DELL Technologies

Lösungsübersicht

CyberSense® für PowerProtect Cyber Recovery

KI-basiertes maschinelles Lernen, Analysen und forensische Tools zur Erkennung, Diagnose und Recovery nach Cyberangriffen

VORTEIL VON CYBERSENSE

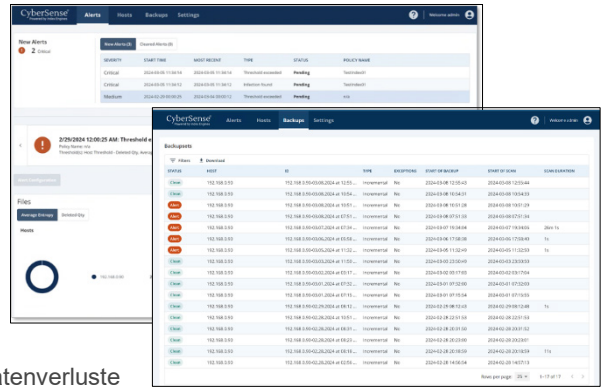
CyberSense® ist vollständig in die Dell PowerProtect Cyber Recovery Vault-Lösung integriert.

- Diese Integration ermöglicht einen automatisierten Ansatz für das regelmäßige Scannen von Backupdaten, um die Integrität der Daten zu überprüfen und Warnmeldungen auszugeben, wenn verdächtige Aktivitäten erkannt werden.
- Da CyberSense in Backup-Images wie von Dell NetWorker, Avamar, PowerProtect Data Manager und mehr direkt scannen kann, ermöglicht es die Analyse von Inhalten, ohne dass die Daten aufbereitet werden müssen.
- Nur CyberSense liefert bei jedem Scannen der Daten vollständige Inhaltsanalysen, um selbst die raffiniertesten Ransomwareangriffe zu erkennen, die von weniger umfangreichen Scantools, die nur Metadaten untersuchen, oft nicht entdeckt werden.
- Bei einem Angriff bietet CyberSense anschließend außerdem forensische Berichte, um die Reichweite und den Umfang des Angriffs zu verstehen. Die Lösung stellt auch eine Liste der letzten fehlerfreien Backupsätze vor der Beschädigung bereit, um den Recovery-Prozess zu vereinfachen.

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.

Wenn herkömmliche Sicherheitstools nicht ausreichen, um Daten vor Cyberangriffen zu schützen, nutzen Sie **CyberSense®**, um Datenbeschädigungen nach einem Cyberangriff mit einer Genauigkeit von 99,5 % zu erkennen und eine intelligente und schnelle Recovery zu ermöglichen. Als letztes Mittel zur Verteidig und erstes Mittel zur Recovery für Tausende von Unternehmen weltweit stellt CyberSense die Integrität ihrer Datenbestände sicher, einschließlich Kerninfrastruktur, Produktionsdatenbanken und kritischer Dokumente, und vermittelt die Gewissheit, dass die Daten vor böswilliger Beschädigung geschützt sind.

CyberSense nutzt Datenbackups, um zu beobachten, wie sich Daten im Laufe der Zeit verändern, und setzt dann KI-basiertes maschinelles Lernen ein, um Anzeichen von Beschädigungen zu erkennen, die auf einen Ransomwareangriff hindeuten. Mithilfe von maschinellem Lernen werden dann diese über 200 inhaltsbasierten Analysen überprüft, um Beschädigungen mit einer Sicherheit von 99,5 % ausfindig zu machen. So werden Sie dabei unterstützt, Ihre geschäftskritische Infrastruktur und geschäftskritische Inhalte zu schützen. CyberSense erkennt Massenlöschungen, Verschlüsselungen und andere verdächtige Änderungen in der Kerninfrastruktur (einschließlich Active Directory, DNS usw.), in Nutzerdateien und in kritischen Produktionsdatenbanken, die aus ausgeklügelten Angriffen resultieren. Wenn CyberSense Anzeichen einer Beschädigung erkennt, wird im Dashboard eine Warnmeldung mit zusätzlichen Informationen angezeigt, die das Ausmaß und die Auswirkungen des Angriffs detailliert beschreiben.



Wenn verdächtige Aktivitäten auftreten, stellt CyberSense nach dem Angriff forensische Berichte bereit, 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.

