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。

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 裝置的特色和功能，對於 PowerProtect Cyber Recovery 解決方案提供的安全性、完整性及復原至關重要。這些功能包括：

1. 不變性
   無法修改或刪除不可變的資料，只能寫入。DD 系統可以在生產系統和網路存放庫中寫入不可變的備份，這表示即使惡意人士以某種方式取得備份系統存取權，也無法修改、刪除或入侵現有的受保護副本。[2] DD 系統在生產環境中建立的任何備份，都會立即成為不可變的備份，並可供 IT 複製到存放庫，以增加安全性。本報告的下一部分將進一步探討不變性。

2. 保留鎖定
   DD Retention Lock 功能可讓資料在預定期間內不可變。一旦解決方案將資料置於保留鎖定下，在鎖定期間到期之前，任何使用者或系統都無法變更、刪除或修改資料。[3]

   Retention Lock 具有管控和法規遵循模式。其法規遵循模式可讓客戶滿足許多法規標準。獨立第三方證明 DD Retention Lock 符合 SEC 規則 17a-4(f)(2) 和 240.18a-6(e)(2) 以及 FINRA 第 4511(c) 條規定的儲存要求。[4]此功能還有助於支援組織努力遵守 FDA 21 CFR Part11、Sarbanes-Oxley Act、IRS 98025 和 97-22、ISO Standard 15489-1，以及 MoREQ2010。[5]

   由於攻擊者可能會嘗試變更系統時鐘，藉此規避 Retention Lock，這就會導致解決方案比預期更早刪除檔案。有鑑於此，DD 提供內部安全時鐘。系統會定期比較安全時鐘和系統時鐘的時間。如果兩者在單一日曆年度中累積了兩週的偏差，系統會自動停用 DD 檔案系統 (DDFS)，以避免資料存取。[6]

3. 使用 **DDBoost** 對流動中資料進行加密
   流動中資料可能會帶來重大的安全性風險。DDBoost 可讓備份伺服器或應用程式用戶端，僅將唯一資料區段 (而非所有資料) 跨網路傳送至 DD 裝置，以限制流動中的資料量。此外，組織可以使用 DDBoost 通訊協定 (含或不含憑證)，來驗證和加密資料。憑證提供更安全的資料傳輸功能。流動中資料加密可讓應用程式加密流動中資料備份，或透過系統的 LAN 還原資料。用戶端可以使用傳輸層服務 (TLS)，來加密用戶端和系統之間的工作階段。[7]

4. **Data Domain Operating System (DD OS)** 安全性
   DD 安全性功能亦可延伸至作業系統。為了安全起見，DD OS 會在 Bash shell 上，實作自訂存取控制和限制。在受限制的 Bash shell 模式下，僅允許使用者根據角色和任務，執行一組必要的預先定義命令。為增強資料完整性，DD OS 可以封鎖未定義命令，這些命令會對系統進行未經授權或非預期的修改。[8]

5. **角色型存取控制 (RBAC) 與 DD 檔案系統 (DDFS) 安全性**
   DD 系統會使用多種措施，來保護檔案系統內的檔案和資料。首先，DD 系統提供 RBAC，讓系統管理員能夠定義具特定權限的角色，並指派使用者這些角色。只有具備適當權限的授權使用者，才能存取裝置及其資料。這可確保使用者僅可存取執行任務所需的功能和資料，進而降低未經授權的存取或意外資料外洩的風險。

   DDFS 也使用雜湊進行資料完整性驗證。雜湊將特定鍵或字串轉換為另一個值。裝置將唯一資料區塊儲存在邏輯儲存容器中，而檔案系統則會對資料區塊和容器進行雜湊處理。系統擷取資料時，會重新計算資料的雜湊值，以比對 DDFS 中儲存的雜湊值，這有助於確保沒有任何內容遭到篡改或損毀資料。[9]

6. **雙重角色授權**
   當組織啟用 DD Retention Lock 法規遵循模式時，DD 系統會以雙登入的形式，提供額外的系統管理安全性。這表示，系統管理員和第二個授權使用者 (例如安全人員) 必須一起登入。在保留期間到期前，DD Retention Lock 法規遵循模式的雙登入機制可作為保護功能，防止任何可能危及鎖定檔案完整性的動作。[10]

7. **資料無損架構**
   DD OS 提供端對端驗證、故障避免與遏制、持續故障偵測與修復，以及檔案系統復原能力，以防範軟硬體故障導致的資料完整性問題。DD 系統收到來自備份軟體的寫入要求時，會先計算資料區段的指紋，並與系統中儲存的現有指紋進行比較，以分析資料區段作為備援使用。系統僅將唯一資料區段及其指紋儲存到磁碟。DD 會持續從磁碟讀取資料、重新計算其讀取到的指紋，並確保其與磁碟上的指紋相符。在此過程中，如果系統偵測到毀損 (例如讀取到的內容與寫入的內容不符)，DD 系統會執行自我修復程序，以重建毀損的資料，並將資料還原至正確的狀態。此外，自我修復程序有助於保護系統，免於可能影響平台完整性的其他變更。

不變性*

維持備份不變 (即為唯讀)，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。

*Dell 的產品旨在支援客戶以保護其重要資料。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性漏洞。客戶務必在 Dell 提供安全性更新後立即安裝。

