DELL Technologies

Resumen de la solución

Dell PowerProtect Cyber Recovery

Protección moderna y resiliente de los datos cruciales contra el ransomware y los ataques cibernéticos destructivos.

¿POR QUÉ ESCOGER CYBER RECOVERY?

Los ataques cibernéticos están diseñados para comprometer los datos valiosos, incluidos los respaldos. Es clave proteger sus datos cruciales y recuperarlos con integridad garantizada para poder reanudar las operaciones comerciales normales después del ataque.

Estos son los componentes de una solución con resiliencia cibernética:

Inmutabilidad de datos
Cree copias de datos sin cambios para conservar la confidencialidad y la integridad de los datos con capas de seguridad y controles.

Aislamiento de datos automatizado
Aísle automáticamente copias de datos no modificables del entorno de respaldo de producción en un vault digital seguro con acceso restringido elevado.

Análisis inteligente
Las comprobaciones de integridad automatizadas mediante el aprendizaje automático basado en IA y la indexación de contenido completo con análisis eficaces dentro de la seguridad del vault determinan si el malware ha afectado los datos.

Recuperación y corrección
Flujos de trabajo y herramientas que permiten realizar la recuperación después de un incidente a través de procesos de restauración dinámica y los procedimientos de DR existentes.

Planificación y diseño de la solución Orientación de expertos para seleccionar conjuntos de datos cruciales, aplicaciones y otros recursos vitales con el fin de determinar los RTO y RPO, y optimizar la recuperación.

El desafío: los ataques cibernéticos son el enemigo de las empresas basadas en los datos.

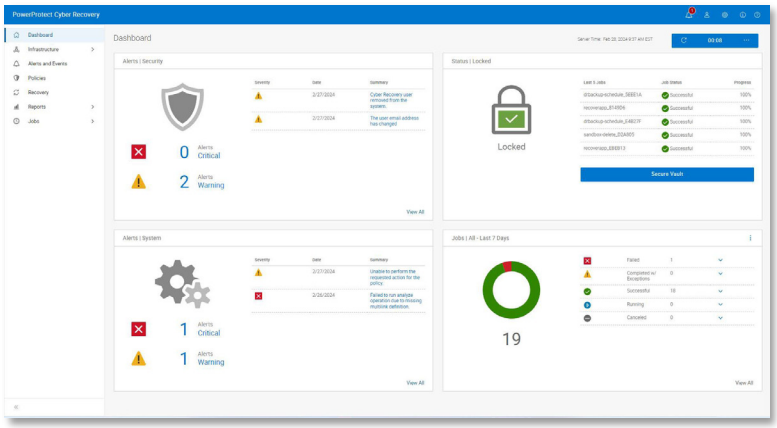
Los datos son la moneda de la economía digital y un activo fundamental. Es necesario protegerlos, mantener su confidencialidad y garantizar el fácil acceso a estos. El mercado global moderno depende del flujo continuo de datos a través de redes interconectadas. Las iniciativas de transformación digital y el creciente uso de la IA generativa aumentan la exposición de la información confidencial.

Esto ocasiona que los datos de su empresa sean un objetivo atractivo y lucrativo para los delincuentes cibernéticos. Independientemente de la industria o el tamaño de la empresa, los ataques cibernéticos exponen de forma continua a las empresas y a los Gobiernos a filtraciones de datos, pérdida de ingresos debido al tiempo de inactividad, daño a la reputación y costosas multas normativas.

Contar con una estrategia de resiliencia cibernética se ha convertido en una obligación para los líderes empresariales y gubernamentales, pero muchas organizaciones no confían en sus soluciones de protección de datos. El Global Data Protection Index informó que al 79 % de los tomadores de decisiones de TI les preocupa que experimenten un evento disruptivo en los próximos 12 meses y al 75 % les preocupa que las medidas de protección de datos existentes en sus organizaciones no sean suficientes para hacer frente a las amenazas de malware y ransomware[1].

La solución: Dell PowerProtect Cyber Recovery

Con el propósito de reducir el riesgo para el negocio que causan los ataques cibernéticos y crear un enfoque con mayor resiliencia cibernética para la protección de los datos, puede modernizar y automatizar sus estrategias de recuperación y continuidad comercial, y aprovechar las últimas herramientas inteligentes para detectar las amenazas cibernéticas y defenderse de estas.



