DELL Technologies

Resumen de la solución

Dell PowerProtect Cyber Recovery

Protección resiliente y moderna de datos críticos contra ransomware y ciberataques destructivos.

¿POR QUÉ OPTAR POR CYBER RECOVERY?

Los ciberataques están diseñados para poner en peligro sus datos valiosos, incluidas las copias de seguridad. Proteger sus datos críticos y recuperarlos garantizando su integridad es esencial para reanudar sus operaciones comerciales habituales después de un ataque.

Estos son los componentes de una solución ciberresiliente:

Inmutabilidad de los datos
Cree copias de datos inalterables para preservar la integridad y la confidencialidad de los datos con capas de seguridad y controles.

Aislamiento de datos automatizado
Aísle automáticamente copias de datos no modificables del entorno de copia de seguridad de producción a un vault digital seguro con acceso muy restringido.

Análisis inteligente
Comprobaciones de integridad automatizadas mediante aprendizaje automático basado en IA e indexación de contenido completo con potentes análisis dentro de la seguridad del vault para determinar si los datos se han visto afectados por malware.

Recuperación y corrección
Flujos de trabajo y herramientas para realizar la recuperación después de un incidente utilizando procesos de restauración dinámicos y sus procedimientos de recuperación de desastres actuales.

Planificación y diseño de soluciones Asesoramiento de expertos para seleccionar conjuntos de datos críticos, aplicaciones y otros activos vitales para determinar los RTO y RPO y agilizar el proceso de recuperación.

El problema: los ciberataques son el enemigo de los negocios basados en datos.

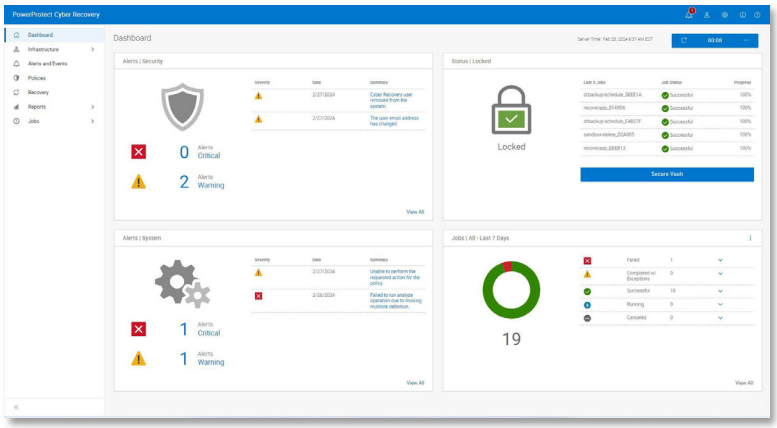
Los datos son la moneda de cambio de la economía digital y un activo vital que debe salvaguardarse, mantener su confidencialidad y ser fácilmente accesible. El mercado mundial actual depende del flujo continuo de datos a través de redes interconectadas. Las iniciativas de transformación digital y el creciente uso de la IA generativa aumentan la exposición de la información confidencial.

Esto hace que los datos de su organización sean un objetivo atractivo y lucrativo para los ciberdelincuentes. Independientemente del sector o el tamaño de la organización, los ciberataques exponen continuamente a las empresas y los gobiernos a datos comprometidos, pérdida de ingresos debido al tiempo de inactividad, daños a la reputación y elevadas sanciones económicas.

Tener una estrategia de ciberresiliencia es obligatorio para las empresas y los líderes de gobierno, pero a pesar de todo muchas organizaciones no confían en sus soluciones de protección de datos. Según el informe Global Data Protection Index, al 79 % de los responsables de toma de decisiones de TI les preocupa padecer un evento disruptivo en los próximos 12 meses, mientras que el 75 % no confía en que las medidas de protección de datos adoptadas por sus organizaciones sean suficiente para hacer frente a las amenazas de malware y ransomware[1].

La solución: Dell PowerProtect Cyber Recovery

Para reducir el riesgo empresarial que suponen los ciberataques y adoptar un enfoque de protección de datos más resistente a estos ataques, puede modernizar y automatizar sus estrategias de recuperación y continuidad empresarial, así como aprovechar las últimas herramientas inteligentes para detectar y defenderse contra las ciberamenazas.



