DELL Technologies

解決方案簡介

Dell PowerProtect Cyber Recovery

為關鍵資料提供靈活的現代化保護機制，使其免受勒索軟體和破壞性網路攻擊的侵擾。

選擇 CYBER RECOVERY 的理由

網路攻擊目的在於入侵您的寶貴資料，包括備份。要在遭受攻擊後恢復正常業務運作，關鍵在於保護您的關鍵資料並以保證的完整性予以復原。

以下是網路韌性解決方案的要素：

資料不變性
建立不可變更的資料複本，以透過多層安全性與控制項，保護資料完整性與機密性。

自動化資料隔離
自動將生產備份環境中不可交換的資料副本，隔離至安全的數位存放庫，並強化存取限制。

智慧分析
使用以 AI 為基礎的機器學習和完整內容索引，搭配強大的分析能力進行自動化完整性檢查，在安全的存放庫內判斷資料是否受到惡意軟體的影響。

復原與補救措施
使用動態還原流程和您現有的災難回復程序，在事件發生後執行復原的工作流程與工具。

解決方案規劃與設計：透過專家指導，選取關鍵資料集、應用程式及其他重要資產，藉此判斷 RTO 和 RPO，並簡化復原作業。

難題：網路攻擊是資料導向型企業的敵人。

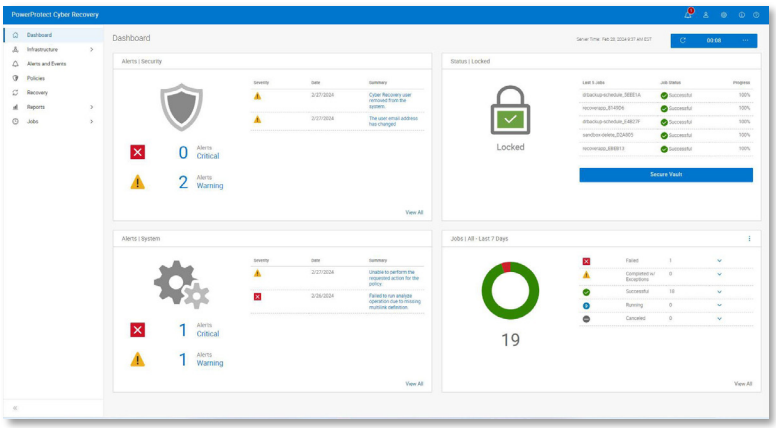
資料是數位經濟的貨幣，也是必須保護、保密，並保持能隨時存取的重要資產。現代全球市場非常依賴跨互聯產品網路的持續資料流，而數位轉型計畫和生成式 AI 的使用率不斷成長，導致更容易暴露各項敏感資訊。

這讓貴組織的資料成為讓網路罪犯覬覦、有利可圖的目標。無論產業或組織的規模大小，網路攻擊都會持續使公司行號和政府機關面臨各種風險，像是資料外洩、因停機而導致營收損失、聲譽受損，以及代價高昂的監管機關罰款。

定有網路韌性策略，對於公司行號和政府機關主管而言，已成為不可或缺的要素，但許多組織對其資料保護解決方案依舊缺乏信心。Global Data Protection Index 的報告指出，79% 的 IT 決策者擔心未來 12 個月內會遭遇營運中斷事件，而 75% 的受訪者則擔心其組織現有的資料保護措施，可能不足以因應惡意軟體和勒索軟體威脅[1]。

解決方案：Dell PowerProtect Cyber Recovery

為了降低網路攻擊所造成的企業風險，以及建立更具網路韌性的資料保護方法，您可以現代化及自動化復原和業務持續性策略，並運用最新的智慧型工具來偵測和防範網路威脅。



PowerProtect Cyber Recovery 提供經實證的靈活現代化智慧型保護機制，可隔離關鍵資料、識別可疑活動，並加快資料復原速度，讓您推動更有智慧的關鍵資料復原方式，藉此快速恢復正常的業務營運。根據 Forrester Consulting 的研究，萬一發生網路攻擊，PowerProtect Cyber Recovery 可協助將停機時間減少 75%，復原時數縮短 80%。[2]

