透過快速行動、更健全的 Cyber Recovery 解決方案支援您的資料保護計畫

我們的研究顯示，Dell Technologies PowerProtect Cyber Recovery 可以為備份存放庫提供實體隔離，並更深入地掃描勒索軟體

備份隔離存放庫實際地進行實體隔離

建立資料無法跨越的實際障礙

更深入地掃描勒索軟體

CyberSense 不只檢視中繼資料，還會檢視檔案內容和資料庫

掃描多 2 倍的異常工作負載

使用單一工具在更多位置搜尋惡意軟體

勒索軟體攻擊造成的平均成本在兩年內增加了近 20%，達到 523 萬美元。[1]高效率的 Cyber Recovery 解決方案可以讓組織立即從事件中復原、減少資料遺失、將停機時間降到最低，並且在過程中保有品牌誠信，藉此降低或甚至避免這些潛在成本。解決方案應在攻擊後找出並修復已知的良好資料，確保組織能夠挽救關鍵資料和系統，同時協助將業務風險和停機時間降到最低。

Dell PowerProtect Cyber Recovery (以下簡稱 Cyber Recovery) 就是這樣的一套解決方案。它可以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。本報告使用可公開取得的資料來對比 Cyber Recovery 與競爭解決方案 Rubrik Security Cloud (以下簡稱 RSC) 的基本資料保護特色和功能。我們特別審視了 Cyber Recovery 解決方案客戶可能認為重要的特色和功能，包括復原存放庫、不變性、工作負載支援、掃描技術、復原能力及隔離。

與 RSC 不同，Cyber Recovery 使用的是多副本方法，這表示在建立備份後，會將這些備份 (通常是選定的子集) 複製到獨立的儲存裝置進行保護和分析。Cyber Recovery 由許多元件組成，包括一或多個儲存存放庫，這些元件可能位於到場的 PowerProtect Data Domain 裝置中，或者透過軟體定義的 Dell APEX Protection Storage for Public Cloud 位於雲端中。相較之下，RSC 不提供區域存放庫選項。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，可掃描存放庫的資料、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 解決方案可以掃描的異常工作負載數量是 Rubrik 解決方案的兩倍，能夠讓 CyberSense 掃描 ML (機器學習) 偵測惡意軟體或其他威脅發動者活動對更多資料的影響。我們將剖析 PowerProtect Cyber Recovery 的工作方式有何不同，以及如何為您的組織帶來更多優勢。

產品概觀

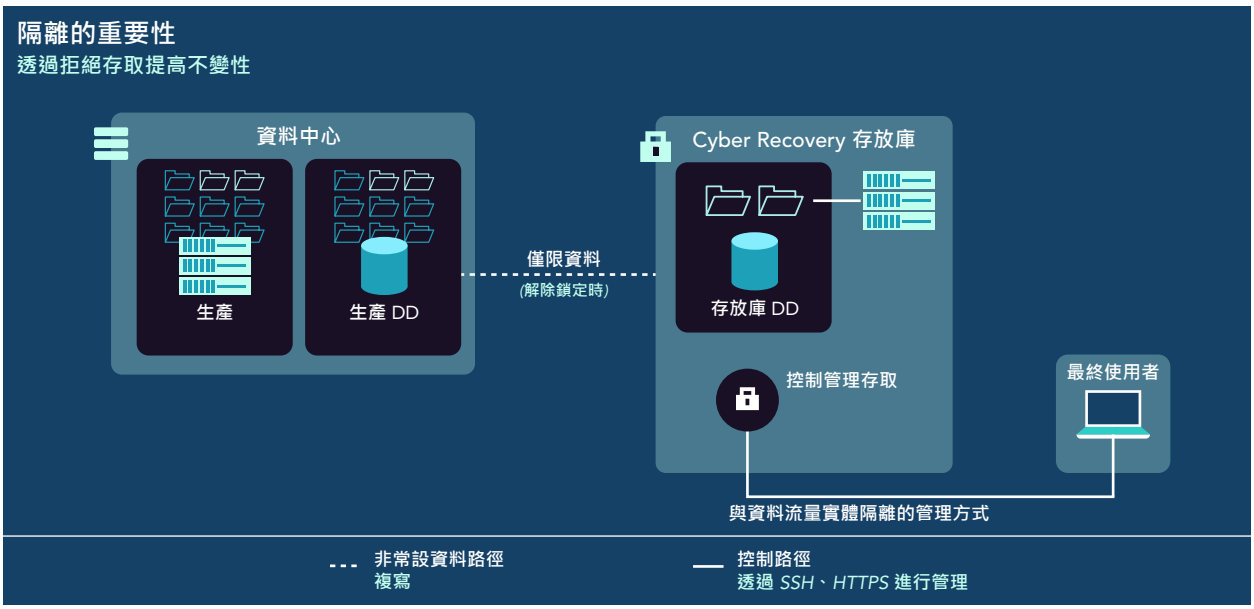
Dell PowerProtect Cyber Recovery 概覽

Dell PowerProtect Cyber Recovery 包含一個儲存生產資料的儲存裝置，以及一個位於存放庫、用於複製的目標儲存裝置。另外還包括 Cyber Recovery 軟體；該軟體可協調同步處理、管理 Cyber Recovery 存放庫中 PowerProtect Data Domain (PPDD) 系統上的多個資料副本、監督復原過程，以及監督 CyberSense 的分析過程。

該解決方案透過 MTree 複製將唯一資料從生產 PPDD MTree 傳輸到對應的存放庫，並在設定的期間內維持資料不變性*。該存放庫會有一個包含 Cyber Recovery 軟體的伺服器，以及一個解決方案還原備份應用程式和資料的元件。每個 Cyber Recovery 存放庫通常會儲存許多這類元件。該存放庫還包含一個配備資料分析軟體的分析/索引編製主機，可直接整合 Cyber Recovery 軟體和 CyberSense。

*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。

圖 1 提供 Dell Cyber Recovery 解決方案概覽。

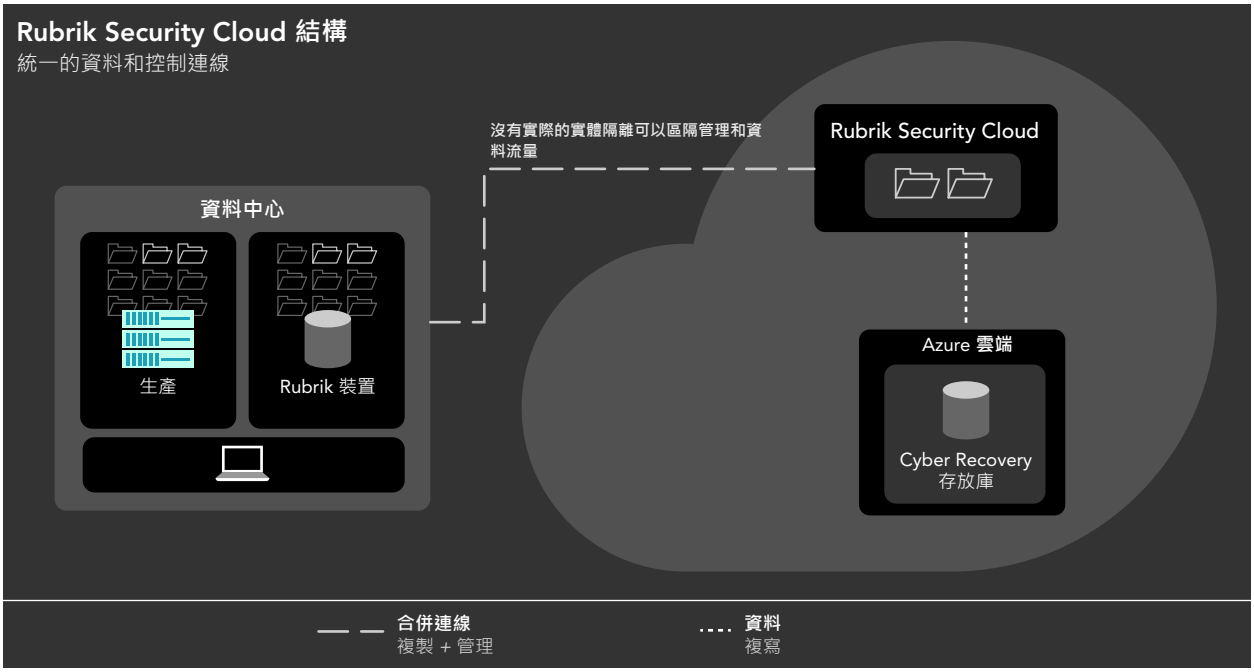


1 Cyber Recovery 存放庫的高階資料和控制路徑架構。資料來源：Principled Technologies。

若要進一步瞭解有關 Dell PowerProtect Cyber Recovery 解決方案的重要元件，請閱讀 Dell PowerProtect Cyber Recovery 解決方案指南。

