DELL Technologies

Solution brief

CyberSense® per PowerProtect Cyber Recovery

Strumenti forensi, di analisi e di apprendimento automatico basati sull'AI per rilevare, diagnosticare e ripristinare l'ambiente da attacchi informatici

IL VANTAGGIO DI CYBERSENSE

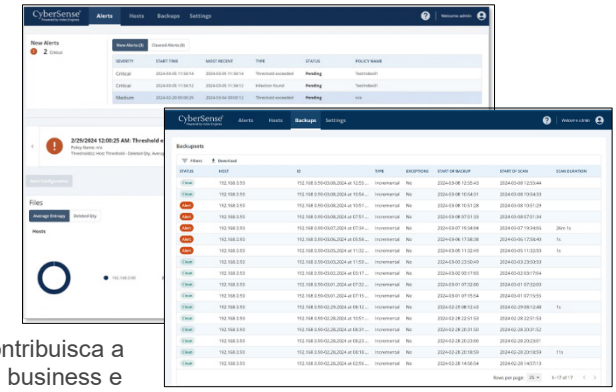
CyberSense® è completamente integrato con la soluzione vault Dell PowerProtect Cyber Recovery.

- Questa integrazione favorisce un approccio automatizzato verso la scansione regolare dei dati di backup per convalidare l'integrità dei dati e avvisare quando viene rilevato un comportamento sospetto.
- Grazie alla capacità di CyberSense di eseguire la scansione diretta all'interno delle immagini di backup, tra cui Dell NetWorker, Avamar, PowerProtect Data Manager e altro ancora, è possibile analizzare i contenuti senza la necessità di riattivare i dati.
- Solo CyberSense offre l'analisi completa dei contenuti a ogni scansione dei dati per rilevare anche gli attacchi ransomware più sofisticati, che facilmente non vengono individuati dagli strumenti di scansione leggeri che ispezionano solo i metadati.
- Quando si verifica un attacco, CyberSense fornisce anche report forensi successivi per comprendere la profondità e l'ampiezza dell'attacco e fornisce un elenco degli ultimi backup set validi prima del danneggiamento, per facilitare il processo di ripristino.

CyberSense si distingue da altri approcci di analisi dei dati e offre un livello più elevato di certezza che i dati di backup siano integri, in modo da ripristinarli rapidamente dopo un attacco.

Quando gli strumenti di sicurezza convenzionali non sono in grado di salvaguardare i dati dagli attacchi informatici, **CyberSense®** interviene per rilevare il danneggiamento dei dati dopo un attacco con una precisione del 99,5% e facilitare il ripristino intelligente e rapido. Ultima linea di difesa e prima linea di ripristino per migliaia di organizzazioni in tutto il mondo, CyberSense garantisce l'integrità dei data asset, tra cui l'infrastruttura core, i database di produzione e i documenti critici, infondendo fiducia che i dati siano protetti da danneggiamenti malevoli.

CyberSense sfrutta i backup di dati per osservare come i dati cambiano nel tempo e quindi utilizza l'apprendimento automatico basato sull'AI per rilevare segni di danneggiamento indicativi di un attacco ransomware. L'apprendimento automatico esamina quindi oltre 200 analisi basate sui contenuti per trovare il danneggiamento con una sicurezza del 99,5%, aiutandoti a proteggere l'infrastruttura e i contenuti business-critical. CyberSense rileva inoltre eliminazioni di massa, crittografia e altri cambiamenti sospetti nell'infrastruttura core (ad esempio Active Directory, DNS e così via), nei file utente e nei database di produzione critici risultanti da attacchi sofisticati. Se CyberSense rileva segni di danneggiamento, viene generato un avviso nel dashboard con informazioni aggiuntive che descrivono in dettaglio la portata e l'impatto dell'attacco.



Quando si verifica un comportamento sospetto, CyberSense fornisce report forensi dopo un attacco per diagnosticare il raggio di esplosione dell'attacco informatico. Quando viene rilevato un danneggiamento dei dati, è disponibile un elenco degli ultimi set di dati di backup validi noti per supportare il ripristino rapido e accurato che contribuisca a ridurre al minimo l'interruzione del business e la perdita di dati.