運作方式

在使用 MTree 儲存資料的方式上，DD 系統提供不變性。MTree 是檔案系統的邏輯磁碟分割。當應用程式將資料寫入 MTree 時，DD 系統會使用稱為「快速複製」的功能，將原始 MTree 的時間點副本，建立至新的 MTree。在新的 MTree 中，DD 會套用保留鎖定，以確保使用者或程序無法在保留期間定義的期間內，刪除新的 MTree。新的 MTree 是不可變的資料副本，而且獨立於原始 MTree。[11]

PowerProtect Cyber Recovery 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 複製到存放庫的另一個 DD。[12] 在兩個 DD 之間的初始同步中，此解決方案會將所有資料複製到存放庫 DD。後續的每次同步處理，只會複製新的和變更的資料區段。CyberSense (我們將在本報告中稍後討論) 會掃描存放庫中所有不可變的副本，以尋找潛在的毀損。

實現不變性的方法

需要刪除不可變備份的情形很少見，但確實會發生。組織在累積無法刪除的不可變備份後，可能會遇到容量和後續成本問題。儲存備份可能需要大量容量，因此除了初始硬體投資外，還需要持續的操作、管理和監控成本。定期刪除不可變的備份，有助於解決這些問題。

如前所述，Dell PowerProtect Cyber Recovery 運用 Retention Lock 和其他工具，提供不變性。Retention Lock 提供一定的彈性，因為法規遵循和管控這兩種模式，在客戶實作不變性的方式上略有改動。不變性表示使用者或惡意人士無法刪除備份，但在某些情境下 (例如儲存容量問題)，PowerProtect Cyber Recovery 可讓客戶使用「保留鎖定 – 管控」模式，刪除備份。

其他公司的類似產品與 PowerProtect Cyber Recovery 的比較結果如何？我們查看了 Cohesity Cyber Recovery、Veeam、Rubrik 和 Veritas NetBackup 的公開資訊。除了 Cohesity Cyber Recovery 之外，解決方案均可置於內部部署或外部部署 (Cohesity 是由 AWS 支援的雲端型解決方案)。這四種解決方案的文件聲稱提供不變性，但值得注意的是，Rubrik 和 NetBackup 與 PowerProtect Cyber Recovery 有一些差異。

對於 Rubrik，管理員可以刪除備份，但不能從用戶端刪除，而且只能在搭配某些控制項時使用。此外，所有寫入都是「異位」(out-of-place) 的，這表示新的寫入永遠不會接觸之前寫入的資料。[13]

儘管提供不變性，系統管理員或惡意人士仍可刪除 NetBackup 可支援 WORM 的儲存裝置中的備份鎖定。然後，他們可以使用 bpexpdate 命令刪除映像。[14]

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 還能夠以可運作實體隔離的形式，同時提供實際和邏輯隔離，協助保護資料。PowerProtect Cyber Recovery 既可以使用實體隔離，也可以使用邏輯實體隔離。前者的備份資料會與生產網路實際中斷連線，並儲存在隔離的位置；而後者則仰賴網路存取控制，將邏輯上中斷連線的備份副本與生產環境分開。同時擁有這兩種類型的實體隔離能帶來很高的價值，因為僅靠邏輯實體隔離，並無法阻止具存放庫網路存取權的內部使用者存取和入侵資料。

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。[15] 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。如前所述，存取隔離資料需要個別的安全性認證，以及多因素驗證 (MFA)。[16]

隔離方法

Gartner 指出，「具有不可變資料存放庫 (IDV) 的隔離式復原環境 (IRE) 可提供最高等級的安全性和復原，並可防範內部威脅、勒索軟體和其他形式的駭客攻擊。」[17] 他們還指出，「透過在配備復原受影響系統所需的所有工具、程序和資源的 IRE 中，提供第三不可變的備份副本，具 IDV 的 IRE 會補強傳統的備份和災難復原 (DR) 系統，而非取代。」[18]

