DELL Technologies

Resumen de la solución

PowerProtect Cyber Recovery para Sheltered Harbor

Protegemos los datos cruciales de los clientes y resguardamos la confianza de los consumidores en los mercados financieros de EE. UU.

¿QUÉ ES SHELTERED HARBOR?

El estándar Sheltered Harbor, creado en 2015 por la industria financiera, incorpora un conjunto de elementos de seguridad y prácticas recomendadas para la resiliencia cibernética y la protección de datos con el objetivo de proteger la información financiera de EE. UU. Las amenazas cibernéticas, que incluyen ransomware, destrucción de datos o robo dirigido a los sistemas de producción y respaldo, ponen en riesgo la información financiera de los consumidores y las empresas.

Un ataque cibernético exitoso a un banco, una cooperativa de crédito o una firma de corretaje de EE. UU. podría dañar la reputación de la institución financiera, socavar la confianza de los consumidores en el sistema financiero de EE. UU. y hasta quizás desencadenar una crisis financiera global.

Sheltered Harbor mejora la estabilidad financiera y la resiliencia cibernética de las instituciones de EE. UU. aislando inalterablemente los registros cruciales de las cuentas de los clientes y otros datos dentro de un vault digital. En caso de que los sistemas principales o de respaldo de una institución se vean comprometidos por un ataque cibernético como ransomware u otro evento, se habilita la recuperación rápida de estos datos cruciales, lo que facilita la continuidad de los servicios de banca primordiales orientados al cliente y garantiza la conservación de la confianza pública.

¿POR QUÉ ESCOGER CYBER RECOVERY?

Dell Technologies es el primer proveedor de soluciones en el programa para partners de la alianza Sheltered Harbor que ha desarrollado una solución de vaulting de datos lista para usar para instituciones financieras que está respaldada por Sheltered Harbor.

PowerProtect Cyber Recovery para Sheltered Harbor es la primera solución de vaulting de datos lista para usar en las instalaciones que cuenta con el respaldo de Sheltered Harbor. Cumple con todos los requisitos técnicos de productos para participantes que implementan el estándar Sheltered Harbor.

Vault de datos: la institución participante o el proveedor de servicio generan los respaldos nocturnos de los datos cruciales en el formato del estándar Sheltered Harbor. El vault de datos está cifrado, es inalterable y está aislado de la infraestructura de la institución, incluido el sistema de respaldo, recuperación ante desastres y otros sistemas de protección de datos.

Aislamiento y gestión: un entorno aislado y seguro desconectado de las redes corporativas restringe a los usuarios y exceptúa a aquellos que tienen la autorización correspondiente. La administración automatizada de copias de datos y brechas de aire garantiza la preservación de la integridad, disponibilidad, seguridad y confidencialidad.

Recuperación y corrección: si se activa un Plan de Resiliencia de Sheltered Harbor, la institución participante puede recuperar rápidamente los datos del vault para que las operaciones bancarias se restauren y reanuden a una velocidad extraordinaria.

El desafío: el ataque cibernético en la industria de los servicios financieros podría desencadenar una crisis financiera global

Todas las organizaciones están preocupadas por el impacto paralizante que podría tener un ataque cibernético malicioso en su negocio, incluso teniendo en cuenta que el 97 % de las organizaciones usarán información confidencial en sus esfuerzos de transformación digital.[1] Existe una enorme ventaja detrás del desbloqueo del valor de los datos.

También existe un riesgo significativo en caso de que la información confidencial caiga en manos equivocadas, se destruya o se divulgue públicamente. El malware y ransomware están evolucionando, y los ataques están en aumento: los ataques de ransomware empresariales aumentaron un 12 % en 2019, es decir, representaron el 81 % de todas las infecciones de ransomware de acuerdo con el Informe de Symantec de amenazas de seguridad en Internet (2019).[2] Además, el 52 % de todas las vulneraciones de datos en 2020 han sido maliciosas, frente al 30 % de hace apenas cinco años, según un informe reciente de Ponemon Institute.[3]

Además, las tácticas y herramientas de los actores de amenazas han evolucionado y hacen que las detecciones resulten casi imposibles y la prevención de ataques sea cada vez más difícil. Las tácticas de los delitos cibernéticos continúan evolucionando. El 30 % de los ataques cibernéticos denunciados involucran personas con información confidencial, frente al 25 % de hace apenas tres años, según el Informe de investigaciones de vulneraciones de datos de Verizon de 2020. [4]

La industria financiera ha sufrido las mayores pérdidas debido a los delitos cibernéticos en los últimos tres años, según el Informe sobre el costo anual de la delincuencia cibernética de Accenture (2019),[5] y estas fuerzas se combinan en una tormenta perfecta de amenazas que los mercados financieros globales deben enfrentar.

