Breve

CyberSense® per Dell PowerProtect Cyber Recovery

Strumenti forensi e di analisi basati sull'AI per processi più intelligenti di rilevamento, diagnosi e ripristino da attacchi informatici

IL VANTAGGIO DI CYBERSENSE

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

- Automatizza la scansione regolare dei dati di backup per convalidarne l'integrità e avvisare in caso di rilevamento di un comportamento sospetto.
- Scansiona direttamente i contenuti all'interno delle immagini di backup da Dell Avamar, NetWorker, CommVault, NetBackup e PowerProtect Data Manager senza la necessità di riattivare i dati.
- Offre analisi complete e approfondite dei contenuti con ogni scansione dei dati, per rilevare anche gli attacchi ransomware più sofisticati.
- Avvisi personalizzati per regole YARA e firme malware per rilevare comportamenti noti associati a ransomware o a malintenzionati interni.
- Facilita un ripristino più rapido e intelligente con report forensi post-attacco per ottenere informazioni dettagliate sulla profondità e l'ampiezza dell'attacco e fornisce un elenco degli ultimi backup set validi prima del danneggiamento.

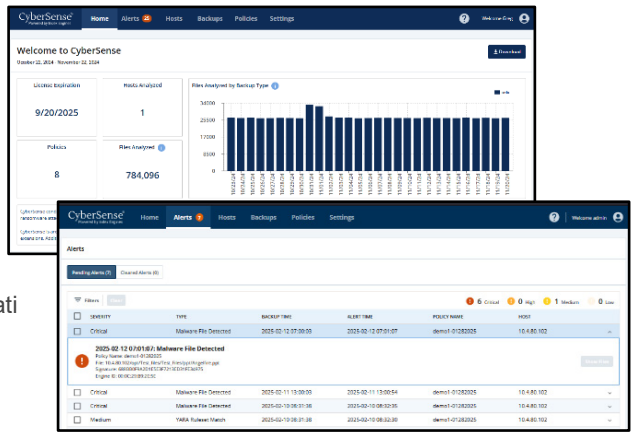
CyberSense si distingue da altri approcci di analisi dei dati e offre un livello più elevato di certezza che i dati di backup siano integri, in modo da ripristinarli rapidamente dopo un attacco.

Con il costante aumento della frequenza degli attacchi informatici e la maggior resilienza degli autori di tali attacchi, gli strumenti di sicurezza convenzionali non riescono a proteggere i dati in modo efficace.

CyberSense® permette di rilevare il danneggiamento dei dati dopo un attacco con il 99,99% di precisione e facilita il recupero rapido e intelligente. Come 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 e i documenti critici, infondendo fiducia che i dati siano protetti da danneggiamenti malevoli.

CyberSense esegue la scansione dei backup dei dati in un vault di Cyber Recovery per osservare le modifiche avvenute nel corso del tempo. Utilizza quindi l'apprendimento automatico e l'AI per rilevare i segni di danneggiamento che indicano un attacco ransomware. I dati vengono confrontati con oltre 200 analisi basate sui contenuti per individuare il danneggiamento con una sicurezza del 99,99%, favorendo la protezione dell'infrastruttura e dei 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 repository di file, nei file system e nei database critici risultanti da attacchi sofisticati.

Quando si verifica un comportamento sospetto, CyberSense fornisce report forensi post-attacco per diagnosticare l'onda d'urto dell'attacco informatico. Quando viene rilevato un danneggiamento dei dati, è disponibile un elenco degli ultimi data set di backup validi noti per supportare ripristini rapidi e accurati che contribuiscano a ridurre al minimo l'interruzione del business e la perdita di dati, limitando così i costi di Cyber Recovery.

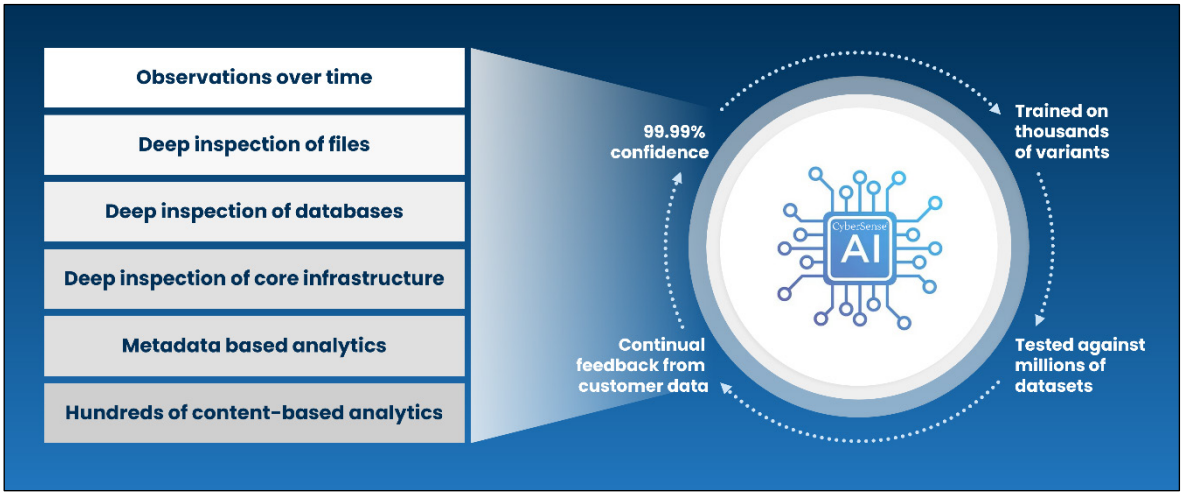


Flusso di lavoro di Cyber Recovery

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. CyberSense monitora meticolosamente le modifiche apportate nei file nel tempo, rilevando con efficacia i dati danneggiati anche dalle minacce informatiche più sofisticate.

Analisi completa dei contenuti

CyberSense è l'unico prodotto sul mercato che offre indicizzazioni e analisi complete basate sui contenuti su tutti i dati protetti. L'approfondita analisi basata sull'AI di CyberSense viene eseguita sulla totalità dei dati e viene generata una decisione probabilistica con una precisione del 99,99%* per stabilire se i dati sono integri oppure se sono stati danneggiati da ransomware. 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 su metadati e rileva il danneggiamento dei dati sfruttando l'analisi completa dei contenuti. Controlla file e database per rilevare eventuali modifiche indicative di un attacco, incluso il danneggiamento completo o parziale dei file. Le analisi tradizionali non individuano queste minacce, generando un falso senso di fiducia. È possibile impostare gli avvisi di soglia personalizzati in base alle modifiche apportate ai file, ai file aggiunti o a quelli eliminati. È inoltre possibile implementare regole YARA personalizzate e firme malware per il rilevamento di malware in avanti e indietro nei backup.

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 analizza i dati del vault e rileva gli indicatori comportamentali di compromissione e danneggiamento. Grazie a CyberSense è possibile comprendere in modo proattivo l'onda d'urto di un attacco informatico in atto, facilitando l'implementazione di un piano per velocizzare la diagnosi e il ripristino e limitare 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

Dati basati sul report ESG commissionato da Index Engines, "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption". Giugno 2024