報告摘要

使用安全隔離存放庫、AI 機器學習 (ML) 分析軟體等提高網路韌性，並保護資料免受網路勒索軟體威脅

利用 Dell Technologies PowerProtect Cyber Recovery with CyberSense

隨著網路威脅的頻率不斷增長和攻擊方式日益演變，資料保護計畫必須採取有效方法由淺入深全面保護和分析所有 IT 元件。Dell PowerProtect Cyber Recovery 可協助保護最關鍵的敏感資料，而在面對網路攻擊或其他破壞性事件時，也能確保妥善復原。

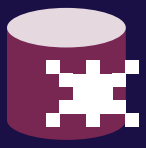
Dell PowerProtect Cyber Recovery 是一款資料管理、保護及復原解決方案，可協助組織保護資料和應用程式免受勒索軟體、破壞性網路攻擊及意外事件的侵害。該解決方案使用多副本方法，這表示在備份後，會將這些備份複製到獨立的儲存裝置保護和分析。PowerProtect Cyber Recovery 由許多元件組成，包括一個或多個儲存存放庫，這些元件可能位於區域的 PowerProtect DD (以前稱為 Data Domain) 裝置中，或者透過軟體定義的 Dell APEX Protection Storage for Public Cloud (以前稱為 DD Virtual Edition) 位於雲端中。無論是哪種情況，隔離存放庫在運作上都是採實體隔離，也就是與生產環境隔離；在區域環境中可能是實際層面的實體隔離，在 APEX 環境中可能就是邏輯上的實體隔離。因此，不肖份子或未經授權的使用者就難以登入並破壞備份複製。

PowerProtect Cyber Recovery 還包含 CyberSense；這是一個全面自動化的整合式智慧安全性分析引擎，可自動掃描隔離存放庫的資料、檔案、資料庫及影像，尋找勒索軟體攻擊所造成的損毀跡象。CyberSense 提供完整的內容分析；從檔案中獲取觀察資料，做為其人工智慧 (AI) 機器學習 (ML) 模型的輸入內容；偵測在核心基礎架構 (包括 Active Directory 和 DNS)、使用者檔案及關鍵生產資料庫中發生的大規模刪除、加密和其他可疑變更等惡意活動，這些活動可能表示受到勒索軟體或破壞性攻擊。當 CyberSense 偵測到損毀模式時，會在 PowerProtect Cyber Recovery 操作面板中產生警報，提供有關攻擊規模和影響的額外資訊。[1]

PowerProtect Cyber Recovery 可幫助組織減少網路攻擊、從不同位置備份多份資料來增強資料復原能力、降低停機時間，並且讓業務持續運作。本報告使用可公開取得的資料來突顯重要的資料保護特色和功能，並展示我們對 CyberSense 進行競爭產品分析的結果。

保護敏感資料

將備份複製到實際和邏輯上的安全隔離存放庫時，為傳輸中的不可變資料加密



偵測 SQL Server 頁面損毀

CyberSense 發現競爭解決方案未發現的感染

識別未損毀的備份複製

CyberSense 識別出最近未受感染的備份複製，可用於復原

安全性

Dell PowerProtect Cyber Recovery 提供多種安全性功能，可協助保護關鍵資料免受勒索軟體和其他複雜威脅的侵害、防止未經授權的使用者存取敏感資訊，並且能夠快速恢復，讓組織可以恢復正常運作。

PowerProtect DD 應用裝置的特色和功能對於 PowerProtect Cyber Recovery 解決方案提供的安全性、完整性及恢復至關重要。這些功能包括保留鎖定、DDBoost、角色存取控制 (RBAC)、雙重授權等。

隔離

資料隔離是指透過設置障礙或邊界將資料分開並限制存取，防止未經授權存取。隔離通常會使用臨時的網路連線，而不是持續性連線。

資料隔離可避免關鍵資料連線到受感染的網路，因為不肖份子可能透過該網路嘗試修改設定、刪除資料、變更策略或測錄網路流量以取得使用者憑證。隔離還可協助減少攻擊面，降低不肖份子獲得存取權和控制的機會。此外，組織可以只將存取權授予取得授權的人員，協助避免未經授權的使用者覆寫資料。

除了我們提到的功能外，PowerProtect Cyber Recovery 還能夠以實體隔離的形式提供實際和邏輯隔離，協助保護資料。實體隔離的區域 PowerProtect DD 可當作隔離存放庫使用，這樣生產環境的使用者或系統就無法存取元件，而且隔離存放庫會實際中斷與生產網路的連線。[2] 透過禁止從生產網路存取復原環境，組織就可以減少攻擊面。

不變性*

維持備份不變 (即為唯讀)，協助確保組織可以信賴這些復原用的備份。在運作上，不變性有助於維護資料的真實性和可靠度。DD 系統 (包含 PowerProtect Cyber Recovery 解決方案中的 DD 系統) 可以使用稱為 MTree 的檔案系統邏輯分區，來為儲存資料的方式提供不變性。這些解決方案也可使用 MTree 複製功能，透過 DDBoost 通訊協定將不可變資料副本從生產 DD 複製到隔離存放庫的另一個 DD。[3]

*Dell 的產品旨在支援客戶保護其重要資料。與所有電子產品相同，資料保護、儲存和其他基礎結構產品可能會出現安全漏洞。客戶務必在 Dell 提供安全性更新後立即安裝。

CyberSense

妥善保護資料需要能夠提供各層級安全性的全面性策略。儘管 Dell PowerProtect Cyber Recovery 解決方案具有各種自我修復、安全性、不變性及隔離功能，但不易察覺的攻擊仍可能深入到企業基礎架構中 (例如資料備份層級)，在生產資料或整個使用者群組遭到入侵之前可能都偵測不到。Dell PowerProtect Cyber Recovery 解決方案提供抵禦網路攻擊的最後防線，並透過 CyberSense 提供加速復原的有效方法。

我們針對規模相似的應用裝置測試了 CyberSense 和競爭對手 (我們稱之為「供應商 X」) 資料管理平台功能類似的工具。在這項測試中，我們發現PowerProtect Cyber Recovery 能夠偵測到 SQL 資料庫頁面中的感染，但供應商 X 解決方案偵測不到。相較於供應商 X 解決方案，PowerProtect Cyber Recovery 判斷資料損毀情況所需的備份數也比較少。

1. Dell，「CyberSense® for PowerProtect Cyber Recovery」，2023 年 9 月 8 日存取，https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf。
2. Dell，「MTree replication」(MTree 複製)，2023 年 9 月 11 日存取，https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3。
3. Principled Technologies，「Dell EMC Cyber Recovery protected our test data from a cyber attack」(Dell EMC Cyber Recovery 保護測試資料免受網路攻擊)，2023 年 8 月 21 日存取，http://facts.pt/rkew01n。

▶ 檢視本摘要的原始英文版本

閱讀報告 ▶

Principled Technologies®

Facts matter.®