Rubrik Security Cloud 概覽

Rubrik 形容 Rubrik Security Cloud 是一個軟體即服務 (SaaS) 平台，讓客戶能夠「確保 [他們的] 資料安全、監控資料風險，並快速復原 [他們的] 資料，無論資料位於企業、雲端還是 SaaS 應用程式都沒問題。」[4] Rubrik 表示，該解決方案的建構基礎是「使用高可用性服務的安全微服務架構，以及在 Google Cloud Platform (GCP) 上執行的基礎結構」。[5]圖 2 顯示 Rubrik Security Cloud 的一般結構。



2 Rubrik Security Cloud 的一般結構。資料來源：Principled Technologies。

功能支援

復原存放庫

存放庫是專用的儲存空間，用來儲存解決方案在生產環境中採用的加密備份副本。存放庫不屬於生產備份解決方案；相反地，每個存放庫都可作為隔離的「備份之備份」位置，客戶可以從該位置復原已驗證的備份。

Dell 提供多種存放庫選項，包括到場、遠端主機託管網站或公有雲內。到場存放庫使用可運作實體隔離的 PPDD；該 PPDD 位於資料中心裡，甚至可能與您的備份解決方案位於同一機架中。實體隔離解決方案通常會與生產環境實體隔離開來。異地主機託管存放庫和到場版本一樣，需要實體存放庫的專用網路連線，但存放庫在遠端資料中心的地理位置是分開的。Dell 還與雲端服務供應商 Amazon Web Services (AWS)、Microsoft Azure 及 Google Cloud 合作，在公有雲中提供存放庫。公有雲存放庫的組態彈性，可以滿足客戶需求。[6, 7, 8]

Rubrik Cyber Recovery 是 Rubrik Security Cloud 的一項元件。復原存放庫透過軟體即服務模型提供，只會使用 Microsoft Azure 上的儲存裝置。我們在研究中找到的許多公開文件都將 Rubrik Cyber Recovery 存放庫與 Rubrik Cloud Vault (提供不變性的備份層) 聯結在一起。[9, 10] 此存放庫不需要額外的硬體，而且可供 6.02 版或更新版本的 Rubrik Cloud Data Management (CDM) 平台使用。

不變性

不變性是指不可變更或永久的狀態。不可變備份和備份副本可讓管理員為檔案建立永久性，直到指定的時限結束，使用者或系統才可修改或刪除。接著檔案就會「過期」— 解決方案會自動移除這些檔案。解決方案通常會透過規範系統如何處理檔案的原則或定義來執行此程序。[11]

Dell PowerProtect Cyber Recovery 不變性仰賴保留鎖定 (透過保留鎖定功能) 來防止備份副本在一段時間內遭到刪除或修改，或是強制提前過期。(無論組織是否啟用了保留鎖定功能，PPDD 都是僅可附加的檔案系統。[12])Dell 客戶使用 PPDD MTree 管理備份；PPDD MTree 是使用者定義的邏輯磁碟分割，擁有獨立的保留設定，客戶可將其指派為備份應用程式目的地。[13] 有兩種保留鎖定類型可供客戶選擇：控管和法規遵循。法規遵循鎖定是兩者中更嚴格、更安全的選擇。客戶根據每個 MTree 啟用保留鎖定，這表示指定 MTree 中的所有檔案都需遵守該 MTree 的保留鎖定定義，並根據檔案層級設定保留的時間長度。客戶定義法規遵循保留鎖定後，任何使用者或系統都無法將其刪除。管理員可以還原控管保留鎖定；此選項比較寬鬆。[14]

Rubrik 解決方案預設不啟用保留鎖定，客戶必須向 Rubrik 支援部門開立工單，或是啟用雙人管理規則 (two-person rule) 才能使用保留鎖定。

Rubrik 解決方案的不變性同樣仰賴保留鎖定，防止備份副本遭到刪除或強制提前過期。Rubrik 解決方案和 PowerProtect Cyber Recovery 類似，都是將新資料附加到檔案系統，而不是覆寫現有資料。該解決方案會對傳入的資料進行指紋辨識，並且和資料一起儲存。**Rubrik 解決方案預設不啟用保留鎖定**，客戶必須向 Rubrik 支援部門開立工單，或是啟用雙人管理規則 (two-person rule) 才能使用保留鎖定。(使用 Rubrik Cloud Data Management 7.0.1 之前的版本，客戶必須聯繫 Rubrik 支援部門才能啟用保留鎖定；Rubrik 文件沒有明確說明客戶是否仍需聯絡支援部門才能啟用。)客戶啟用保留鎖定後，此功能會防止使用者或系統刪除定義參數以外的資料。Rubrik 保留鎖定需要外部網路時間通訊協定 (NTP) 伺服器進行時間同步，不肖份子可能會藉機操控參考 NTP 來源，進而讓保留鎖定提前過期。[15]

授權和訂閱

Dell PowerProtect Cyber Recovery 是一款取得授權的解決方案。安裝時，Dell 會預設安裝 90 天評估授權。90 天後，客戶必須購買新授權才能繼續使用該產品。Dell 提供標準 (永久) 授權和訂用方案型授權。

Rubrik 將 Rubrik Cyber Recovery 整合到 Rubrik Security Cloud (RSC) 中。客戶必須訂用 Rubrik Enterprise Edition 才能使用 Rubrik Cyber Recovery。訂用方案期限為三年。[16, 17] 如果 RSC 發生故障，SAP HANA 和 Db2 工作負載需要第三方工具來復原資料，這可能會產生額外的訂用方案費用。[18]

管理存取權

Dell PowerProtect Cyber Recovery 系統的管理對於客戶選擇用來部署的拓撲來說，都屬於區域性質。由於該解決方案會啟動從存放庫復原，因此管理員可以從存放庫所在的任何位置登入管理 UI。到場存放庫可讓管理員進行區域存取，不必透過網際網路，而網際網路存取正是網路攻擊會嚴重影響的層面，因為可能遭到拒絕服務攻擊；切斷網際網路連線則可保護資料安全，這也是美國國家標準與技術協會 (NIST) 的建議做法。主機託管存放庫可透過遠端站點實體存取裝置，並使用公開網際網路之外的連線。雲端型存放庫需要存取網際網路才能復原，這可能會使現場復原作業延遲，需等到網路攻擊結束並且恢復正常的網路連線才能進行。

管理 Rubrik Cyber Recovery 時，必須透過網際網路才能存取 Rubrik Security Cloud。正如我們所說，這種連線方式可能會使現場復原作業延遲，需等到網路攻擊結束後，網路功能恢復正常為止。

由於客戶必須能存取 RSC 才可使用 Rubrik Cyber Recovery 功能，因此 RSC 會成為單一故障點。如果該服務無法使用，會阻礙受影響客戶從存放庫復原。Rubrik 可以在 RSC 服務中斷期間復原 10 個工作負載，但兩個資料庫工作負載則需要第三方工具和 Rubrik 支援部門的協助才能復原。[19, 20] 此外，遭入侵的管理員帳戶或是可存取 RSC 平台的不肖份子，將取得整個資產的存取權，而不是單一存放庫。

