Zusammenfassung

Bessere Ausfallsicherheit bei Cyberangriffen und Schutz Ihrer Daten vor Ransomware-Cyberbedrohungen durch Nutzung eines isolierten Vault, einer KI-basierten ML-Analysesoftware und mehr

Mit Dell Technologies PowerProtect Cyber Recovery mit CyberSense

Da die Häufigkeit von Cyberbedrohungen kontinuierlich zunimmt und sich Angriffsmethoden weiterentwickeln, müssen Data-Protection-Pläne einen Ansatz verfolgen, mit dem alle IT-Komponenten gesichert und analysiert werden – von den oberflächlichsten bis hin zu den tiefsten Bereichen. Dell PowerProtect Cyber Recovery kann dazu beitragen, die kritischsten und sensibelsten Daten zu schützen und gleichzeitig eine ordnungsgemäße Recovery bei einem Cyberangriff oder einem anderen unterbrechenden Ereignis sicherzustellen.

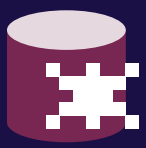
Dell PowerProtect Cyber Recovery ist eine Datenmanagement-, Schutz- und Recovery-Lösung, mit der Unternehmen ihre Daten und Anwendungen vor Ransomware, destruktiven Cyberangriffen und unerwarteten Ereignissen schützen können. Die Lösung basiert auf einem Multi-Copy-Ansatz, was bedeutet, dass Backups nach der Erstellung zur Sicherung und Analyse in einen isolierten Storage kopiert werden. PowerProtect Cyber Recovery umfasst viele Komponenten, darunter einen oder mehrere Storage Vaults, die sich entweder in einer PowerProtect DD-On-Premise-Appliance (ehemals Data Domain) oder über den softwarebasierten Dell APEX Protection Storage for Public Cloud (ehemals DD Virtual Edition) in der Cloud befinden können. In beiden Fällen wird der Vault mit einem Air Gap betrieben, d. h., dass er von der Produktionsumgebung isoliert ist – potenziell mit einem physischen Air Gap bei der On-Premise-Umgebung und einem logischen Air Gap im Falle der Dell APEX-Umgebung. Dies macht es für böswillige AkteurInnen oder unbefugte NutzerInnen extrem schwierig, sich anzumelden und Sicherungskopien zu beschädigen.

PowerProtect Cyber Recovery umfasst außerdem CyberSense, eine vollständig automatisierte und integrierte intelligente Sicherheitsanalysen-Engine, die Daten, Dateien, Datenbanken und Images im Vault automatisch auf Anzeichen von Beschädigung durch einen Ransomwareangriff scannt. CyberSense bietet eine vollständige Inhaltsanalyse und nimmt Beobachtungen aus Dateien als Eingaben für sein auf künstlicher Intelligenz (KI) basierendes ML-Modell (maschinelles Lernen) auf. Die Lösung erkennt bösartige Aktivitäten, die Massenlöschungen, Verschlüsselung und andere verdächtige Änderungen in der Kerninfrastruktur (einschließlich Active Directory und DNS), den Nutzerdateien und den kritischen Produktionsdatenbanken umfassen, die auf Ransomware oder einen destruktiven Angriff hinweisen könnten. Wenn CyberSense Muster von Beschädigungen erkennt, wird eine Warnmeldung im PowerProtect Cyber Recovery-Dashboard erzeugt, die zusätzliche Informationen über die Größe und die Auswirkungen des Angriffs enthält.[1]

PowerProtect Cyber Recovery unterstützt Unternehmen dabei, Cyberangriffe abzuwehren, die Datenausfallsicherheit mit mehreren Kopien von Datenbackups an separaten Standorten zu verbessern, Ausfallzeiten zu reduzieren und die Business Continuity aufrechtzuerhalten. In diesem Bericht werden öffentlich verfügbare Daten verwendet, um wichtige Data-Protection-Funktionen aufzuzeigen. Außerdem werden unsere Ergebnisse einer Wettbewerbsanalyse von CyberSense vorgestellt.

Schützen sensibler Daten

Verschlüsseln Sie unveränderliche In-Flight-Daten während der Backupreplikation in physisch und logisch isolierten Vaults.



Erkennen der Beschädigung einer SQL Server-Seite

CyberSense hat eine Infektion gefunden, die von einer Konkurrenzlösung nicht erkannt wurde.

Identifizieren nicht beschädigter Sicherungskopien

CyberSense hat die neueste nicht infizierte Sicherungskopie für die Recovery identifiziert.

Sicherheit

Dell PowerProtect Cyber Recovery bietet mehrere Sicherheitsfunktionen, um kritische Daten vor Ransomware und anderen ausgefeilten Bedrohungen zu schützen. Diese verhindern, dass unbefugte NutzerInnen Zugriff auf vertrauliche Informationen erhalten, und ermöglichen eine schnelle Recovery, damit Unternehmen den normalen Betrieb fortsetzen können.

Die Funktionen und Merkmale von PowerProtect DD Appliances können entscheidend für die Sicherheit, Integrität und Recovery sein, die PowerProtect Cyber Recovery-Lösungen bieten. Zu diesen Funktionen gehören Retention Lock, DDBoost, rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC), eine doppelte Autorisierung und mehr.