PowerProtect Cyber Recovery ofrece una protección probada, moderna, inteligente y resiliente para aislar los datos cruciales, identificar las actividades sospechosas y acelerar la recuperación de datos. Esto facilita una recuperación más inteligente de los datos cruciales para reanudar rápidamente las operaciones normales de la empresa. Según una investigación de Forrester Consulting, en caso de un ataque cibernético, Dell PowerProtect Cyber Recovery ayuda a reducir el tiempo de inactividad en un 75 % y a reducir las horas dedicadas a la recuperación en un 80 %.[2]

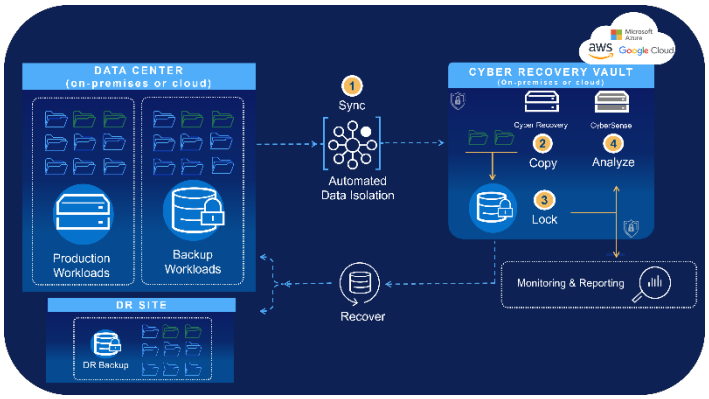
PowerProtect Cyber Recovery: inmutabilidad, aislamiento e inteligencia

Inmutabilidad: PowerProtect Data Domain

PowerProtect Data Domain es la base de Dell PowerProtect Cyber Recovery. Con varias capas de seguridad de confianza cero, esta opción proporciona copias de respaldo inmutables para garantizar la integridad y la confidencialidad de los datos. Las características como la raíz de confianza de hardware, el arranque seguro, el cifrado, el bloqueo de retención, el acceso basado en funciones y la autenticación de múltiples factores ayudan a garantizar la capacidad de recuperación de los datos.

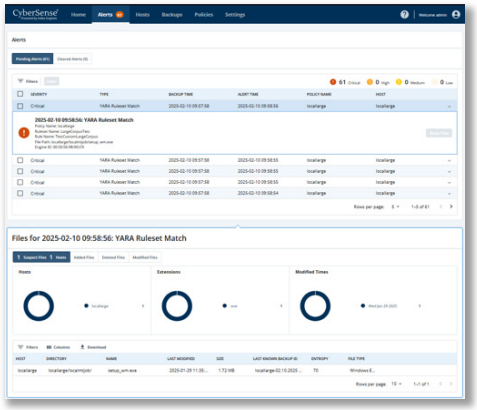
Aislamiento: Vault de Cyber Recovery

El vault de PowerProtect Cyber Recovery es un entorno aislado que ofrece varias capas de protección para brindar resiliencia frente a los ataques cibernéticos, incluso ante una amenaza interna. Su aislamiento de datos automatizado copia (sincroniza) de forma segura los datos de respaldo esenciales (incluidos los de sistemas abiertos y de mainframe) en un vault físicamente aislado, lejos de la superficie de ataque de producción, sin exponer nunca la ruta de administración a un agente de amenazas.
A continuación, se crea automáticamente una copia inmutable para evitar que se modifiquen los datos.
Para la administración, la red y los servicios dedicados independientes del entorno de producción, se requieren credenciales de seguridad independientes y autenticación de múltiples factores para acceder a los datos de las operaciones de recuperación y prueba.



Inteligencia: CyberSense®

PowerProtect Cyber Recovery es la primera solución que integra completamente CyberSense® para lograr recuperaciones más inteligentes contra las amenazas cibernéticas, todo dentro de la seguridad del vault de Cyber Recovery. CyberSense va más allá de las soluciones que solo se basan en metadatos, ya que sus análisis de contenido completo detectan daños en los datos después de un ataque con una precisión del 99,99 %[3] y facilitan la restauración inteligente y rápida. CyberSense aprovecha los respaldos de datos inmutables para observar cómo cambian con el tiempo y utiliza el aprendizaje automático basado en IA para detectar los indicios de daños que indican un ataque de ransomware. CyberSense detecta eliminaciones masivas, cifrado total y parcial, y otros cambios sospechosos en la infraestructura central (incluidos Active Directory, DNS, etc.), los archivos de usuario y las bases de datos que surgen de los ataques sofisticados. Es posible crear alertas de umbral personalizadas y, si se detectan indicios de daños, el panel de alertas y los informes forenses posteriores al ataque facilitan un diagnóstico rápido de la escala y el impacto del ataque, incluida la identificación de una copia limpia de los datos para recuperar los sistemas cruciales. Las reglas YARA personalizadas y la búsqueda de firmas de malware ayudan a personalizar y potenciar a las organizaciones para que se defiendan proactivamente contra las amenazas cibernéticas.



PowerProtect Cyber Recovery: Opciones de implementación

Cyber Recovery en entornos híbridos y de múltiples nubes

Pueden existir datos cruciales en muchas ubicaciones diferentes dentro de una empresa, ya sea en las instalaciones, en diferentes centros de datos o globalmente en múltiples nubes y regiones. Independientemente de la ubicación, los datos deben estar seguros y no verse comprometidos cuando se requiera una recuperación después de un ataque cibernético.