Cyber Recovery-Workflow

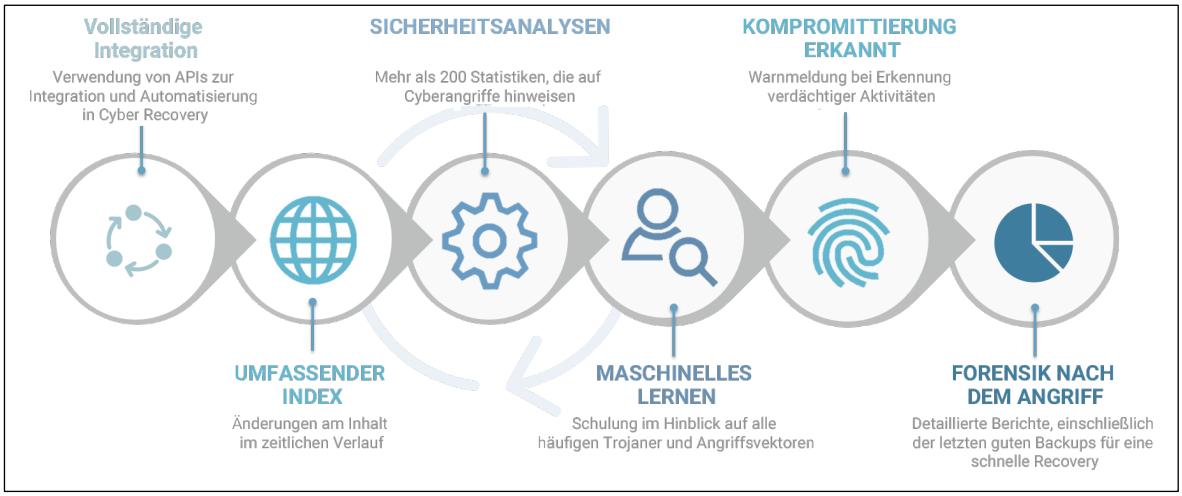
CyberSense lässt sich nahtlos in Dell PowerProtect Cyber Recovery integrieren und überwacht Dateien und Datenbanken aktiv, um durch die Analyse der Datenintegrität Beschädigungen durch Ransomware zu erkennen. Sobald die Daten in den Cyber Recovery Vault repliziert und die Aufbewahrungssperre angewendet wurde, startet CyberSense automatisch einen umfassenden Scan der Backupdateien und erstellt Point-in-Time-Beobachtungen von Dateien, Datenbanken und der Kerninfrastruktur. Diese Beobachtungen ermöglichen es CyberSense, Änderungen an Dateien im Laufe der Zeit genau zu verfolgen und so selbst die raffiniertesten Cyberbedrohungen aufzudecken.

Der CyberSense-Scan greift direkt auf die Daten im Backup-Image zu, wodurch die ursprüngliche Backupsoftware und die Aufbereitung der Daten überflüssig werden. Durch fortschrittliche Analysen identifiziert CyberSenseVerschlüsselungen/Beschädigungen von Dateien oder Datenbankseiten und erkennt bekannte Malwareerweiterungen sowie Massenlöschungen/Erstellungen von Dateien und vieles mehr.

Mithilfe von KI-basierten Algorithmen für maschinelles Lernen, die mit den neuesten Trojanern und der neuesten Ransomware trainiert wurden, trifft CyberSense deterministische Entscheidungen über die Beschädigung von Daten, die auf einen Cyberangriff hindeuten. Im Falle eines Angriffs wird umgehend eine kritische Warnmeldung im Cyber Recovery-Dashboard angezeigt. Darüber hinaus bietet CyberSense forensische Berichte nach einem Angriff, die eine schnelle Diagnose und Recovery nach Ransomwareangriffen ermöglichen, um Datenverluste zuminimieren.

Vollständige Inhaltsanalysen

CyberSense ist das einzige Produkt auf dem Markt, das vollständige inhaltsbasierte Analysen aller geschützten Daten ermöglicht. 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 ist mehr als nur eine reine Metadatenlösungen, da die Erkennung von Datenbeschädigungen auf vollständigen Inhaltsanalysen basiert. Dateien und Datenbanken werden auf Angriffe geprüft, die eine rein inhaltsbasierte Beschädigung der Dateistruktur oder eine teilweise Verschlüsselung innerhalb eines Dokuments oder einer Datenbankseite beinhalten. Diese Angriffe können nicht mithilfe von Analysen entdeckt werden, die nicht in der Datei scannen, um Veränderungen im Laufe der Zeit miteinander zu vergleichen. Ohne eine vollständige inhaltsbasierte Analyse ergibt sich eine erhebliche Anzahl falscher negativer Ergebnisse, was zu einem trügerischen Vertrauen in die Integrität und Sicherheit Ihrer Daten führt. Darüber hinaus können benutzerdefinierte Warnmeldungen zu Schwellenwerten basierend auf der Menge oder dem Prozentsatz der geänderten Dateien oder des Dateityps, der hinzugefügten oder gelöschten Dateien und der Entropie auf einem Host erstellt 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, überwacht Ihre Daten und erkennt Anzeichen für Gefährdungen und Beschädigungen. Mit CyberSense erkennen Sie den Umfang eines laufenden Cyberangriffs proaktiv. 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