Resumen ejecutivo

Mejore la ciberresiliencia y proteja los datos contra las ciberamenazas de ransomware utilizando un vault aislado, software de análisis de aprendizaje automático basado en IA y mucho más.

Con Dell Technologies PowerProtect Cyber Recovery con CyberSense

A medida que la frecuencia de las ciberamenazas no para de aumentar y los métodos de ataque evolucionan, los planes de protección de datos deben adoptar un enfoque que proteja y analice todos los componentes de TI, desde los más superficiales hasta los más profundos. Dell PowerProtect Cyber Recovery puede ayudar a proteger los datos más críticos y confidenciales, a la vez que ayuda a garantizar una recuperación adecuada ante un ciberataque u otro evento disruptivo.

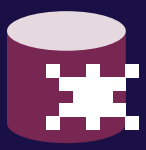
Dell PowerProtect Cyber Recovery es una solución de gestión, protección y recuperación de datos que ayuda a las organizaciones a proteger sus datos y aplicaciones contra ransomware, ciberataques destructivos y eventos inesperados. La solución utiliza un enfoque de varias copias, lo que significa que, después de crear copias de seguridad, las copia en un almacenamiento aislado para su protección y análisis. PowerProtect Cyber Recovery consta de muchos componentes, incluidos uno o varios vaults de almacenamiento, ubicados potencialmente en las instalaciones en un dispositivo PowerProtect DD (anteriormente conocido como Data Domain) o en la cloud a través de Dell APEX Protection Storage for Public Cloud (anteriormente conocido como DD Virtual Edition) definido por software. En ambos casos, el vault está operativamente aislado, es decir, aislado del entorno de producción (potencialmente aislado físicamente en el caso del entorno en las instalaciones y aislado lógicamente en el caso del entorno APEX). Esto hace que a los atacantes o usuarios no autorizados les resulte extremadamente difícil iniciar sesión y comprometer las copias de seguridad.

PowerProtect Cyber Recovery también incluye CyberSense, un motor de análisis de seguridad inteligente totalmente automatizado e integrado que analiza automáticamente datos, archivos, bases de datos e imágenes en el vault en busca de signos de daños de un ataque de ransomware. CyberSense proporciona un análisis completo del contenido; observa patrones en los archivos para utilizarlos como entradas para su modelo de aprendizaje automático (ML) basado en inteligencia artificial (IA); y detecta actividades maliciosas que incluyen eliminaciones masivas, cifrado y otros cambios sospechosos en la infraestructura principal (incluidos Active Directory y DNS), archivos de usuario y bases de datos de producción críticas que podrían indicar un ransomware o un ataque destructivo. Cuando CyberSense detecta patrones de daños, genera una alerta en el panel de PowerProtect Cyber Recovery que proporciona información adicional sobre la magnitud y el impacto del ataque.[1]

PowerProtect Cyber Recovery ayuda a las organizaciones a mitigar los ciberataques, mejorar la resiliencia de los datos con varias copias de seguridad de datos desde ubicaciones independientes, reducir el tiempo de inactividad y mantener la continuidad empresarial. Este informe utiliza datos disponibles públicamente para resaltar las características y funcionalidades clave de protección de datos, y presenta nuestros resultados de un análisis comparativo de CyberSense.

Proteja los datos confidenciales

Cifre los datos inmutables en transferencia durante la replicación de copia de seguridad en vaults aislados física y lógicamente



Detecte daños en páginas de SQL Server

CyberSense detectó una infección que una solución de la competencia no pudo detectar

Identifique copias de seguridad no dañadas

CyberSense identificó la copia de seguridad no infectada más reciente para la recuperación

Seguridad

Dell PowerProtect Cyber Recovery ofrece varias características de seguridad para ayudar a proteger los datos críticos frente a ransomware y otras amenazas sofisticadas, evitar que los usuarios no autorizados obtengan acceso a información confidencial y acelerar la recuperación para que las organizaciones puedan reanudar su funcionamiento normal.

