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 son fundamentales para la seguridad, la integridad y la recuperación que ofrecen las soluciones PowerProtect Cyber Recovery. Funciones incluidas:

1. **Inmutabilidad**
   Los datos inmutables no se pueden modificar ni eliminar, solo se escriben. Los sistemas DD pueden escribir copias de seguridad inmutables tanto en sistemas de producción como en Cyber Vault, lo que significa que si un atacante obtiene de alguna manera acceso al sistema de copia de seguridad, no puede modificar, eliminar o poner en riesgo las copias protegidas existentes.[2] Cualquier copia de seguridad que el sistema DD cree en el entorno de producción es inmediatamente inmutable y está disponible para que el departamento de TI la copie en el vault para mayor seguridad. La siguiente sección de este informe analiza la inmutabilidad en mayor profundidad.

2. **Bloqueo de retención**
   La función DD Retention Lock hace que los datos sean inmutables durante un periodo predeterminado. Una vez que la solución pone los datos en un bloqueo de retención, ningún usuario o sistema puede alterar, eliminar o modificar los datos hasta que expire el periodo de bloqueo.[3]

   Retention Lock tiene modos de gobernanza y cumplimiento normativo. Su modo de cumplimiento normativo puede permitir a los clientes cumplir con muchos estándares normativos. Un tercero independiente certificó que DD Retention Lock cumple con los requisitos de almacenamiento especificados en las Reglas 17a-4(f)(2) y 240.18a-6(e)(2) de SEC y la Regla 4511(c) de FINRA.[4] Esta capacidad también puede ayudar a respaldar los esfuerzos de una organización para cumplir con la FDA 21 CFR Parte 11, la Ley Sarbanes-Oxley, IRS 98025 y 97-22, la norma ISO 15489-1 y MoREQ2010.[5]

   Dado que los atacantes podrían intentar eludir el bloqueo de retención cambiando el reloj de un sistema, lo que haría que la solución eliminara los archivos antes de lo esperado, DD tiene un reloj de seguridad interno. El sistema compara regularmente las horas de los relojes de seguridad y del sistema. Si hay un sesgo acumulado de dos semanas entre los dos en un solo año natural, el sistema deshabilita automáticamente el sistema de archivos de DD (DDFS) para evitar el acceso a los datos.[6]

3. **Cifrado de datos en transferencia con DDBoost**
   Los datos en transferencia pueden suponer un riesgo importante para la seguridad. DDBoost limita la cantidad de datos en transferencia al permitir que el servidor de copia de seguridad o el cliente de aplicaciones envíen solo segmentos de datos únicos, en lugar de todos los datos, a través de la red al dispositivo de DD. Además, las organizaciones pueden utilizar el protocolo DDBoost con o sin certificados para la autenticación y el cifrado de datos. Los certificados ofrecen una capacidad de transporte de datos más segura. El cifrado en transferencia permite a las aplicaciones cifrar copias de seguridad en transferencia o restaurar datos a través de LAN desde el sistema. El cliente puede utilizar servicios de capa de transporte (TLS) para cifrar la sesión entre el cliente y el sistema.[7]

4. **Seguridad del sistema operativo DD (DD OS)**
   Las características de seguridad de DD también se extienden al sistema operativo. DD OS implementa controles de acceso personalizados y restricciones en la shell bash con fines de seguridad. El modo de shell bash restringido permite a los usuarios realizar solo un conjunto de comandos predefinidos necesarios para sus funciones y tareas. DD OS mejora la integridad de los datos bloqueando los comandos no definidos que realizan modificaciones no autorizadas o no intencionadas en el sistema.[8]

5. **Control de acceso basado en funciones (RBAC) y seguridad del sistema de archivos DD (DDFS)**
   Los sistemas DD utilizan varias medidas para proteger los archivos y datos dentro del sistema de archivos. En primer lugar, los sistemas DD proporcionan RBAC, que permite a los administradores definir funciones con privilegios específicos y asignar usuarios a esas funciones. Solo los usuarios autorizados con los privilegios adecuados pueden acceder al dispositivo y a sus datos. Esto garantiza que los usuarios solo tengan acceso a las funciones y los datos que necesitan para realizar sus tareas, lo que reduce el riesgo de acceso no autorizado o exposición accidental de los datos.

   DDFS también utiliza hashing para la verificación de la integridad de los datos. El hashing transforma una clave o cadena de caracteres determinada en otro valor. El dispositivo almacena fragmentos de datos únicos en contenedores de almacenamiento lógico, y el sistema de archivos almacena hashes tanto de los fragmentos de datos como de los contenedores. Cuando el sistema recupera datos, vuelve a calcular el valor de hash de los datos para que coincida con el valor de hash almacenado en DDFS, lo que ayuda a garantizar que nada haya manipulado o dañado los datos.[9]

6. **Autorización de dos funciones**
   Cuando una organización habilita el modo de cumplimiento normativo de DD Retention Lock, el sistema DD proporciona seguridad administrativa adicional en forma de doble inicio de sesión. Esto significa que tanto el administrador del sistema como un segundo usuario autorizado (por ejemplo, el responsable de seguridad) deben iniciar sesión juntos. El mecanismo de inicio de sesión doble del modo de cumplimiento normativo de DD Retention Lock funciona como una protección contra cualquier acción que pueda comprometer la integridad de los archivos bloqueados antes de que venza el periodo de retención.[10]

7. **Arquitectura de invulnerabilidad de datos**
   DD OS proporciona verificación integral, prevención y contención de fallos, detección y reparación continuas de fallos, y capacidad de recuperación del sistema de archivos para protegerse de los problemas de integridad de los datos causados por fallos de hardware y software. Cuando el sistema DD recibe solicitudes de escritura del software de copia de seguridad, primero analiza un segmento de datos en busca de redundancia calculando la huella digital del segmento de datos y comparándola con las huellas digitales existentes almacenadas en el sistema. Solo almacena segmentos de datos únicos y sus huellas digitales en el disco. A continuación, DD lee continuamente los datos del disco, vuelve a calcular la huella digital que lee y garantiza que coincida con la huella digital del disco. El sistema DD lleva a cabo un proceso de autorreparación para reconstruir los datos dañados y restaurar los datos a su estado correcto si el sistema detecta daños durante este proceso (es decir, si lo que lee no coincide con lo que está escrito). Además, el proceso de autorreparación ayuda a proteger el sistema contra otros cambios que podrían afectar a la integridad de la plataforma.