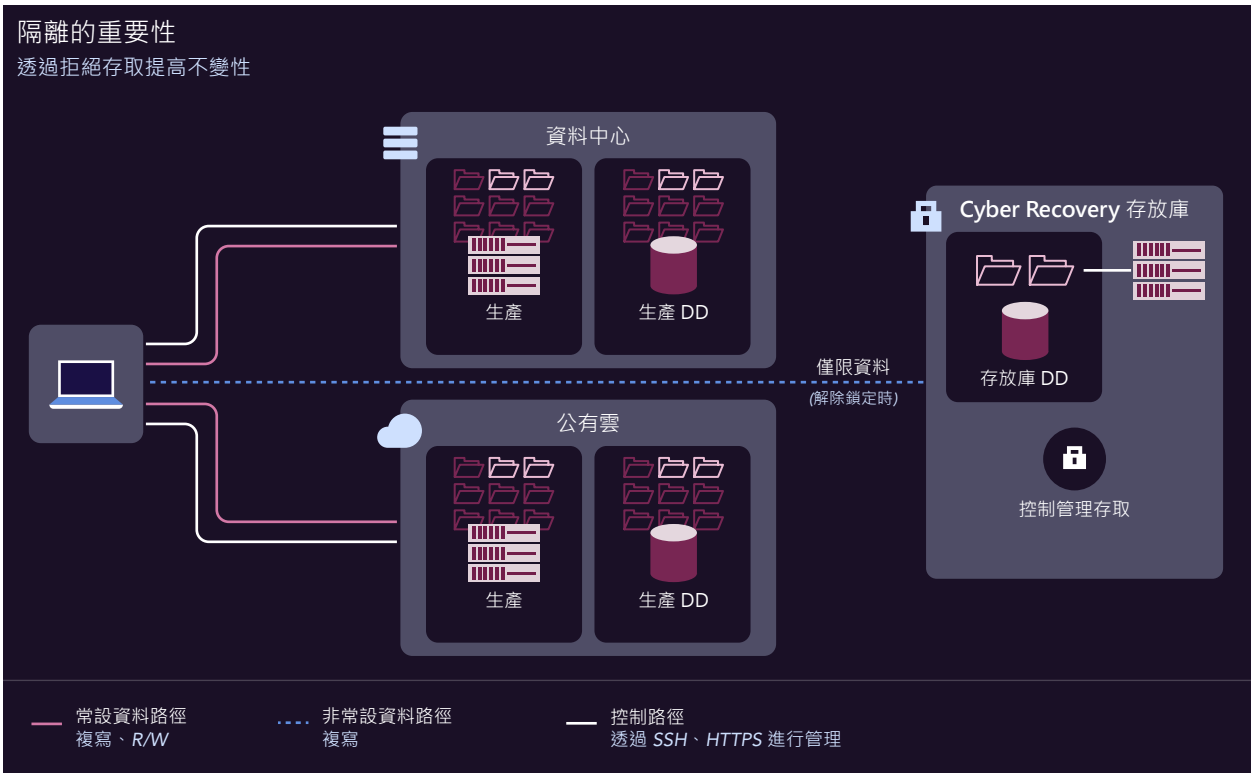
在檢閱 Cohesity、Veeam、Rubrik 和 Veritas 解決方案的公開資訊時，我們發現，與 PowerProtect Cyber Recovery 的 IRE 相比，每個解決方案的方法都略有不同。透過 Dell 解決方案，客戶可以透過實體或邏輯方式，隔離其 DD 存放庫與生產環境，讓生產環境的控制層和資料層與存放庫分開。此外，PowerProtect Cyber Recovery 還能自動處理實體隔離，這不是所有其他解決方案都具備的功能。

根據文件：

- Cohesity Cyber Recovery 僅為其 AWS 型 FortKnox 存放庫，提供動態自動化邏輯實體隔離。[19]
- Veeam 透過 Veeam Cloud Connect，為公有雲和私有雲供應商提供邏輯實體隔離支援，但並非自動化。Veeam 還提供 Veeam Hardened Repository，可作為解決方案的內部部署存放庫，而且組織可以將其設定為具有實體隔離。[20]
- Rubrik 沒有為 Rubrik Cloud Vault 提供自動實體隔離，但客戶可以透過與 Microsoft 的第三方合作夥伴關係，新增邏輯實體隔離。[21]
- NetBackup 客戶必須手動啟用邏輯實體隔離，並且可以透過內部部署和外部部署解決方案，來建立實體隔離。[22]

運作方式

圖 1 顯示隔離的 Cyber Recovery 存放庫網路路徑。請注意，為減少攻擊面，存放庫沒有通往生產環境的管理或控制路徑。



1 Cyber Recovery 存放庫的高階資料和控制路徑架構。資料來源：Principled Technologies。

Cyber Recovery 存放庫唯一必要的連線，是用於定期資料同步的資料路徑。同步是指 Cyber Recovery 解決方案以較短、原則導向的時間間隔，來擷取資料以進行複製。[23] 《PowerProtect Cyber Recovery 解決方案指南》指出，「基礎層級的 Cyber Recovery 解決方案架構，是由一組 PowerProtect DD 系統和 Cyber Recovery 管理主機所組成。在此基本層級組態中，在管理主機上執行的 Cyber Recovery 軟體，會在 Cyber Recovery 存放庫中的 PowerProtect DD 系統上，啟用和停用複製乙太網路介面以及複製內容，以控制從生產環境到存放庫環境的資料流量。」[24] Dell 提出其他方法建議，讓組織可以保護和隔離資料路徑。在測試中，我們觀察到 Cyber Recovery 會在複製期間和之後，解除鎖定和鎖定存放庫的情況。

若要實際實作存放庫，Dell 建議「將 Cyber Recovery 存放庫設備安裝在專屬機房或機櫃內，並搭配實體進出控制功能。這間安全管制機房應具備限制進出清單，採用鑰匙簽出或雙人鑰匙進出機制。針對設備機櫃或機房的入口，應進行監視攝影。為確保最高安全性，必須只能透過實體存取 Cyber Recovery 管理伺服器，以及相關聯的鍵盤與滑鼠，來存取 Cyber Recovery 軟體。」[25]

由於管理與控制路徑分離，Cyber Recovery 的實體和邏輯實體隔離選項，有別於其他解決方案。某些解決方案允許從生產環境介面，存取其存放庫資料。這會將存放庫資料置於與生產資料相同的攻擊面上，可能會讓惡意人士使用遭入侵的登入資料，來存取備份副本。

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。CyberSense 是一種分析引擎，使用 AI 機器學習分析演算法，來掃描和驗證存放庫中備份的完整性，以及備份中檔案的使用者內容。

