Construcción de resiliencia empresarial para proteger contra un ataque cibernético destructivo

Cyber Recovery con Dell Technologies

DELL Technologies

Tabla de contenido

3 ¿Qué es Cyber Recovery? ¿Por qué es importante?	4 Los datos son su negocio... y las amenazas cibernéticas ponen en riesgo su empresa	5 Las 10 razones principales para elegir Dell EMC PowerProtect Cyber Recovery	6 La recuperación ante desastres y la continuidad comercial no son suficientes para abordar las amenazas cibernéticas modernas.
7 Protección contra Ransomware y Ataques destructivos	8 Ventajas de PowerProtect ¿Cyber Recovery?	9 Ventajas de PowerProtect Cyber Recovery es el mejor	10 CyberSense para Detectar, diagnosticar y Recuperación rápida de Ataques cibernéticos
11 8 formas de CyberSense Combates poderosos Ransomware y Otros ataques cibernéticos	12 CyberSense permite Detección temprana y Recuperación garantizada	13 Dell EMC PowerProtect Cyber Recovery en Acción	14 Probada, con experiencia Cyber Recovery Servicios de consultoría
15 Protección del cliente Datos y preservación Confianza pública en EE. UU. Mercados financieros	17 Caso de estudio: Industria de la salud	18 Caso de estudio: Servicios financieros	19 ¡Comenzar ahora!Su Lista de comprobación para crear Resiliencia cibernética

¿Qué es Cyber Recovery? ¿Por qué es importante?

Independientemente del sector, los datos impulsan la empresa actual. El mercado global se basa en el flujo constante de datos a través de redes interconectadas, y los esfuerzos de transformación digital ponen en riesgo aún más datos.

El aumento en el volumen y el valor de los datos presenta una oportunidad para los delincuentes que utilizan herramientas y tácticas modernas; de hecho, el 68 % de los líderes empresariales afirma que sus riesgos de seguridad cibernética van en aumento (Accenture). La amenaza moderna de los ataques cibernéticos y la importancia de mantener la confidencialidad, la disponibilidad y la integridad de los datos requieren soluciones y estrategias modernas y comprobadas para proteger los datos y los sistemas vitales.

Lamentablemente, en el entorno actual basado en datos, la recuperación ante desastres (DR) tradicional y la continuidad comercial no son suficientes para abordar las amenazas cibernéticas modernas. El 69 % de los encuestados con confía en poder recuperar todos los datos cruciales para la empresa en caso de un ataque cibernético.[1] A pesar de que los ataques cibernéticos adoptan muchas formas y los atacantes tienen una variedad de motivaciones, el objetivo de sus esfuerzos es una constante: destruir, robar y exigir rescate de datos digitales valiosos para obtener ganancias financieras y con motivos sociales o políticos.

Cyber Recovery, que a veces se denomina recuperación aislada, es un nuevo segmento de soluciones de protección de datos diseñadas para abordar la amenaza moderna de ransomware y otras amenazas cibernéticas para limitar la propagación del malware y reducir la superficie de ataque de manera global.

La estabilidad de los ingresos y la propia existencia de una empresa depende de su capacidad de aislar los datos y de garantizar su disponibilidad para respaldar una estrategia de continuidad del negocio y operaciones de recuperación después de un ataque cibernético.

71 %

de las violaciones tienen motivaciones económicas

USD 5,2 B

de riesgo global en los próximos 5 años

Se produce un ataque cibernético cada

39 s

1. Índice de protección de datos globales de Dell Technologies

Los datos son su negocio...
y las amenazas cibernéticas ponen en riesgo su empresa

Riesgos técnicos

- Todos los datos son susceptibles a un ataque cibernético.
- La replicación de almacenamiento principal puede replicar datos corruptos.
- El catálogo de respaldo no se replica.
- La recuperación desde la cinta es lenta y propensa a fallas
- Las copias de respaldo no se aíslan de la red.