Inmutabilidad*

Hacer que las copias de seguridad sean inmutables y, por lo tanto, de solo lectura, garantiza que una organización pueda confiar en estas 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 productos Dell se han diseñado para ayudar a los clientes en sus esfuerzos 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.

Cómo funciona

Los sistemas DD proporcionan inmutabilidad en la forma en que almacenan los datos mediante MTrees. Los MTrees son particiones lógicas del sistema de archivos. Cuando una aplicación escribe datos en un MTree, el sistema DD utiliza una función denominada copia rápida para crear una copia puntual del MTree original en un nuevo MTree. En el nuevo MTree, DD aplica bloqueo de retención para garantizar que un usuario o proceso no pueda eliminar el nuevo MTree durante la duración definida por el periodo de retención. El nuevo MTree es una copia inmutable de los datos y es independiente del MTree original.[11]

Las soluciones PowerProtect Cyber Recovery también utilizan la replicación de MTree para realizar copias de datos inmutables de un DD de producción a otro DD en el vault a través del protocolo DDBoost.[12] En la sincronización inicial entre los dos DD, la solución copia todos los datos en el DD del vault. Cada sincronización posterior copiará solo los segmentos de datos nuevos y modificados. CyberSense, del cual hablaremos más adelante en este informe, escanea todas las copias inmutables en el vault en busca de posibles daños.

Enfoques sobre la inmutabilidad

La necesidad de eliminar copias de seguridad inmutables es rara, aunque esta situación se produce. Las organizaciones podrían encontrarse con problemas de capacidad y costes posteriores tras acumular copias de seguridad inmutables que no pueden eliminar. El almacenamiento de copias de seguridad puede requerir una gran capacidad, lo que a su vez requiere costes continuos de funcionamiento, gestión y supervisión, además de la inversión inicial en hardware. La eliminación periódica de copias de seguridad inmutables puede ayudar a resolver esos problemas.

Como hemos señalado, Dell PowerProtect Cyber Recovery ofrece inmutabilidad gracias al uso de Retention Lock y otras herramientas. Retention Lock ofrece cierta flexibilidad, ya que los dos modos, cumplimiento normativo y gobernanza, ofrecen ligeras modificaciones en la forma en que los clientes pueden implementar la inmutabilidad. La inmutabilidad significa que los usuarios o los atacantes no pueden eliminar las copias de seguridad, pero en ciertos casos, como problemas de capacidad de almacenamiento, PowerProtect Cyber Recovery permite a los clientes eliminarlas con el modo de gobernanza de Retention Lock.

¿Cómo se comparan las ofertas similares de otras empresas con PowerProtect Cyber Recovery? Hemos analizado la información disponible públicamente sobre Cohesity Cyber Recovery, Veeam, Rubrik y Veritas NetBackup. A excepción de Cohesity Cyber Recovery, las soluciones pueden residir en las instalaciones o fuera de ellas (Cohesity es una solución basada en la cloud respaldada por AWS). La documentación de las cuatro soluciones afirma ofrecer inmutabilidad, pero es evidente que Rubrik y NetBackup tienen algunas diferencias con PowerProtect Cyber Recovery.

En Rubrik, los administradores pueden eliminar las copias de seguridad, pero no desde el lado del cliente y solo con ciertos controles establecidos. Además, todas las escrituras están "fuera de lugar", lo que significa que las escrituras nuevas nunca tocan datos escritos previamente.[13]

A pesar de ofrecer inmutabilidad, los administradores o los atacantes pueden eliminar el bloqueo de las copias de seguridad dentro de un almacenamiento compatible con NetBackup WORM. A continuación, pueden eliminar la imagen mediante el comando bpexpdate.[14]

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 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 operativas, para ayudar a proteger los datos. PowerProtect Cyber Recovery puede utilizar una cámara de aire física, en la que los datos de copia de seguridad se desconectan físicamente de la red de producción y se almacenan en una ubicación aislada, y una cámara de aire lógica, que depende de los controles de acceso a la red para separar las copias de seguridad desconectadas lógicamente del entorno de producción. Es importante contar con ambos tipos de cámaras de aire porque una cámara de aire lógica por sí sola no puede impedir que un usuario interno con acceso de red al vault acceda a los datos y los ponga en riesgo.

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.[15] Al eliminar el acceso al entorno de recuperación de la red de producción, una organización puede reducir su superficie de ataque. Como se ha indicado, para acceder a los datos aislados se requieren credenciales de seguridad independientes, así como autenticación multifactor (MFA).[16]

Enfoques del aislamiento

Gartner afirma que "los entornos de recuperación aislados (IRE) con vaults de datos inmutables (IDV) proporcionan el nivel más alto de seguridad y recuperación frente a amenazas internas, ransomware y otras formas de piratería informática".[17] También señala que un "IRE con un IDV no reemplaza, sino que complementa, los sistemas tradicionales de copia de seguridad y recuperación ante desastres (DR) mediante la entrega de una copia de seguridad terciaria inmutable en un IRE equipado con todas las herramientas, procesos y recursos para recuperar los sistemas afectados".[18]

Al revisar la información pública disponible sobre las soluciones Cohesity, Veeam, Rubrik y Veritas, determinamos que cada una tiene al menos un enfoque ligeramente diferente de un IRE en comparación con PowerProtect Cyber Recovery. Con la solución de Dell, los clientes pueden aislar física o lógicamente sus vaults de DD de la producción para mantener los planos de control y datos de producción separados de los vaults. Además, PowerProtect Cyber Recovery automatiza las cámaras de aire, algo que no todas las otras soluciones hacen.