Isolierung

Datenisolierung bezieht sich auf die Trennung und eingeschränkte Zugänglichkeit von Daten, ermöglicht durch Barrieren oder Grenzen, die einen unbefugten Zugriff zu verhindern. Für die Isolierung werden häufig temporäre Netzwerkverbindungen anstelle von persistenten Verbindungen verwendet.

Die Datenisolierung trägt dazu bei, dass kritische Daten nicht mit einem infizierten Netzwerk verbunden bleiben, in dem böswillige AkteurInnen versuchen könnten, Konfigurationen zu modifizieren, Daten zu löschen, Richtlinien zu ändern oder den Netzwerkverkehr auf Nutzerzugangsdaten zu durchsuchen. Mithilfe einer Isolierung kann außerdem die Angriffsfläche verkleinert werden, sodass böswillige AkteurInnen weniger Möglichkeiten haben, Zugriff und Kontrolle zu erhalten. Darüber hinaus können Unternehmen den Zugriff auf autorisierte MitarbeiterInnen einschränken und so verhindern, dass unbefugte NutzerInnen Daten überschreiben.

Zusätzlich zu den erwähnten Funktionen kann PowerProtect Cyber Recovery eine physische und logische Isolierung in Form von Air Gaps bieten, um Daten zu schützen. Eine physisch isolierte PowerProtect DD-On-Premise-Lösung kann als Vault fungieren, in dem NutzerInnen oder Systeme aus der Produktionsumgebung nicht auf die Komponenten zugreifen können und der Vault physisch vom Produktionsnetzwerk getrennt ist.[2] Durch die Beseitigung des Zugriffs auf die Recovery-Umgebung über das Produktionsnetzwerk kann ein Unternehmen seine Angriffsfläche verkleinern.

Unveränderlichkeit*

Wenn Backups unveränderlich und somit schreibgeschützt sind, kann ein Unternehmen diesen Backups für die Recovery vertrauen. Betrieblich trägt die Unveränderlichkeit dazu bei, die Authentizität und Zuverlässigkeit der Daten aufrechtzuerhalten. DD-Systeme, einschließlich derjenigen in PowerProtect Cyber Recovery-Lösungen, können Unveränderlichkeit bei der Speicherung von Daten mithilfe logischer Partitionen des Dateisystems bereitstellen, die als MTrees bezeichnet werden. Die Lösungen nutzen außerdem eine MTree-Replikation, um unveränderliche Datenkopien von einem Produktions-DD-System über das DDBoost-Protokoll auf ein anderes DD-System im Vault zu kopieren.[3]

* Ziel der Produkte von Dell ist, Kunden bei ihren Bemühungen zum Schutz ihrer kritischen Daten zu unterstützen. Wie bei jedem elektronischen Produkt können auch bei Data-Protection-, Storage- und anderen Infrastrukturprodukten Sicherheitslücken auftreten. Es ist wichtig, dass Kunden Sicherheitsupdates installieren, sobald sie von Dell zur Verfügung gestellt werden.

CyberSense

Für einen guten Schutz Ihrer Daten ist eine umfassende Strategie erforderlich, die Sicherheit auf jeder Ebene bietet. Trotz aller Funktionen für automatische Fehlerkorrektur, Sicherheit, Unveränderlichkeit und Isolierung einer Dell PowerProtect Cyber Recovery-Lösung könnten weniger offensichtliche Angriffe dennoch tiefer in eine Unternehmensinfrastruktur eindringen, z. B. auf Datenbackupebene, und potenziell unbemerkt bleiben, bis Produktionsdaten oder eine gesamte Nutzergruppe kompromittiert wurden. Dell PowerProtect Cyber Recovery-Lösungen bieten eine letzte Verteidigungslinie gegen Cyberangriffe und einen effizienten Ansatz, um die Recovery über CyberSense zu beschleunigen.

Wir haben CyberSense und ein vergleichbar funktionierendes Tool der Datenmanagementplattform eines Mitbewerbers (den wir als „Anbieter X" bezeichnen) für eine Appliance ähnlicher Größe getestet. In unseren Tests haben wir festgestellt, dass PowerProtect Cyber Recovery eine Infektion auf SQL-Datenbankseiten erkannt hat – was bei der Lösung von Anbieter X nicht der Fall war. PowerProtect Cyber Recovery benötigte außerdem weniger Backups als die Lösung von Anbieter X, um die Beschädigung der Daten zu ermitteln.

1. Dell, „CyberSense® für PowerProtect Cyber Recovery", abgerufen am 8. September 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, „MTree Replication", abgerufen am 11. September 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. Principled Technologies, „Dell EMC Cyber Recovery protected our test data from a cyber attack", abgerufen am 21. August 2023, http://facts.pt/rkew01n.

▶ Originalversion dieser Zusammenfassung in englischer Sprache lesen

Bericht lesen ▶

Principled Technologies®

Facts matter.®

Principled Technologies ist eine eingetragene Marke von Principled Technologies, Inc.
Alle anderen Produktnamen sind Marken der jeweiligen Inhaber.
Weitere Informationen finden Sie im Bericht.