Las personas y los riesgos de procesos

- La TI y las operaciones acceden a la mayoría de los recursos de respaldo, si no a todos
- Los equipos de seguridad no están asignados a los recursos.
- Los agentes malintencionados dentro del firewall pueden eliminar los respaldos principales.
- Los datos cruciales y no cruciales del negocio no están segregados.
- Las imágenes de respaldo pueden "caducar" sin aprobación.

atención médica

minorista

petróleo y gas

petróleo y gas

servicios financieros

gobierno corporativo

fabricación

bufetes de abogados / corp. legal

10 principales razones para elegir Dell EMC PowerProtect Cyber Recovery

1. Vault digital reforzada y dedicada con una brecha de aire física y operativa
2. Protege contra ataques internos al solicitar varios inicios de sesión separados para acceder a la vault
3. Los datos escritos en la vault son inmutables e invariables.
4. El malware puede ingresar a la vault, pero NO tiene la capacidad de ejecutar ni infectar los datos fuera de la vault.
5. Primero en integrar la indexación de contenido completa, el análisis inteligente, el aprendizaje automático y las herramientas forenses
6. Identifique y restaure rápidamente el último archivo o conjunto de datos bueno conocido para una rápida recuperación
7. Automatización de flujo de trabajo de recuperación completa para reanudar rápidamente las operaciones empresariales
8. Primer proveedor de soluciones tecnológicas en el programa para partners de la alianza Sheltered Harbor
9. Primer proveedor de tecnología que desarrolla una solución de vaulting de datos lista para usar de Sheltered Harbor
10. Fuente única para el diseño de soluciones, la implementación y el soporte para soluciones de Cyber Recovery, CyberSense y Sheltered Harbor

La recuperación ante desastres y la continuidad comercial no son suficientes para abordar las amenazas cibernéticas modernas.

Los atacantes están atacando sistemas, datos y respaldos. Están cifrando el catálogo de respaldo, además de los sistemas y los datos. La recuperación ante desastres está en línea y no está aislada en el grado en que está una vault cibernética, y eso hace que la recuperación ante desastres sea vulnerable a estos ataques. Una solución de vault cibernética de brecha de aire garantiza que un la copia protegida de los datos críticos se mantiene en su formato original.

La verdadera resiliencia cibernética requiere Cyber Recovery.

La solución de PowerProtect Cyber Recovery incluye una vault digital segura que se aísla física y lógicamente de la red de productos y respaldos con una brecha de aire operativa. Los datos cruciales están protegidos dentro de la vault en un formato inmutable con períodos de retención bloqueados. Esto le brinda la mejor oportunidad posible para la recuperación si sus respaldos principales se han visto comprometidos o si su ubicación de recuperación ante desastres ha sido vulnerada o infectada. Sin una solución de Cyber Recovery, una empresa invierte un tiempo significativo en recuperar los últimos respaldos sin saber si son buenos o no. Este es un trabajo largo, intenso, iterativo y costoso.

Categoría	Recuperación ante desastres	Resiliencia cibernética
Tiempo de recuperación	Casi de manera instantánea	Confiable y rápido
Punto de recuperación	Idealmente continuo	Promedio de 1 día
Naturaleza de Desastre	Inundación, Interrupción de suministro eléctrico, Clima	Ataque cibernético, Objetivo
Impacto de los desastres	Regional; generalmente contenido	Global; se propaga rápidamente
Topología	Conectada, varios destinos	Aislado, además de DR
Volumen de datos	Completo, todos los datos	Selectivo, incluye servicios fundacionales
Recuperación	DR estándar (p. ej., conmutación por recuperación)	Recuperación iterativa y selectiva; parte de la CR

Protección contra ataques de ransomware y destructivos

Los reguladores globales en una variedad de sectores acuerdan cómo proteger mejor los datos cruciales y los recursos digitales de amenazas cibernéticas. Han determinado que la protección de una copia de datos cruciales de manera aislada es la manera más conocida de proporcionar recuperación de los ataques de ransomware y destructivos.

"Una arquitectura de respaldo de datos con brecha de aire..."

"Confidencialidad, integridad, disponibilidad y resiliencia"

"Considere mantener los respaldos sin conexión y no disponibles"

"Asegúrese de que los respaldos no estén conectados a las redes que están respaldando".

