IBM FlashSystem Cyber Vault

Características destacadas

- Detecte los ciberataques de forma temprana para minimizar los daños
- Acelere la recuperación tras un ataque
- Reduzca el tiempo de recuperación de días o semanas a tan solo horas
- Facilite el análisis forense de un ataque

Las consecuencias económicas y empresariales de los ciberataques son cada vez mayores. Los ciberataques se pueden producir de varias maneras: pueden tomar muchas formas diferentes y evolucionan continuamente. Tanto si el objetivo del atacante es robar datos confidenciales del cliente como retener información valiosa para pedir un rescate, las organizaciones deben contar con una estrategia general de ciberseguridad.

El almacenamiento juega un papel fundamental a la hora de ayudar a detectar ataques y también para recuperarse rápidamente.

IBM® Safeguarded Copy crea instantáneas de datos inmutables y aisladas para reforzar la protección contra ciberataques, malware, posibles acciones de empleados descontentos y otras formas de corrupción de datos. Y puesto que las instantáneas de Safeguarded Copy están en el mismo almacenamiento de FlashSystem que los datos operativos, la recuperación está diseñada para ser más rápida que la restauración de las copias almacenadas por separado.

IBM Safeguarded Copy se complementa con la solución IBM FlashSystem® Cyber Vault, que explora automáticamente las copias creadas periódicamente por Safeguarded Copy en busca de señales de corrupción de datos provocada por malware o ransomware. Esta exploración tiene dos finalidades. En primer lugar, ayuda a identificar rápidamente un ataque de ransomware clásico una vez que ha comenzado. En segundo lugar, está diseñada para identificar qué copias de datos no se han visto afectadas por un ataque. Al disponer de esta información, los clientes pueden detectar antes que se está produciendo un ataque e identificar y recuperar más rápidamente una copia limpia de sus datos.

Visión general

La ciberdelincuencia sigue siendo una de las principales preocupaciones para las empresas. Casi todos los días se notifican nuevos ataques. El coste medio es de 4,24 millones de dólares y la recuperación puede tardar días o semanas.Los ciberataques tienen un impacto inmediato sobre las empresas, pero también pueden tener un impacto perdurable sobre la reputación si el negocio tarda mucho en volver a estar disponible.[1]

Por desgracia, es muy probable que los ciberataques sigan consolidándose como una grave amenaza en 2022 y más adelante. La cuestión no es *si* ha sufrido un ataque, sino *cuándo.*

Cuando se produce un ciberataque, la respuesta de su organización marca la diferencia entre un daño económico y sobre la reputación permanente o una perturbación relativamente breve.

Las soluciones tradicionales de continuidad del negocio que la mayoría de las organizaciones desarrollan e implementan incluyen alta disponibilidad (HA) y recuperación tras desastre (DR) para proteger sus datos frente a amenazas convencionales (pero aun así relevantes) a los datos. Lamentablemente, estas soluciones no ofrecen protección contra la creciente gama de ciberataques.

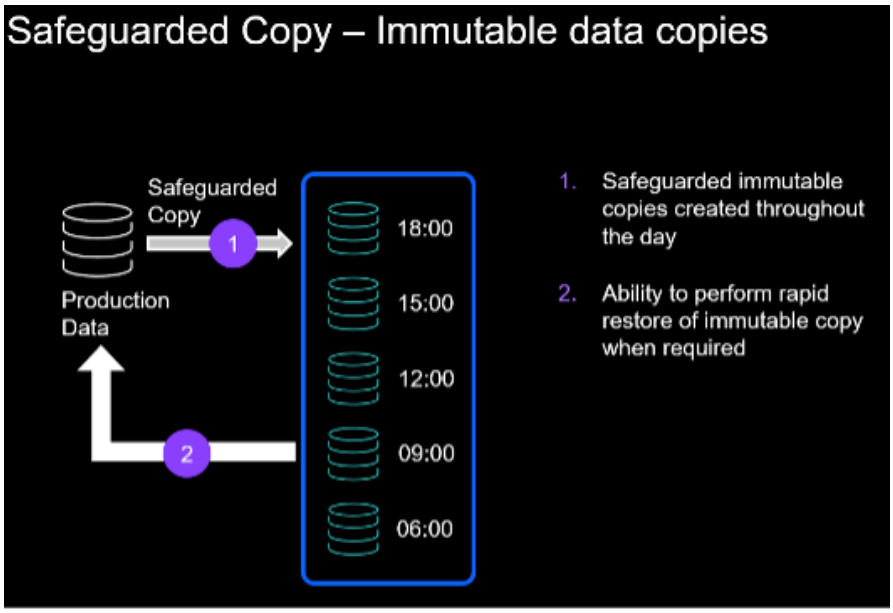
La única alternativa es invertir en tecnología actualizada y procesos automatizados que ayudan a protegerse contra un cibersuceso, además de acelerar la recuperación de las operaciones de negocio más importantes. Durante un cibersuceso, la recuperación rápida es la máxima prioridad para cualquier organización. Independientemente del tamaño de la empresa y del sector en el que opere, toda organización debe tener una estrategia de resiliencia de datos bien definida, que incluya ciberresiliencia, para poder recuperarse rápidamente tras una brecha de datos y ataques similares.

