DELL Technologies

備份滲透：使用 Dell Technologies 強化網路安全和復原能力

執行摘要

備份滲透對各產業企業構成越來越大的威脅，其會利用旨在保護重要資訊之系統中的漏洞來進行。這些攻擊會損害資料復原系統、破壞信任並危及運作。從重大財務損失到長時間停機和聲譽損害，可能導致嚴重後果。

Dell Technologies 提供一套端對端防禦措施以保護敏感性資料及防範此類攻擊，包括 Dell Trusted Device、Dell Trusted Infrastructure，以及整合至我們所有解決方案的廣泛安全性功能。隨著策略合作關係和專業服務的加入，Dell 可協助組織建立具復原能力的多層式安全性架構，以有效率地偵測、防堵備份滲透事件並從中復原。

透過導入 Dell 的創新解決方案和專家支援，企業將可做好更充分的準備來保護基礎結構，並維持營運持續性。

備份滲透威脅日益加劇

備份系統對於業務持續性至關重要，有助於在發生勒索軟體或硬體故障等網路事件後的復原作業。不幸的是，這些重要的生命線逐漸成為網路犯罪分子的目標。備份滲透會損毀或刪除備份資料，使其在最需要時無法存取。

這些不斷演進的威脅必須採取積極主動的措施來因應。未能保護備份系統，將會危及運作並暴露敏感性資料。從小型企業到跨國公司，各種規模的企業都是潛在的目標，醫療保健、金融和製造業等產業尤其面臨風險。

Dell Technologies 體認到強化備份環境的迫切性，並提供進階工具和指導方針來抵禦這些複雜攻擊。

備份滲透攻擊

當網路犯罪分子利用備份系統中的漏洞入侵、損壞或加密重要復原資料時，即發生備份滲透。這些複雜的攻擊可能與勒索軟體或惡意軟體部署等其他事件同時發生或緊接著發生，進而擴大對營運和財務的負面影響。

備份攻擊的運作方式

1. **初始入侵：**攻擊者常透過網路釣魚、弱式認證或未修補的漏洞，未經授權存取網路。
2. **橫向移動：**一旦進入網路，攻擊者就會使用工具在不被發現的情況下移動，並鎖定備份儲存庫和重要資料集。
3. **備份入侵：**關鍵手法包括加密備份檔案、刪除復原點或毀損資料。

常用手法

- **竊取憑證**以入侵管理帳戶，啟用對備份系統的完全存取權。
- **部署勒索軟體**以加密即時資料和備份，要求支付解密費用。
- **定時損毀**以逐漸入侵備份以規避偵測，同時在需要復原時讓企業暴露在風險之下。

這些手法突顯出這些威脅的複雜性和嚴重性，因而需要採取先發制人的行動。

對企業的影響

財務損失

備份滲透會提高復原成本和停機時間，通常會使因應費用翻倍或變為三倍。從加密或遭入侵的備份中復原可能需要支付攻擊者、新的基礎結構或昂貴的顧問費用。

營運中斷

如果沒有可用的備份，組織將面臨冗長的回復時間，導致服務中斷、專案延遲及關鍵功能停擺。

聲譽影響

永久性資料遺失或長時間停機會削弱利害關係人的信任，進而可能損害企業的長期生存能力。

現實範例

一家全球醫療保健供應商在勒索軟體攻擊期間發現其備份已毀損。儘管支付了贖金，但三週的患者資料永久遺失，手術延遲並引發訴訟。復原成本總額超過 **$5,000 萬美元**。

令人擔憂的統計資料

最近的研究估計，遭入侵的備份系統所造成的平均財務損失超過 **$445 萬美元**[1]，其中包括罰款、停機時間和復原費用。尤其令人擔憂的是此類事件的頻率不斷上升，全球報告顯示，與備份相關的威脅比去年同期增加 **39%**。

57%
以備份為目標的攻擊成功滲透備份儲存庫

資料來源：2024 年：Index Engines

透過 Dell Technologies 對抗備份滲透

Dell Technologies 提供一套健全的工具和服務，可因應備份滲透攻擊帶來的獨特難題，讓企業能有效預防、偵測和復原。

伺服器和儲存安全性解決方案

Dell 的伺服器和儲存解決方案可針對備份目標工作提供無與倫比的復原能力。內建功能可確保備份安全無虞，且快照不受影響。

- **不可變的備份/快照**可建立防篡改的還原點。
- **實體隔離復原**可將資料與即時網路隔離，以防止損毀。

[1] Ponemon - Cost of a Data Breach Report 2024 (Ponemon - 2024 年資料違規的成本報告)

