DELL Technologies

解決方案摘要

CyberSense® for PowerProtect Cyber Recovery

用於偵測、診斷和從網路攻擊中復原的 AI 機器學習、分析和鑑識工具

CYBERSENSE 優勢

CyberSense® 已與 Dell PowerProtect Cyber Recovery 存放庫解決方案完全整合。

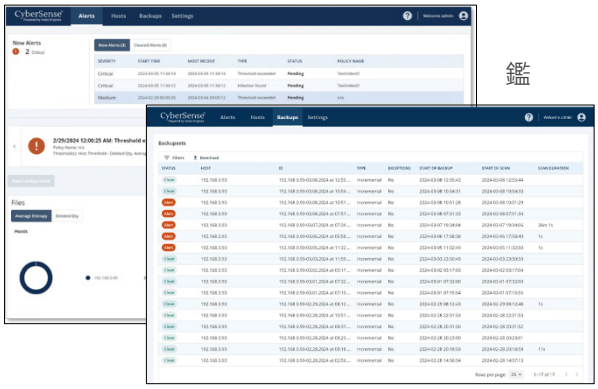
- 這項整合支援對備份資料的自動定期掃描，以驗證資料的完整性，並在偵測到可疑行為時發出警示。
- CyberSense 能夠直接掃描備份映像內部，包括 Dell NetWorker、Avamar、PowerProtect Data Manager 等，不必將資料解除凍結就能分析內容。
- CyberSense 的獨特功能之一，就是可在每次掃描資料後提供完整的內容分析，即便是複雜的勒索軟體攻擊也將無所遁形，僅檢查中繼資料的輕量級掃描工具很容易忽略這類攻擊。
- 當攻擊發生時，CyberSense 會提供攻擊後的鑑識報告，以便讓您瞭解攻擊的深度和廣度，並提供損毀前最後的良好備份集清單以加速修復程序。

CyberSense 不同於其他資料分析方法，可提供信心水準更高的完整備份資料，並能在攻擊發生後迅速修復。

當傳統的安全性工具無法保護資料免受網路攻擊時，**CyberSense®** 會主動介入，以 99.5% 的準確率偵測攻擊後的資料損毀情形，並促進智慧型快速復原。CyberSense 是全球數以千計組織的最後一道防線和第一線復原機制，可確保其資料資產 (包括核心基礎結構、生產資料庫和關鍵文件) 的完整性，組織無需擔心資料遭到惡意損毀。

CyberSense 會運用資料備份觀察這段時間的資料變化，接著利用 AI 機器學習來偵測指出勒索軟體攻擊的損毀跡象。機器學習隨後會根據來檢驗這超過 200 項的內容型分析，以 99.5% 的信心度找出損毀，幫助您保護業務關鍵的基礎結構和內容。CyberSense 可偵測核心基礎結構 (包括 Active Directory、DNS 等)、使用者檔案，以及關鍵生產資料庫中因複雜攻擊所導致的的大量刪除、加密及其他可疑變更活動。CyberSense 在偵測到損毀跡象後會在操作介面中產生警示，並附上該攻擊的規模和影響相關資訊。

當發生可疑行為時，CyberSense 會提供攻擊後的鑑識報告，協助診斷網路攻擊的損害範圍。在偵測到資料損毀時，將可使用最後已知良好的備份資料集清單來支援精心打造的快速復原功能，並有助於有效減少業務中斷和資料遺失。



