DELL Technologies

Lösungsüber

CyberSense® für Dell PowerProtect Cyber Recovery

KI-basierte Analysen und forensische Tools zur Erkennung, Diagnose und intelligenten Recovery nach Cyberangriffen

VORTEIL VON CYBERSENSE

CyberSense® ist vollständig in die Dell PowerProtect Cyber Recovery Vault-Lösung integriert.

- Automatisiert das regelmäßige Scannen von Backupdaten, um die Integrität der Daten zu überprüfen und Warnmeldungen auszugeben, wenn verdächtige Aktivitäten erkannt werden.
- Scannt Inhalte direkt von Backup-Images von Dell Avamar, NetWorker, Commvault, NetBackup und PowerProtect Data Manager, ohne dass die Daten aufbereitet werden müssen.
- Liefert bei jedem Scannen der Daten vollständige Inhaltsanalysen, um selbst die raffiniertesten Ransomwareangriffe zu erkennen.
- Benutzerdefinierte Warnmeldungen für YARA-Regeln und Malware-Signaturen zur Erkennung von bekannten Verhaltensweisen von Ransomware oder internen böswilligen AkteurInnen.
- Vereinfacht eine intelligentere und schnellere Recovery durch forensische Berichte nach einem Angriff und bietet detaillierte Einblicke in die Reichweite und den Umfang des Angriffs. Die Lösung stellt auch eine Liste der letzten fehlerfreien Backupsätze vor der Beschädigung bereit.

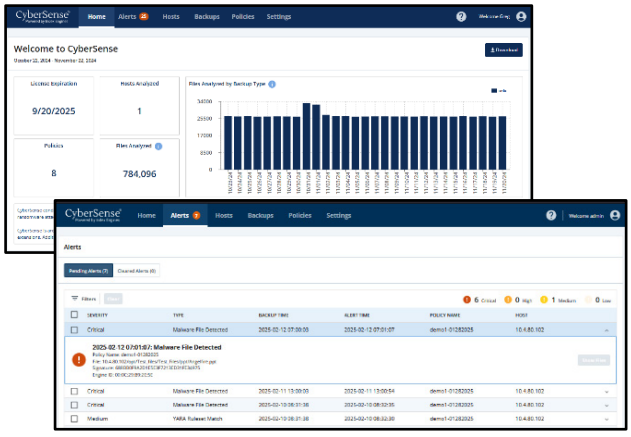
CyberSense hebt sich von anderen Datenanalyseansätzen ab und bietet ein höheres Maß an Vertrauen in die Integrität von Backupdaten, die nach einem Angriff schnell wiederhergestellt werden können.

Da die Häufigkeit von Cyberangriffen weiter zunimmt und Cyberkriminelle widerstandsfähiger werden, reichen herkömmliche Sicherheitstools nicht mehr aus, um Daten vor Cyberangriffen zu schützen.

CyberSense® erkennt beschädigte Daten nach einem Angriff mit einer Genauigkeit von 99,99 %* und ermöglicht eine intelligente und schnelle Wiederherstellung. Als erstes Mittel zur Recovery für Tausende von Unternehmen weltweit stellt CyberSense die Integrität Ihrer Datenbestände sicher, einschließlich Kerninfrastruktur, Datenbanken und kritischer Dokumente, und vermittelt die Gewissheit, dass die Daten vor böswilliger Beschädigung geschützt sind.

CyberSense scannt Datenbackups in einem Cyber Recovery Vault, um zu beobachten, wie sich Daten im Laufe der Zeit verändern. Anschließend setzt es maschinelles Lernen und KI ein, um Anzeichen von Beschädigungen zu erkennen, die auf einen Ransomwareangriff hinweisen. Die Daten werden mit über 200 inhaltsbasierten Analysen abgeglichen, um Beschädigungen mit einer Sicherheit von 99,99 %* ausfindig zu machen. So werden Sie dabei unterstützt, geschäftskritische Infrastruktur und Inhalte zu schützen. CyberSense erkennt Massenlöschungen, Verschlüsselungen und andere verdächtige Änderungen in der Kerninfrastruktur (einschließlich Active Directory, DNS usw.), in Datei-Repositorys, Dateisystemen und kritischen Datenbanken, die aus ausgeklügelten Angriffen resultieren.

Wenn verdächtige Aktivitäten auftreten, stellt CyberSense nach dem Angriff forensische Berichte zur Verfügung, um den Umfang des Cyberangriffs zu diagnostizieren. Wenn eine Datenbeschädigung erkannt wird, steht eine Liste der letzten fehlerfreien Backupdatensätze zur Verfügung, die eine schnelle, kuratierte Recovery unterstützen. Dies trägt dazu bei, Geschäftsunterbrechungen und Datenverluste zu minimieren und verringert so die Kosten für die Cyber Recovery.

