

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

網路攻擊目的在於銷毀、竊取或破壞包括備份在內的寶貴資料。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。貴企業能否安然度過危機？以下是網路韌性解決方案的要素：

資料隔離與管控

一種隔離的資料中心環境，其並未與企業和備份網路連線，且僅限於擁有適當許可的使用者方能使用。

自動化資料複製與實體隔離在安全的數位存放庫與程序中建立不可變更的資料複本，藉此在生產/備份環境和存放庫之間建立可操作的實體隔離區。

智慧型分析與工具機器學習與完整內容索引功能，可在存放庫的安全範圍內提供強大的分析功能。自動化完整性檢查，以判斷資料是否受到惡意軟體和工具的影響，並視需要支援補救措施。

復原與補救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

專家指導以選取關鍵資料集、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

資料是網際網路經濟的貨幣，也是必須受到保護、保密且可隨時取用的關鍵資產。現今的全球市場依賴於跨互聯網路的持續資料流，而數位轉型工作使得更多敏感資料面臨風險。

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，已成為不可或缺的元素，但許多組織對其資料保護解決方案依舊缺乏信心。根據 [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。

那麼，您該如何保護組織、客戶、員工及其寶貴的資料？

解決方案：Dell PowerProtect Cyber Recovery



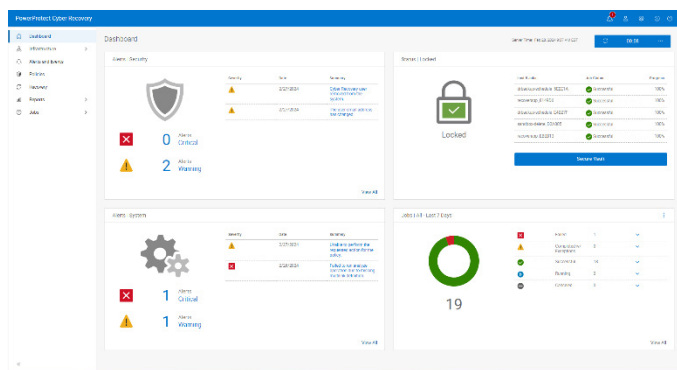
為了降低網路攻擊所造成的企業風險，以及建立更具網路韌性的資料保護方法，您可以現代化及自動化復原和業務持續性策略，並運用最新的智慧型工具來偵測和防範網路威脅。

Dell PowerProtect Cyber Recovery 提供經實證、靈活的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，讓您快速恢復正常的業務營運。

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

Cyber Recovery 存放庫

PowerProtect Cyber Recovery 存放庫具備多層保護機制，提供對抗網路攻擊的彈性，即使是內部威脅也能因應。本產品可移動關鍵資料使其遠離攻擊面，將其實體隔離在資料中心的受保護部分，且需要個別的安全性認證和多因素驗證才能存取。其他保護措施包括自動化實體隔離機制，以隔離網路並消除可能遭到入侵的管理介面。PowerProtect Cyber Recovery 可自動化生產系統 (包括開放式系統和大型主機) 以及存放庫 (使用鎖定保留原則建立不可變複本) 之間的資料同步。如果發生網路攻擊，您便可快速找出無汙染的資料複本、還原關鍵系統，並讓業務恢復正常運作。



CyberSense

PowerProtect Cyber Recovery 是第一項完全整合 CyberSense 的解決方案，新增了智慧型保護層，可在攻擊滲透到資料中心時找出資料損毀位置。這項創新方法提供完整的內容索引功能，並使用 AI 機器學習 (ML) 來分析 200 多個內容型統計資料，並找出勒索軟體造成的損毀跡象。CyberSense 發現損毀的可信度高達 99.5%，協助您識別威脅並診斷攻擊媒介，同時保護業務關鍵內容，且一切都在存放庫的安全機制之內進行。

復原與補救措施

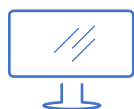
PowerProtect Cyber Recovery 提供自動化還原和復原程序，可讓您快速安心地將業務關鍵系統重新上線。復原功能會與您的事件應變程序整合。事件發生後，事件應變團隊會分析生產環境以確定事件的根本原因。CyberSense 也會提供攻擊後的鑑識報告，以便讓您瞭解攻擊的深度和廣度，並提供損毀前最後的良好備份集清單。接著，當生產環境準備好復原時，Cyber Recovery 提供的管理工具和技術便可執行實際的資料復原作業。這會自動建立用於復原或安全性分析作業的還原點。

解決方案規劃與設計

選購的 Dell 諮詢服務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，以及予以還原所需的基礎結構。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。

為了保護您的重要資料免於網路攻擊，需要有經實證的現代化靈活解決方案。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。

¹ 根據 Dell Technologies 委託 Vanson Bourne 於 2023 年 10 月進行的研究，「Global Data Protection Index 2023 Snapshot」(2023 年 Global Data Protection Index 摘要)。



深入瞭解 Dell
PowerProtect Cyber
Recovery



連絡
Dell Technologies 專家



檢視更多資源



加入與 #PowerProtect 的
對話