IBM Safeguarded Copy

IBM Safeguarded Copy crea periódicamente instantáneas de datos inmutables (no se pueden cambiar) y aisladas (separadas de los servidores) para protegerse contra ciberataques, malware, posibles acciones de empleados descontentos y otras formas de corrupción de datos. Y puesto que las instantáneas de Safeguarded Copy están en el mismo almacenamiento de

FlashSystem que los datos operativos, la recuperación está diseñada para ser más rápida que la restauración de las copias almacenadas por separado.

En este ejemplo, una política de Safeguarded Copy realiza automáticamente copias de instantáneas inmutables cada tres horas.



Funcionamiento de IBM Safeguarded Copy

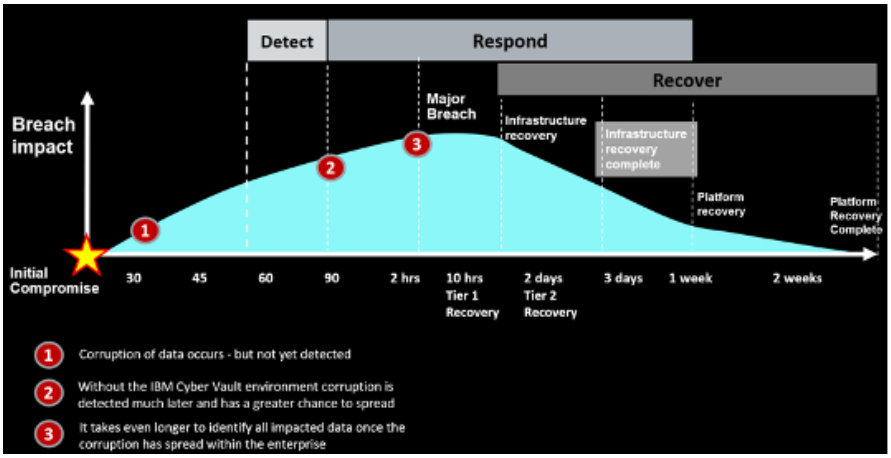
IBM FlashSystem Cyber Vault

La ciberresiliencia completa implica la detección de intrusiones y la supervisión para identificar cualquier comportamiento inusual en todos los niveles de la infraestructura, incluidas las personas, los programas y los sistemas interconectados, además de los proveedores externos y los recursos de cloud. Los informes a tiempo y los paneles de control son fundamentales para detectar los problemas y alertar a los equipos de actividades y comportamientos inusuales.

Todos los empleados, contratistas y demás personas que trabajan con herramientas o sistemas de TI deben renovar periódicamente su formación y competencias sobre cómo prevenir los puntos de ataque más comunes, tales como phishing, smishing, vishing o ingeniería social. También deben sentirse comprometidos y saber reconocer sucesos para notificar comportamientos inusuales, ya que esto requiere un esfuerzo de equipo.

En pocas palabras, si el primer signo de un ataque de ransomware se detecta después de que se haya producido el ataque, es demasiado tarde. La inversión, la utilización y la dedicación a las tecnologías, las herramientas, los procesos, la supervisión, la formación y la comunicación adecuados son fundamentales antes de que se produzca un incidente. Estos elementos son clave para alcanzar los niveles de ciberseguridad y resiliencia que requieren las empresas.