透過 Dell 取得有關 Managed Detection and Response 的更多說明

有些組織可能不習慣「單打獨鬥」的網路安全性方法。Dell 為這些客戶提供 Managed Detection and Response (MDR) 這項全面管理型的服務；此服務可監控和偵測威脅與風險，並且和客戶合作來降低這些風險。Dell 表示，該服務的特色如下：[21]

- 值得信賴的支援，包括針對部署和設定 Dell 支援的 Extended Detection and Response (XDR) 安全性分析平台提供專家建議
- 威脅回應和安全性組態，包括每季高達 40 小時的服務相關安全性組態
- 24 小時全天候偵測和調查，包括針對每個客戶環境主動進行威脅搜捕，探索能夠規避安全性系統的新威脅或已知威脅變體
- 啟動網路事件回應，包括 40 小時的年度遠端事件回應協助，使調查活動能夠迅速開始

MDR 搭配 APEX Cyber Recovery Services 使用時，可以提供許多選項讓客戶監控、偵測及緩解威脅和風險。選項可用與否表示覆蓋範圍擴大，或是適合組織需求的混合式方法。

有關 MDR 的詳細資訊，請造訪 **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**。

順暢

安裝

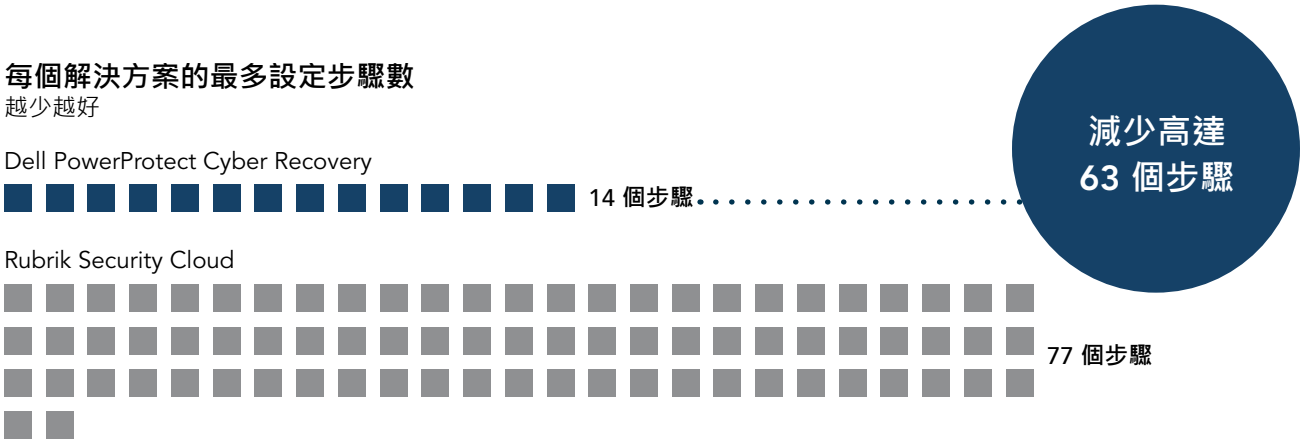
Dell PowerProtect Cyber Recovery 設定包括在 Linux 系統上安裝軟體，或是從開放虛擬化格式 (OVF) 範本建立 VMware® vSphere® 裝置。軟體安裝需要 14 個步驟，[22] 而替代用的 vSphere 裝置部署需要 8 個步驟，為時 5 分鐘。[23]安裝後，管理員可以在隔離環境中透過網頁瀏覽器存取該解決方案。

客戶需要獨立部署 CyberSense，這是一個全面自動化的整合式智慧安全性分析引擎。[24] 在 Dell PowerProtect Cyber Recovery 中安裝 CyberSense 的相關說明未公開發佈。[25]

Dell 提供多個使用者可以調整的指標，包括銷毀偵測目標 (DDO)、銷毀評估目標 (DAO)、Cyber Recovery 點 (CRP)、Cyber Recovery 時間 (CRT)、Cyber Recovery 同步間隔以及 Cyber Recovery 資料副本計數。Dell 也建議描述需要保護的資料。這些資料可能是任務關鍵型、業務關鍵型、依賴核心基礎結構服務或其他應用程式，也可能是一般資料，例如應用程式二進位檔、開機映像及備份目錄。客戶可以透過這些選項完全掌握備份環境，而且能夠自訂資料分類。Dell 諮詢服務還可提供進一步的協助和建議。[26]

Rubrik 設定也包含多個步驟。在建立叢集之前，Rubrik 支援服務必須安裝和設定 Rubrik CDM。然後，管理員下載並安裝最新或所需的 CDM 版本 (15 個步驟)。[27] 接下來，管理員可以使用 UI 或 CLI 設定 Rubrik 叢集。您可以使用 UI 或 CLI 設定叢集，兩種方法都需要 24 個步驟。[28, 29] 然後，管理員可以使用線上方法 (12 個步驟)[30] 或離線方法 (18 個步驟) 註冊 Rubrik 叢集。[31] 接下來，管理員啟用多因素驗證 (MFA)，這需要 13 個步驟。[32] 最後，管理員新增初始帳戶 (6 個步驟) 和任何其他帳戶。[33]圖 3 顯示每個 Cyber Recovery 解決方案可能的最大設定步驟數。

Rubrik 客戶無法調整其他指標，可能會降低滿足客戶需求的彈性。某位評論家聲稱：「大多數的使用者介面都相當簡單明瞭，但有些區域未能詳細說明選項的用途，或是沒有選項。儘管使用者體驗變得輕鬆簡單，但是許多可調整的參數卻沒有，需要開啟支援通道，讓支援人員可以在客戶環境中進行變更。」[34]



3 Dell PowerProtect Cyber Recovery 和 Rubrik Security Cloud 可能的最大設定步驟數。
越少越好。資料來源：Principled Technologies。

維護

我們觀察到，設定完畢後，Dell 和 Rubrik UI 在執行日常維護作業方面很相似。設定完畢後，客戶可以設定 Dell PowerProtect Cyber Recovery 執行下列操作：[35, 36]

- 根據排程自動產生 Cyber Recovery 工作報告，並回應手動使用者要求
  - 使用者或排程在啟動原則、復原作業、系統備份或清理作業時建立工作
- 自動監控存放庫狀態、儲存容量、Cyber Recovery 作業、複製/同步失敗或 Cyber Recovery 存放庫關閉時的警示，以及 Cyber Recovery 工作
- 持續地自動掃描攻擊，然後依嚴重程度在掃描後顯示 CyberSense 警示，提供受影響的檔案、主機及原則數量、偵測到的特定威脅、攻擊時間點，以便您可以找到無錯誤的備份資料，以及用來分析攻擊的損毀檔案清單

同樣地，客戶可以設定 Rubrik 執行下列操作：[37]

- 自動使用 Rubrik Security Cloud 追蹤、監控及顯示所有已連線 Rubrik 叢集的所有事件。它可提供三種事件類型：[38]
  - 重要 - 需要注意的事件，例如備份、歸檔或複製失敗
  - 警告 - 備份、歸檔或復原已完成
  - 資訊 - 僅供參考
- 使用 Threat Monitor 持續地自動掃描快照，找出新的和現有的入侵指標；這可提供解決方案上次拍攝快照的時間、事件時間線、偵測時間、變更的檔案數、可疑檔案數、叢集名稱以及物件類型和名稱

異常工作負載支援

Rubrik Security Cloud Data Threat Analytics 和 CyberSense 都會掃描多種工作負載類型，但我們找到的資料來源顯示，CyberSense 支援的異常偵測工作負載多出兩倍。這包括掃描以下類型的工作負載：

- 虛擬機器
- 核心基礎結構
- 可能包含文件、合約及智慧財產權的使用者檔案
- 資料庫
- 其他用戶端進行的備份

如果我們計算在可公開取得資料中找到的支援工作負載數量，會發現 CyberSense 支援 21 個異常偵測工作負載，而 Rubrik 則支援 7 個。

如果我們計算在可公開取得資料中找到的支援工作負載數量，會發現 CyberSense 支援 21 個異常偵測工作負載，而 Rubrik 則支援 7 個。因此，根據各方分享的可公開取得資料，CyberSense 支援的工作負載比 Rubrik Security Cloud Data Threat Analytics 多兩倍。Cyber Recovery 解決方案可以掃描的資料越多，發現隱匿惡意軟體或其他損毀情況的機會就越高。