Según la documentación:

- Cohesity Cyber Recovery solo ofrece una cámara de aire lógica automatizada y dinámica para su vault FortKnox basado en AWS.[19]
- Veeam ofrece una cámara de aire lógica para proveedores de cloud pública y privada a través de Veeam Cloud Connect, pero no está automatizada. Veeam también ofrece Veeam Hardened Repository, que funciona como vault local para la solución y que las organizaciones pueden configurar para disponer de una cámara de aire física.[20]
- Rubrik no ofrece una cámara de aire automatizada para Rubrik Cloud Vault, pero los clientes pueden añadir una cámara de aire lógica a través de una asociación de terceros con Microsoft.[21]
- Los clientes de NetBackup deben habilitar manualmente una cámara de aire lógica y pueden crear una cámara de aire física dentro o fuera de las instalaciones.[22]

Cómo funciona

La figura 1 muestra las rutas de red del vault de Cyber Recovery aislado. Tenga en cuenta que el vault no tiene ninguna ruta de gestión ni control hacia el entorno de producción para reducir la superficie de ataque.

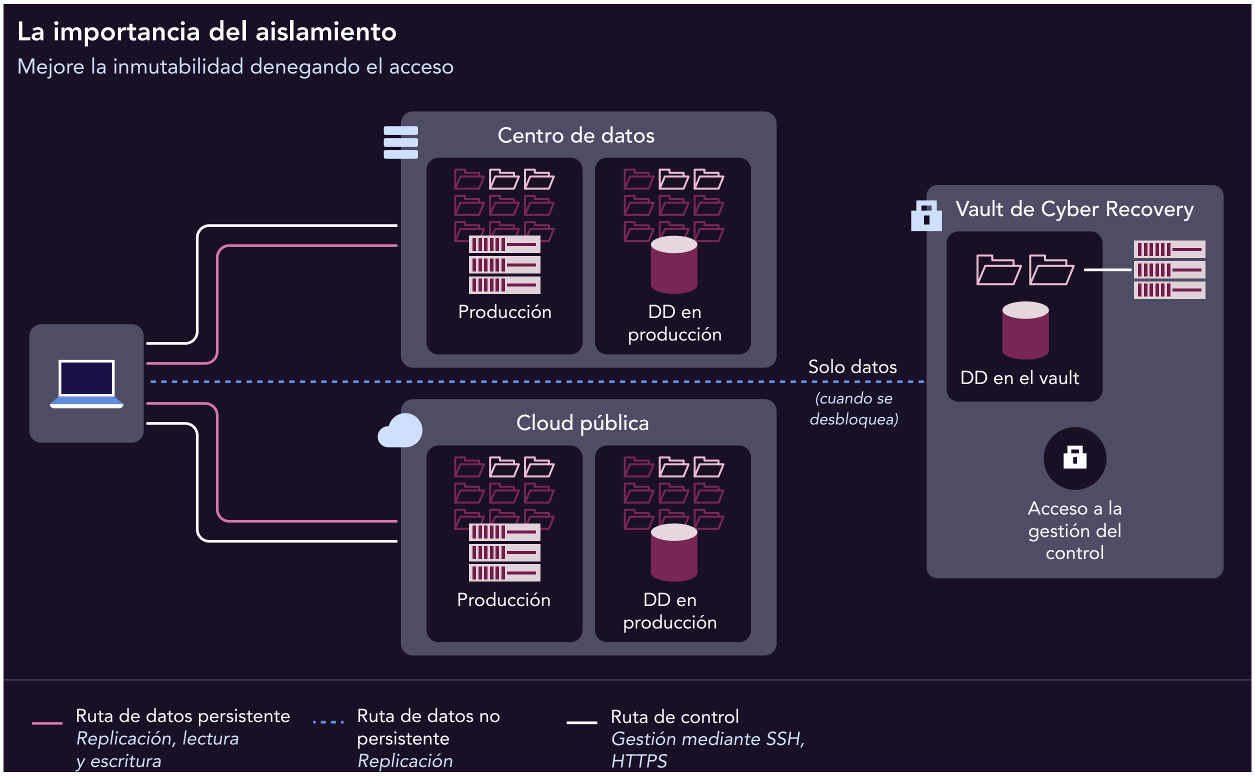


Figura 1: Arquitectura de ruta de control y datos de alto nivel del vault de Cyber Recovery. Fuente: Principled Technologies.

La única conexión necesaria para el vault de Cyber Recovery es una ruta de datos para la sincronización periódica de datos. La sincronización es cuando la solución Cyber Recovery recopila datos en intervalos cortos basados en políticas para la replicación.[23] En la guía de la solución PowerProtect Cyber Recovery se indica que "la arquitectura de la solución Cyber Recovery de nivel base consiste en un par de sistemas PowerProtect DD y el host de gestión de Cyber Recovery. En esta configuración de nivel base, el software Cyber Recovery, que se ejecuta en el host de gestión, habilita y deshabilita la interfaz Ethernet de replicación junto con los contextos de replicación del sistema PowerProtect DD en el vault de Cyber Recovery para controlar el flujo de datos del entorno de producción al entorno del vault".[24] Dell sugiere formas adicionales de que las organizaciones puedan proteger y aislar las rutas de datos. Observamos que Cyber Recovery desbloqueaba y bloqueaba el vault durante y después de la replicación en nuestras pruebas.

Para la implementación física del vault, Dell recomienda "instalar el equipo del vault de Cyber Recovery en una sala o carcasa específica con controles de acceso físico. Esta sala segura debe tener una lista de acceso limitado con registro de salida con llave o acceso con clave de dos personas. Se debe instalar videovigilancia en los puntos de acceso a la carcasa o sala y en el equipo. Para obtener la máxima seguridad, el software Cyber Recovery solo debe ser accesible mediante acceso físico al servidor de gestión de Cyber Recovery y a un teclado y ratón asociados".[25]

Con la separación de las rutas de gestión y control, las opciones de aislamiento físico y lógico de Cyber Recovery se distinguen de otras soluciones. Algunas soluciones permiten acceder a los datos de su vault desde una interfaz de entorno de producción. Esto coloca los datos del vault en la misma superficie de ataque que los datos de producción, lo que posiblemente permite a los atacantes acceder a las copias de seguridad con credenciales comprometidas.

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. CyberSense es un motor de análisis que utiliza algoritmos de análisis de aprendizaje automático basados en IA para analizar y validar la integridad de las copias de seguridad en el vault y el contenido de usuario de los archivos dentro de las copias de seguridad.