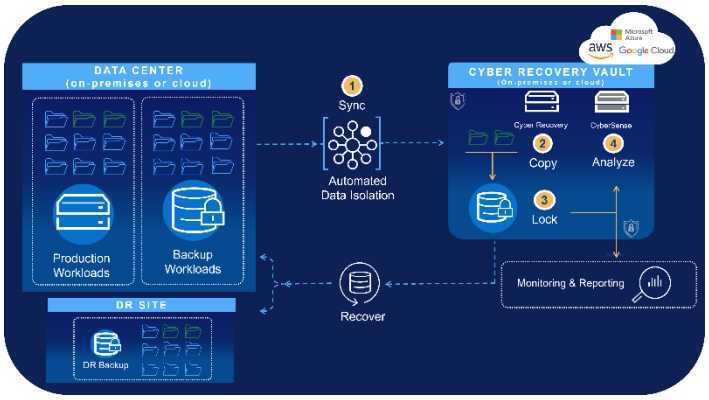
PowerProtect Cyber Recovery – 不變性、隔離機制及智慧功能

不變性 - PowerProtect Data Domain

PowerProtect Data Domain 是 Dell PowerProtect Cyber Recovery 的基礎，具備多層零信任安全性，提供不可變的備份複本，以確保資料完整性和機密性。再加上硬體信任根、安全開機、加密、保留鎖定、角色型存取控制和多因素驗證等功能，可協助確保資料的完整性和復原能力。

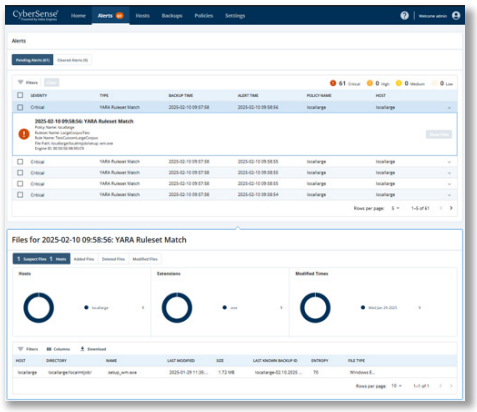
隔離 - Cyber Recovery 存放庫

PowerProtect Cyber Recovery 存放庫是一種隔離的環境，具備多層保護機制，可在遭受網路攻擊時提供復原能力，即使是內部威脅也能因應。其自動化資料隔離功能可將 (同步) 重要備份資料 (包括開放系統及大型主機) 安全地複製至實體隔離的存放庫，遠離生產環境的攻擊面，絕不將管理路徑曝露供威脅發動者得知。接著，它會自動建立不可變的副本，以防資料遭竄改。由於具備不受生產環境影響的專屬管理、網路和服務，需有個別的安全性認證和多因素驗證，才能存取復原和測試作業所需資料。



智慧功能 - CyberSense®

PowerProtect Cyber Recovery 是第一個完全整合 CyberSense® 的解決方案，可在網路復原存放庫的安全性範圍內，以更聰明的方式解決網路威脅，並進行復原工作。CyberSense 超越僅使用中繼資料的解決方案，其完整內容能分析可在遭受攻擊後，以 99.99% 的準確率偵測資料損毀[3]，並推動智慧快速修復。CyberSense 會運用不可變資料備份觀察這段時間的資料變化，並利用 AI 型機器學習來偵測指出勒索軟體攻擊的損毀跡象。CyberSense 可偵測核心基礎結構 (包括 Active Directory、DNS 等)、使用者檔案，以及資料庫中因複雜攻擊所導致大量刪除行為、部份及完全加密行動及其他可疑變更活動。您可以建立自訂閾值警示，如果偵測到損毀跡象，警示儀表板和攻擊後鑑識報告有助於快速診斷攻擊的規模和影響，包括識別乾淨的資料複本以還原您的關鍵系統。自訂 YARA 規則與惡意軟體特徵搜尋，有助於自訂功能並讓組織能主動抵禦網路威脅。