VM 工作負載支援

VM 工作負載是指 VM 在實體主機伺服器或雲端環境中執行的應用程式、服務或工作。由於這些工作負載在功能和其他許多方面可能有所不同，會增加工作負載暴露於惡意軟體的風險，因此掃描 VM 至關重要。Rubrik Security Cloud Data Threat Analytics (包括 Anomaly Detection、Threat Monitoring、Threat Hunting 及資料復原服務，都可在受保護的資源上使用)[39] 支援掃描下列的 VM 工作負載：[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense 支援掃描下列的 VM 工作負載：[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- 具有 Dell Avamar 或 Dell NetWorker 備份的 Hyper-V

VMware 聲稱「多達 80% 的虛擬化工作負載都採用 VMware 技術執行」。[44] 在 2024 年第一季，雲端基礎結構服務市場最受歡迎的供應商 Amazon Web Services (AWS) 掌握了整個市場的 31%。Microsoft Azure 以 25% 的市佔率位居第二。[45]

核心基礎結構

核心基礎結構是實現技術環境運作的基礎元件和服務。在此層級偵測惡意軟體有助於降低攻擊的嚴重程度，因為核心基礎結構功能可能會影響許多系統和使用者。Rubrik Security Cloud 文件未提及支援掃描任何核心基礎結構。[46]

相較之下，CyberSense 支援掃描下列的核心基礎結構：[47]

- Active Directory
- DNS
- LDAP

可能包含文件、合約及智慧財產權的使用者檔案

Rubrik Security Cloud Data Threat Analytics 支援掃描下列的使用者檔案：[48]

- NAS 檔案集和資料集
- Windows 磁碟區群組
- Linux 和 Windows

CyberSense 可以掃描 Linux 和 Windows 使用者檔案。[49]

資料庫

應用程式會因為許多原因而可以使用不同類型的資料庫，因此能夠偵測各種資料庫中是否有惡意軟體，是快速回應的關鍵所在。Rubrik Security Cloud Data Threat Analytics 可以備份資料庫，但我們找不到該軟體可以掃描這些資料庫備份的公開文件。

CyberSense 支援使用頁面層級掃描來掃描下列資料庫：[50]

- SQL
- PostgreSQL
- Oracle®
- Epic® Caché
- SAP HANA
- MariaDB/MySQL
- Db2

其他用戶端進行的備份

有些組織可能擁有多家供應商的資料備份，以便提供備援、遵守法規或某些其他重要原因。Rubrik Security Cloud 文件未提及支援掃描其他備份用戶端製作的備份。[51]

CyberSense 在此類別中具有明顯優勢，可支援掃描下列備份用戶端製作的備份：[52, 53, 54]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Exchange
- Avamar
- CommVault

掃描技術

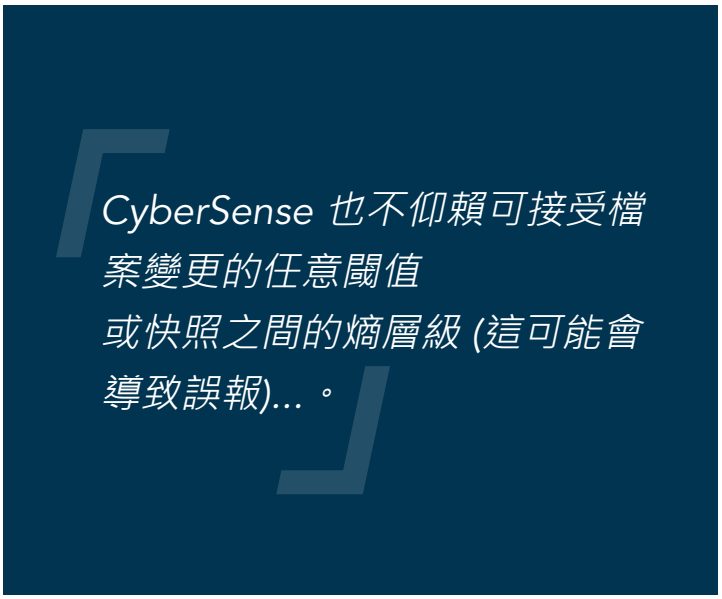
Rubrik Security Cloud 包含許多掃描用的工具，可協助在 Data Threat Analytics 中進行掃描：

- Rubrik Anomaly Detection 顯示可疑檔案、快照變更[55] 以及異常詳細資訊，並做為異常事件供客戶在快照調查中研究和使用。[56]該軟體還提供復原選項。[57]
- Rubrik VM Encryption Detection 可偵測對 VMware vSphere 虛擬磁碟檔案的攻擊。[58]
- Rubrik Threat Monitoring 顯示偵測到的威脅和相符項目相關資訊。[59]
- Rubrik Threat Hunt 是使用者發起的掃描，用以尋找入侵指標。[60]
- Rubrik Quarantine 會隔離出現在威脅搜捕中的物件。[61]

Rubrik RSC 還為每個 Rubrik 叢集提供 Rubrik Backup Service Connectors。

Rubrik 客戶必須為工作選擇正確的工具、可能必須手動啟動掃描，或是使用多項工具來完成工作。相較之下，Dell 只有一個 CyberSense 掃描選項，客戶可能會發現這樣更容易管理。

相較於 Rubrik RSC Data Threat Analytics 的「僅限表層」掃描，CyberSense 能夠掃描得更深入。CyberSense 可完整掃描檔案內容，並以頁面層級掃描資料庫，也可以偵測部分加密的檔案。[62] 該工具使用由 Index Engines 針對數千種資料威脅進行訓練的機器學習 (ML) 資料庫，並包含 200 多個分析點，可偵測資料損毀情況。[63] 與 Rubrik Threat Monitoring 和 Threat Hunt 不同的是，CyberSense 不仰賴外部威脅情報機構提供惡意軟體簽章，而是自己探索新的威脅。[64] **CyberSense 也不仰賴可接受檔案變更的任意閾值或快照之間的熵層級 (這可能會導致誤報)**，更不會將 ML 訓練成符合以前客戶行為的基準。[65, 66, 67]



Rubrik 異常偵測軟體僅依靠中繼資料來判斷快照是否損毀，然後再進行任何內容分析。相較於 CyberSense 持續進行的 ML，Rubrik 軟體會在取得簽章後探索損毀。Rubrik 異常偵測需要建立一個行為模型來定義客戶的正常基準。這可能需要多個備份才能建立。Rubrik 行為模型至少需要兩個備份，才能在沒有攻擊時建立檔案系統典型變更的基準。但是，只有一組變更統計資料可能不足以建立典型情況。業務事件可能會觸發更多或更少的活動，或者觸發更多未在第一個和第二個 Rubrik 快照之間發生的可疑類型活動。Rubrik 解決方案分析的備份越多，就越能準確地訓練出符合基準的行為模型。[68, 69]

CyberSense 將所有分析結果儲存在存放庫中。在檔案系統行為分析管道中，Rubrik 將有關客戶檔案系統變更的中繼資料傳送到 Polaris 雲端平台進行行為分析，從而開啟攻擊面。[70]

客戶只能透過 Rubrik Enterprise Edition 使用 Rubrik Threat Monitoring 和 Threat Hunt。[71] 客戶必須使用角色型存取控制 (RBAC) 權限執行 Threat Hunt 掃描，而且使用者必須指明想要搜捕哪個特定入侵指標 (IOC)。[72] 這不是業界最佳實務。[73] Threat Hunt 與 CyberSense 相似，都支援 VMware、AHV、Hyper-V、NAS 檔案集以及 Linux 和 Windows 伺服器。[74]