Cyber Recovery 工作流程

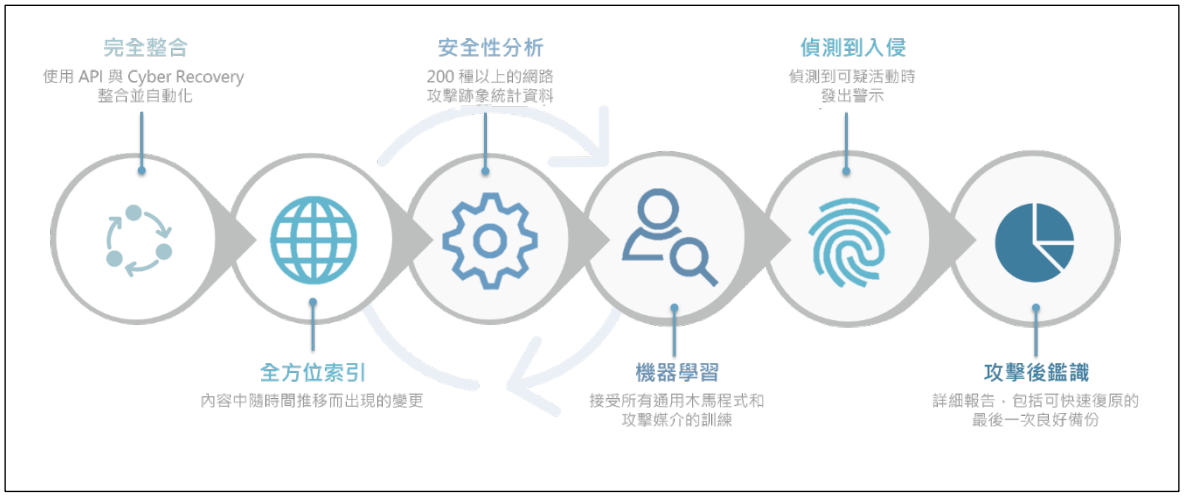
CyberSense 緊密整合 Dell PowerProtect Cyber Recovery，可主動監控檔案和資料庫，藉由分析資料的完整性來偵測勒索軟體造成的損毀。在資料複製到 Cyber Recovery 存放庫並套用保留鎖定後，CyberSense 就會自動啟動對備份檔案的全方位掃描，建立檔案、資料庫以及核心基礎結構的時間點觀察。這些觀察結果可讓 CyberSense 嚴謹地追蹤檔案如何隨時間變更，即便最複雜的網路威脅也將無所遁形，有效找出資料損毀情形。

CyberSense 能夠直接掃描備份映像內的資料，無需使用原始備份軟體，也不必解除凍結資料。CyberSense 可藉由進階分析來識別檔案或資料庫頁面的加密/損毀、辨識已知的惡意軟體副檔名、偵測大量刪除/建立檔案等。

利用經最新木馬程式和勒索軟體訓練的 AI 機器學習演算法，CyberSense 可對指出網路攻擊的資料損毀做出確定性的決策。Cyber Recovery 在發生攻擊時會在操作介面中立即顯示嚴重警示。此外，CyberSense 還會提供攻擊後的鑑識報告，有助於快速診斷並從勒索軟體攻擊中復原，有效減少資料遺失。

完整內容分析

CyberSense 是目前市面上唯一能夠對所有受保護資料提供完整內容分析的產品。這項功能使得 CyberSense 從其他解決方案中脫穎而出，而不僅僅是對資料進行高階檢視，運用分析根據中繼資料尋找損毀的明顯跡象。中繼資料層級的損毀並不難偵測，例如將檔案副檔名變更為 .encrypted，或檔案大小不尋常的變化。這些類型的攻擊無法代表現今網路犯罪者所採用的複雜攻擊。



CyberSense 並非僅使用中繼資料的解決方案，而是採用完整內容分析來偵測資料損毀。此功能可稽核檔案和資料庫是否遭受攻擊，包括僅限內容的檔案結構損毀，或是文件或資料庫頁面內的部分加密。這些攻擊無法透過分析來發現，只能透過掃描檔案內部，比較檔案長時間的變化才能察覺。如果沒有基於完整內容的分析，誤報數量將非常可觀，進而混淆您對於資料完整性和安全性的判斷。此外，還可根據已更改檔案或檔案類型的數量或百分比、新增或刪除的檔案以及整個主機中的熵值，來建立自訂閾值警示。

支援的資料類型

CyberSense 可透過各種資料類型來產生分析。其中包括核心基礎結構 (如 DNS、LDAP、Active Directory 等)、非結構化檔案 (如文件、合約、智慧財產權)，以及資料庫 (包括 Oracle、DB2、SQL、PostgreSQL、Epic Caché 等)。

摘要

CyberSense 已與 Dell PowerProtect Cyber Recovery 完全整合，可稽核資料並偵測入侵和損毀指標。CyberSense 讓您能夠主動瞭解發動中網路攻擊的損害範圍，促進實施快速診斷和復原計畫，進而減少業務中斷情形和相關重大支出。

深入瞭解 Dell PowerProtect Cyber Recovery	連絡 Dell Technologies 專家	深入瞭解 CyberSense	加入與 #PowerProtect 的對話