CyberSense 在存放庫內執行，與生產環境隔離。它會監控存放庫內的檔案、VM 映像和資料庫，藉由分析資料的完整性，來判斷是否發生了網路攻擊。當 Cyber Recovery 解決方案將備份副本複製到存放庫，並套用 Retention Lock 功能後，CyberSense 便會自動掃描副本，並建立對檔案、資料庫和核心基礎結構的時間點觀察。分析引擎會掃描檔案和每個資料庫頁面的完整內容，而不僅是中繼資料。其他解決方案會尋找資料閾值或中繼資料的變更，而 CyberSense 則是在檔案內容中尋找，以驗證資料完整性。這些觀察結果可讓 CyberSense 追蹤檔案和資料庫如何隨時間變更，並找出許多進階類型的隱藏式攻擊。然後，CyberSense 會產生偵測毀損模式的分析，這些模式可能表示有惡意人士活動，包括加密、刪除、建立或混淆檔案等。[26] 其他解決方案會將分析推送至雲端，因此可能會擴大攻擊面；與此相反，組織可以選擇在內部部署，或 Cyber Recovery 支援的眾多雲端選項之一，來執行 CyberSense。

CyberSense 結合超過 200 種分析與資料觀察結果，隨著觀察結果增加，長時間下來會變得更加實用。而機器學習演算法使用有關數千種惡意軟體感染的資訊，來尋找異常行為模式，並區分使用者活動與勒索軟體，同時將偽陽性誤報和偽陰性誤判降到最低。此演算法透過持續研究，接受有關攻擊變體等事物的新教育。另外，機器學習演算法還會根據現有 CyberSense 客戶的實際資料，接收更新。[27]

除此之外，CyberSense 還支援以 Dell、IBM、Commvault 及 Veritas 的常見磁碟備份格式，建立資料索引。[28] 能夠支援其他廠商的備份格式，展現出 Dell 積極滿足客戶在資料備份方面各種不同需求的意願。

我們針對規模相似的裝置，測試了兩個統包式企業資料保護和網路復原解決方案的機器學習導向智慧分析軟體：Dell PowerStore™ 7000T 的 CyberSense for Dell PowerProtect Cyber Recovery，以及競爭對手 (以下簡稱「供應商 X」) 資料管理平台功能類似的工具。

測試方式

我們遠端執行所有測試，可以完全控制和不受限制地存取測試平台。Dell 解決方案 (包括 CyberSense、PowerProtect Data Manager 備份應用程式、APEX Protection Storage (原稱 DD Virtual Edition) 和 PowerProtect Cyber Recovery 解決方案) 及供應商 X 解決方案皆位於非現場資料中心實驗室。

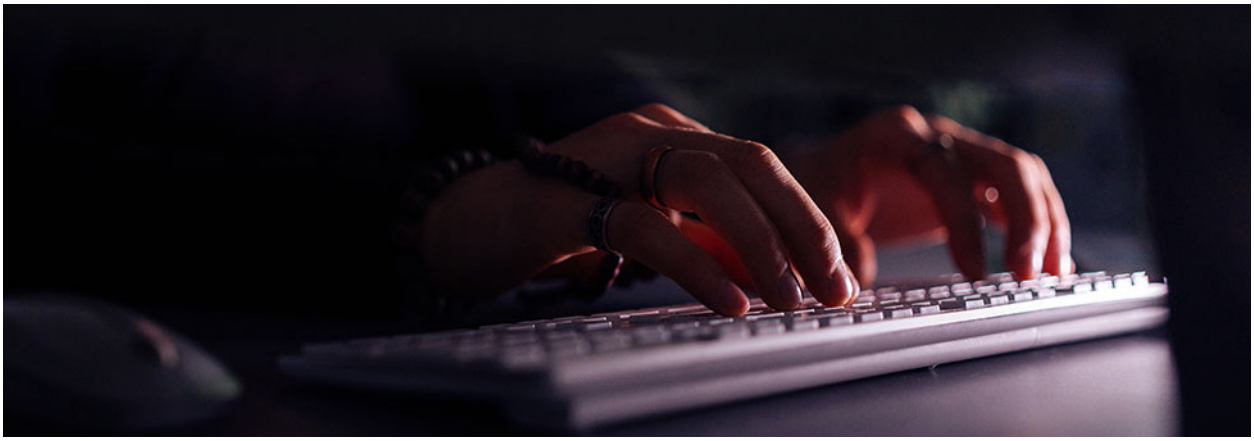
在這兩種解決方案上，我們執行了三個以指令檔為基礎的惡意事件情境，以備份為目標：

圖 2： 我們的測試情境。資料來源：Principled Technologies。

對於這兩種解決方案，前兩個情境都遵循相同的一般程序。首先，我們在 Dell PowerProtect Data Manager 和供應商 X 儲存裝置上，建立所有乾淨 VM 的完整備份、建立用於掃描的增量備份，並確認目標解決方案未偵測到威脅。這為我們提供了一組基準備份，我們可以在上面執行攻擊指令檔。

接下來，我們在四個具有不同作業系統和應用程式類型的 VM 上，執行勒索軟體模擬指令檔，在目標裝置上進行新的增量備份，並檢查目標分析軟體是否偵測到加密威脅。

針對第三個情境 (感染 SQL Server 頁面)，我們按照與其他兩個情境類似的程序進行，但改為著重在 SQL VM，並使用頁面損毀指令檔，而不是加密指令檔。我們在單一 VM 上執行了指令檔。