強化 Dell Data Protection 應用裝置

Dell Data Protection 應用裝置內嵌的功能包括用於韌體完整性的 Dell SafeBIOS，以及用於安全加密的 SafeData，以協助防範備份攻擊。此外，這些解決方案還具有多因素驗證 (MFA)、角色型存取控制 (RBAC) 和雙重驗證等功能，可阻止威脅發動者進入。

使用 CrowdStrike 實現進階威脅偵測

CrowdStrike 與 Dell Data Protection 之間的整合，透過一系列進階功能，專注於強化資料保護環境的安全性和監控能力。

1. **端點和資料保護：**Dell 將 CrowdStrike 的端點安全性及延伸偵測和回應 (EDR/XDR) 與其 Data Protection Solutions 整合。其中包括從 Dell 的 PowerProtect Data Manager 和 PowerProtect Data Domain 收集的遙測資料，以及 CrowdStrike Falcon 主控台和新一代 SIEM 軟體的安全性深入解析
2. **監控和回應：**Dell 的 Managed Detection and Response (MDR) 服務能代表客戶管理 CrowdStrike 軟體、收集記錄，並調查任何入侵指標 (IoC) 或異常偵測。此整合功能可讓 Dell 持續監控，並與客戶的 SOC 協同合作，以確保實現快速有效的威脅補救
3. **即時可見度和資料移動控制：**CrowdStrike Falcon Data Protection 平台可讓您即時掌握不同來源和通道的資料移動情況，並依內容和情境對資料進行分類。這有助於防止資料遭竊，並透過結合內容與情境分析，確保有效執行資料保護原則
4. **統一管理和簡化部署：**整合功能可讓您透過單一平台和代理程式管理端點和資料保護，從而降低複雜性和營運負擔。這得益於 CrowdStrike Falcon 平台的輕量級雲端原生方法，進而實現快速部署並將中斷降至最低

CrowdStrike 與 Dell Data Protection 之間的整合運用進階 EDR/XDR 功能、即時監控和全方位資料管理功能，以提升資料保護環境的整體安全性和復原能力。

一家頂尖的金融機構最近部署 PowerProtect Cyber Recovery，在侵駭期間防止攻擊者存取 90% 的重要備份，無須支付贖金即可順暢還原。

適用於備份完整性的 Dell PowerProtect 解決方案

Dell PowerProtect 提供全方位的備份保護，運用不變性、隔離和壓縮，防止備份系統遭入侵。PowerProtect 與勒索軟體偵測工具整合，確保可疑變更會觸發警示，以便立即採取行動。

多層式安全性方法

保護資料需要經過協調的多層面安全性策略。Dell 可協助企業實作業界最佳實務，打造具復原能力的備份環境。

增強防禦的關鍵步驟

- **採用零信任原則：**持續驗證所有使用者、裝置和程序，降低未經授權存取的風險。
- **加密所有備份：**確保資料在傳輸中和靜態下，若遭入侵將無法讀取。
- **教育員工：**教導員工識別導致初始入侵的網路釣魚嘗試和其他社交工程手法。
- **定期漏洞測試：**頻繁的測試可協助組織在攻擊者利用弱點之前，識別和修補弱點。

Dell 將這些實務與尖端解決方案搭配，打造健全且反應迅速的基礎結構，以因應新興挑戰。

加強安全性的策略合作關係

Dell 與 Microsoft、CrowdStrike 和 Secureworks 等網路安全領導者合作。每段合作關係均可強化 Dell 的解決方案，為客戶提供無與倫比的保護功能，例如進階威脅情報、端點監控和全方位回應策略。

運用 Dell Professional Services

Dell Technologies 的 Professional Services 可提供專業知識和指引，協助企業有效應對複雜的網路安全挑戰。從建立事件回應計畫到實作零信任架構，Dell 專家會確保用戶端環境具有復原能力，可因應備份滲透等現代威脅。

透過 Dell 打造企業復原能力

選擇 Dell Technologies 可讓企業戰勝老練的攻擊者，同時維持營運連續性。Dell 透過創新、合作關係及專業知識，確保組織能預防、偵測和從最嚴重的備份滲透攻擊中復原。

跨出下一步

請立即聯絡 Dell Technologies，保護您的企業安全。我們將攜手合作確保您的重要資產安全無虞、保護您的聲譽，並打造具復原能力的未來。

Dell 持續致力在數位時代建立信心，為組織提供安全營運並蓬勃發展所需的工具、知識和支援。

備份復原能力始於 Dell Technologies。立即行動，讓營運能與時俱進，建立對網路安全態勢的信心。

造訪 **Dell.com/SecuritySolutions**，瞭解如何解決當今一些首要網路安全挑戰

深入瞭解
Dell 解決方案

聯絡 Dell
Technologies 專家

檢視更多資源

使用 #HashTag 加入對話

DELL Technologies