El siguiente diagrama muestra los promedios del sector del tiempo que tarda una organización en recuperar el funcionamiento del negocio. Verá que es muy frecuente tardar entre 2 y 3 semanas.



Duración media de una ciberrecuperación

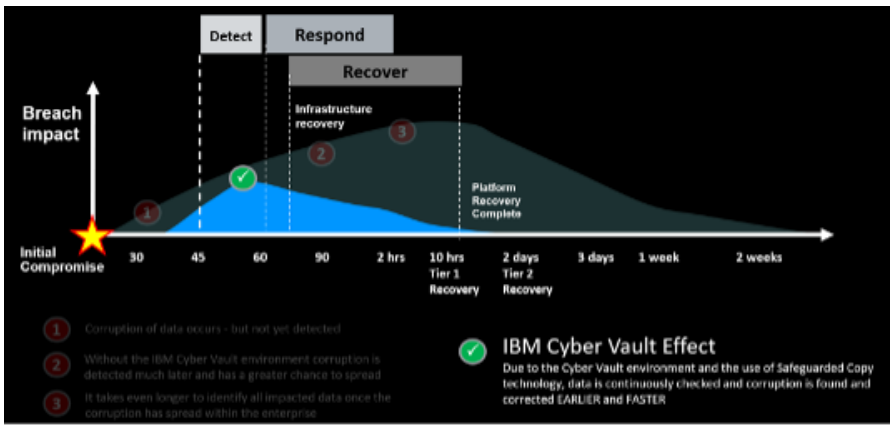
Aun así, según un estudio, el 41 por ciento de las empresas afectadas por un ataque de ransomware pudo recuperarse en un mes, más de la mitad (58 por ciento) reconoció que tardó más de un mes en recuperarse, el 29 por ciento afirmó que necesitó más de tres meses, y el *9 por ciento admitió que requirió más de cinco o incluso seis meses.*[2]

Una solución de almacenamiento de ciberresiliencia debe proporcionar prestaciones para protegerse frente a los desafíos únicos que presenta un ciberataque. Lo primero es la necesidad absoluta de aislamiento lógico o físico; copias inmutables de datos que un ciberatacante no pueda corromper ni borrar.

En segundo lugar, se necesitan herramientas para validar continuamente estos datos con el objetivo de detectar un ataque y generar confianza en la calidad y la validez de una copia de seguridad, para recuperarse una vez que se ha producido un ciberataque. Estas herramientas también ayudarán al personal de TI a realizar el análisis forense necesario para evaluar el incidente, a formular estrategias y opciones de recuperación óptimas y a determinar el alcance de la recuperación, los archivos, las bases de datos o sistemas completos.

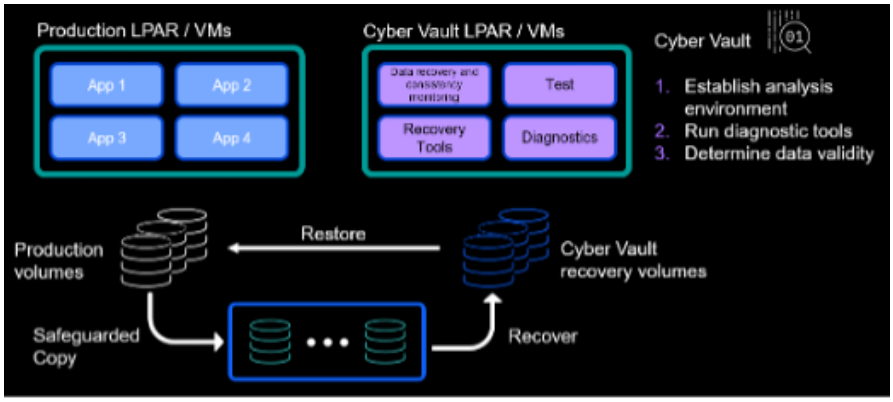
La solución IBM FlashSystem Cyber Vault consiste en un plan implementado por IBM Lab Services o Business Partners de IBM, diseñado para ayudar a acelerar la detección de ciberataques y su recuperación. La solución Cyber Vault se ejecuta de forma continua y supervisa las instantáneas a medida que Safeguarded Copy las crea. Mediante herramientas estándar de base de datos y software de automatización, FlashSystem Cyber Vault comprueba que las instantáneas de Safeguarded Copy no estén corruptas.