Las características y la funcionalidad de los dispositivos de DD PowerProtect pueden ser fundamentales para la seguridad, la integridad y la recuperación que ofrecen las soluciones PowerProtect Cyber Recovery. Entre las características se incluyen el bloqueo de retención, DDBoost, el control de acceso basado en funciones (RBAC), la autorización dual y muchas más.

Aislamiento

El aislamiento de datos se refiere a la separación y el acceso restringido a los datos creados por barreras o límites para evitar el acceso no autorizado. El aislamiento a menudo utiliza conexiones de red temporales en lugar de conexiones persistentes.

El aislamiento de datos ayuda a que los datos críticos permanezcan desconectados de una red infectada en la que un atacante podría intentar modificar configuraciones, eliminar datos, cambiar políticas o detectar el tráfico de red para obtener credenciales de usuario. El aislamiento también ayuda a reducir la superficie de ataque, lo que da a los atacantes menos oportunidades de obtener acceso y control. Además, las organizaciones pueden restringir el acceso solo al personal autorizado, lo que ayuda a evitar que los usuarios no autorizados sobrescriban datos.

Además de las características que hemos señalado, PowerProtect Cyber Recovery puede proporcionar aislamiento físico y lógico, en forma de cámaras de aire, para ayudar a proteger los datos. Un PowerProtect DD en las instalaciones aislado físicamente podría funcionar como vault, en el que los usuarios o sistemas del entorno de producción no pueden acceder a los componentes y el vault se desconecta físicamente de la red de producción.[2] Al eliminar el acceso al entorno de recuperación de la red de producción, una organización podría reducir su superficie de ataque.

1. Dell, "CyberSense® for PowerProtect Cyber Recovery", acceso el 8 de septiembre de 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", acceso el 11 de septiembre de 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", acceso el 21 de agosto de 2023, http://facts.pt/rkew01n.

▶ Consulte la versión original en inglés de este resumen

Inmutabilidad*

Hacer que las copias de seguridad sean inmutables y, por lo tanto, de solo lectura, ayuda a garantizar que una organización pueda confiar en esas copias de seguridad para su recuperación. Desde el punto de vista operativo, la inmutabilidad ayuda a mantener la autenticidad y fiabilidad de los datos. Los sistemas DD, incluidos los de las soluciones PowerProtect Cyber Recovery, pueden proporcionar inmutabilidad en la forma en que almacenan los datos mediante particiones lógicas del sistema de archivos denominadas MTrees. Las soluciones también utilizan la replicación MTree para copiar copias de datos inmutables de un DD de producción a otro DD en el vault a través del protocolo DDBoost.[3]

*Los productos Dell se han diseñado para respaldar los esfuerzos de los clientes por proteger los datos críticos. Igual que en el caso de cualquier producto electrónico, los productos de protección de datos y de almacenamiento, y otros productos de infraestructura pueden sufrir vulneraciones de seguridad. Es importante que los clientes instalen las actualizaciones de seguridad tan pronto como Dell las haga públicas.

CyberSense

Proteger bien sus datos requiere una estrategia integral que ofrezca seguridad en todos los niveles. A pesar de todas las características de autorreparación, seguridad, inmutabilidad y aislamiento de una solución Dell PowerProtect Cyber Recovery, existen ataques menos obvios que podrían seguir profundizando en una infraestructura empresarial. Por ejemplo, a nivel de copia de seguridad de datos, podrían pasar desapercibidos hasta que los datos de producción o todo un grupo de usuarios se vieran comprometidos. Las soluciones Dell PowerProtect Cyber Recovery proporcionan una última línea de defensa contra ciberataques y un enfoque eficiente para ayudar a acelerar la recuperación a través de CyberSense.

Probamos CyberSense y una herramienta que funciona de forma similar desde la plataforma de gestión de datos de un competidor (al que nos referimos como "proveedor X") en un dispositivo del mismo tamaño. En nuestras pruebas, descubrimos que PowerProtect Cyber Recovery detectó una infección en páginas de bases de datos SQL, algo que la solución del proveedor X no pudo hacer. PowerProtect Cyber Recovery también requirió menos copias de seguridad que la solución del proveedor X para determinar los daños en los datos.

Lea el informe ▶

Principled Technologies®

Facts matter.®