無效的變更，Resiliency Orchestration 會依據預建的政策和適用的管理同意權，採用最新的完整版裝置設定副本迅速還原至生產基礎架構。專屬設定和虛擬機器設定也會還原至完整無瑕的生產基礎架構中。

將 Cyber Incident Recovery 用於資料

Cyber Incident Recovery 的資料功能會針對可造成資料損毀的網路攻擊，展開迅速可靠的復原作業。這項功能運用氣隙隔離式防護和固定式儲存空間來保護資料，同時在客戶的 DR 站台進行協調，快速展開復原作業。

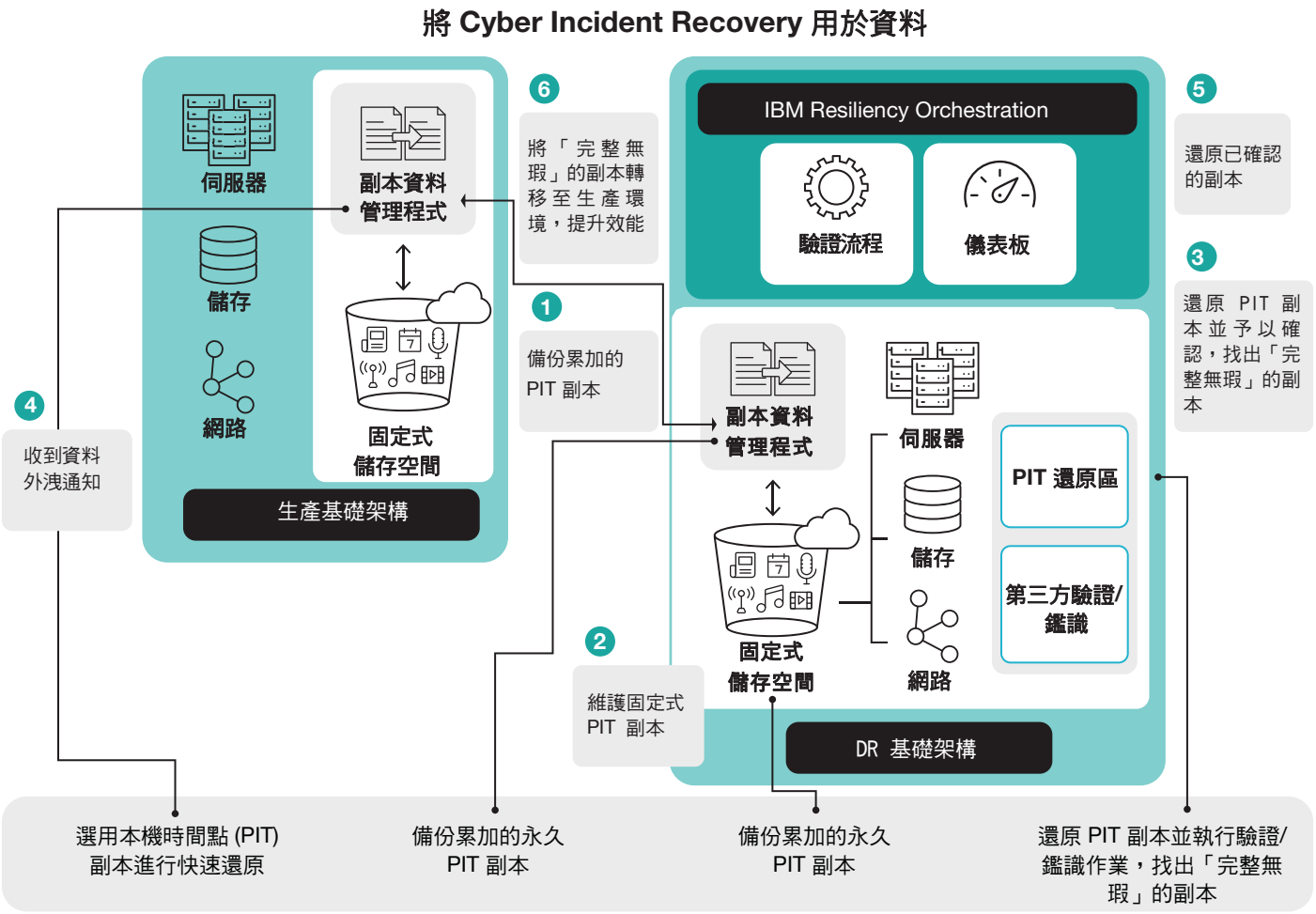

圖 2. 將 Cyber Incident Recovery 用於資料上，不僅能夠以極高的效率備份大量資料，還能確保測試不中斷、還原作業迅速順暢。

Cyber Incident Recovery 專為處理大量應用程式資料而精心設計，採用副本資料管理技術，能夠建立及維護不斷累加的時間點 (PIT) 資料副本。由於這些副本存放在雲端物件儲存空間或具備 WORM 功能的儲存空間內，自然成為無法更動的「永久版」副本。如同圖 2 所示，副本資料管理軟體會將資料複製到災難復原或替代站台，建立 PIT 副本。此外，您也可選擇在生產站台建立及儲存 PIT 副本，實現迅速還原能力。

災難復原管理程式收到資料外洩通知，或發現遭到加密式惡意軟體感染時，會在 DR 站台自動執行 PIT 副本測試，確認資料的可復原性。系統執行測試或驗證程序，找出「完整無瑕」的最新版副本後，就會透過副本資料管理軟體的快速復原程序，在 DR 基礎架構上復原這個副本。您也可在 DR 站台上頻繁執行測試，藉此確保資料的可復原性，同時不影響業務營運。Resiliency Orchestration 有助於確保各平台可同步復原，作業迅速。

簡化管理的儀表板和報表功能