下列章節會進一步詳細說明 Rubrik 解決方案如何提供威脅偵測。

中繼資料和檔案系統統計資料

Rubrik Anomaly Detection ML 行為模型將上次快照以來的檔案系統變更 (例如新增、刪除或移動的檔案數) 記錄為中繼資料。[75] 然後，ML 模型會根據這些變更進行訓練，為檔案系統建立行為模型「基準」。如果 Rubrik 偵測到太多變更，會將快照標記為異常。在行為分析標記快照後，該解決方案就會開始分析檔案內容。[76]監控中繼資料可多提供一層安全性，但可能無法提供必要保護來協助防止或減少事件造成的停機時間。

相反地，**CyberSense 不需要基準；它可以監視和分析從第一個備份副本開始的檔案和資料庫內容變更。** CyberSense 的方法更加細膩，因為該軟體甚至可以分析檔案片段，或是資料庫的個別頁面。CyberSense 掃描與 Rubrik 解決方案類似，都包含中繼資料屬性，並將結果饋送到 ML 引擎。相較於 Rubrik 解決方案，CyberSense 不只有中繼資料掃描，而且 Index Engines 會使用自己記錄的攻擊來訓練 ML 引擎，而不是使用簽章或客戶以前的行為訓練。[77, 78]

> *CyberSense 不需要基準；它可以監視和分析從第一個備份副本開始的 檔案和資料庫內容變更。*

閾值

Rubrik ML 在分析行為時，會判斷檔案系統發生異常的可能性。如果 Rubrik 解決方案發現可能性很高，就會執行內容分析。這可能是由行為模型決定的「異常行為」閾值。例如，當 Rubrik 解決方案看到許多新檔案或修改過的檔案，或是隨機性或加密指標增加時，就可能標記為異常行為。[79] 在分析內容時，Rubrik Anomaly Detection會顯示檔案內容的變更，並透過計算檔案系統的熵，來計算加密的可能性。檔案系統的熵有助於顯示勒索軟體攻擊已經加密檔案的可能性。如果熵超過異常閾值，解決方案會提醒使用者。[80, 81] 偵測資料損毀的有效性取決於閾值有多嚴格。過度寬鬆可能會導致誤報，進而產生虛假的安全感。[82]客戶必須妥善地設定閾值。

相較之下，CyberSense 是透過掃描檔案內容來檢查部分加密的檔案，在偵測資料損毀情況時能提供 99.99% 的信心 (根據 Dell 和 Index Engines)。[83]

簽章和副檔名

Rubrik Threat Monitoring 和 Threat Hunt 會掃描快照來尋找 IOC。Rubrik 監控的多個威脅情報來源之一探索到新的 IOC 時，Threat Monitoring 會將包含 Yet Another Ridiculous Acronym (YARA) 規則 (用來識別新的惡意軟體，也稱為惡意軟體簽章) 的威脅資料推送到所有 Rubrik 叢集。然後，叢集會開始掃描。[84] 最新的 WatchGuard 報告指出，有 57.8% 的惡意軟體會避開簽章偵測。BianLian 等進階惡意軟體可以使用方法來避開簽章識別，而且新惡意軟體變體的簽章可能與原始惡意軟體略有不同。因此，威脅情報可能更難隨時掌握最新資訊。[85]

相較之下，CyberSense 使用 200 多筆分析資料，並提供由數千種勒索軟體變體訓練而成的 ML 模型。Index Engines 已經證實，CyberSense 方法無須下載簽章，即可偵測從未見過的複雜變體，[86] 這是在事件發生時不仰賴網際網路的另一個優勢。

大量加密事件

Rubrik 解決方案會計算整個檔案系統的熵，藉此監控大量加密事件。[87] CyberSense 的做法更加細膩，不僅會掃描一般的檔案系統，甚至是每個單獨的檔案，還會掃描檔案的內部內容片段。根據 Index Engines 的說法，只計算整個檔案的熵，而不計算檔案片段，「只會偵測到極端加密的整個檔案」，或是大量加密事件。[88]

復原能力

根據文件內容，我們認為使用 Dell PowerProtect Cyber Recovery 執行復原，比使用 Rubrik 更簡單、更精簡。本報告章節及其子章節對比了兩種解決方案的復原功能，以及解決方案如何執行這些功能。

Rubrik 文件指出他們有哪些復原功能適用於哪些 VM 類型。這似乎提供了實用的層級細節，但這許多規定和變化也使復原過程變得複雜。例如，當 Rubrik 客戶需要復原資料、檔案及系統時，必須選擇要納入復原計畫中的快照物件。Rubrik 建立一或多個復原計畫後，會提供許多復原能力選項，包括：[89, 90, 91, 92, 93]

- 透過下載或覆寫復原檔案，並復原到獨立資料夾、匯出到其他主機，或是匯出到叢集服務
- 透過下載或覆寫復原 VM 檔案，並復原到獨立資料夾，或是匯出到另一個虛擬機器
- 透過下列方式對 VM 或磁碟快照進行完整的快照復原：
  - Live Mount，從快照建立新的 VM
  - 掛載虛擬磁碟，從快照建立新的虛擬磁碟
  - 即時復原，將目前的 VM 替換成快照所建立的新 VM
  - 匯出，透過所選資料儲存區的快照建立新的 VM
  - 批次復原 VM
- 透過 Live Mount 和匯出，為復原計畫提供大量 Cyber Recovery
- Rubrik Security Cloud Orchestrated Application 復原作業可將 VM 災難復原到隔離的沙箱、遠端網站或是就地復原

Rubrik 批次復原進一步展示了有多複雜。表 1 顯示 Rubrik 根據 Hypervisor 提供的批次復原功能。[94]

1 Rubrik 為不同 Hypervisor 提供的批次復原功能。資料來源：Rubrik。

VM 建立選項				
	Live Mount	**Live Mount，可選擇遷移**	**匯出**	**即時復原**
vSphere VM	可用，使用 Rubrik 叢集作為其資料儲存區	無法使用	可用，使用已復原 Hypervisor 的資料儲存區	可用，使用 Rubrik 叢集作為其資料儲存區
AHV VM	可用，使用 Rubrik 叢集作為其資料儲存區	可用，使用 Rubrik 叢集作為其資料儲存區，並使用 Nutanix 容器進行所有後續寫入	可用，使用 Nutanix 容器作為其資料儲存區	無法使用
Hyper-V 虛擬機器	可用，使用 Rubrik 叢集作為其資料儲存區	無法使用	可用，使用已復原 Hypervisor 的資料儲存區	可用，將目前的 VM 替換成快照中的新 VM。使用 Rubrik 叢集做為其資料儲存區。

至於 Rubrik 解決方案，復原的資料儲存區通常位於 Rubrik 叢集，而不是生產環境；這可能會產生問題。我們將在下一節 "Rubrik limitations" 介紹這些問題。相較之下，PowerProtect 可以將復原的資料放在復原或生產環境中，讓復原過程更快、更順暢，將停機時間降到最低。

表 2 顯示 Rubrik 有關復原 vSphere VM 的其他資訊。[95]如該表所示，大部分的 vSphere 復原資料儲存區都位於 Rubrik 叢集。

2 Rubrik 為 vSphere VM 提供的復原功能。資料來源：Rubrik。

Rubrik 為 vSphere 提供的復原功能				
動作	**資料存放區**	**電源狀態**	**網路**	**來源 VM**
復原檔案	不適用	不適用	不適用	無影響
Live Mount	本機 Rubrik 叢集	開啟或關閉	已中斷連線	無影響
掛載虛擬磁碟	本機 Rubrik 叢集	時間：	已中斷連線	無影響
即時復原	本機 Rubrik 叢集	時間：	已連線 (選用)	已關閉電源並重新命名
匯出	Hypervisor 的資料儲存區	關閉	已中斷連線	無影響
就地復原	Hypervisor 的資料儲存區	時間：	與來源 VM 相同	就地復原會使用快照中的虛擬磁碟資料覆寫來源 VM 的虛擬磁碟檔案，不必變更 VM 的屬性

Rubrik 解決方案並未廣泛執行大量復原，而且大量復原選項有限又複雜。正如本報告 "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" 一節進一步說明，Dell PowerProtect 更加簡化又簡單。