CyberSense se ejecuta dentro del vault, aislado del entorno de producción. Supervisa los archivos, las imágenes de máquinas virtuales y las bases de datos dentro del vault para determinar si se ha producido un ataque mediante el análisis de la integridad de los datos. Una vez que la solución Cyber Recovery replica las copias de seguridad en el vault y aplica la función de bloqueo de retención, CyberSense escanea automáticamente las copias, creando observaciones de un punto en el tiempo de los archivos, las bases de datos y la infraestructura principal. El motor de análisis explora todo el contenido de los archivos y de cada página de la base de datos, no solo los metadatos. Mientras que otras soluciones buscan cambios en los umbrales de datos o metadatos, CyberSense busca dentro del contenido de los archivos para validar la integridad de los datos. Estas observaciones permiten a CyberSense realizar un seguimiento de cómo cambian los archivos y las bases de datos con el tiempo y descubrir muchos tipos avanzados de ataques ocultos. CyberSense genera análisis que detectan patrones de daños que podrían indicar la actividad de un atacante, lo que incluye el cifrado, la eliminación, la creación o la ocultación de archivos, etc.[26] Otras soluciones llevan el análisis a la cloud, lo que puede ampliar la superficie de ataque, mientras que las organizaciones pueden optar por ejecutar CyberSense en las instalaciones o en una de las muchas opciones de cloud compatibles con Cyber Recovery.

CyberSense combina más de 200 análisis con observaciones de datos que se vuelven más útiles con el tiempo a medida que aumentan las observaciones. El algoritmo de aprendizaje automático utiliza información sobre miles de infecciones de malware para encontrar patrones inusuales de comportamiento y distinguir la actividad de los usuarios del ransomware, al tiempo que minimiza los falsos positivos y negativos. El algoritmo recibe nueva información sobre aspectos como las variantes de ataque, a través de investigaciones continuas. Además, el algoritmo de aprendizaje automático recibe actualizaciones basadas en datos reales de los clientes existentes de CyberSense.[27]

Además, CyberSense admite la indexación de datos en formatos de copia de seguridad de disco comunes de Dell, IBM, Commvault y Veritas.[28] Al ser compatibles los formatos de copia de seguridad de otros proveedores, Dell demuestra su voluntad de satisfacer las necesidades de los clientes en lo que respecta a las copias de seguridad de datos.

Probamos el software de análisis inteligente basado en ML de dos soluciones listas para usar de protección de datos y ciberrecuperación para empresas: CyberSense para Dell PowerProtect Cyber Recovery en un Dell PowerStore™ 7000T y una herramienta funcionalmente similar de la plataforma de gestión de datos de un competidor ("proveedor X") para un dispositivo de tamaño similar.

Método de las pruebas

Realizamos todas las pruebas de forma remota y tuvimos control total y acceso sin restricciones a los bancos de pruebas. Tanto la solución de Dell (que incluye CyberSense, la aplicación de copia de seguridad PowerProtect Data Manager, APEX Protection Storage (anteriormente conocida como DD Virtual Edition) y la solución PowerProtect Cyber Recovery) como la solución del proveedor X se encontraban en un laboratorio de centro de datos fuera del sitio.

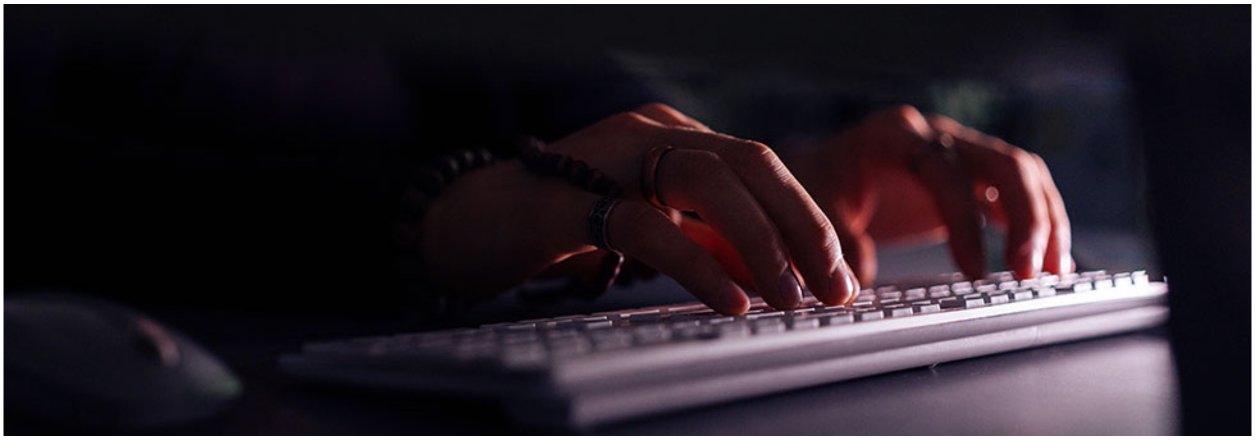
En ambas soluciones, ejecutamos tres supuestos de eventos maliciosos basados en scripts dirigidos a copias de seguridad:

Figura 2: Nuestros supuestos de prueba. Fuente: Principled Technologies.

Para ambas soluciones, seguimos el mismo procedimiento general en los dos primeros supuestos. En primer lugar, creamos una copia de seguridad completa de todas las máquinas virtuales limpias en los dispositivos de almacenamiento de Dell PowerProtect Data Manager y del proveedor X, creamos copias de seguridad incrementales para analizar y verificamos que la solución de destino no detectaba una amenaza. Esto nos dio un conjunto de copias de seguridad de referencia en las que podíamos ejecutar los scripts de ataque.

A continuación, ejecutamos el script de simulación de ransomware en cuatro máquinas virtuales con diferentes sistemas operativos y tipos de aplicaciones, realizamos nuevas copias de seguridad incrementales en el dispositivo de destino y comprobamos si el software de análisis de destino detectaba la amenaza de cifrado.

Para el tercer supuesto (infectar una página de SQL Server), seguimos un procedimiento similar al de los otros dos, pero en su lugar nos centramos en máquinas virtuales de SQL y usamos un script de corrupción de páginas en lugar de un script de cifrado. Ejecutamos el script en una sola máquina virtual.