PowerProtect Cyber Recovery se encuentra disponible y se puede comerciar a través de mercados de nube pública para *AWS, Microsoft Azure* y *Google Cloud,* a fin de proporcionar un acceso rápido para proteger los datos en un vault de Cyber Recovery en la nube. PowerProtect Cyber Recovery automatiza la sincronización de datos críticos entre los sistemas de producción y el vault de Cyber Recovery en la nube pública. A diferencia de las soluciones de respaldo estándar basadas en la nube, los controles de red bloquean el acceso a las interfaces de administración, y requieren credenciales de seguridad separadas y una autenticación de múltiples factores para el acceso. La dispersión y la duplicación de datos en múltiples nubes puede generar riesgos de seguridad y cumplimiento, posibles problemas de sincronización y mayores costos de recursos. Este enfoque también puede reducir la visibilidad en los distintos entornos, lo que ocasiona que sea insuficiente la protección contra las amenazas cibernéticas, que están en constante evolución.

Dell PowerProtect Data Domain All-Flash Ready Node

Si bien los datos cruciales continúan creciendo, la capacidad de recuperarse de un evento cibernético de manera rápida y eficiente es primordial para garantizar la continuidad comercial y la resiliencia cibernética. Las organizaciones en proceso de expandir la administración de datos cruciales deben sobresalir en la recuperación de sus datos desde entornos de recuperación aislados, como el vault de Cyber Recovery. Dell PowerProtect Data Domain All Flash Ready Node ofrece una solución de recuperación cibernética optimizada, rentable y eficiente energéticamente que cuenta con análisis mejorados de CyberSense y funcionalidades de restauración rápida para cumplir con los SLA de la organización. Mediante el uso de menos hardware, espacio y energía, las organizaciones pueden mejorar las velocidades de acceso a datos, aumentar la eficiencia operacional y garantizar la integridad de los datos. En última instancia, todo esto reduce el tiempo de inactividad y los costos generales de mantenimiento.

PowerProtect Cyber Recovery: Retomar las actividades empresariales

Recuperación y corrección

PowerProtect Cyber Recovery proporciona procedimientos automatizados de restauración y recuperación para que los sistemas cruciales de la empresa vuelvan a estar en línea con rapidez y confianza. La recuperación está integrada en el proceso de respuesta ante incidentes. Después de que se produce un evento, el equipo de respuesta a incidentes analiza el entorno de producción para determinar la causa raíz del evento. CyberSense proporciona informes forenses posteriores al ataque para comprender la profundidad y la amplitud del ataque, y brinda una lista de los últimos conjuntos de respaldo en buen estado realizados antes de que se produjeran daños. Luego, cuando la producción está lista para la recuperación, Cyber Recovery proporciona herramientas de administración y la tecnología que realiza la recuperación de datos propiamente dicha.

Planificación y diseño de la solución

Dell Professional Services for Cyber Recovery ayuda a determinar qué sistemas cruciales para la empresa es necesario proteger, y permite crear mapas de dependencias para las aplicaciones y los servicios asociados, así como la infraestructura necesaria para la recuperación. El servicio también genera requisitos de recuperación y alternativas de diseño e identifica las tecnologías necesarias para analizar, alojar y proteger sus datos, junto con un modelo comercial y una línea de tiempo de implementación.

Conclusión

Las iniciativas del sector como Sheltered Harbor han estado utilizando PowerProtect Cyber Recovery para proteger a los clientes, las instituciones financieras y la confianza pública en el sistema financiero de los EE. UU. en caso de que ocurra un ataque cibernético que cause que los sistemas críticos fallen, incluidas las copias de seguridad. Con miles de clientes, Cyber Recovery con CyberSense brinda confianza a los líderes empresariales y ha demostrado que acelera la recuperación de datos en caso de una amenaza cibernética.

PowerProtect Cyber Recovery puede brindarle la confianza para poder identificar y restaurar rápidamente los datos buenos conocidos y reanudar las operaciones comerciales normales después de un ataque cibernético.

Es momento de retomar las actividades empresariales.

Obtenga más información sobre Dell PowerProtect Cyber Recovery

Comuníquese con un experto de Dell Technologies

Vea más recursos

Únase a la conversación con #PowerProtect

[1] Información basada en un estudio de Vanson Bourne encargado por Dell Technologies, “Instantánea del Global Data Protection Index 2024”. Octubre de 2023.
[2] Investigación de Forrester Consulting realizada por encargo de Dell Technologies, “Total Economic Impact de Dell PowerProtect Cyber Recovery”, agosto de 2023
[3] Información basada en un informe de ESG encargado por Index Engines, “CyberSense de Index Engines demostró una eficacia del 99,99 % en la detección de daños causados por ransomware”. Junio de 2024