Si FlashSystem Cyber Vault detecta cambios, es una señal inmediata de que se puede producir un ataque.Al preparar una respuesta, saber cuáles son las últimas instantáneas que no presentan ningún indicio de ataque permite determinar más rápido qué instantánea utilizar. Y puesto que las instantáneas de Safeguarded Copy están en el mismo almacenamiento de FlashSystem que los datos operativos, la recuperación está diseñada para ser más rápida que la restauración de las copias almacenadas por separado. Con estas ventajas, FlashSystem Cyber Vault está diseñada para ayudar a reducir el tiempo de recuperación tras ciberataques de días a tan solo horas.



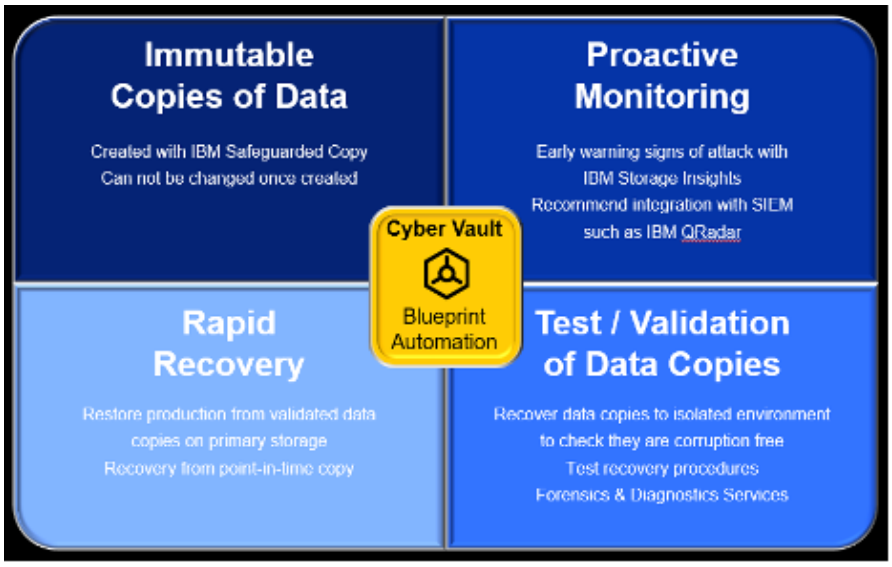
Efecto de IBM Cyber Vault

La solución IBM FlashSystem Cyber Vault proporciona un entorno seguro y aislado, en el que se mantiene una réplica del entorno de producción. El entorno de IBM FlashSystem Cyber Vault no afecta al entorno de producción, ya que aprovecha un entorno limpio/recinto de seguridad (particiones lógicas o máquinas virtuales) para ejecutar procesos de validación de datos sin afectar a las cargas de trabajo de producción. Este entorno de recinto de seguridad también es el lugar donde formar a sus equipos, realizar análisis forenses después de que se detecte una corrupción de datos y, basándose en el análisis, aplicar procedimientos de recuperación con la tranquilidad de que si algo va mal con cualquier paso de la recuperación, sus equipos siempre pueden volver a la copia de Safeguarded Copy original de un momento específico.



Entorno de IBM Cyber Vault

IBM FlashSystem Cyber Vault consta de los siguientes cuatro elementos clave:



Operaciones de IBM Cyber Vault

Veamos brevemente cada uno de estos elementos.

Copias de datos inmutables

IBM Safeguarded Copy es el mecanismo de protección más reciente para los datos de la familia IBM FlashSystem y de los sistemas de almacenamiento IBM SAN Volume Controller. De igual modo que en los sistemas IBM DS8000®, Safeguarded Copy ayuda a proteger los datos para evitar su corrupción accidental o deliberada. También facilita una rápida recuperación de copias protegidas de un momento específico cuando se produce un ciberataque.

Safeguarded Copy proporciona copias seguras de un momento específico o instantáneas de datos de producción activos que no se pueden modificar ni suprimir (conocidas como copias inmutables). Estas copias protegidas normalmente se crean en un entorno de almacenamiento separado de la producción y solo puede acceder a ellas el sistema de recuperación de IBM FlashSystem Cyber Vault.