Qué descubrimos

Supuesto 1: detección de archivos cifrados con nombres de archivo ocultos

Este supuesto simulaba un evento malicioso que cifraba archivos y ocultaba sus nombres, lo que cambiaba los metadatos del archivo además de su contenido. Este tipo de ataque se conoce normalmente como ransomware, un evento de seguridad en el que el software malicioso bloquea el acceso a un sistema informático hasta que el propietario o el usuario del sistema pague una cantidad predeterminada de dinero. Según la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) de EE. UU., "el impacto económico y en la reputación del ransomware y la extorsión de datos ha demostrado ser difícil y costoso para organizaciones de todos los tamaños durante la interrupción inicial y, a veces, la recuperación prolongada".[29] El uso de software de análisis inteligente para detectar el cifrado en las copias de seguridad puede fortalecer la estrategia de protección de datos de cualquier organización, ayudar a proteger la información valiosa y confidencial, y reducir la posibilidad de costosos tiempos de inactividad debido a ciberataques.

En nuestras pruebas, ambas aplicaciones de análisis inteligentes descubrieron los archivos cifrados con nombres de archivo cambiados. La solución del proveedor X necesitó una base de 15 copias de seguridad antes de detectar infecciones (una copia de seguridad completa y 14 copias de seguridad incrementales), mientras que CyberSense detectó infecciones después de una copia de seguridad completa, lo que significa que la solución del proveedor X necesitó 14 copias de seguridad adicionales en comparación con CyberSense.

Cuando la solución del proveedor X nos alertó de la actividad sospechosa, solo indicó que algo había eliminado muchos archivos y agregado un número igual de archivos, lo que era actividad sospechosa según la clasificación de entropía de la copia de seguridad.[30] La solución del proveedor X no indicó que los archivos se habían cifrado o que los nombres de los archivos habían cambiado. Por el contrario, Cyber Recovery con CyberSense nos alertó de que algo había cifrado y ocultado los nombres de archivos.

Los resultados del proveedor X podrían indicar un falso positivo. En otras palabras, si asumimos que una organización ejecuta copias de seguridad diarias con la solución del proveedor X, podría haber recopilado 14 días de archivos infectados antes de la detección de anomalías. Por el contrario, CyberSense necesitó solo una copia de seguridad de referencia para alertar con inteligencia sobre la infección y sus detalles. En esta fase de nuestro ejemplo, la recuperación con Cyber Recovery se realiza desde el vault aislado, lo que garantiza a la organización que no se ha expuesto la red de producción a las 14 copias de seguridad infectadas, como podría haber hecho la solución del proveedor X.

Figura 3: El número de copias de seguridad que cada solución requirió para crear una referencia para detectar daños. Fuente: Principled Technologies.

Supuesto 2: detección de archivos cifrados con nombres de archivo originales

Este supuesto era similar al primer, pero el script conservaba los nombres de archivo originales de los archivos cifrados. Este cambio no afectaba a los metadatos de los archivos, solo a los archivos en sí. Un acto como este podría ser un ransomware de tipo bomba de tiempo, en el que el ataque permanece inactivo durante un periodo de tiempo antes de activarse. El ransomware de tipo bomba de tiempo puede evadir la detección y atacar las copias de seguridad, lo que hace que queden inutilizables cuando la organización las necesita.[31] Sin cambios en los metadatos, el archivo puede parecer que no está infectado a simple vista, lo que ayuda a mantener oculto el ataque inactivo.

En nuestras pruebas, ambas aplicaciones de análisis inteligentes descubrieron los archivos cifrados. De nuevo, la solución del proveedor X necesitó una referencia de 15 copias de seguridad, incluidas 14 copias de seguridad incrementales, antes de poder detectar una anomalía. CyberSense necesitó una referencia de solo una copia de seguridad completa antes de detectar una anomalía.

Al igual que en el primer supuesto, la solución del proveedor X solo nos alertó de que algo había cambiado en muchos archivos, lo cual era sospechoso según la clasificación de entropía de la copia de seguridad. No indicó que algo hubiera cifrado los archivos, mientras que Cyber Recovery con CyberSense sí nos lo indicó. Detectar daños de esta manera significa que CyberSense está analizando el contenido de los archivos, no solo los metadatos en el nivel superficial. Este tipo de análisis añade otra capa de seguridad a sus copias de seguridad y, por lo tanto, a su infraestructura digital o al entorno en general. Se podría sugerir que CyberSense es una aplicación de análisis inteligente "real". Además, las organizaciones pueden detectar daños antes con CyberSense, ya que la solución necesitó muchas menos copias de seguridad para crear una referencia. Dependiendo del programa de copias de seguridad de una organización, eso podría producirse muchos días antes.

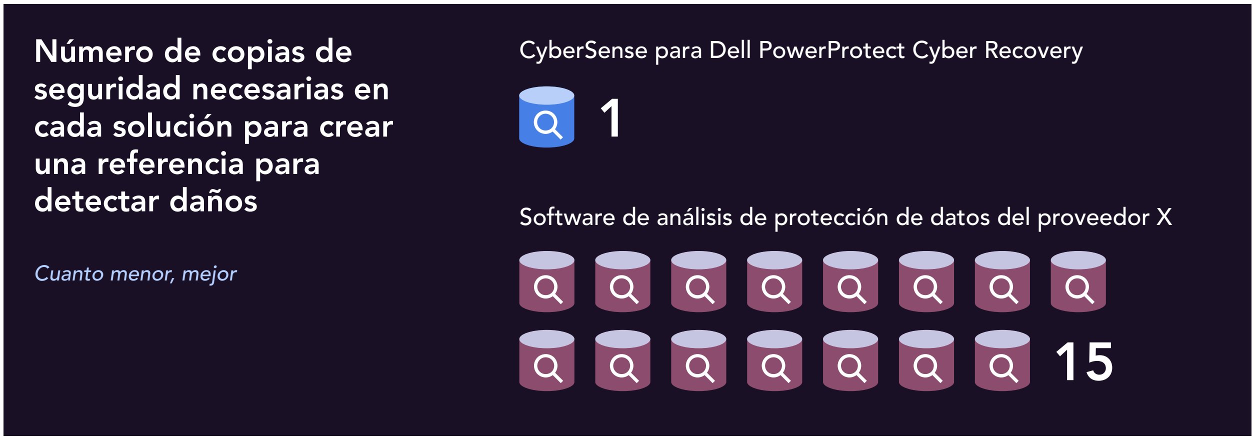


Figura 4: El número de copias de seguridad que cada solución necesitó para detectar daños. Fuente: Principled Technologies.