PowerProtect Cyber Recovery - 部署選項

混合式雲端和多雲端環境中的 Cyber Recovery

關鍵數據可以存在於企業的許多不同位置，無論是本地、並置於不同資料中心，還是全球多種雲端和區域中。無論資料位於何處，在需要從網路攻擊中復原時，資料都必須安全無虞。

PowerProtect Cyber Recovery 可透過 *AWS*、*Microsoft Azure* 和 *Google Cloud* 的公有雲市集進行交易，提供快速存取能力，保護雲端中網路復原存放庫裡的資料。PowerProtect Cyber Recovery 可自動同步生產系統與公有雲網路復原存放庫之間的關鍵資料。與標準雲端型備份解決方案不同的是，網路控制項可鎖定管理介面的存取權，而且需要個別的安全性登入資料和多因素驗證才能存取。將資料分散複製到多個雲端，可能會導致安全性和法規遵循風險、潛在的同步問題以及資源成本增加，還可能降低各種環境的可見性，導致缺乏足夠的保護力來抵禦不斷推陳出新的網路威脅。

Dell PowerProtect Data Domain All-Flash Ready Node

隨著關鍵資料持續成長，要確保業務持續性和網路韌性，就必需有能力快速且有效率地從網路事件中復原。正在擴展關鍵資料管理的組織，必須具備從隔離的復原環境 (例如 Cyber Recovery 存放庫) 擷取資料的能力。Dell PowerProtect Data Domain All-Flash Ready Node 提供精簡、節能且符合成本效益的網路復原解決方案，具備增強型 CyberSense 分析和快速還原功能，可符合組織 SLA。藉由減少硬體、空間及使用能源，組織就能提升資料存取速度、提升營運效率，並確保資料完整性，最終減少停機時間與整體維護成本。

PowerProtect Cyber Recovery – 恢復正常作業

復原與補救措施

PowerProtect Cyber Recovery 提供自動化還原和復原程序，可讓您快速安心地將業務關鍵系統重新上線。復原功能會與您的事件應變程序整合。事件發生後，事件應變團隊會分析生產環境以確定事件的根本原因。CyberSense 會提供攻擊後的鑑識報告，讓您瞭解攻擊的深度和廣度，並提供損毀前最後的良好備份集清單。接著，當生產環境準備好復原時，Cyber Recovery 提供的管理工具和技術便可執行實際的資料復原作業。

解決方案規劃與設計

Dell Professional Services for Cyber Recovery 可協助您決定要保護的業務關鍵系統，並可為相關聯的應用程式和服務建立相依性對應，以及還原時所需的基礎結構。此服務亦會產生復原需求和設計替代方案，並找出用來分析、託管及保護資料的技術，以及商業個案和實作時間表。

結論

一直以來，Sheltered Harbor 等產業計畫都使用 PowerProtect Cyber Recovery 來保護美國財務系統內的客戶、金融機構和公眾信心，避免因網路攻擊導致關鍵系統故障，包括備份。Cyber Recovery with CyberSense 擁有數千名客戶，可讓企業領導者放心，並已證明能在發生網路威脅時加快資料復原速度。

在您不幸遭遇網路攻擊後，PowerProtect Cyber Recovery 可快速識別並還原已知良好資料，讓您放心恢復正常業務營運。

該是讓業務回到正軌的時刻了。

深入瞭解
Dell PowerProtect
Cyber Recovery

聯絡 Dell
Technologies 專家

檢視更多資源

加入與 #PowerProtect 的
對話

[1] 根據 Dell Technologies 委託 Vanson Bourne 進行的研究《Global Data Protection Index 2024 Snapshot》(2024 年 Global Data Protection Index 快照)。2023 年 10 月。
[2] 由 Dell Technologies 委託 Forrester Consulting 研究《The Total Economic Impact Of Dell PowerProtect Cyber Recovery》(Dell PowerProtect Cyber Recovery 對整體經濟的影響)，2023 年 8 月
3 根據 Index Engines 委託企業策略集團 (ESG) 發表的報告《Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption》(Index Engines 的 CyberSense 經驗證在偵測勒索軟體損毀的有效率為 99.99%)。 2024 年 6 月

© 2025 Dell Inc. 或其子公司。保留所有權利。Dell 及其他商標均為 Dell Inc. 或其子公司的商標。其他商標是其各自擁有者之商標。