Supervisión proactiva

Detectar una amenaza antes de que se inicie es fundamental para acelerar el tiempo de recuperación y la disponibilidad operativa.

IBM Security® QRadar® es una solución de gestión de sucesos e información de seguridad (SIEM) que puede supervisar, inspeccionar, detectar y extraer información para identificar posibles amenazas a los datos almacenados en IBM FlashSystem e IBM Spectrum® Virtualize. Proporciona potentes funciones de detección de amenazas y ciberresiliencia, como visibilidad centralizada, despliegue flexible, inteligencia automatizada, machine learning, búsqueda proactiva de amenazas y mucho más.

IBM QRadar puede detectar patrones maliciosos utilizando un buen número de orígenes de datos y herramientas y técnicas de análisis, incluidos registros de acceso; heurística; correlación con registros de otros sistemas, como registros de red o registros de servidor; flujo de red y datos de paquetes, e incluso detección de vectores de amenazas desconocidos gracias a los recursos de IBM Watson® for Security. IBM QRadar se integra con IBM Safeguarded Copy para realizar una instantánea protegida de los datos a la primera señal de un posible ataque.

IBM Security Guardium® Data Protection descubre y clasifica automáticamente los datos confidenciales de toda la empresa, y supervisa la actividad de los datos en tiempo real. Su protección se refuerza con Guardium Vulnerability Assessment, que detecta vulnerabilidades derivadas del comportamiento, como el uso compartido de cuentas, un número excesivo de errores de inicio de sesión o actividad poco habitual fuera del horario de oficina. También

identifica amenazas y brechas de seguridad en las bases de datos que los hackers podrían explotar. Y para ayudar a los directores de seguridad a comprender dónde residen las amenazas para el negocio, Guardium Data Risk Manager presenta un panel de control ejecutivo que permite visualizar los riesgos de negocio relacionados con los datos, de modo que tanto los ejecutivos como la dirección puedan tomar acciones inmediatas para proteger el negocio.

IBM Storage Insights e IBM Spectrum Control supervisan el almacenamiento flash de IBM. Ofrecen la capacidad de ver una comparativa de una carga de trabajo de E/S actual con una línea base anterior y proporcionan una indicación de un ataque en curso.

Las alertas se pueden establecer para que se activen si un sistema de almacenamiento está bajo muchos tipos de estrés. Por ejemplo, si la relación de reducción de datos cambia repentinamente de forma radical, podría indicar que un ciberataque está cifrando datos. Un ataque también podría provocar un cambio significativo en el rendimiento. Asimismo, las desviaciones o anomalías en la cadencia de cambio de escritura pueden indicar que se está produciendo un ciberataque.

Prueba y validación de copias de datos

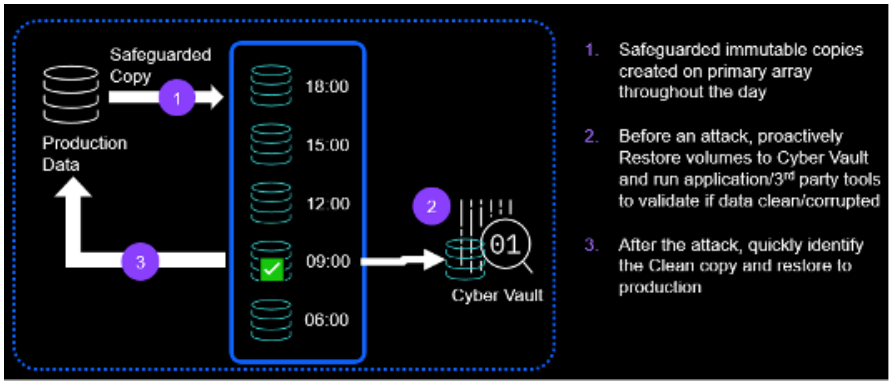
La solución IBM FlashSystem Cyber Vault proporciona las siguientes prestaciones de ciberresiliencia:

- **Validación de datos:** validación operativa periódica de las copias de Safeguarded Copy de un momento específico para ofrecer una detección proactiva de la corrupción de datos o la garantía de que la copia se ha validado y está limpia antes de cualquier otra acción.
- **Análisis forense:** inicie una copia del sistema de producción y utilícela para investigar un problema y determinar las medidas de recuperación. Planifique qué herramientas y procedimientos se utilizarían para identificar la causa y el alcance de un ataque.
- **Recuperación quirúrgica:** extraiga los datos de Safeguarded Copy y restáurelos lógicamente en el entorno de producción. Esta operación es de vital importancia para restaurar datos, archivos o sistemas al uso de producción si se ha producido una pérdida de datos, ya sea intencionada o no intencionada.
- **Recuperación tras catástrofe:** es la última opción, la que nadie quiere llegar a utilizar nunca. La solución IBM FlashSystem Cyber Vault proporciona esta prestación. De hecho, una práctica recomendada es realizar periódicamente un ejercicio de recuperación tras catástrofe completo en un sistema de prueba o desarrollo para asegurarse de que podrá recuperarse si se produce un ataque.
- **Copia de seguridad fuera de línea:** realice una copia de seguridad nueva con su solución de copia de seguridad habitual del entorno validado correctamente para añadir una capa de protección adicional y retención de datos a largo plazo.

Recuperación rápida

IBM FlashSystem Cyber Vault está diseñada para proporcionar una recuperación rápida y fiable, en minutos o unas horas, de sus aplicaciones más importantes, para proteger la reputación y el valor de marca de su organización. Después de un ciberataque, el viejo dicho es aún más cierto: *¡el tiempo es oro!*

Como hemos visto, la combinación de las instantáneas de IBM Safeguarded Copy, la validación de Cyber Vault y la automatización ofrece la capacidad de restaurar rápidamente un entorno de producción tras un ataque.



Rápida recuperación de datos de IBM Cyber Vault

Marcos para la ciberresiliencia de TI

Las regulaciones y marcos específicos varían según el país o la región del mundo. Un marco citado con frecuencia es el publicado en 2013 y actualizado en 2018 por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology).

El marco de ciberseguridad del NIST proporciona un marco de políticas de referencia en torno a la seguridad informática sobre cómo las organizaciones pueden evaluar y mejorar su capacidad para prevenir, detectar y responder a ciberataques. Este marco básico es una metodología aceptada por el sector para establecer un plan de desarrollo e implementación de protecciones para garantizar la prestación de los servicios de negocio más importantes. El siguiente diagrama describe las cinco categorías del maco del NIST:

Marco de seguridad del NIST

Identificar: consiste en preparar un plan para que cuando sufra un ataque, esté preparado y confíe en su capacidad para restaurar los sistemas de TI de negocio a su estado anterior, lo que requiere un conocimiento pormenorizado del alcance de sus activos de negocio cruciales necesarios para continuar las operaciones y una estrategia para la recuperación rápida.

Proteger: se centra en descubrir las debilidades antes de que los atacantes lo hagan y asegurarse de que los datos se almacenen en una infraestructura que no pueda verse comprometida por ninguna actividad maliciosa. Esto incluye temas de gestión de ID, control de accesos, reconocimiento, seguridad de datos y protección de datos, así como tecnología de protección proactiva.

Detectar: esto es, encontrar amenazas desconocidas mediante la supervisión y el análisis avanzado para descubrir rápidamente cuándo existen amenazas.

Responder: se refiere a la coordinación de su respuesta: análisis, contención, mitigación y comunicación.

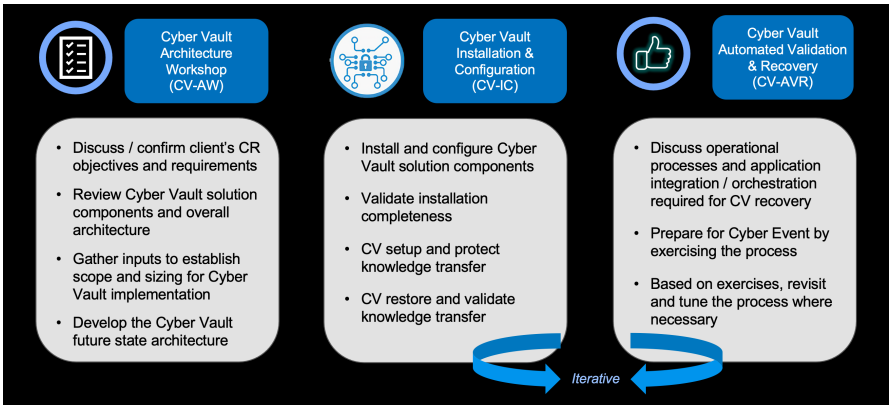
Recuperar: volver a ponerse en marcha de forma rápida y eficaz. Esto implica orquestar muchos elementos móviles y, una vez analizadas las acciones necesarias, automatizar la mayor parte posible del proceso de recuperación.