PowerProtect Cyber Recovery le ofrece una protección eficaz, moderna, resiliente e inteligente para aislar sus datos críticos, identificar actividades sospechosas y acelerar el proceso de recuperación de datos, lo que le permitirá facilitar una recuperación más inteligente de sus datos críticos y reanudar rápidamente las operaciones normales de su empresa. Según una investigación de Forrester Consulting, en caso de ciberataque, PowerProtect Cyber Recovery ayuda a reducir el tiempo de inactividad en un 75 % y las horas dedicadas a la recuperación en un 80 %.[2]

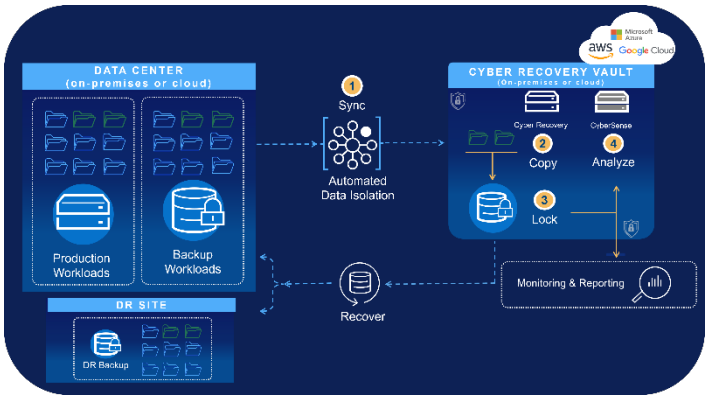
PowerProtect Cyber Recovery: inmutabilidad, aislamiento e inteligencia

Immutabilidad - PowerProtect Data Domain

Dell PowerProtect Cyber Recovery se basa en PowerProtect Data Domain. Con varias capas de seguridad basada en la confianza cero, proporciona copias de seguridad inmutables para garantizar la integridad y confidencialidad de los datos. 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 multifactor garantizan la capacidad de recuperación de sus datos.

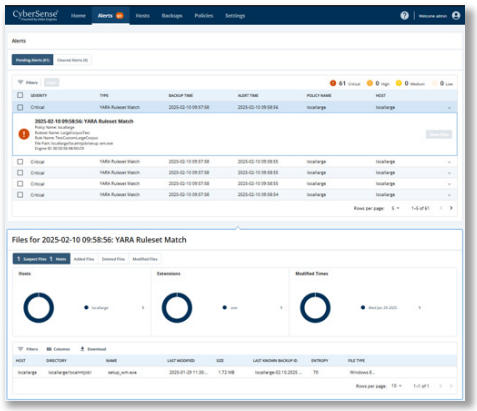
Aislamiento - Vault de Cyber Recovery

El vault de PowerProtect Cyber Recovery es un entorno aislado que ofrece varias capas de protección para proporcionar resistencia contra los ciberataques, incluso de personal interno. Su aislamiento de datos automatizado copia de forma segura (sincronización) los datos de copia de seguridad críticos (incluidos los sistemas abiertos y ordenadores centrales) a un vault físicamente aislado, lejos de la superficie de ataque de producción, sin exponer la ruta de gestión a un agente de amenazas. A continuación, se crea automáticamente una copia inmutable para evitar que se modifiquen los datos. Con una gestión, red y servicios dedicados independientes del entorno de producción, se requieren credenciales de seguridad independientes y autenticación multifactor para acceder a los datos para las operaciones de recuperación y prueba.



Inteligencia - CyberSense®

PowerProtect Cyber Recovery es la primera solución que integra completamente CyberSense® para ofrecer una recuperación más inteligente frente a ciberamenazas, todo ello dentro de la seguridad del vault de Cyber Recovery. CyberSense va más allá de las soluciones basadas únicamente en metadatos. Con análisis de contenido completo, detecta la corrupción de datos tras un ataque con una precisión del 99,99 %[3] y facilita la restauración inteligente y rápida. CyberSense aprovecha las copias de seguridad de datos inmutables para observar cómo cambian a lo largo del tiempo y utiliza el aprendizaje automático basado en IA para detectar signos de corrupción que indican un ataque de ransomware. CyberSense detecta eliminaciones masivas, cifrado total o parcial y otros cambios sospechosos en la infraestructura principal (incluidos Active Directory, DNS, etc.), los archivos de usuarios y las bases de datos como consecuencia de ataques sofisticados. Se pueden crear umbrales de alerta personalizados y, si se detectan signos de daños, el panel de alertas y los informes forenses posteriores al ataque facilitan un diagnóstico rápido de la magnitud y el impacto del ataque, incluida la identificación de una copia limpia de los datos para recuperar sus sistemas críticos. Las reglas personalizadas de YARA y la búsqueda de firmas de malware ayudan a personalizar y capacitar a las organizaciones para defenderse proactivamente contra las ciberamenazas.



PowerProtect Cyber Recovery – Opciones de implementación

Cyber Recovery en entornos híbridos y multicloud

Puede haber datos críticos en muchas ubicaciones diferentes de una empresa, ya sea en las instalaciones, en diferentes centros de datos o globalmente en diferentes clouds y regiones. Independientemente de su ubicación, los datos deben mantenerse seguros y no verse incluidos cuando se necesita recuperación tras un ciberataque.