破解大量復原

Rubrik 宣稱具備大量復原，其定義是透過大規模復原應用程式、檔案或使用者的方式，快速恢復業務營運；[96] 並提供許多大量復原的選項。但是，Rubrik 解決方案通常會將復原的資料儲存在 Rubrik 叢集，而不是生產環境。[97]工作負載取決於 Rubrik 系統的可用性，直到解決方案完成遷移。本機 Rubrik 叢集是層級 3 的儲存裝置，因此客戶必須額外遷移到叢集的生產環境，才能恢復至預定的效能層級。由於系統完成遷移時會遇到這種單一故障點和效能降低情況，因此我們認為 Rubrik 解決方案將工作負載復原到生產環境後，復原作業才算完成。

Dell PowerProtect 可讓使用者在復原 UI 中選擇多個要復原的 VM，這樣就能進行大量復原。

Dell PowerProtect Data Manager 可提供等同於 Rubrik「大量復原」的操作

相較於 Rubrik 解決方案，Dell 解決方案還為 vSphere VM 提供多個程度相同的復原選項。Dell PowerProtect 可以將 VM 資料放在復原或生產環境中。大部分 Rubrik 選項只能將資料放在 Rubrik 叢集。表 3 顯示 Dell 復原選項。[98, 99, 100, 101]

3 Dell 復原選項。資料來源：Principled Technologies。

Dell 復原選項	
類型	**關於此功能**
檔案層級還原	只能就地或透過復原方式還原受感染的檔案
即時 VM	將 VM 還原到叢集，稍後再遷移到生產環境
還原至新環境	還原到原始環境或新環境 (例如無塵室或復原基礎結構)，在此期間，使用者可以一次選擇多個 VM 進行大量還原或大規模還原
存取/即時 VM	建立生產資料的隔離副本
Recovery Orchestration	讓管理員能夠安排復原或隨需提供；優先將 VM 自動復原到生產環境或復原環境

Rubrik 限制

Rubrik 解決方案會隔離遭惡意軟體感染的快照，供日後分析使用。但是，Rubrik 解決方案預設為不隔離快照。客戶可以自行手動或使用第三方工具下載隔離檔案，並對其執行鑑識分析，而這可能會使自己面臨惡意軟體的攻擊。[102, 103]

> *CyberSense 會自行分析，使用者不必自己執行鑑識，而且此軟體會自動建立還原點。*

CyberSense 預設為分析檔案和資料庫。使用者無須手動隔離快照。**CyberSense 會自行分析，使用者不必自己執行鑑識，而且此軟體會自動建立還原點。**[104]

對許多功能來說，僅限 RSC 管理模式下的 Rubrik RSC 是單一故障點。最令人擔憂的是，攻擊可能會導致 RSC 服務中斷，影響到使用者網際網路連線，或是使用者網站與 RSC 之間的連線。經過此類攻擊之後，該解決方案會透過 Rubrik CDM UI 或 API 式自動化，為使用者提供一組有限的功能，但前提是使用者在攻擊之前已經建立 RSC 服務帳戶。[105, 106] 組織可以在沒有 RSC 的情況下復原下列工作負載和資料：MongoDB、Microsoft Exchange、檔案、Hyper-V 快照、從管理磁碟區進行的 Live Mount、NAS 主機檔案、Oracle、SQL Server、VCD 以及 VMware。[107] 在沒有 RSC 的情況下復原 SAP HANA 需要第三方工具，例如 Studio 和 Cockpit Cross，以及透過支援通道提供的 Rubrik 支援。在沒有 RSC 的情況下復原 IBM Db2 需要 IBM 第三方工具，以及透過支援通道提供的 Rubrik 支援。[108]

實體隔離/隔離

NIST 將實體隔離定義為「兩個系統之間的介面，在該介面上 (a) 彼此沒有實體連接，而且 (b) 不會自動化任何邏輯連線 (也就是資料只會在人為控制下透過介面手動傳輸)。」[109]

實體隔離可協助控制從來源到目標的資料流，也可成為任何勒索軟體防護和 Cyber Recovery 策略的重要環節。如果攻擊或事件侵害到您的生產備份系統，阻止生產系統和 Cyber Recovery 存放庫中受保護備份之間的流量，就可提供安全防護。

實體隔離

您可能在電影《不可能的任務》中看過實體隔離解決方案的範例；主角必須繞過其他所有設施的安全性功能，才能使用未連線到任何外部網路的電腦系統存取敏感資料。實體隔離還可以運用專屬實體網路通常會中斷連線的區段，將備份副本從生產系統傳輸到存放庫。中斷連線時，這些可運作實體隔離會形成資料無法自動跨越的實際障礙，讓不肖份子更難取得存取權。

組織可以實體隔離 Dell PowerProtect Cyber Recovery，協助實現可運作實體隔離策略。該解決方案使用專屬的實體連線，並且在複製資料時從存放庫提取，而不是透過備份解決方案推送。複製時，解決方案會啟動連線、加密資料，並透過專屬線路遷移資料。[110]複製完畢後，解決方案會再次停用與存放庫的連線。此解決方案透過鎖定保留原則讓存放庫副本維持不可變，因此，即便使用者或系統取得存取權，也無法修改或刪除存放庫副本。管理流

量未經過複製路徑，因此，**即使不肖份子控制了到場備份解決方案，存放庫也會啟動並中斷與複製路徑的連線，而且只能單向從資料來源提取資料，進而限制直接存取存放庫。**[111]

邏輯隔離

另一方面，邏輯隔離使用可能位於同一實體網路的系統，但是會建立邏輯網路分隔和控制，確保系統無法互相傳送資料。此解決方案還會使用其他安全性實作，例如加密、雜湊以及 RBAC 和多因素驗證，確保未經授權的系統或使用者無法讀取位於另一個系統的資料。

Rubrik 表示自己的 Cyber Recovery 功能採用邏輯實體隔離策略。[112, 113] Rubrik 有許多的公開聲明都對實體隔離的必要性提出質疑。Rubrik 在一篇名為《Rubrik Security – Air Gap and Immutability》(Rubrik 安全性—實體隔離和不變性) 的簡報中聲稱，他們的原生解決方案採用實體隔離，因為一旦解決方案取得備份後，就無法存取或編輯，即便 Rubrik 裝置仍在實體網路上也一樣。[114] 但是，取得驗證的不肖份子仍然可以取得裝置 GUI 的存取權，這會影響到復原作業。為了緩解此情況，Rubrik 使用保留鎖定來防止備份過期，讓備份維持不可變。啟用保留鎖定後，還可以防止 Rubrik 叢集執行原廠重設和抹除。根據 Rubrik CDM 安全性指南，該解決方案預設在叢集上全域停用保留鎖定，客戶必須聯絡 Rubrik 支援部門才能啟用。[115]公開資料來源沒有說明 Rubrik 支援部門是否也可停用保留鎖定，不禁令人擔憂，取得授權的不肖份子仍可繞過安全性層級。

「管理流量未經過複製路徑，因此，即使不肖份子控制了到場備份解決方案，存放庫也會啟動並中斷與複製路徑的連線，而且只能單向從資料來源提取資料，進而限制直接存取存放庫。」

結論

組織必須積極考量針對資料中心的眾多攻擊手法。完善的資料保護計畫是要保護所有資料安全，尤其是對營運至關重要的關鍵資料。我們查看 Dell PowerProtect Cyber Recovery 和 Rubrik Secure Cloud 可公開取得的資訊，藉此瞭解這兩種解決方案如何管理、保護及復原資料。

PowerProtect Cyber Recovery 將關鍵資料的備份副本實體隔離在存放庫中，萬一遭遇網路攻擊，可以確保得以復原。此解決方案採用實體隔離的可運作實體隔離策略，這是仰賴邏輯隔離的 Rubrik Secure Cloud 解決方案無法宣稱的特色。

Cyber Recovery 在 CyberSense 中使用 ML 型分析來評估存放庫中資料的完整性，並識別復原用的無錯誤備份資料。相較之下，Rubrik Secure Cloud 則是提供經過 ML 訓練的分析工具來尋找異常情況，而不是深入掃描檔案。