Ventajas de PowerProtect Cyber Recovery

La última línea de defensa de la protección de datos contra ataques cibernéticos

Dell EMC PowerProtect Cyber Recovery automatiza los flujos de trabajo de manera integral para proteger los datos cruciales, identificar la actividad sospechosa y realizar la recuperación de datos cuando sea necesario. La vault de Cyber Recovery está desconectada de la red a través de una brecha de aire automatizada y almacena todos los datos cruciales sin conexión a la red para aislarlos del ataque. Esto promueve la resiliencia empresarial, proporciona garantía después de la pérdida o destrucción extrema de datos e incluye datos de configuración empresariales y de tecnología para permitir una rápida recuperación del entorno y reanudación de las operaciones empresariales normales.

- Los datos cruciales se encuentran fuera de la red y se aíslan de ataques cibernéticos.
- La vault de Cyber Recovery está separada de la red por una brecha de aire para evitar el acceso
- Se actualizó a través del proceso de replicación según los límites de exposición a riesgos aceptables de los parámetros de conectividad de tiempo de actividad y pérdida de datos.
- Corregida contra amenazas mientras se está offline y capaz de conservar copias iterativas en las versiones –n actuales (según las necesidades del negocio)
- Permite una visibilidad completa de la integridad de todos los datos y metadatos protegidos.
- Para aumentar la eficacia en la prevención o detección de la seguridad cibernética cuando se ejecuta en un ambiente protegido
- El diagnóstico de los vectores de ataque puede generarse en un ambiente de vault aislado.
- El análisis monitorea la integridad de los datos que se respaldan y la integridad del catálogo de respaldo.

Por qué PowerProtect Cyber Recovery es el mejor

Solo PowerProtect Cyber Recovery combina múltiples capas de protección y seguridad en una solución lista para usar para proporcionar la máxima protección para datos cruciales.

bueno...	mejor...	óptimo...
		
Cumple con LockSEC 17a-4(f) integrado Inmutables de WORM Credenciales de seguridad elevadas	Protección contra ataques internos Compatibilidad heterogénea con proveedores de software de respaldo	Brecha de aire automatizada y en vault Indexación de contexto completa con análisis de IA/ML Herramientas de recuperación mejoradas

Resiliencia cibernética

CyberSense para detectar, diagnosticar y recuperarse rápidamente de ataques cibernéticos

CyberSense está totalmente integrado con Dell EMC PowerProtect Cyber Recovery, audita sus datos y detecta indicadores de compromiso y ataques:

- Comprenda de manera proactiva cuando se está produciendo un ataque con más del 99 % de precisión.
- Le permite identificar y diagnosticar posibles amenazas y recuperar rápidamente datos "buenos y conocidos"
- Reduzca el tiempo de inactividad y las interrupciones del negocio para poder reanudar las operaciones normales con confianza

Cuando un ataque supera las defensas en tiempo real y corrompe los archivos o las bases de datos, usted tiene la confianza de que los datos limpios están aislados en la vault de Cyber Recovery y han sido analizados por CyberSense. CyberSense supervisa constantemente la integridad de los datos dentro de la vault y detecta eliminaciones masivas, cifrado y más de 100 tipos de cambios en archivos y bases de datos que resultan de ataques comunes. Si CyberSense detecta señales de corrupción, se genera una alerta con el vector de ataque y la lista de archivos afectados. Esto permite que las operaciones empresariales continúen con una interrupción mínima o nula y con rapidez en lugar de tener que esperar semanas o meses.