Supuesto 3: detección de daños en una página de SQL Server

Este supuesto simulaba un evento malicioso que dañaba una página de SQL Server. En SQL Server, la unidad fundamental de almacenamiento de datos es la página y la base de datos lee o escribe páginas de datos completas.[32] De nuevo, este cambio no afectó a los metadatos, solo a los archivos en sí. Este tipo de ataque se conoce comúnmente como inyección de SQL, en el que los atacantes de dirigen a aplicaciones basadas en datos de SQL mediante la inyección de código malicioso en declaraciones de SQL a través de la entrada de páginas web.[33] Incluso si están infectadas, es posible que las bases de datos sigan ejecutándose. Además del robo de datos, la corrupción de páginas de SQL Server puede provocar problemas de integridad de los datos, pérdida de datos e interrupciones en la funcionalidad de la base de datos. Estos resultados pueden dañar la reputación de una organización, interrumpir los flujos de trabajo operativos, provocar pérdidas monetarias e incluso suponer responsabilidades legales.

Aunque CyberSense y la solución del proveedor X detectaron el cifrado en los dos primeros supuestos, solo CyberSense fue capaz de analizar con la suficiente profundidad para detectar los daños en la página de SQL Server en este tercer supuesto. Esto muestra que, si bien las dos soluciones ofrecen capacidades de detección similares en algunos niveles, CyberSense ofrece un análisis más profundo de las copias de seguridad para aplicaciones basadas en SQL Server potencialmente críticas para la empresa. De esta manera, CyberSense añade una capa de resiliencia de seguridad con análisis más profundos y una protección más completa.

SQL Server impulsa muchas aplicaciones en los sectores financiero, minorista, sanitario y otros. Debido a que SQL Server puede funcionar como el back-end de la arquitectura de desarrollo, un ataque de SQL Server puede provocar tiempo de inactividad, interrumpir las operaciones y, potencialmente, poner en riesgo los ingresos que generan estas aplicaciones.

Restauración y recuperación con Dell PowerProtect Cyber Recovery

La estrategia de ciberresiliencia de Dell proporciona una amplia gama de capacidades de recuperación. Estas opciones de recuperación incluyen capacidades comunes del sector, como el acceso instantáneo o la recuperación tradicional de las copias de seguridad inmutables mantenidas en producción. Además, Dell ofrece las capacidades de recuperación únicas de la solución PowerProtect Cyber Recovery. Debido a que PowerProtect Cyber Recovery mantiene las copias aisladas y las analiza en busca de integridad con CyberSense, las organizaciones pueden acceder a las copias inmediatamente después de un ataque y utilizarlas para iniciar los pasos de recuperación o restauraciones inmediatas en plataformas de recuperación alternativas, como salas limpias.

Comparemos este caso de uso inmediato con una organización que solo puede acceder a los datos en producción o en la cloud pública. La organización no puede acceder de forma segura a los datos almacenados en el área comprometida hasta que haya determinado y corregido la causa raíz, haya acabado con la persistencia de los agentes maliciosos, haya tomado imágenes forenses para las aseguradoras y su departamento legal, haya vuelto a analizar los datos y tenga suficiente infraestructura disponible (AD, DNS) para acceder a la infraestructura de copia de seguridad. Este proceso podría tardar días o semanas en función del alcance y la sofisticación del ataque.

Cómo funciona

Durante la producción normal, PowerProtect Cyber Recovery crea automáticamente puntos de restauración para los análisis de seguridad y recuperación. En caso de ciberataque, Cyber Recovery utiliza sus procedimientos automatizados de restauración y recuperación y esos puntos de restauración para volver a poner en marcha los sistemas críticos para la empresa. Los informes forenses y de CyberSense ayudan a los equipos de ciberseguridad y recuperación a diagnosticar el impacto del ataque. Una vez que el entorno de producción esté limpio y listo para la recuperación, Cyber Recovery proporciona las herramientas y la tecnología que llevan a cabo la recuperación de datos real.

Tras un ciberataque, entran en juego varias métricas de protección de datos para determinar la velocidad de recuperación (el tiempo de ciberrecuperación o CRT) y el punto en el tiempo al que los usuarios pueden regresar después de un ataque destructivo (el punto de ciberrecuperación o CRP). En una solución Cyber Recovery, estas métricas incluyen las siguientes:

- **Objetivo de detección de destrucción (DDO):** se trata de un plazo determinado basado en el tiempo transcurrido entre un ataque y la detección del ataque. Los análisis y otros mecanismos de Cyber Recovery deben funcionar durante este periodo.
- **Objetivo de evaluación de destrucción (DAO):** es la cantidad de tiempo asignado al equipo de ciberseguridad tras una incursión para determinar el alcance de los daños y las posibles respuestas.
- **Intervalo de sincronización de Cyber Recovery:** es la frecuencia con la que la solución Cyber Recovery copia los datos del entorno de producción en el vault. El tiempo se basa en un objetivo de punto de recuperación (RPO) establecido previamente para la solución. El periodo de retención de copias varía según la solución, pero normalmente oscila entre una semana y un mes.
- **Recuento de copias de datos de Cyber Recovery:** es el número de copias de datos que se guardan en el vault de Cyber Recovery. Cuando se combina con el intervalo de sincronización, esta métrica proporciona una medida aproximada del tiempo que se puede retroceder para recuperar los datos en una organización. Por ejemplo, siete copias junto con un intervalo de 24 horas permiten a los usuarios recuperar datos de hasta una semana de antigüedad.