此外，Cyber Recovery 解決方案提供多種復原選項，並利用存放庫中未受損的資料順暢有效率地恢復營運。在許多情況下，PowerProtect Cyber Recovery 可提供 Rubrik Secure Cloud 所欠缺的功能和優勢，因此能提供可能更安全的解決方案，透過更深入的分析，將停機時間降到最低並加速復原。

---

1. Anastasia Dergacheva 和 Jesse R. Taylor，《Study Finds Average Cost of Data Breaches Continued to Rise in 2023》(研究發現資料違規的平均成本在 2023 年持續上升)，存取時間：2024 年 7 月 25 日，https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023。
2. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)，存取時間：2024 年 4 月 18 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. Rubrik，《Rubrik Security Cloud Architecture and Security Implementation》(Rubrik 安全性雲端架構與安全性時作)，存取時間：2024 年 4 月 18 日 https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf。
5. Rubrik，《Rubrik Security Cloud Architecture and Security Implementation》(Rubrik 安全性雲端架構與安全性時作)，存取時間：2024 年 4 月 18 日，https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf。
6. Rob Emsley，《Public Cloud Vault to Secure, Isolate and Recover Data》(保護、隔離及復原資料用的公有雲存放庫)，存取時間：2024 年 3 月 20 日，https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/。

7. Brian White，《Dell’s PowerProtect Cyber Recovery Expands to Microsoft Azure》(Dell PowerProtect Cyber Recovery 擴展到 Microsoft Azure)，存取時間：2024 年 3 月 20 日，https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/。
8. Dell，《Cyber Recovery on Google Cloud Platform》(Google Cloud Platform 上的 Cyber Recovery)，存取時間：2024 年 3 月 20 日，https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/。
9. Chris Mellor，《Up to $5m compensation if Rubrik Cloud Vault recovery busted》(如果 Rubrik Cloud Vault 復原失敗會獲得最高 500 萬美元補償)，存取時間：2024 年 3 月 20 日，https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/。
10. Kristina Avrionova，《Frequently Asked Questions about Rubrik Cloud Vault》(Rubrik Cloud Vault 常見問題集)，存取時間：2024 年 3 月 20 日，https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault。
11. 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：2024 年 3 月 22 日，https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf。
12. Dell，《Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability》(Data Domain 無損架構：提升資料完整性與復原能力)，存取時間：2024 年 6 月 7 日，https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf。
13. Dell，《Consolidate Governance and Compliance Archive Data》(整合控管和法規遵循的歸檔資料)，存取時間：2024 年 4 月 4 日，https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/。
14. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)，存取時間：2024 年 3 月 24 日，https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf。
15. Rubrik，《Retention-locked SLA Domain attributes》(保留鎖定的 SLA 網域屬性)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html。
16. Rubrik，《Rubrik Cyber Recovery》(Rubrik 網路復原)，存取時間：2024 年 3 月 20 日，https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf。
17. Rubrik，《Rubrik Licensing: Subscribe to Simplicity》(Rubrik 授權：訂閱簡潔性)，存取時間：2024 年 3 月 20 日，https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf。
18. Rubrik，《Workloads require third-party tools for recovery》(工作負載需要第三方工具來進行復原)，存取時間：2024 年 5 月 6 日，https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html。
19. Rubrik，《Recoverable workloads during RSC service disruption》(RSC 服務中斷期間的可復原工作負載)，存取時間：2024 年 5 月 6 日，https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html。
20. Rubrik，《Workloads require third-party tools for recovery》(工作負載需要第三方工具來進行復原)。
21. Dell，《Strengthen your security posture with Managed Detection and Response》(運用 Managed Detection and Response 強化安全性狀態)，存取時間：2024 年 4 月 2 日 https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf。
22. Dell，《Dell PowerProtect Cyber Recovery 19.13 Installation Guide》(Dell PowerProtect Cyber Recovery 19.13 安裝指南)，存取時間：2024 年 3 月 20 日，https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us。
23. Dell，《Dell PowerProtect Cyber Recovery 19.13 Installation Guide》(Dell PowerProtect Cyber Recovery 19.13 安裝指南)。
24. Dell，《Dell PowerProtect Cyber Recovery 19.13 Installation Guide》(Dell PowerProtect Cyber Recovery 19.13 安裝指南)。
25. Dell，《Installing CyberSense in Dell PowerProtect Cyber Recovery》(在 Dell PowerProtect Cyber Recovery 中安裝 CyberSense)，存取時間：2024 年 3 月 20 日，https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/。
26. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。
27. Rubrik，《Downloading and installing Rubrik CDM》(下載和安裝 Rubrik CDM)，存取時間：2024 年 3 月 20 日，https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html。
28. Rubrik，《Setting up a Rubrik cluster using the UI》(使用 UI 設定 Rubrik 叢集)，存取時間：2024 年 3 月 20 日，https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html。
29. Rubrik，《Setting up a Rubrik cluster using the CLI》(使用 UI 設定 Rubrik 叢集)，存取時間：2024 年 3 月 20 日，https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html。
30. Rubrik，《Registering Rubrik clusters using the online method》(使用線上方法註冊 Rubrik 叢集)，存取時間：2024 年 3 月 20 日，https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html。
31. Rubrik，《Registering Rubrik clusters using the offline method》(使用離線方法註冊 Rubrik 叢集)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html。
32. Rubrik，《Enabling MFA》(啟用 MFA)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html。
33. Rubrik，《Adding the initial account》(新增初始帳戶)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html。
34. TrustRadius，《Learning Rubrik by putting the pieces together Brik by Brik》(逐步拼湊來瞭解 Rubrik)，存取時間：2024 年 3 月 21 日，https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04。
35. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。

36. Index Engines，《CyberSense®: How it Works》(CyberSense®：運作方式)，存取時間：2024 年 3 月 21 日，https://www.indexengines.com/how-it-works
37. Rubrik，《Anomaly event details》(異常事件詳細資料)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html。
38. Rubrik，《Events page》(事件頁面)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/common/events_page.html。
39. Rubrik，《RSC Data Threat Analytics》(RSC 資料威脅分析)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html。
40. Rubrik，《RSC Data Threat Analytics》(RSC 資料威脅分析)。
41. Dell Technologies，《Dell PowerProtect Cyber Recovery: Reference Architecture》(Dell PowerProtect Cyber Recovery：參考架構)，存取時間：2024 年 5 月 6 日，https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf。
42. Dell Technologies，《Dell EMC Avamar for Hyper-V》，存取時間：2024 年 5 月 16 日https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf。
43. Dell Technologies，《Dell EMC NetWorker Module for Microsoft for Hyper-V》，存取時間：2024 年 5 月 16 日 https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf。
44. VMware，《Accelerate IT.Innovate with your cloud.》(加速 IT。利用雲端創新。)，2024 年 5 月 9 日，https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf。
45. Statista，《Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024》(2017 年第四季到 2024 年第一季全球雲端基礎結構服務供應商市佔率)，2024 年 7 月 17 日，https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/。
46. Rubrik，《RSC Data Threat Analytics》(RSC 資料威脅分析)。
47. Dell Technologies，《CyberSense® for PowerProtect Cyber Recovery》，存取時間：2024 年 6 月 27 日，https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf。
48. Rubrik，《RSC Data Threat Analytics》(RSC 資料威脅分析)。
49. Index Engines，《CyberSense® Support Matrix》(CyberSense® 支援矩陣)，存取時間：2024 年 3 月 21 日，https://www.indexengines.com/csmatrix。
50. Dell Technologies，《CyberSense® for PowerProtect Cyber Recovery》。
51. Rubrik，《Keep Your Databases Running in the Face of Any Threat》(不論遇到任何威脅都讓資料庫保持運作)。
52. Index Engines，《CyberSense® Support Matrix》(CyberSense® 支援矩陣)。
53. Dell Technologies，《Dell EMC Avamar for Hyper-V》。
54. Dell Technologies，《Dell EMC NetWorker Module for Microsoft for Hyper-V》。
55. Rubrik，《Anomaly incidents》(異常事件)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html。
56. Rubrik，《Data Threat Analytics events》(資料威脅分析事件)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/ri_events.html。
57. Rubrik，《Viewing Anomaly Detection》(檢視異常偵測)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html。
58. Rubrik，《VM Encryption Detection》(VM 加密偵測)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html。
59. Rubrik，《Viewing the Threat Monitoring page》(檢視威脅監控頁面)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html。
60. Rubrik，《Initiating a threat hunt》(啟動威脅搜捕)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html。
61. Rubrik，《Quarantining matched files or objects》(隔離比對到的檔案或物件)，存取時間：2024 年 4 月 2 日，https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html。
62. Dell，《CyberSense® for PowerProtect Cyber Recovery》。
63. Dell，《CyberSense® for PowerProtect Cyber Recovery》。
64. Index Engines，《The Power of CyberSense’s Machine Learning》(CyberSense 機器學習的強大之處)，存取時間：2024 年 4 月 2 日 https://go.indexengines.com/csmachinelearning。
65. Index Engines，《The Power of CyberSense’s Machine Learning》(CyberSense 機器學習的強大之處)。
66. Index Engines，《The Power of CyberSense’s Machine Learning》(CyberSense 機器學習的強大之處)。
67. Dell，《CyberSense® for PowerProtect Cyber Recovery》。
68. Rubrik，《Anomaly Detection behavioral model》(異常偵測行為模型)，存取時間：2024 年 5 月 20 日，https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html。
69. Amazon，《Training ML Models》(訓練 ML 模型)，存取時間：2024 年 4 月 2 日 https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html。
70. Rubrik，《Defense in Depth with Polaris Radar》(透過 Polaris Radar 全面防禦)，存取時間：2024 年 3 月 21 日，https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf。
71. Rubrik，《Data Threat Analytics dashboard》(資料威脅分析儀表板)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html。
72. Rubrik，《Initiating a threat hunt》(啟動威脅搜捕)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html。
73. SentinelOne，《What Is A Malware File Signature (And How Does It Work)?》(惡意程式檔案簽章是什麼 (以及如何運作)？)，存取時間：2024 年 4 月 4 日，https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/。

