DELL Technologies

解決方案簡介

CyberSense® for Dell PowerProtect Cyber Recovery

以採用 AI 技術的分析和鑑識工具，用更智慧的方式偵測、診斷和從網路攻擊中復原

CYBERSENSE 優勢

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

- 自動定期掃描備份資料，以驗證資料完整性，並在偵測到可疑行為時發出警示。
- 直接掃描 Dell Avamar、NetWorker、Commvault、NetBackup 及 PowerProtect Data Manager 中的備份映像內容，無需重新水合資料。
- 每次資料掃描皆提供深層的完整內容分析，以偵測最複雜的勒索軟體攻擊。
- 針對 YARA 規則和惡意軟體特徵自訂警示，以偵測勒索軟體或內部惡意人士的已知行為。
- 提供攻擊後的鑑識報告以促成更智慧且更快速的復原，讓您詳細掌握攻擊的深度和廣度，並提供損毀前最後的良好備份集清單。

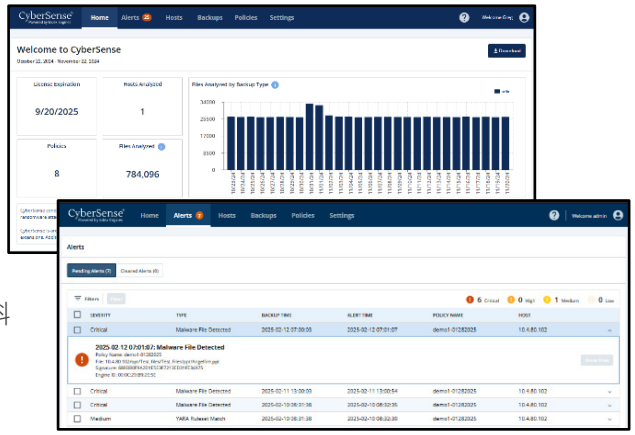
CyberSense 不同於其他資料分析方法，可讓您更放心相信備份資料完整無缺，並能在攻擊發生後迅速修復。

隨著網路攻擊頻率持續上升，網路犯罪者變得更加強韌，傳統的安全工具已不足以保護資料免於網路攻擊。

CyberSense® 可在遭受攻擊後以 99.99% 的準確率偵測資料損毀*，並推動智慧快速修復。CyberSense 是全球數以千計組織的第一線復原機制，可確保資料資產 (包括核心基礎結構、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 會掃描 Cyber Recovery 存放庫中的資料備份，觀察資料的長時間變化。接著，再運用機器學習與 AI 技術，偵測可能代表勒索軟體攻擊的毀損跡象。系統會將資料與超過 200 項內容型分析比對，以 99.99% 的信心度* 找出損毀，協助您保護關鍵業務基礎結構和內容。CyberSense 可偵測核心基礎結構 (包括 Active Directory、DNS 等)、檔案保存庫、檔案系統以及資料庫中，因複雜攻擊所導致的大量刪除行為、加密及其他可疑變更活動。

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。偵測到資料損毀時，系統會提供最後已知良好的備份資料集清單來支援快速的精選復原功能，協助盡可能減少業務中斷和資料遺失，進而降低網路復原的成本。

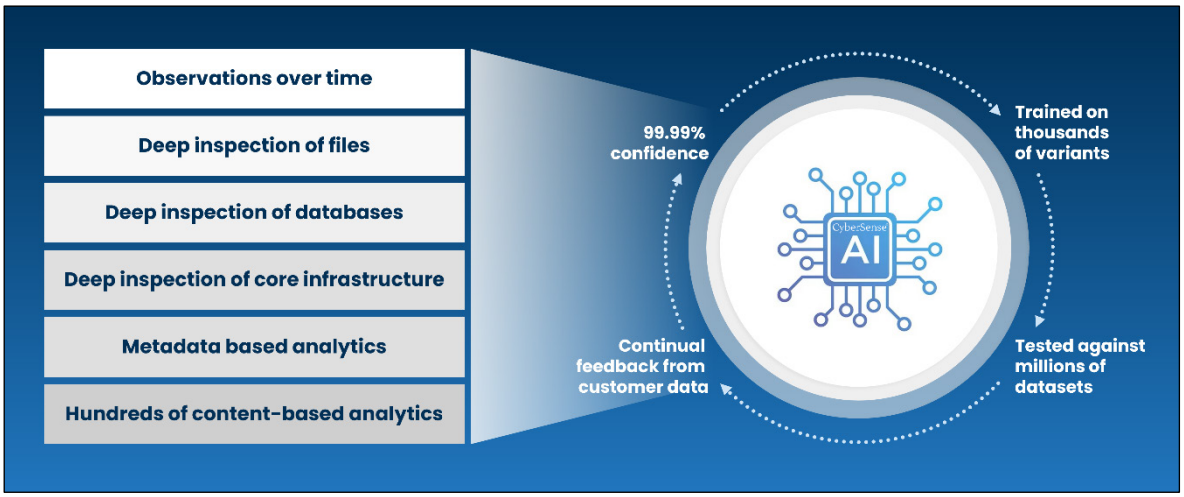


Cyber Recovery 工作流程

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。 CyberSense 會嚴謹地追蹤檔案的長時間變化，有效找出資料損毀情形，即便最複雜的網路威脅也將無所遁形。

完整內容分析

CyberSense 是目前市面上唯一能針對所有受保護資料，提供完整內容索引與分析的產品。CyberSense 深度 AI 分析執行涵蓋所有資料，產生準確度達 99.99%* 的機率性決策，判定資料是否完整，抑或是已遭勒索軟體損毀。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 超越僅使用中繼資料的解決方案，使用完整內容分析來偵測資料損毀。它會稽核檔案及資料庫，偵測可能代表發生攻擊的變更，包括全檔案或部分檔案的損毀。傳統的分析工具會忽視這些威脅，造成錯誤的信心。使用者可根據檔案內的變更、新增的檔案或刪除的檔案，自訂閾值警示，也可以實作自訂 YARA 規則與惡意軟體特徵，對備份內容執行順向和逆向的惡意軟體偵測。

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，可分析存放庫資料並偵測入侵和損毀的行為跡象。CyberSense 讓您能夠主動瞭解發動中網路攻擊的損害範圍，有助於實施快速診斷和復原計畫，進而減少業務中斷情形和相關高昂代價。

深入瞭解 Dell PowerProtect Cyber Recovery

聯絡 Dell Technologies 專家

深入瞭解 CyberSense

加入與 #PowerProtect 的對話

*根據 Index Engines 委託企業策略集團 (ESG) 發表的報告《Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption》(Index Engines 的 CyberSense 經驗證在偵測勒索軟體損毀的有效率為 99.99%)。2024 年 6 月