我們的發現

情境 1：偵測具有混淆檔案名稱的加密檔案

此情境模擬了會加密檔案，並混淆其名稱的惡意事件，除了變更檔案內容外，還變更其中繼資料。這種類型的攻擊通常稱為勒索軟體，這是一種安全性事件，其中惡意軟體會封鎖對電腦系統的存取，直到系統的擁有者或使用者支付預定金額。根據美國網路安全性和基礎結構安全性機構 (CISA) 的說法，「對各種規模的組織來說，在最初的中斷，以及某些例子的漫長復原過程中，勒索軟體和資料勒索的經濟和商譽影響，都展現出巨大的挑戰，而且成本高昂。」[29] 使用智慧分析軟體偵測備份中的加密，可以強化任何組織的資料保護策略、協助保護有價值的敏感資訊，並減少網路攻擊可能造成的代價昂貴的停機時間風險。

在我們的測試中，兩個智慧型分析應用程式都發現了檔案名稱經過變更的加密檔案。供應商 X 解決方案在偵測到感染前，需要的基準備份數為 15 個 (1 個完整備份和 14 個增量備份)，而 CyberSense 僅在一次完整備份後，就偵測到感染。這表示與 CyberSense 相比，供應商 X 解決方案需要額外 14 個備份。

當供應商 X 解決方案發出警示，提醒我們出現可疑活動時，它僅指出有某個東西移除了許多檔案，並新增了相同數量的檔案，這是基於備份的熵等級的可疑活動。[30] 供應商 X 解決方案並未指出檔案已加密，或檔案名稱已變更。相比之下，Cyber Recovery with CyberSense 會發出警示，提醒有東西已加密並混淆檔案名稱。

供應商 X 的結果可能顯示偽陽性誤報。換言之，假設組織使用供應商 X 解決方案執行每日備份，則在異常偵測之前，他們可能已擷取 14 天的受感染檔案。相比之下，CyberSense 只需要一個基準備份，即可發出警示，並提供感染及其詳細資料的情報。在我們的範例中，在這個階段使用 Cyber Recovery 進行復原，是從隔離的存放庫進行，這不會像供應商 X 解決方案那樣，將生產網路暴露給 14 個受感染的備份，所以組織可以放心。

圖 3： 每個解決方案能夠偵測損毀所需的備份數量。
資料來源：Principled Technologies。

情境 2：偵測具有原始檔案名稱的加密檔案

此情境與第一個情境類似，但指令檔保留了加密檔案的原始檔案名稱。此變更不會影響檔案的中繼資料，只會影響檔案本身。像這樣的行為可能是定時炸彈勒索軟體，其中攻擊在啟動之前，會休眠一段時間。定時炸彈勒索軟體可以躲避偵測，並以備份為目標，讓組織在需要備份時，才發現備份遭到感染而毫無用處。[31] 如果不變更中繼資料，檔案在表面上看起來可能未受感染，反而幫助隱藏休眠攻擊。

在我們的測試中，兩個智慧型分析應用程式都發現了加密檔案。同樣地，供應商 X 解決方案需要 15 個備份基準，其中包括 14 個增量備份，然後才能偵測到異常。CyberSense 在偵測到異常之前，只需要一個完整備份基準。

與第一個情境一樣，供應商 X 解決方案僅發出警示，提醒我們某個東西變更了許多檔案，並根據備份的熵等級，判斷為可疑活動。供應商 X 解決方案並未指出有東西加密了檔案，但 Cyber Recovery with CyberSense 確實告訴我們這一點。以這種方式偵測損毀，表示 CyberSense 會審視文件內容，而不僅是表面層級的中繼資料。這種類型的掃描，為您的備份增加了另一層安全防護，進而保護您的數位基礎結構或整體資產。有人可能會認為 CyberSense 是一個「真正的」智慧型分析應用程式。此外，使用 CyberSense 的組織可能會更快偵測到損毀，因為此解決方案建立基準所需的備份數量大幅減少。根據組織的備份排程，可能會提前很多天就偵測到損毀。

圖 4： 每個解決方案偵測損毀所需的備份數量。資料來源：Principled Technologies。

情境 3：偵測 SQL Server 頁面損毀

此情境模擬了損毀 SQL Server 頁面的惡意事件。在 SQL Server 中，資料儲存的基本單位是頁面，而資料庫會讀取或寫入整個資料頁面。[32] 同樣地，此變更不會影響中繼資料，只會影響檔案本身。這種類型的攻擊通常稱為 SQL 注入，攻擊者透過網頁輸入，將惡意程式碼注入 SQL 陳述式中，進而瞄準 SQL 資料型應用程式。[33] 即使受到感染，資料庫也可能會繼續執行。除了資料竊盜之外，損毀的 SQL Server 頁面還會導致資料完整性問題、資料遺失，以及資料庫功能中斷。這些結果可能會損害組織的聲譽、中斷營運工作流程、造成金錢損失，甚至需要承擔法律責任。

雖然在前兩個情境下，CyberSense 和供應商 X 解決方案皆偵測到加密，但在這第三個情境下，只有 CyberSense 能夠確實地深入掃描，以偵測 SQL Server 頁面中的損毀。這顯示出，雖然這兩種解決方案在某些層級提供相似的偵測功能，但 CyberSense 可為潛在的業務關鍵 SQL Server 型應用程式，提供更深入的備份掃描。如此一來，CyberSense 便可透過更深入的掃描和更全面的保護功能，增加一層安全性復原能力。

SQL Server 支援金融、零售、醫療照護和其他產業的許多應用程式。由於 SQL Server 可以充當開發架構的後端，因此 SQL Server 攻擊可能會導致停機、中斷營運，並可能威脅到這些應用程式產生的營收。