74. Rubrik，《Threat hunts》(威脅搜捕)，存取時間：2024 年 3 月 21 日，https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html。
75. Rubrik，《Anomaly Detection features》(異常偵測功能)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/ri_features.html。
76. Rubrik，《Behavioral model》(行為模型)。
77. Index Engines，《The Power of CyberSense’ s Machine Learning》(CyberSense 機器學習的強大之處)。
78. Dell，《CyberSense® for PowerProtect Cyber Recovery》。
79. Rubrik，《Behavioral model》(行為模型)。
80. Rubrik，《Anomaly Detection features》(異常偵測功能)。
81. Rubrik，《Behavioral model》(行為模型)。
82. Dell，《CyberSense® for PowerProtect Cyber Recovery》。
83. Morningstar，《Index Engines’ CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery》(Index Engines 的 CyberSense 宣稱在偵測勒索軟體損毀方面有 99.99% SLA，為更智慧化的復原提供助力)，存取時間：2024 年 7 月 17 日，https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery。
84. Rubrik，《Threat Monitoring》(威脅監控)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html。
85. Index Engines，《The Power of CyberSense’ s Machine Learning》(CyberSense 機器學習的強大之處)。
86. Index Engines，《The Power of CyberSense’ s Machine Learning》(CyberSense 機器學習的強大之處)。
87. Rubrik，《Anomaly Detection features》(異常偵測功能)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/ri_features.html。
88. Index Engines，《The Power of CyberSense’ s Machine Learning》(CyberSense 機器學習的強大之處)。
89. Rubrik，《Investigating and recovering anomalous files for filesets》(針對檔案集調查和復原異常檔案)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html。
90. Rubrik，《Investigating and recovering anomalous files for virtual machines》(針對虛擬機器調查和復原異常檔案)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html。
91. Rubrik，《Full snapshot recovery of a virtual machine》(虛擬機器的完整快照復原)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html。
92. Rubrik，《Recovery of a batch of virtual machines》(批次復原虛擬機器)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html。
93. Rubrik，《Performing bulk recovery for Recovery Plans》(針對復原計畫執行大量復原)，存取時間：2024 年 3 月 22 日，https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html。
94. Rubrik，《Recovery of a batch of virtual machines》(批次復原虛擬機器)，存取時間：2024 年 4 月 4 日，https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html。
95. Rubrik，《Recovery of virtual machines》(復原虛擬機器)，存取時間：2024 年 4 月 16 日，https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html。
96. 復原的資料儲存區通常位於 Rubrik 叢集，而不是生產環境。
97. Rubrik，《Recovery of a batch of virtual machines》(批次復原虛擬機器)，存取時間：2024 年 4 月 16 日，https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html。
98. Dell，《Restore plan》(還原計畫)，存取時間：2024 年 4 月 16 日，https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/。
99. Dell，《PowerProtect Data Manager overview》(PowerProtect Data Manager 概覽)，存取時間：2024 年 4 月 16 日，https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/。
100. Dell，《PowerProtect Data Manager 19.9 Administration and User Guide》(PowerProtect Data Manager 19.9 管理和使用者指南)，存取時間：2024 年 4 月 16 日，https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client。
101. Dell，《Recovery Orchestration with PowerProtect Data Manager Overview》(使用 Recovery Orchestration 搭配 PowerProtect Data Manager 概覽)，存取時間：2024 年 4 月 16 日 https://www.youtube.com/watch?v=po2oMnAg_x4。
102. Rubrik，《Quarantine files or objects》(隔離檔案或物件)，2024 年 3 月 24 日，https://docs.rubrik.com/en-us/saas/saas/quarantine.html。
103. Rubrik，《Downloading quarantined files for forensic analysis》(下載隔離的檔案以進行鑑識分析)，2024 年 3 月 24 日，https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html。
104. Forrester，《The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery》(Dell PowerProtect Cyber Recovery 的總體經濟影響)，存取時間：2024 年 4 月 16 日，https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf。
105. Rubrik，《Workload recovery during an RSC service disruption》(RSC 服務中斷期間的工作負載復原)，存取時間：2024 年 4 月 16 日，https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html。
106. Rubrik，《Rubrik CDM APIs and service account workflows》(Rubrik CDM API 與服務帳戶工作流程)，存取時間：2024 年 4 月 16 日，https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html。
107. Rubrik，《Recoverable workloads during RSC service disruption》(RSC 服務中斷期間的可復原工作負載)，存取時間：2024 年 4 月 16 日，https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html。
108. Rubrik，《Workloads require third-party tools for recovery》(工作負載需要第三方工作來進行復原)，存取時間：2024 年 4 月 16 日，https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html。

109. NIST，《Computer Security Resource Center Glossary: air gap》(電腦安全性資源中心詞彙：實體隔離)，存取時間：2024 年 7 月 29 日，https://csrc.nist.gov/glossary/term/air_gap。

110. Dell，《Dell PowerProtect Cyber Recovery Solution Guide》(Dell PowerProtect Cyber Recovery 解決方案指南)。

111. Dell，《Dell PowerProtect Cyber Recovery: Reference Architecture》(Dell PowerProtect Cyber Recovery：參考架構)。

112. Adam Eckerle，《Debunking the Myths about Air Gaps》(破解實體隔離的誤解)，存取時間：2024 年 3 月 14 日，https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps。

113. Rubrik，《Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value》(實體隔離、隔離復原與勒索軟體 - 成本與價值的比較)，存取時間：2024 年 3 月 14 日，https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf。

114. Brian Williams，《Rubrik Air Gap and Immutability》(Rubrik 實體隔離與不變性)，存取時間：2024 年 3 月 14 日，https://vimeo.com/561870246。

115. Rubrik，《Retention locks in the Rubrik cluster》(Rubrik 叢集中的保留鎖定)，存取時間：2024 年 3 月 18 日，https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html。

▶ 檢視本報告的原始英文版本

此專案是由 Dell Technologies 委託執行。