Análisis

Aprendizaje automático

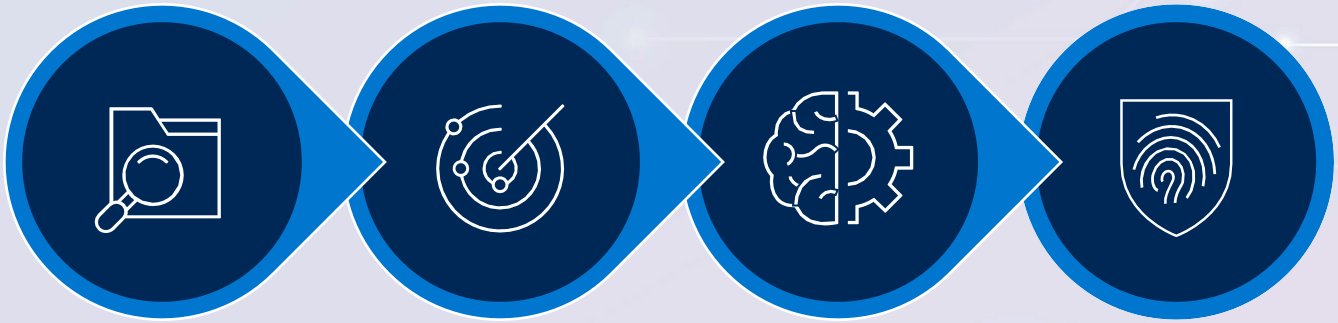
Herramientas forenses

8 formas en las que CyberSense combate poderosamente el ransomware y otros ataques cibernéticos

1. Detecte riesgos de ataques cibernéticos que los competidores no pueden identificar
2. Aprendizaje automático y análisis único y completo a nivel de contenido
3. Proporciona más de 100 heurísticas para identificar actividad sospechosa.
4. Integración profunda con Cyber Recovery para la automatización del flujo de trabajo y las alertas
5. Análisis forense posterior al ataque para determinar rápidamente el vector de ataque y la lista de datos afectados
6. Identifique el último conjunto de datos buenos y conocidos para la recuperación
7. Resiliencia incomparable para recuperar y restaurar datos rápidamente después de un ataque
8. Todo se realiza dentro de la seguridad de la vault de Cyber Recovery.

CyberSense permite una detección temprana y una recuperación garantizada

CyberSense realiza una indexación de contenido completa de todos los datos que ingresan a la vault y genera estadísticas que se comparan con los escaneos anteriores. Luego, los análisis se ingresan al modelo de aprendizaje automático y los resultados se utilizan para determinar la integridad de los datos y si fueron dañados. Asimismo, CyberSense proporciona informes y detalles para ayudar en el diagnóstico y la recuperación del ataque, y proporciona el vector de ataque utilizado para manipular los datos.



índice integral

Cambios en el contenido a través del tiempo

análisis de seguridad

Más de 100 estadísticas que indican ataque cibernético

aprendizaje automático

Capacitado para miles de troyanos y más de 20 vectores de ataque

Cyber Recovery con CyberSense

- Indexación de contenido completa
- Notificación del vector de ataque
- Identificación de archivos dañados
- Cambios/eliminaciones de datos
- Cuentas de usuario vulneradas
- Ejecutables vulnerados
- Identificación de la última copia buena

Dell EMC PowerProtect Cyber Recovery en acción

"Los ataques cibernéticos cambian a cada minuto, en todos los rincones del mundo. Para tener éxito en este entorno, tuvimos que cambiar la forma en que pensamos acerca de los datos, cómo los usamos y cómo los protegemos. Queremos mantenerlos limpios al ingresar y asegurarnos de que estén respaldados. Luego, debemos probar esa protección y asegurarnos de que se encuentre en un búnker de datos, de modo que, sea cual fuere el plan de ataque proveniente del malware en el futuro, contemos con una protección del 100 % de esa copia dorada y podamos retirarla del área segura y protegida, y devolverla, para que la vida de las personas vuelva a la normalidad y no experimenten interrupciones".

Bob Bender
Director de tecnología,
Founders Federal Credit Union
más información

Caso de uso: Sheltered Harbor

La preservación de la confianza pública en caso de un evento devastador, como un ataque cibernético, hace que los sistemas críticos de una institución fallen.

Caso de estudio: Atención médica

Protección de la información confidencial y las operaciones empresariales críticas

Caso de estudio: Servicios financieros

Protección de la plataforma de comercio de valores y los datos cruciales

Servicios probados y con experiencia de consultoría de Cyber Recovery

Con un equipo de consultores que aportan una profunda experiencia en el diseño y la implementación de soluciones de Cyber Recovery, como también, décadas de conocimientos empresariales y de recuperación ante desastres, Dell puede ayudar a su empresa a poner en funcionamiento una vault de Cyber Recovery. Esto puede incluir la identificación de requisitos de vault, conjuntos de datos, aplicaciones, secuenciación de cargas de trabajo y más para la vault.