使用 Dell PowerProtect Cyber Recovery 進行還原和復原

Dell 網路韌性策略可提供廣泛的復原功能。這些復原選項包括常見的產業功能，例如即時存取，或從在生產環境中維護的不可變備份，進行傳統復原。此外，Dell 還可透過 PowerProtect Cyber Recovery 解決方案，實現獨特的復原功能。由於 PowerProtect Cyber Recovery 會隔離維護副本，並使用 CyberSense 掃描其完整性，因此組織可在遭受攻擊後立即存取副本，並使用這些副本開始復原步驟或立即還原至其他復原平台，例如無塵室。

將此即時使用案例，與只能存取生產環境資料或公有雲資料的組織進行比較。組織需要先確定並補救根本原因、隔離惡意人士的持續動作、拍攝鑑識影像並提供給保險公司及其法務部門、重新掃描資料，並有足夠的可用基礎結構 (AD、DNS) 來存取備份基礎結構，才能安全地存取儲存在遭入侵區域中的資料。根據攻擊的範圍和複雜程度，此程序可能需要數天或數週的時間。

運作方式

在正常生產期間，PowerProtect Cyber Recovery 會自動建立還原點，以進行復原和安全性分析。發生網路攻擊時，Cyber Recovery 會使用其自動化還原和復原程序，以及那些還原點，讓業務關鍵系統重新上線。CyberSense 和鑑識報告可協助網路安全和復原團隊診斷攻擊的影響。生產環境清理完畢並準備好復原後，Cyber Recovery 就會提供執行實際資料復原的工具和技術。

網路攻擊發生後，多種資料保護指標會發揮作用，來決定復原速度 (網路復原時間或 CRT)，以及使用者在遭受破壞性攻擊後，可返回的時間點 (網路復原點或 CRP)。若為 Cyber Recovery 解決方案，這些指標包括下列事項：

- **銷毀偵測目標 (DDO)**：這是 rolling window 方法，以攻擊和攻擊偵測之間的時間量為基礎。分析和其他 Cyber Recovery 機制必須在此期間內運作。
- **銷毀評估目標 (DAO)**：這是在發生入侵後，分配給網路安全團隊的時間量，用於確定損害的範圍和可能的應變方式。
- **Cyber Recovery 同步間隔**：這是 Cyber Recovery 解決方案將資料從生產環境複製到存放庫的頻率。根據以前為解決方案建立的回復點目標 (RPO)，來安排時間。副本保留期間因解決方案而異，但通常為一週到一個月。
- **Cyber Recovery 資料副本數量**：這是 Cyber Recovery 存放庫中所保留的資料副本數量。搭配同步間隔時，此指標可以概略衡量組織可以復原資料的回溯時間範圍，例如，七個副本搭配 24 小時的間隔，允許使用者復原長達一週的資料。

除了復原要求之外，解決方案保護的資料類型，還有助於確定資料同步間隔和保留時間。根據 Cyber Recovery 解決方案指南，為了獲得最佳的復原彈性，使用者可能會將解決方案保護的資料，分類到下列其中一個備份串流中：[34]

- 二進位和可執行備份，包括基層作業系統發佈版本和應用程式組建
- 完整應用程式和檔案系統備份，包括映像和應用程式專用資料

這些獨立的備份串流，會帶來兩種不同的復原策略：

1. **在 Cyber Recovery 存放庫中，還原資料和應用程式二進位檔：**
   此解決方案可識別可用的還原點、惡意軟體及其持續存在的位置，並決定是清除備份映像中的惡

意軟體，還是使用 Cyber Recovery 存放庫副本進行重建。套用安全性修補程式後，解決方案會使用應用程式的 DR 執行腳本，將資料還原到復原主機，然後判斷復原程序是否已消除惡意軟體的影響。然後，解決方案會使用存放庫運算，在應用程式上執行測試，並清理生產環境，或為生產環境重新建立映像。最後，Cyber Recovery 會將復原主機連結到生產環境，並將應用程式和資料複製回生產環境。圖 5 顯示此程序。

