使用 Dell PowerProtect Backup Services 加快遭遇勒索軟體後的復原速度

從勒索軟體復原僅需數小時，無須耗費多日

重要功能

勒索軟體攻擊頻率日益升高、手法不斷精進，且代價也在不斷攀升

- 無法快速識別和還原未受感染的備份或檔案
- 從回復資料中傳播和再次感染
- 資料丟失，無法回復完整資料集
- 難以協調事件回應協調流程
- 需要更快的 RPO/RTO 時間
- 業務停機時間代價高昂，會導致收入損失和品牌商譽受損
- 因資料保護不充分而遭到法律及監管罰款

挑戰

勒索軟體對每家企業都是嚴重的威脅。網路攻擊頻繁發生，並可能造成災難性的損害。79% 的組織擔心會在未來 12 個月內遭遇服務中斷事件1。丟失資料的公司有可能在災難發生後申請破產。勒索軟體攻擊不僅發生得更頻繁，而且技術也變得更加先進和昂貴。

解決方案

快速可靠的回復甚至消除了所有考慮支付贖金的可能性。但是，當發生安全事件或網路攻擊時，組織需要在回復之前瞭解損害範圍和根本原因。憑藉 24 小時全年無休的原始、實體隔離工作負載和虛擬機器快照、對使用者和資料異常的持續監控、與安全性工具整合，以及自動復原乾淨資料，您可以改善安全性狀態並將毀滅性的磨難轉變為可生存的事件。

功能

針對所有工作負載：

• 確保您擁有 24 小時全年無休的不可變更實體隔離備份

• 使用 RPO/RTO 僅需數小時即可在內部部署或雲端回復乾淨資料，無須耗費數日

• Managed Data Detection and Response (MDDR) 服務提供 24 小時全年無休的備份環境即時監控

• 使用生產部門的資料並建立許多資料副本，並儲存在多個位置，以回復跨 AWS 地區/帳戶的工作負載和 VM 時，會使組織面臨極大的風險。

加快關鍵工作負載遭遇勒索軟體後的復原速度：

• 使用基於 ML 的演算法監控和主動檢測異常

• 透過 SIEM 和 SOAR 整合協調回應和復原活動

• 復原之前先掃描惡意軟體快照，並從備份中刪除受感染的快照和檔案

• 從黃金快照的指定時間點自動復原所有檔案最新的乾淨版本

保護

防止勒索軟體損害的第一步，是確保您有實體隔離且不可變更的資料副本。Dell PowerProtect Backup Services 建立在具高復原能力的雲端基礎架構上，使勒索軟體無法對備份軟體加密。零信任架構 (包括多因素驗證、信封加密和個別帳戶存取權) 確保勒索軟體無法使用受侵害的主要環境憑證來竄改備份環境或資料。最後，預防超額刪除和軟刪除 (資源回收桶) 功能提供另一層安全保護，以防止備份遭到刪除。

偵測

儘快檢測出勒索軟體能幫助事件回應團隊進行處理並預防感染傳播。Dell PowerProtect Backup Services 加快遭遇勒索軟體後的復原速度模組提供安全命令中心，用於監控備份環境的狀態。藉由存取洞察和異常檢測，您可以快速識別整個環境和資料中的異常活動。查看使用者及 API 之所有存取嘗試的位置、身分和活動資訊。使用專有的 ML 演算法檢測異常，對異常資料活動 (例如刪除、加密等) 發出警示。該演算法會學習您特定備份環境的模式，因此不需要任何規則設定或調整。其也會採用以熵為基礎的洞察，來減少誤報

回應

當安全性或 IT 分析師檢測到可疑活動，或更糟的情況，確認已發生勒索軟體事件，回應速度即變得極為重要。儘管有許多寶貴的主要環境安全性工具可用於檢測和回應協調流程，但來自次要資料 (備份系統) 的分析數據和變更記錄資料，可改善調查、回應和取證活動。Dell PowerProtect Backup Services 遭遇勒索軟體後的復原速度模組提供健全的 API 整合開箱即用，讓您可輕鬆將解決方案融入整體安全性生態系統中。使用 SIEM 和 SOAR 解決方案的協調程序回應活動，可自動完成隔離受感染系統或快照，或者根據預先決定的勒索軟體手冊掃描 IOC 備份，從而大幅縮短平均回應時間 (MTTR)。

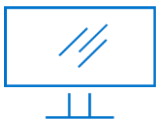
復原

在最初的回應階段後，緊接著是艱苦的復原作業。對許多公司而言，這是一個要手動作業且曠日廢時的過程。惡意人士和勒索軟體的停留時間可能從數週到數月不等，因此難以得知要回溯到多久之前的乾淨資料。即使在找出最佳快照後，隱藏的惡意軟體也可能導致再次感染。但是，

大多數的業務用戶無法接受 2 週前的復原點。而尋找與驗證遭遇勒索軟體事件之後更近期的資料必須要手動作業、乏味且通常難以克服。

Dell PowerProtect Backup Services 透過有效的備份架構和自動化工具來加速復原，從而減輕這一負擔。Dell PowerProtect Backup Services 雲端平台會將工作負載直接備份到雲端，準備好可在發生勒索軟體攻擊時立即進行復原。

加快遭遇勒索軟體後的復原速度模組透過確保復原資料的潔淨，讓您能安心進行復原。您可以使用內建的防毒檢測功能或使用您自己的取證調查或威脅情報來源，來掃描惡意軟體和 IOC 的快照。在復原之前掃描快照可以排除再次感染。



深入瞭解 PowerProtect Backup Services

聯絡Dell Technologies 專家