Además de los requisitos de recuperación, el tipo de datos que protege la solución puede ayudar a determinar el intervalo de sincronización y el tiempo de retención de los datos. Según la guía de soluciones de Cyber Recovery, para obtener la mayor flexibilidad de recuperación, los usuarios pueden categorizar los datos que protege la solución en uno de los siguientes flujos de copia de seguridad:[34]

- Copias de seguridad binarias y ejecutables, incluidas las distribuciones de sistemas operativos de nivel básico y las compilaciones de aplicaciones

- Copias de seguridad completas de aplicaciones y sistemas de archivos, incluidas imágenes y datos específicos de la aplicación

Estos flujos de copia de seguridad independientes llevan a dos estrategias de recuperación diferentes:

1. **Restauración de datos y binarios de aplicaciones en el vault de Cyber Recovery:** La solución identifica los puntos de restauración útiles, junto con el malware y dónde ha permanecido, y decide si limpiar el malware de la imagen de copia de seguridad o reconstruirla utilizando copias del vault de Cyber Recovery. Después de aplicar parches de seguridad, la solución restaura los datos en un host de recuperación utilizando el runbook de DR para la aplicación, y luego determina si el proceso de recuperación ha eliminado los efectos del malware. A continuación, realiza una prueba de ejecución en la aplicación utilizando la computación del vault y limpia o vuelve a crear una imagen del entorno de producción. Por último, Cyber Recovery conecta el host de recuperación con la producción y copia la aplicación y los datos de nuevo en el entorno de producción. Este proceso se muestra en la figura 5.

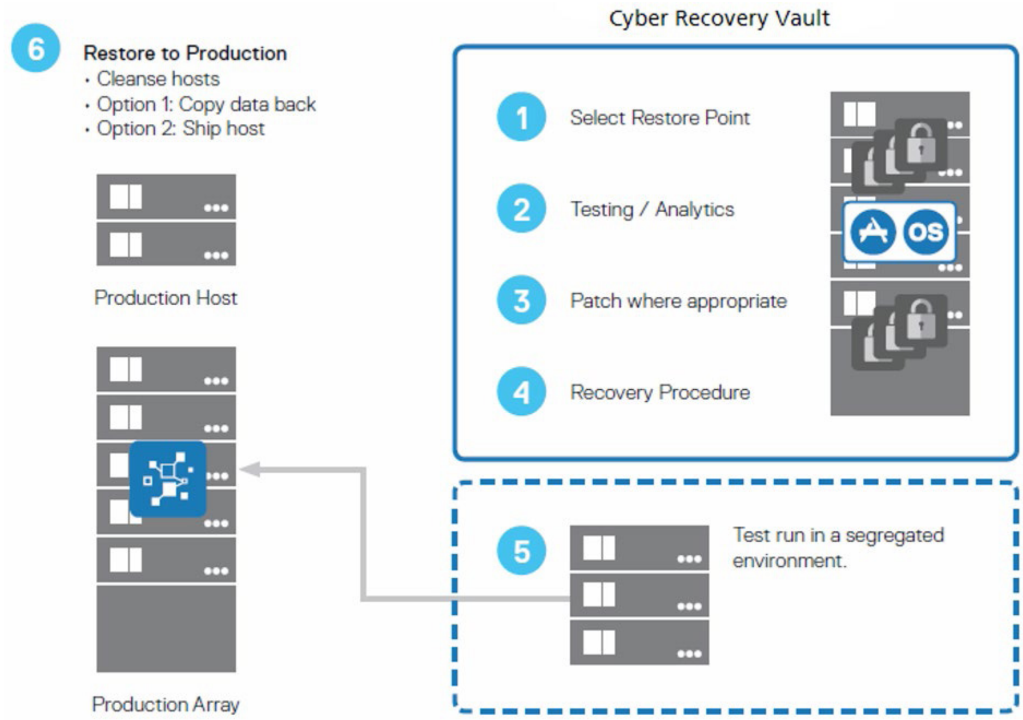


Figura 5: El proceso para restaurar datos y binarios de aplicaciones. Fuente: Dell Technologies.[35]

2. **Reconstrucción completa desde el vault de Cyber Recovery:**
   En este enfoque, la solución Cyber Recovery reformatea los sistemas de producción en función del nivel de daño determinado por la evaluación forense durante la respuesta ante incidentes. A continuación, la solución reconstruye los binarios a través de copias en el vault de Cyber Recovery y aplica los parches de seguridad disponibles. Por último, restaura las copias adecuadas de las aplicaciones, los datos y los archivos de configuración en el entorno de producción mediante los runbooks de DR asociados para la aplicación. Este proceso se muestra en la figura 6.

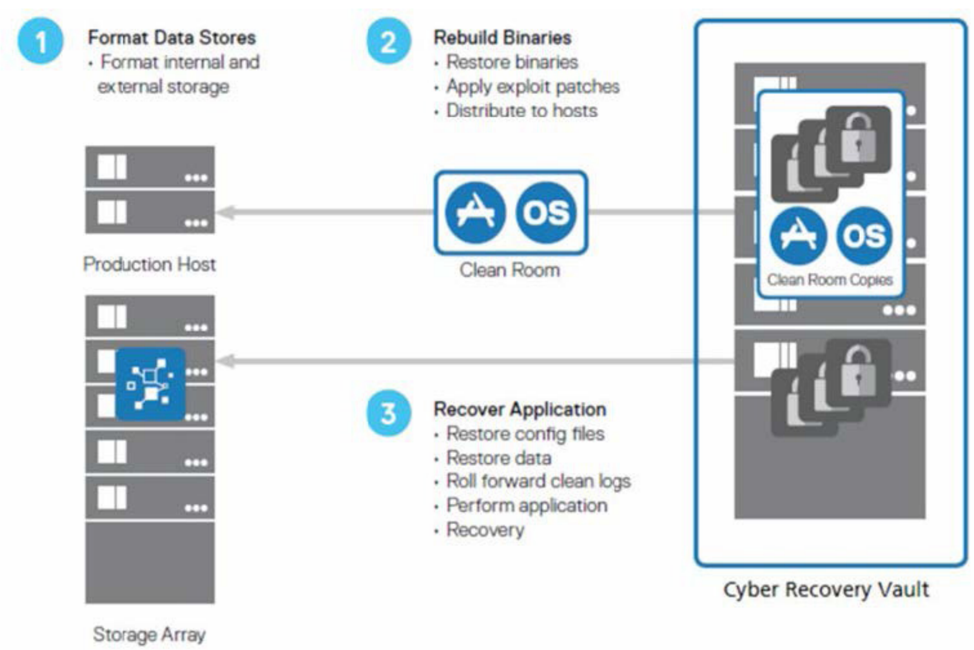


Figura 6: El proceso para la reconstrucción completa desde el vault de Cyber Recovery. Fuente: Dell Technologies.[36]