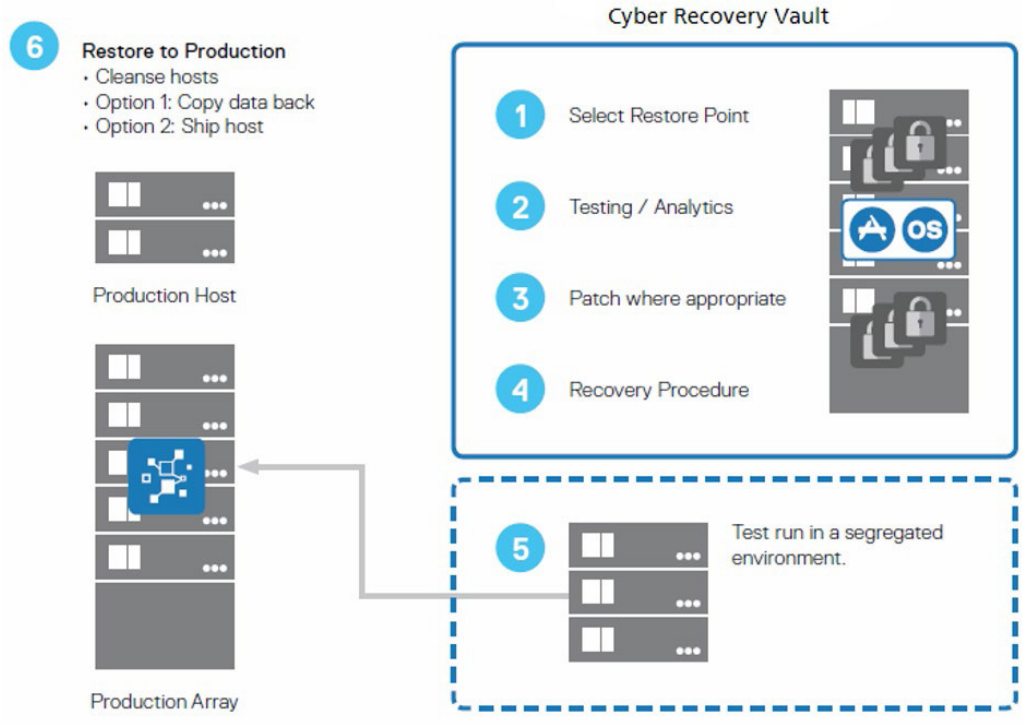


圖 5： 還原資料和應用程式二進位檔的程序。來源：Dell Technologies。[35]

2. **從 Cyber Recovery 存放庫完全重建：**
   在此方法中，Cyber Recovery 解決方案會根據在事件應變期間，鑑識評估判定的損毀程度，來重新格式化生產系統。接著，解決方案會透過 Cyber Recovery 存放庫中的副本，來重建二進位檔，並套用可用的安全性修補程式。最後，解決方案會使用應用程式的相關聯 DR 執行腳本，將應用程式、資料和組態檔案的適當副本還原到生產環境。圖 6 顯示此程序。

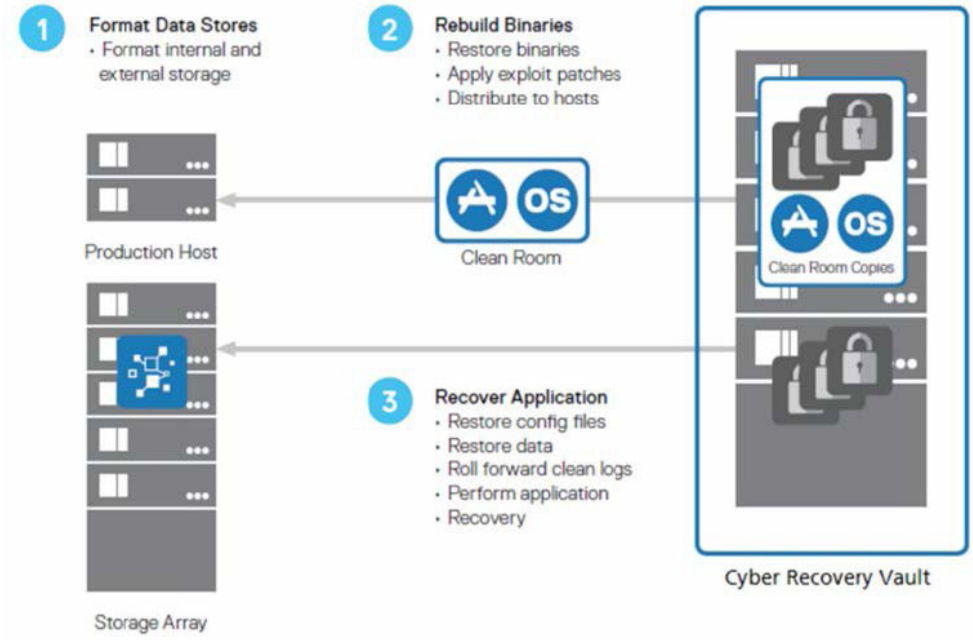


圖 6： 從 Cyber Recovery 存放庫完全重建的程序。來源：Dell Technologies。[36]

Cyber Recovery 解決方案包括 Cyber Recovery 軟體可用於復原的實體或虛擬復原主機 (或兩者)。這些主機包括備份應用程式復原伺服器 (會將備份應用程式和備份應用程式目錄復原到此指定伺服器)，以及應用程式復原伺服器。組織可以根據解決方案的復原要求，部署多個伺服器。Cyber Recovery 軟體可以向任何主機公開沙箱 (測試環境，用於安全執行全新或未經測試的軟體) 資料副本，以執行存放庫內資料的復原，例如檔案系統資料；IBM、Commvault 及 Veritas 備份資料；或受 Dell NetWorker、Dell Avamar、Dell PowerProtect DP 系列裝置或 Dell PowerProtect Data Manager 軟體保護的資料。在存放庫中復原備份應用程式後，解決方案可以將該資料還原到存放庫中的其他復原主機。

組織可提前調整備份應用程式復原伺服器的大小，讓使用者可以還原 Cyber Recovery 解決方案保護的所有備份應用程式。同樣地，解決方案會將應用程式復原到指定伺服器，即應用程式復原伺服器。某些應用程式可能要求客戶先復原其他相依應用程式。存放庫內的基礎結構，可支援復原解決方案所保護的最大生產應用程式。

結論

組織在建構資料保護計畫時，必須考慮許多攻擊面向。這包括保護所有資料，但最重要的是，保護對營運至關重要的關鍵資料。PowerProtect Cyber Recovery 可隔離關鍵資料，並在發生網路攻擊時，協助確保妥善復原資料。Cyber Recovery 在 CyberSense 中使用機器學習型分析，來判斷存放庫中資料的完整性，並識別復原用的無錯誤備份資料。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，但競爭對手解決方案偵測不到。相較於競爭對手解決方案，PowerProtect Cyber Recovery 判斷資料損毀情境所需的備份數也比較少。除此之外，Cyber Recovery 解決方案還提供多種復原選項，依靠存放庫中未遭入侵的資料，以高效率且順暢的方式恢復營運。