Cyber Incident Recovery 具備儀表板功能（如圖 3 所示），可協助監控平台設定異動和資料變更，也能夠為高階管理人員或董事會提供即時的關鍵資安事件復原資訊，讓他們能夠迅速做出明智決策。資安事件儀表板可提供各種詳細資訊，例如漏洞的數量和嚴重度，並且追蹤不設防的漏洞。資安資料儀表板則可讓您全面透視資安 RPO 偏差、資安 RTO 偏差、快照驗證狀態和當下的資安整備度。

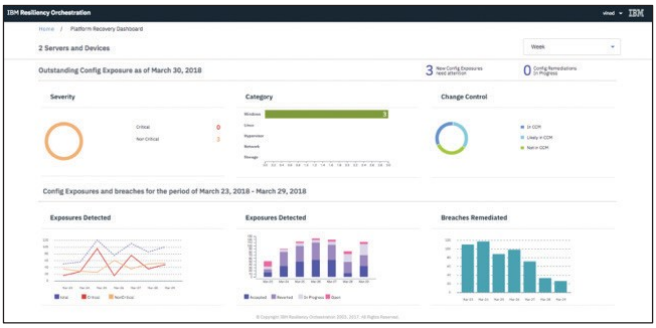

圖 3. 中央儀表板

內建報表模組提供豐富的報表組合，內含網路防護或 DR 狀態，可匯出及分享給主管機關因應合規需求，也包括在企業正常營運期間所擷取的圖表。

為何選擇 IBM？

IBM Business Resiliency Services 累積將近 60 年的豐富經驗，可協助因應全球客戶的備份和復原需求。目前，我們提供的災害復原和資料管理服務已為 9,000 多位客戶提供周全保護；我們每年備份的資料量超過 3.5 艾位元組，且所有資料皆受到妥善管理。IBM 設有 300 個以上的 IBM Resiliency Center，遍及全球 60 多個國家/地區，提供管理化災害復原和資料防護服務；全球更有 6,000 多位 IBM 專家專門提供應變諮詢服務。

詳細資訊

若要深入瞭解 Cyber Incident Recovery，請聯絡您的 IBM 代表或造訪以下網站：

ibm.com/services/business-continuity/cyber-resilience

IBM 全球融資事業部提供數個付款方式，讓您可以購買 IBM 技術來滿足您的業務成長。從採購到處置，IBM 為 IT 產品與服務提供了完整的生命週期管理服務。如需更多資訊，請造訪下列網站：**ibm.com**/financing

IBM Business Resiliency
Services
台灣國際商業機器股份有限公司
台北市 110 松仁路 7 號 3 樓

2018 年 8 月

89017289USEN-02