Entrega de la base de Cyber Recovery

Instale e inicie rápidamente el funcionamiento de la vault de Cyber Recovery

Implementación avanzada de Cyber Recovery

Proporciona una capacidad limitada para ofrecer algunas opciones personalizadas, generar un Runbook de muestra y trabajar con algún software de otros fabricantes

Asesorías de Cyber Recovery

Los servicios de Asesorías de Cyber Recovery ofrecen diferentes niveles de opciones estratégicas y arquitecturas de destino, e incluso, un plan de trabajo procesable para la adopción de Cyber Recovery.

Cyber Recovery personalizado

Los servicios de Cyber Recovery personalizados implementan opciones avanzadas, planes de recuperación personalizados, Runbooks adicionales y más.

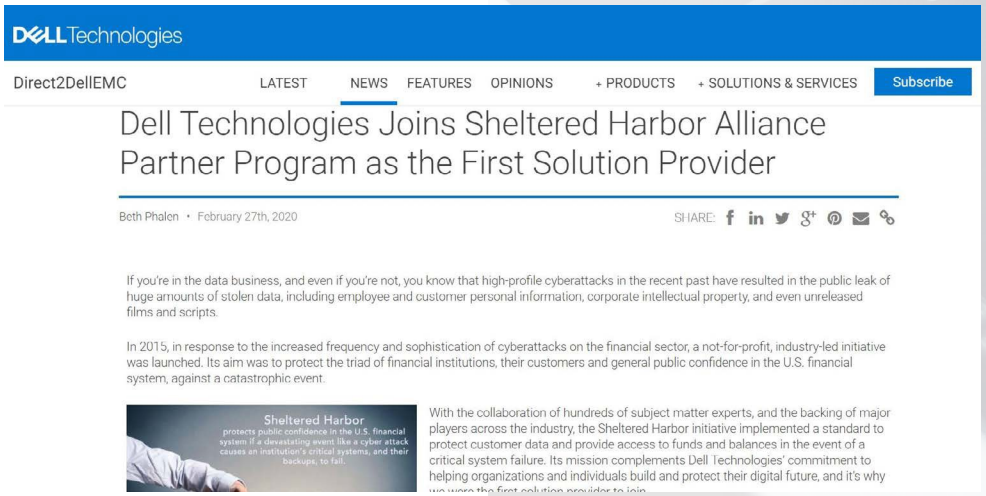
Protección de datos del cliente y preservación Confianza pública en EE. UU. Mercados financieros

A la vanguardia de la preparación en relación con Sheltered Harbor

Sheltered Harbor se creó para proteger a clientes, instituciones financieras y la confianza pública en el sistema financiero si un evento catastrófico, como un ataque cibernético, hace que los sistemas críticos (incluidos los respaldos) fallen. Al implementar el estándar Sheltered Harbor, las instituciones pueden estar preparadas para ofrecer a los clientes un acceso oportuno a saldos y fondos en estos escenarios más desfavorables.

Dell Technologies es el primer proveedor de soluciones en el Programa para partners de la alianza Sheltered Harbor y anticipa el respaldo de su solución en junio de 2020.

Más información


DELL Technologies

Direct2DellEMC LATEST NEWS FEATURES OPINIONS + PRODUCTS + SOLUTIONS & SERVICES Subscribe

Dell Technologies Joins Sheltered Harbor Alliance Partner Program as the First Solution Provider

Beth Phalen • February 27th, 2020 SHARE:

If you're in the data business, and even if you're not, you know that high-profile cyberattacks in the recent past have resulted in the public leak of huge amounts of stolen data, including employee and customer personal information, corporate intellectual property, and even unreleased films and scripts.