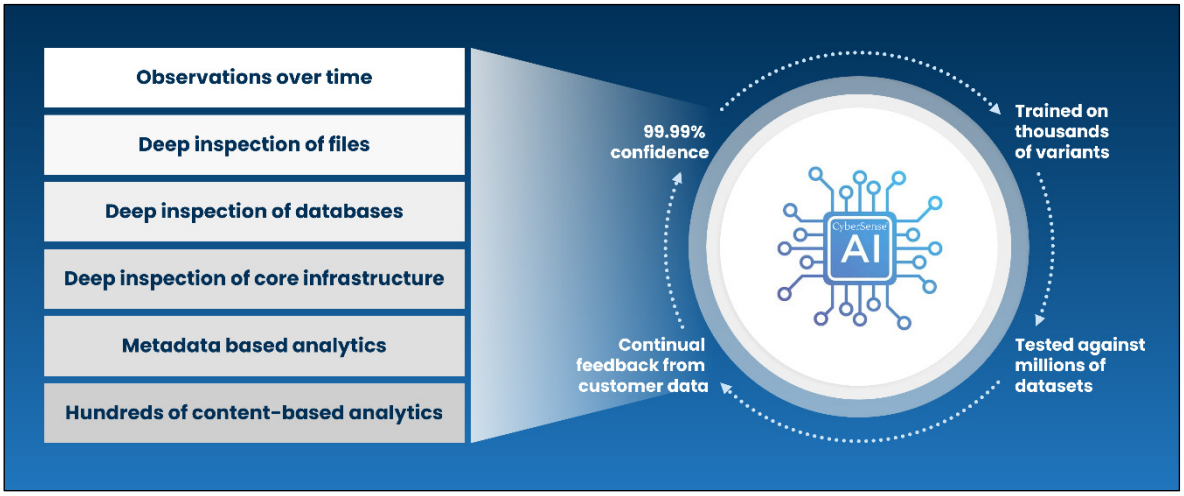


Cyber Recovery-Workflow

CyberSense lässt sich nahtlos in Dell PowerProtect Cyber Recovery integrieren und überwacht Dateien und Datenbanken aktiv, um durch die Analyse der Datenintegrität Beschädigungen durch Ransomware zu erkennen. Sobald die Daten in den Cyber Recovery Vault repliziert und die Aufbewahrungssperre angewendet wurde, startet CyberSense automatisch einen umfassenden Scan der Backupdateien und erstellt Point-in-Time-Beobachtungen von Dateien, Datenbanken und der Kerninfrastruktur. CyberSense verfolgt Änderungen an Dateien im Laufe der Zeit mit höchster Präzision und deckt auch Datenbeschädigungen durch die ausgeklügeltsten Cyberbedrohungen auf.

Vollständige Inhaltsanalysen

CyberSense ist das einzige Produkt auf dem Markt, das vollständige Inhaltsindexierung und Analysen aller geschützten Daten ermöglicht. Die CyberSense Deep AI-Analyse durchläuft die Gesamtheit aller Daten und generiert mit einer Genauigkeit von 99,99 %* eine probabilistische Entscheidung, ob die Daten unbeschädigt sind oder durch Ransomware beschädigt wurden. Diese Funktion unterscheidet CyberSense von anderen Lösungen, die eine Übersicht der Daten und Analysen nutzen und auf Grundlage von Metadaten nach offensichtlichen Anzeichen von Beschädigungen suchen. Beschädigungen auf Metadatenebene sind leicht zu erkennen: Dabei handelt es sich beispielsweise um die Änderungen einer Dateierweiterung in „.encrypted“ oder um eine erheblich abweichenden Dateigröße. Heutzutage verwenden Cyberkriminelle jedoch ausgeklügeltere Angriffe.



CyberSense geht über reine Metadatenlösungen hinaus und erkennt Datenbeschädigungen durch die Analyse des gesamten Inhalts. Es prüft Dateien und Datenbanken hinsichtlich Veränderungen, die auf einen Angriff hindeuten, einschließlich vollständiger oder teilweiser Datenbeschädigung. Herkömmliche Analysetools übersehen diese Bedrohungen, was zu einem trügerischen Gefühl von Sicherheit führt. Benutzerdefinierte Schwellenwertwarnmeldungen können auf der Grundlage von geänderten, hinzugefügten oder gelöschten Dateien erstellt werden. Benutzerdefinierte YARA-Regeln und Malware-Signaturen können für die Vorwärts- und Rückwärtserkennung von Malware auch in Backups implementiert werden.

Unterstützte Datentypen

CyberSense generiert Analysen aus einer umfassenden Anzahl an Datentypen. Dazu gehören Kerninfrastrukturen wie DNS, LDAP, Active Directory, unstrukturierte Dateien wie Dokumente, Verträge, geistiges Eigentum und Datenbanken wie Oracle, DB2, SQL, PostgreSQL, Epic Caché usw.

Zusammenfassung

CyberSense ist vollständig in Dell PowerProtect Cyber Recovery integriert, analysiert Ihre Daten im Vault und erkennt Anzeichen für Gefährdungen und Beschädigungen. Mit CyberSense erkennen Sie proaktiv den Umfang eines laufenden Cyberangriffs. Dies erleichtert die Implementierung eines Plans für eine schnelle Diagnose und Recovery, wodurch Geschäftsunterbrechungen und die damit verbundenen erheblichen Kosten gemindert werden.

Weitere Informationen zu Dell PowerProtect Cyber Recovery

Kontakt mit dem Dell Technologies Expertenteam

Weitere Informationen zu CyberSense

Reden Sie mit: #PowerProtect Mögliches Ersatzbild für Seite 2

* Basierend auf dem von Index Engines in Auftrag gegebenen ESG-Bericht „Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption“. Juni 2024