PowerProtect Cyber Recovery está disponible y se puede adquirir a través de los mercados de cloud pública para *AWS, Microsoft Azure* y *Google Cloud* con el fin de proporcionar un acceso rápido para proteger los datos de un vault de Cyber Recovery en la cloud. PowerProtect Cyber Recovery automatiza la sincronización de datos críticos entre los sistemas de producción y el vault de Cyber Recovery en la cloud pública. A diferencia de las soluciones estándar de copia de seguridad basadas en la cloud, el acceso a las interfaces de gestión está bloqueado por controles de red y requieren credenciales de seguridad independientes y una autenticación multifactor para acceder. La dispersión y duplicación de datos en varias clouds puede generar riesgos de seguridad y de cumplimiento de normas de seguridad, posibles problemas de sincronización y un aumento del coste de los recursos. Este planteamiento también puede reducir la visibilidad en sus distintos entornos, lo que da lugar a una protección insuficiente frente a las ciberamenazas en constante evolución.

Dell PowerProtect Data Domain Ready Node todo flash

Los datos críticos siguen en aumento, por lo que la capacidad de recuperarse de un ciberataque de forma rápida y eficiente es de vital importancia para garantizar la continuidad empresarial y la ciberresiliencia. Las organizaciones que están ampliando la gestión de datos críticos deben destacar a la hora de recuperar sus datos desde entornos de recuperación aislados, como el vault de Cyber Recovery. Dell PowerProtect Data Domain Ready Node todo flash ofrece una solución de Ciber Recovery optimizada, rentable y de bajo consumo que incluye análisis mejorados de CyberSense y capacidades de restauración rápida para cumplir con los SLA de la organización. Al utilizar menos hardware, espacio y energía, las organizaciones pueden mejorar la velocidad de acceso a los datos, aumentar la eficiencia operativa y garantizar la integridad de los datos, lo que en última instancia conlleva una reducción del tiempo de inactividad y de los costes generales de mantenimiento.

PowerProtect Cyber Recovery - Vuelta a la actividad empresarial

Recuperación y corrección

PowerProtect Cyber Recovery ofrece procedimientos automatizados de restauración y recuperación para volver a poner en marcha los sistemas críticos de la empresa de forma rápida y fiable. La recuperación está integrada en el proceso de respuesta ante incidentes. Cuando se produce un evento, el equipo de respuesta ante incidentes analiza el entorno de producción para determinar la causa principal del evento. CyberSense ofrece informes forenses después del ataque para conocer su alcance, así como una lista de los últimos conjuntos de copias de seguridad correctas previas a la corrupción de datos. Una vez que la producción está lista para reanudarse, Cyber Recovery lleva cabo la recuperación de datos mediante herramientas de gestión y una tecnología diseñada con este propósito.

Diseño y planificación de soluciones

Dell Professional Services para Cyber Recovery le ayudan a determinar qué sistemas críticos de su empresa hay que proteger, y pueden crear mapas de dependencia para las aplicaciones y servicios asociados, así como la infraestructura necesaria para recuperarlos. El servicio también genera requisitos de recuperación y alternativas de diseño, e identifica las tecnologías para analizar, alojar y proteger sus datos, junto con un caso de negocios y un cronograma de implementación.

Conclusión

Iniciativas del sector, como Sheltered Harbor, han utilizado PowerProtect Cyber Recovery para proteger a clientes, instituciones financieras y la confianza pública en el sistema financiero de EE. UU. en caso de que un ciberataque cause el fallo de sistemas críticos, incluidas las copias de seguridad. Con miles de clientes, Cyber Recovery con CyberSense da confianza a los líderes empresariales y ha demostrado acelerar la recuperación de datos en caso de ciberamenaza.

PowerProtect Cyber Recovery le da la confianza de que podrá identificar y restaurar rápidamente los datos fiables conocidos y reanudar las operaciones comerciales normales después de un ciberataque.

Es hora de volver a la actividad empresarial.

Más información sobre Dell PowerProtect Cyber Recovery

Póngase en contacto con un experto de Dell Technologies

Ver más recursos

Únase a la conversación con #PowerProtect

[1] Datos basados en la investigación "Global Data Protection Index 2024 Snapshot", realizada por Vanson Bourne y encargada por Dell Technologies. Octubre de 2023.
[2] Investigación "The Total Economic Impact of Dell PowerProtect Cyber Recovery", realizada por Forrester Consulting y encargada por Dell Technologies. Agosto de 2023.
[3] Datos basados en el informe "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption" de ESG y encargado por Index Engines. Junio de 2024.