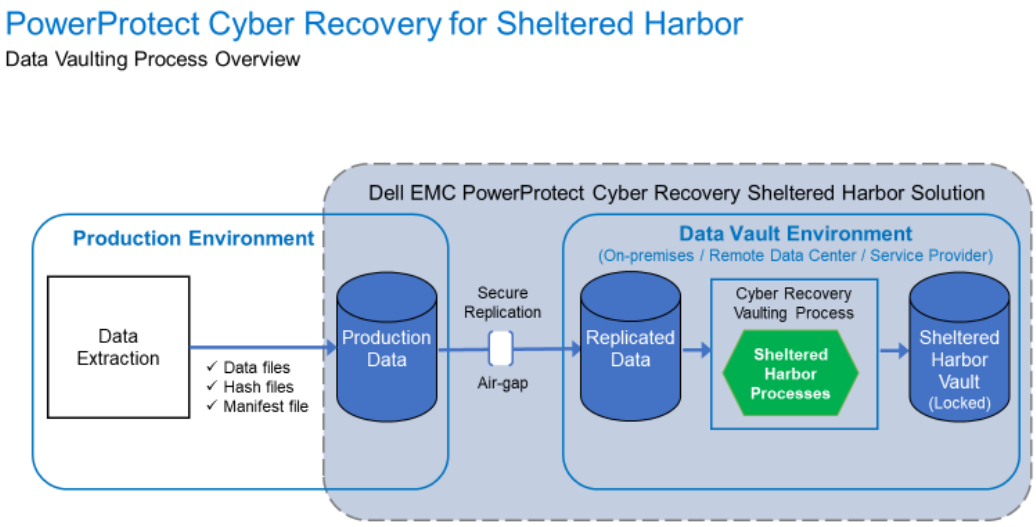
Sheltered Harbor, una iniciativa sin fines de lucro conformada por la propia industria en 2015, tiene como objetivo guiar a las instituciones financieras de EE. UU. en la reducción del riesgo de ataques cibernéticos que comprometan los datos de clientes e interrumpan los servicios bancarios normales. El ecosistema de Sheltered Harbor comprende las instituciones participantes (bancos, cooperativas de crédito, firmas de corretaje, administradores de recursos de EE. UU.), las asociaciones nacionales de comercio, los proveedores de soluciones y los proveedores de servicio dedicados a mejorar la estabilidad y resiliencia cibernética del sector financiero.

La tradicional recuperación ante desastres y la continuidad comercial son necesarias para ayudar a restaurar las capacidades operativas completas después de un evento causado por la naturaleza o por el hombre. Sheltered Harbor tiene como objetivo garantizar que, tras un ataque cibernético sofisticado y dirigido, los datos necesarios para restaurar las operaciones bancarias básicas estén disponibles de forma íntegra y fácil al tiempo que los procedimientos de recuperación completa continúan.

Dell EMC PowerProtect Cyber Recovery para Sheltered Harbor – Resiliencia cibernética robusta para la mayoría de los datos cruciales de las instituciones financieras

Dell Technologies es el primer proveedor de soluciones que se une al programa para partners de la alianza Sheltered Harbor. Nuestra solución respaldada por Sheltered Harbor se basa en Dell PowerProtect Cyber Recovery, una solución líder del mercado que hace casi cinco años protege los datos más cruciales de las organizaciones de los ataques cibernéticos, como ransomware.

Para cumplir con la especificación de Sheltered Harbor, la arquitectura del vault de Cyber Recovery se ha ampliado para que ejecute los procesos de generación de archivos y repositorio seguro. Los datos extraídos para Sheltered Harbor se guardan en producción, luego se replican de forma segura a través de una conexión lógica y exclusiva con brecha de aire al entorno protegido por el vault, donde se realizan los pasos restantes, como el bloqueo de retención.



Al crear un entorno aislado y dedicado, físicamente separado de las redes corporativas y los sistemas de respaldo, los conjuntos de datos cruciales, que los participantes de Sheltered Harbor deben proteger, están disponibles en formato estandarizado para que los servicios bancarios básicos se puedan reanudar rápidamente para los clientes. La implementación se mide en semanas, en lugar de meses, y con la certeza de cumplimiento de la especificación de Sheltered Harbor.

Resumen

Dell EMC PowerProtect Cyber Recovery para Sheltered Harbor proporciona a las instituciones participantes una alternativa completamente respaldada, rápida, rentable y eficiente para que cada institución construya un vault propio y exclusivo con el fin de cumplir con la especificación de Sheltered Harbor. Los bancos, las cooperativas de crédito y las firmas de corretaje que eligen implementar el estándar Sheltered Harbor pueden recurrir a Dell Technologies para obtener una solución de vaulting de datos completamente respaldada, totalmente compatible y lista para usar.

Con el beneficio adicional de aprovechar una tecnología basada en un vault maduro, los participantes de Sheltered Harbor que elijan PowerProtect Cyber Recovery para Sheltered Harbor pueden satisfacer con confianza sus necesidades de implementación inmediatas, así como establecer un punto de equilibrio para sus futuros requisitos de vaulting de datos. La institución participante cuenta con un medio para sobrevivir al tiempo que se preserva la confianza pública en el sistema financiero de EE. UU.

Fuentes:

1. Informe de amenazas de datos de Thales (2019) (www.thalessecurity.com/DTR)
2. Informe de Symantec de amenazas de seguridad en Internet (2019) (https://www.symantec.com/security-center/threat-report)
3. Informe sobre el costo de las vulneraciones de datos de Ponemon Institute, LLC (2020) (https://www.ibm.com/security/data-breach)
4. Informe de investigaciones de vulneraciones de datos de Verizon (2020) (https://enterprise.verizon.com/resources/reports/dbir/)
5. Informe sobre el costo de la delincuencia cibernética de Accenture (2019) (https://www.accenture.com/us-en/insights/security/cost-cybercrime-study)