---

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，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)，存取時間：2024 年 8 月 23 日，https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf。
3. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。
4. Cohasset Associates, Inc，《Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)》(Dell Technologies PowerProtect DD 和 DDVE – 法規遵循評估：SEC 17a-4(f)、SEC 18a-6(e) 和 FINRA 4511(c))，2023 年 10 月 27 日存取，https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment。
5. Dell，《Data Domain: Retention Lock Frequently Asked Questions》(Data Domain：保留鎖定常見問題)，2023 年 9 月 12 日存取，https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq。
6. Dell，《Data Domain: Retention Lock Frequently Asked Questions》(Data Domain：保留鎖定常見問題)。
7. Dell，《Encryption types offered by DD series encryption appliance》(DD 系列加密裝置提供的加密類型)，2023 年 9 月 8 日存取，https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance。
8. Dell，《Dell EMC Data Domain – Security Configuration Guide》(Dell EMC Data Domain – 安全性組態指南)，2023 年 9 月 11 日存取，https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf。
9. Dell，《Role based access control (RBAC) in Data Domain》(Data Domain 中的角色型存取控制 (RBAC))，2023 年 9 月 11 日存取，https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99。
10. Dell，《Dell EMC Data Domain – Security Configuration Guide》(Dell EMC Data Domain – 安全性組態指南)。
11. 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。

12. Veeam，《Dell EMC Data Domain - DataDomain MTree overview and limits》(Dell EMC Data Domain - DataDomain MTree 概觀與限制)，2023 年 9 月 11 日存取，https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl，《Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture》(快速從勒索軟體攻擊復原：不可變備份架構的魔術)，存取時間：2023 年 12 月 13 日，https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf。
14. Veritas，《NetBackup™ Security and Encryption Guide》(NetBackup™ 安全性與加密指南)，2023 年 12 月 13 日存取，https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528。
15. 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。
16. Dell，《Dell PowerProtect Cyber Recovery》，存取時間：2023 年 9 月 12 日，https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf。
17. Jerry Rozeman 和 Michael Hoeck，《Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware》(創新深入解析：運用隔離的復原環境和不可變的資料存放庫，來防範勒索軟體及從中復原)，2023 年 12 月 14 日存取，https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb。
18. Jerry Rozeman 和 Michael Hoeck，《Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware》(創新深入解析：運用隔離的復原環境和不可變的資料存放庫，來防範勒索軟體及從中復原)。
19. Nikitha Okmar，《Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era》(超越實體隔離 - 現代的資料隔離與復原)，2023 年 12 月 13 日存取，https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/。
20. Marco Horstmann，《How to protect your data from ransomware and encryption Trojans》(如何保護您的資料免受勒索軟體和加密木馬威脅)，2023 年 12 月 13 日存取，https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html。
21. Rubrik，《Rest easy with immutable, off-site data storage》(不可變的非現場資料儲存讓您高枕無憂)，2023 年 12 月 13 日存取，https://www.rubrik.com/products/rubrik-cloud-vault。
22. Veritas，《NetBackup Isolated Recovery Environment》(NetBackup 隔離式復原環境)，2023 年 12 月 13 日存取，https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf。
23. CSI Group，《Dell Cyber Recovery Vault (overview by CSI)》(Dell Cyber Recovery 存放庫 (CSI 概觀))，2023 年 8 月 23 日存取，https://youtu.be/ej5nZzWNRM0。
24. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。
25. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。
26. Dell，《CyberSense® for PowerProtect Cyber Recovery》。
27. Dell，《CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines》(CyberSense® for Dell PowerProtect Cyber Recovery – 採用索引引擎技術)，2023 年 9 月 13 日存取，https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf。
28. Index Engines，《CyberSense for Dell Cyber Recovery》，2023 年 9 月 25 日存取，https://indexengines.com/csmatrix。
29. CISA，《#StopRansomware Guide》(#StopRansomware 指南)，2023 年 8 月 1 日存取，https://www.cisa.gov/stopransomware/ransomware-guide。
30. 「在安全性方面，大多數人使用 Shannon 提出的熵，這是一種特定演算法，會傳回介於 0 到 8 之間的值。數字越大，資料越隨機。而且很多時候，值越高也表示資料被封裝或加密。」Mueller, Clint，《How to Use Entropy Analysis in Penetration Testing》(如何在滲透測試中使用熵分析)，2023 年 8 月 28 日，https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy。
31. Steven Cooper，《How to Protect your Backups from Ransomware in 2023》「在 2023 年，如何保護您的備份免受勒索軟體的侵害」，2023 年 8 月 1 日，https://www.comparitech.com/net-admin/protect-backups-from-ransomware/。
32. Microsoft，《Pages and extents architecture guide》(頁面和範圍架構指南)，2023 年 8 月 3 日存取，https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16。
33. W3 Schools，《SQL Injection》(SQL 注入)，2023 年 8 月 3 日存取，https://www.w3schools.com/sql/sql_injection.asp。
34. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。
35. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。
36. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。

閱讀本報告背後的科學依據 ▶

▶ 檢視本報告的原始英文版本，網址為 https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

此專案是由 Dell Technologies 委託執行。