In 2015, in response to the increased frequency and sophistication of cyberattacks on the financial sector, a not-for-profit, industry-led initiative was launched. Its aim was to protect the triad of financial institutions, their customers and general public confidence in the U.S. financial system, against a catastrophic event.

Sheltered Harbor protects public confidence in the U.S. financial system if a devastating event like a cyber attack causes an institution's critical systems, and their backups, to fail.

With the collaboration of hundreds of subject matter experts, and the backing of major players across the industry, the Sheltered Harbor initiative implemented a standard to protect customer data and provide access to funds and balances in the event of a critical system failure. Its mission complements Dell Technologies' commitment to helping organizations and individuals build and protect their digital future, and it's why

SHELTERED HARBOR

Elementos principales de Sheltered Harbo

Vaulting de datos

Planificación de resiliencia

Certificación

PowerProtect Cyber Recovery aborda los requisitos de resiliencia de Sheltered Harbor.

SHELTERED HARBOR DATEN-VAULT	PowerProtect Cyber Recovery para Sheltered Harbor
Invariable	Los datos en Vault cuentan con retención bloqueada.
Separado	(evaluado para cumplir con la 17a-4(f)(2))
Capacidad para perdurar	Aislamiento físico y de red: brecha de aire a través de la activación/desactivación del puerto de replicación. Totalmente automatizado y autónomo
Accesible	Diseñado para soportar un ataque cibernético enfocado: APT, Ataque interno, Ransomware
Descentralizado	La metodología de transferencia es accesible para el propietario y flexible
Propiedad del participante	Ubicación física flexible: una por participante, consolidada, etc.

Industria de la salud

Proteja información confidencial y operaciones empresariales críticas

Retos

- El ataque a instituciones de servicios de salud y el impacto de los grandes ataques
- Restricciones en el presupuesto
- Presiones reglamentarias

PowerProtect Cyber Recovery

- Rápida implementación de una brecha de aire operativa lista para usar y vault
- CyberSense para análisis/alertas de amenazas cibernéticas activas

Resultados

- "Nadie cuenta con una brecha de aire como la de Dell Technologies".
- Preparado para una respuesta con inversión mínima en comparación con el riesgo de incidente catastrófico por el valor de USD 10 millones

Servicios financieros

Proteja la plataforma de comercio de valores y los datos cruciales

Retos

- Riesgos de interrupción de USD 10 millones por día
- La dirección está preocupada por el cumplimiento con FFIEC y las normativas de la Reserva Federal

PowerProtect Cyber Recovery

- Proceso automatizado y orquestado para minimizar los impactos operativos
- Runbooks de recuperación para todos los entornos de almacenamiento y respaldo

Resultados

- Cumplimiento del pedido de la dirección para una recuperación eficiente y confiable ante la destrucción cibernética
- Se proporcionó un entorno fundacional para proteger las aplicaciones adicionales con el tiempo.

¡Comenzar ahora! Su lista de comprobación para crear resiliencia cibernética

Dé un paso adelante

Autenticación, identidad y seguridad

- Active Directory/ LDAP
- Volcados de DNS
- Certificados
- Registros de eventos (incluidos los datos de SIEM)

Redes

- Configuración de switch/enrutador
- Configuración de firewall/balanceador de carga
- Diseño de servicios IP
- Configuración de control de acceso
- Firmware/microcódigo/parches

Almacenamiento

- Configuración del hardware de respaldo.
- Configuraciones de SAN/arreglo
- Configuración de abstracción de almacenamiento
- Firmware/microcódigo/parches

Documentación

- CMDB, D/R de recursos, Runbooks de Cyber Recovery y listas de comprobación
- Extractos de administración
- Listas de recursos y contactos de RH

Host y herramientas de creación

- Compilaciones de plataforma física/virtual
- Herramientas de operaciones de desarrollo y scripts de automatización
- Firmware/microcódigo/parches
  - > Binarios (imágenes doradas)
  - > Configuraciones y ajustes

Propiedad intelectual

- Código fuente
- Algoritmos exclusivos
- Bibliotecas de desarrolladores

La protección de su empresa comienza con la protección de sus datos.

Obtenga más información en www.DellTechnologies.com/CyberRecovery