Flusso di lavoro di Cyber Recovery

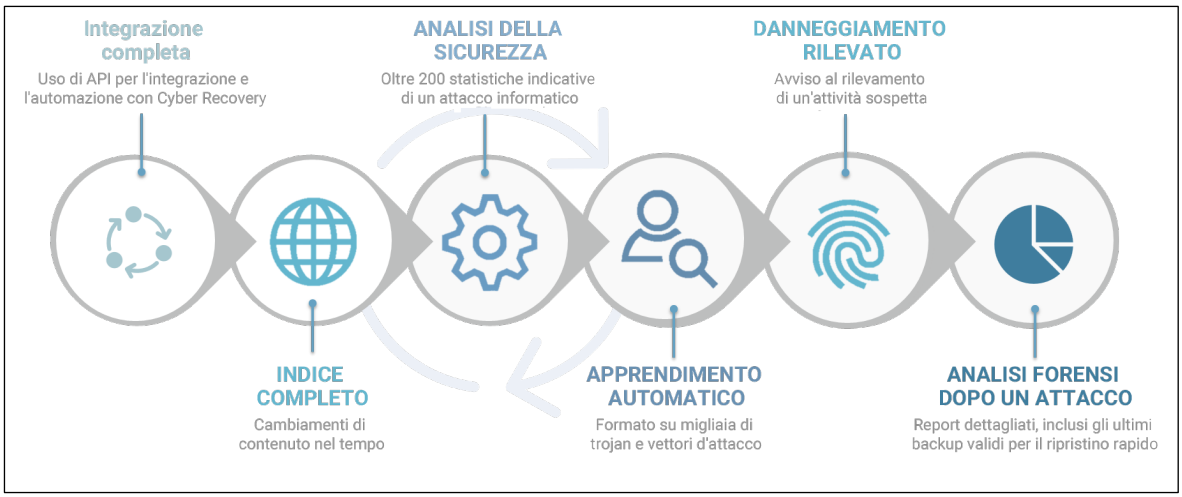
CyberSense si integra perfettamentecon Dell PowerProtect Cyber Recovery, monitorando attivamente file e database per rilevare il danneggiamento da ransomware analizzando l'integrità dei dati. Una volta replicati i dati nel vault di Cyber Recovery e applicato il blocco di retention, CyberSense avvia automaticamente una scansione completa dei dati di backup, creando osservazioni point-in-time di file, database e infrastruttura core. Grazie a queste osservazioni CyberSense monitora meticolosamente le modifiche apportate nei file nel tempo, rilevando efficacemente i dati danneggiati anche dalle minacce informatiche più sofisticate.

La scansione di CyberSense opera direttamente sui dati all'interno dell'immagine di backup, eliminando la necessità del software di backup originale e della riattivazione dei dati. Tramite l'analisi avanzata, CyberSense identifica la crittografia/il danneggiamento di file o pagine del database, riconosce le estensioni malware note, rileva eliminazioni/creazioni di file di massa e altro ancora.

Utilizzando algoritmi di apprendimento automatico basati sull'AI e addestrati con i trojan e i ransomware più recenti, CyberSense prende decisioni deterministiche sul danneggiamento dei dati che sono indicative di un attacco informatico. In caso di attacco, un avviso critico viene prontamente visualizzato nel dashboard di Cyber Recovery. Inoltre, CyberSense offre report forensi dopo un attacco, velocizzando la diagnosi e il ripristino dagli attacchi ransomware per ridurre al minimo la perdita di dati.

Analisi completa dei contenuti

CyberSense è l'unico prodotto sul mercato che offre analisi complete basate sui contenuti su tutti i dati protetti. Questa funzionalità distingue CyberSense da altre soluzioni che offrono una vista generale dei dati e utilizzano analisi che individuano segni evidenti di danneggiamento sulla base dei metadati. La corruzione a livello di metadati non è difficile da rilevare, ad esempio, modificando l'estensione di un file in .encrypted o modificando radicalmente le dimensioni del file. Questi tipi di attacco non rappresentano gli attacchi sofisticati che i criminali informatici utilizzano oggi.



CyberSense va oltre le soluzioni basate solo sui metadati, perché si basa sull'analisi completa dei contenuti per rilevare il danneggiamento dei dati. Controlla i file e i database alla ricerca di attacchi che includono il danneggiamento della struttura dei file basato solo sui contenuti o la crittografia parziale all'interno di un documento o di una pagina di un database. Non è possibile rilevare questi attacchi utilizzando analisi che non eseguono la scansione all'interno del file per confrontarne le modifiche nel tempo. Senza l'analisi completa basata sui contenuti, il numero di falsi negativi sarà significativo, fornendo un falso senso di fiducia nell'integrità e nella sicurezza dei dati. Inoltre, è possibile creare avvisi di soglia personalizzati in base alla quantità o alla percentuale di file modificati o al tipo di file, ai file aggiunti o eliminati e all'entropia in un host.

Tipi di dati supportati

CyberSense genera analisi da una gamma completa di tipi di dati, tra cui l'infrastruttura core come DNS, LDAP, Active Directory, file non strutturati come documenti, contratti, proprietà intellettuale e database come Oracle, DB2, SQL, PostgreSQL, Epic Caché e così via.

Riepilogo

Completamente integrato con Dell PowerProtect Cyber Recovery, CyberSense controlla i dati e rileva gli indicatori di compromissione e danneggiamento. Grazie a CyberSense è possibile comprendere in modo proattivo il raggio di esplosione di un attacco informatico in atto, facilitando l'implementazione di un piano per velocizzare la diagnosi e il ripristino, mitigando così l'interruzione del business e le spese significative ad essa associate.

Ulteriori informazioni su Dell PowerProtect Cyber Recovery	Contatta un esperto Dell Technologies	Ulteriori informazioni su CyberSense	Partecipa alla conversazione con #PowerProtect