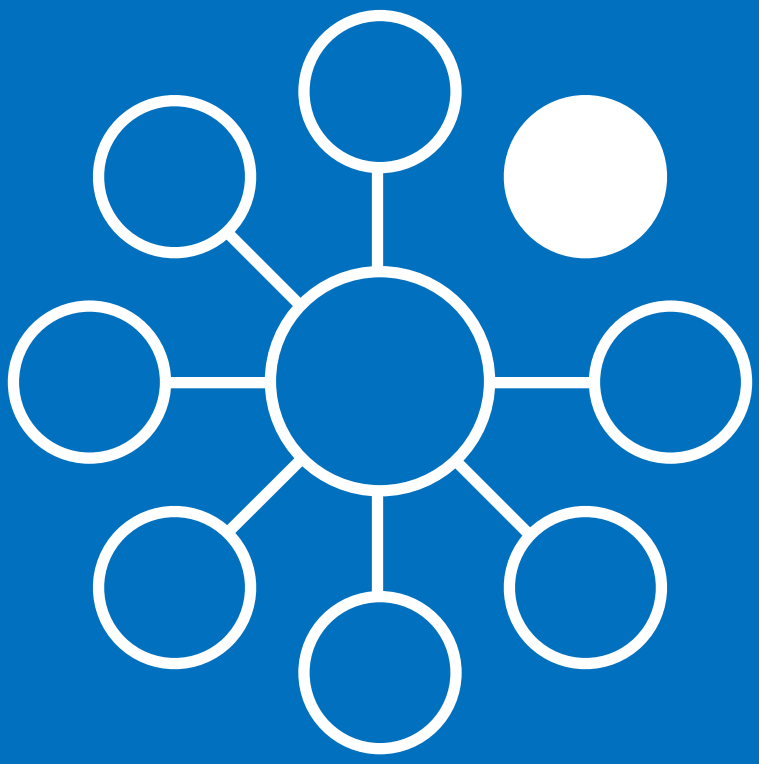

Principales razones para Confiar en Dell Power Protect Cyber Recovery

Proteja y recupere datos críticos con confianza

Powered by:

DELL Technologies

ARROW

1 | Aislamiento físico y lógico de datos críticos

PowerProtect Cyber Recovery protege los datos críticos a través de un entorno de bóveda con espacio de aire. El almacén de PowerProtect Cyber Recovery ofrece múltiples capas de protección para brindar resiliencia contra los ataques cibernéticos, incluso de una amenaza interna. Los datos críticos están lejos de la superficie de ataque, aislándolos físicamente dentro de una parte protegida de un centro de datos o en la nube. Requiere credenciales de seguridad separadas y autenticación multifactor para un acceso diferente a otros controles de acceso administrativo, como la recuperación ante desastres o la administración de copias de seguridad de datos. Las medidas de seguridad incluyen un espacio de aire operativo automatizado para proporcionar aislamiento de red y eliminar las interfaces de administración que podrían verse comprometidas.

2 | Inmutabilidad para preservar la integridad original de sus datos

PowerProtect Cyber Recovery ofrece varias capas de seguridad y controles que protegen contra la destrucción, la eliminación y la alteración de los datos almacenados. Con la función de bloqueo de retención del modo de cumplimiento de PowerProtect DD, se evita que los datos se eliminen o cambien durante un período de tiempo establecido, generalmente de dos semanas a un mes (configurable por el cliente). El bloqueo no puede ser anulado, ni siquiera por un administrador con todos los privilegios. Las mejoras exclusivas de PowerProtect DD protegen aún más el bloqueo de un ataque al reloj (o al servidor NTP), que de lo contrario podría permitir que un mal actor cree un vencimiento anticipado del bloqueo. Quienes no deseen o requieran un control tan fuerte, o deseen flexibilidad operativa, pueden configurar el bloqueo de retención de gobierno (que también es el modo disponible en nuestro PowerProtect DD Virtual Edition (DDVE)).

3 | Aprendizaje automático con CyberSense para una capa inteligente de protección

CyberSense permite la recuperación segura de buenos datos y ofrece información sobre los vectores de ataque dentro de la bóveda protegida. Ejecutar análisis de los datos en la bóveda es un componente vital para permitir una recuperación rápida después de un ataque. Los análisis ayudan a determinar si un conjunto de datos es válido y utilizable para la recuperación; o si de alguna manera se ha alterado o corrompido incorrectamente de modo que es "sospechoso" y potencialmente inutilizable. Los análisis de CyberSense son poderosos porque pueden leer y evaluar el formato de la copia de seguridad, por lo que no es necesario restaurar los datos. Se evalúa todo el contenido de los archivos de datos críticos, no solo sus metadatos, para ofrecer un análisis superior sin exposición en la bóveda a riesgos potenciales.

4 | Opciones de recuperación flexibles

Dell Technologies ofrece opciones de recuperación flexibles para cumplir con sus requisitos de resiliencia cibernética. Los procedimientos de recuperación en su mayoría siguen procesos estándar, pero se aplican consideraciones especiales en varios escenarios. La recuperación está integrada con su proceso de respuesta a incidentes. Después de que ocurre un evento, el equipo de respuesta a incidentes analiza el entorno de producción para determinar la causa raíz del evento. CyberSense también proporciona informes forenses posteriores al ataque para comprender la profundidad y amplitud del ataque y proporciona una lista de

los últimos conjuntos de copias de seguridad buenos antes de la corrupción. Luego, cuando la producción está lista para la recuperación, Cyber Recovery proporciona herramientas de administración y la tecnología que realiza la recuperación de datos real. Automatiza la creación de los puntos de restauración que se utilizan para la recuperación o el análisis de seguridad.

5 | Estrategia de confianza con los servicios de resiliencia de Dell

Los servicios de Dell Technologies crearán estrategias, implementarán, adoptarán y escalarán un programa de recuperación cibernética para respaldar a la organización. Ya sea que alinee la protección y la recuperación con las necesidades comerciales, implemente tecnologías de recuperación cibernética, responda a un incidente cibernético o se asegure de que sus equipos estén capacitados en las últimas habilidades de nuestros expertos, están aquí para ayudarlo en cada paso del camino. La última encuesta del Índice de protección de datos global mostró que al 62 % le preocupa que las medidas de protección de datos existentes en su organización no sean suficientes para hacer frente a las amenazas de malware y ransomware1. Con Dell Technologies, las organizaciones pueden proteger su negocio del ransomware, los ataques internos y otras amenazas cibernéticas con confianza.

Descubra más en:
www.moderndatacenter.es

1Índice mundial de protección de datos 2021.