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 destruir, robar o de otra manera comprometer sus datos valiosos, incluidos sus respaldos. Es clave proteger sus datos cruciales y recuperarlos con integridad garantizada para poder reanudar las operaciones comerciales normales después del ataque. ¿Su empresa podría sobrevivir? Estos son los componentes de una solución con resiliencia cibernética:

Aislamiento y gobernanza de datos Un entorno de centro de datos aislado que se desconecta de las redes corporativas y de respaldo y está restringido de los usuarios que no cuentan con una autorización adecuada.

Copia de datos automatizada y brecha de aire Cree copias de datos sin cambios en un vault digital seguro y procesos que crean una brecha de aire operativa entre el entorno de respaldo o producción y el vault.

Herramientas y análisis inteligentes Aprendizaje automático e indexación de contenido completo con análisis potentes dentro de la seguridad del vault. Comprobaciones de integridad automatizadas para determinar si los datos se han visto afectados por el malware y herramientas para respaldar la corrección si es necesario.

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

Planificación y diseño de la solución Orientación de expertos para seleccionar conjuntos de datos cruciales, aplicaciones y otros activos vitales a 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 de Internet y un activo crítico que debe protegerse, mantenerse confidencial y ponerse a disposición en un instante. El mercado global actual se basa en el flujo constante de datos a través de redes interconectadas y los esfuerzos de la transformación digital ponen en riesgo más 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. En Global Data Protection Index se 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].

Entonces, ¿qué puede hacer para proteger su empresa, sus clientes, sus empleados y sus datos valiosos?

La solución: Dell PowerProtect Cyber Recovery

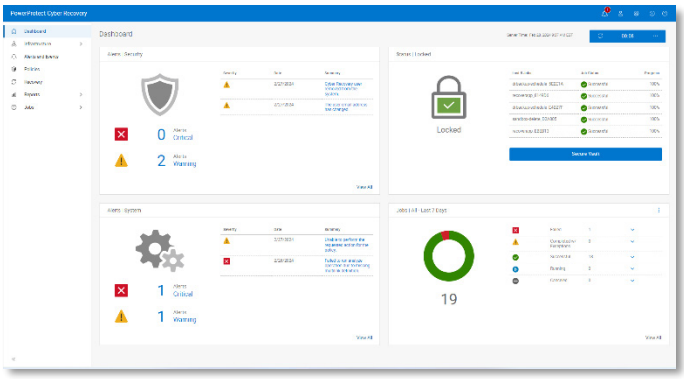
Para reducir el riesgo al negocio que causan los ataques cibernéticos y crear un enfoque con mayor resiliencia cibernética a fin de proteger los datos, puede modernizar y automatizar sus estrategias de recuperación y continuidad comercial y aprovechar las últimas herramientas inteligentes para detectar y defenderse ante las amenazas cibernéticas.

Dell PowerProtect Cyber Recovery ofrece una protección probada, moderna, resiliente e inteligente para aislar los datos cruciales, identificar las actividades sospechosas y acelerar la recuperación de datos, lo que le permite reanudar rápidamente las operaciones normales de la empresa.

PowerProtect Cyber Recovery: inmutabilidad, aislamiento e inteligencia

Vault de Cyber Recovery

El vault de PowerProtect Cyber Recovery ofrece varias capas de protección que brindan resiliencia frente a los ataques cibernéticos, incluso frente a una amenaza interna. Mueve los datos cruciales lejos de la superficie del ataque, los aísla físicamente dentro de una parte protegida del centro de datos y, para poder acceder, se necesitan credenciales de seguridad separadas y una autenticación de múltiples factores. Las protecciones adicionales incluyen una brecha de aire operativa automatizada para proporcionar aislamiento de la red y eliminar las interfaces de administración que podrían verse comprometidas. PowerProtect Cyber Recovery automatiza la sincronización de datos entre los sistemas de producción que incluyen sistemas abiertos y mainframes y el vault, lo que crea copias inmutables con políticas de retención con bloqueo. Si se produce un ataque cibernético, podrá identificar rápidamente una copia limpia de los datos, recuperar sus sistemas cruciales y volver a poner en funcionamiento su empresa.



CyberSense

PowerProtect Cyber Recovery es la primera solución que integra completamente CyberSense, lo que agrega una capa inteligente de protección que facilita la búsqueda de corrupción de datos cuando un ataque penetra en el centro de datos. Este enfoque innovador proporciona una indexación de contenido completo y utiliza el aprendizaje automático (ML) basado en IA para analizar más de 200 estadísticas basadas en contenido y detectar indicios de daño debido al ransomware. CyberSense detecta la corrupción con hasta un 99,5 % de confianza, lo que ayuda a identificar las amenazas, diagnosticar los vectores de ataque y, al mismo tiempo, proteger el contenido crucial de la empresa, todo dentro de la seguridad del vault.

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 también proporciona informes forenses posteriores al ataque para comprender la profundidad y la amplitud del ataque y proporciona una lista de los últimos conjuntos de respaldo en buen estado antes de que se produzcan 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. La herramienta automatiza la creación de los puntos de restauración que se utilizan para la recuperación o el análisis de seguridad.

Planificación y diseño de la solución

Los servicios de asesoría de Dell opcionales lo ayudarán a determinar qué sistemas cruciales para la empresa hay que proteger y pueden crear mapas de dependencias para las aplicaciones y los servicios asociados, así como también 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.

La protección de los datos vitales contra los ataques cibernéticos requiere soluciones probadas, modernas y resilientes. 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.

[1] Información basada en un estudio de Vanson Bourne encargado por Dell Technologies, “Global Data Protection Index 2023 Snapshot”, realizado entre agosto y octubre de 2023.

Obtenga más información sobre Dell PowerProtect Cyber Recovery	Comuníquese con un experto de Dell Technologies	Ver más recursos	Únase a la conversación con #PowerProtect