Las soluciones Cyber Recovery incluyen hosts de recuperación físicos o virtuales (o ambos) que el software Cyber Recovery puede utilizar para la recuperación. Estos hosts incluyen tanto un servidor de recuperación de aplicaciones de copia de seguridad, que es un servidor designado para el que se recuperan la aplicación de copia de seguridad y el catálogo de aplicaciones de copia de seguridad, como un servidor de recuperación de aplicaciones. Las organizaciones pueden implementar varios servidores en función de los requisitos de recuperación de la solución. El software Cyber Recovery puede exponer las copias de datos de entorno aislado (un entorno de prueba para ejecutar software nuevo o no probado de manera segura) a cualquier host para realizar recuperaciones de datos dentro del vault, como datos del sistema de archivos, datos de copia de seguridad de IBM, Commvault y Veritas o datos protegidos por Dell NetWorker, Dell Avamar, una dispositivo Dell PowerProtect serie DP o software Dell PowerProtect Data Manager. Después de recuperar una aplicación de copia de seguridad dentro del vault, la solución puede restaurar esos datos en hosts de recuperación adicionales en el vault.

Las organizaciones dimensionan el servidor de recuperación de aplicaciones de copia de seguridad con antelación para que los usuarios puedan recuperar todas las aplicaciones de copia de seguridad que protege la solución Cyber Recovery. Del mismo modo, el servidor de recuperación de aplicaciones es un servidor designado en el que la solución recupera las aplicaciones. Algunas aplicaciones pueden requerir que los clientes recuperen primero otras aplicaciones dependientes. La infraestructura dentro del vault puede admitir la recuperación de la aplicación de producción más grande que protege la solución.

Conclusión

Las organizaciones deben tener en cuenta muchos vectores de ataque a la hora de elaborar un plan de protección de datos. Esto incluye la protección de todos los datos, pero lo más importante, el imperativo de datos críticos para las operaciones. PowerProtect Cyber Recovery aísla los datos críticos y ayuda a garantizar una recuperación adecuada de los datos en caso de ciberataque. Cyber Recovery utiliza análisis basados en ML en CyberSense para determinar la integridad de los datos en el vault e identificar datos limpios de copia de seguridad para la recuperación. En nuestras pruebas, descubrimos que PowerProtect Cyber Recovery detectó una infección en páginas de bases de datos SQL, algo que la solución de la competencia no pudo hacer. PowerProtect Cyber Recovery también requirió menos copias de seguridad que la solución de la competencia para determinar los daños en los datos. Además de todo esto y mucho más, la solución Cyber Recovery ofrece muchas opciones de recuperación, basándose en datos protegidos del vault para garantizar un retorno eficiente y fluido a las operaciones.

---

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, "Dell PowerProtect Cyber Recovery Solution Guide", acceso el 23 de agosto de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
4. Cohasset Associates, Inc, "Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)", acceso el 27 de octubre de 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, "Data Domain: Retention Lock Frequently Asked Questions", acceso el 12 de septiembre de 2023, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, "Data Domain: Retention Lock Frequently Asked Questions".
7. Dell, "Encryption types offered by DD series encryption appliance", acceso el 8 de septiembre de 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, "Dell EMC Data Domain – Security Configuration Guide", acceso el 11 de septiembre de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, "Role based access control (RBAC) in Data Domain", acceso el 11 de septiembre de 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, "Dell EMC Data Domain – Security Configuration Guide".
11. Dell, "MTREE replication", acceso el 11 de septiembre de 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, "Dell EMC Data Domain - DataDomain MTree overview and limits", acceso el 11 de septiembre de 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", acceso el 13 de diciembre de 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, "NetBackup™ Security and Encryption Guide", acceso el 13 de diciembre de 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. 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.
16. Dell, "Dell PowerProtect Cyber Recovery", acceso el 12 de septiembre de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman y Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware", acceso el 14 de diciembre de 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman y Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware".
19. Nikitha Okmar, "Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era", acceso el 13 de diciembre de 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, "How to protect your data from ransomware and encryption Trojans", acceso el 13 de diciembre de 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, "Rest easy with immutable, off-site data storage", acceso el 13 de diciembre de 2023, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, "NetBackup Isolated Recovery Environment", acceso el 13 de diciembre de 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, "Dell Cyber Recovery Vault (overview by CSI)", acceso el 23 de agosto de 2023, https://youtu.be/ej5nZzWNRM0.
24. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
25. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
26. Dell, "CyberSense® for PowerProtect Cyber Recovery".
27. Dell, "CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines", acceso el 13 de septiembre de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, "CyberSense for Dell Cyber Recovery", acceso el 25 de septiembre de 2023, https://indexengines.com/csmatrix.
29. CISA, "#StopRansomware Guide", acceso el 1 de agosto de 2023, https://www.cisa.gov/stopransomware/ransomware-guide.
30. "En seguridad, la mayoría de las personas utilizan Shannon Entropy, un algoritmo específico que devuelve un valor entre 0 y 8. Cuanto mayor sea el número, más aleatorios serán los datos y, en muchas ocasiones, un valor más alto significa que los datos están comprimidos o cifrados". Mueller, Clint, "How to Use Entropy Analysis in Penetration Testing", 28 de agosto de 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, "How to Protect your Backups from Ransomware in 2023", 1 de agosto de 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, "Pages and extents architecture guide", acceso el 3 de agosto de 2023, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, "SQL Injection", acceso el 3 de agosto de 2023, https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
36. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".

Lea la ciencia detrás de este informe ▶

▶ Consulte la versión original en inglés de este informe en https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

Este proyecto fue encargado por Dell Technologies.