La solución IBM FlashSystem Cyber Vault aborda los componentes principales del marco de ciberseguridad del NIST.

IBM Lab Services

IBM Systems Lab Services ofrece servicios de infraestructura para ayudarle a crear soluciones de cloud híbrido y de TI empresarial. Los asesores de Lab Services colaboran con las organizaciones ofreciendo su amplia experiencia técnica, herramientas valiosas y metodologías de éxito. Los expertos ayudan a los clientes a resolver los desafíos de negocio y a formar a los departamentos de TI con nuevas competencias y las mejores prácticas. IBM Lab Services ofrece una extensa experiencia técnica en una amplia gama de servicios de infraestructura de TI, incluido el almacenamiento.

IBM Lab Services ofrece un conjunto completo de servicios para ayudar a los clientes a acelerar su adopción y uso de la solución Cyber Vault. Estos servicios para Cyber Vault pueden incluir la preparación, la planificación y la implementación de la solución Cyber Vault y, en caso necesario, asistencia con la recuperación tras un ciberincidente.



Servicios de despliegue para IBM FlashSystem Cyber Vault

Resumen

Las consecuencias económicas y empresariales de los ciberataques son cada vez mayores. Los ciberataques se pueden producir de varias maneras. Pueden tomar muchas formas diferentes y evolucionan continuamente. Tanto si el objetivo del atacante es robar datos confidenciales del cliente como retener información valiosa para pedir un rescate, las organizaciones deben contar con una estrategia general de ciberseguridad.

Los enfoques tradicionales de HA/DR para la protección de datos funcionan bien para sus fines previstos, pero son insuficientes para protegerse ante ciberataques. La réplica remota basada en almacenamiento para alta disponibilidad o recuperación tras desastre replica todos los cambios (maliciosos o no) en la copia remota.

Los datos que se almacenan en los medios fuera de línea o en el cloud pueden tardar demasiado tiempo en recuperarse de un ataque generalizado. La recuperación a gran escala puede tardar entre días y semanas, lo que puede suponer demasiado tiempo de inactividad para las empresas.

La funcionalidad Safeguarded Copy de IBM FlashSystem e IBM SAN Volume Controller está diseñada para crear automáticamente instantáneas inmutables y eficientes de acuerdo con una planificación. El sistema almacena específicamente estas instantáneas, que no se pueden conectar a servidores, lo que crea un entorno de aislamiento virtual, alejado del malware u otras amenazas. Tampoco se pueden cambiar ni suprimir, excepto de acuerdo con una planificación, con lo cual también se protegen contra posibles acciones o errores cometidos por el personal.

La solución IBM FlashSystem Cyber Vault se basa en Safeguarded Copy para acelerar la detección y recuperación de ciberataques. Mediante herramientas estándar de base de datos y software de automatización, FlashSystem Cyber Vault comprueba que las instantáneas de Safeguarded Copy no estén corruptas.

Si FlashSystem Cyber Vault detecta cambios, es una señal inmediata de que se puede producir un ataque, lo que permite iniciar rápidamente la recuperación mediante las últimas instantáneas sin ningún indicio de ataque. Y puesto que las instantáneas de Safeguarded Copy están en el mismo almacenamiento de FlashSystem que los datos operativos, la recuperación está diseñada para ser más rápida que la restauración de las copias almacenadas por separado. Con estas ventajas, FlashSystem Cyber Vault está diseñada para ayudar a reducir el tiempo de recuperación tras ciberataques de días a tan solo horas.

1.Fuente: IBM Institute for Business Value, Informe sobre el coste de una brecha de seguridad en los datos de 2021, https://www.ibm.com/security/data-Breach

2. IT World Canada, "Average ransomware payment for Canadian firms hits $450,000", https://www.itworldcanada.com/article/average-ransomware-payment-for-canadian-firms-hits-450000/467792

¿Por qué IBM?

IBM ofrece una amplia gama de hardware, software y servicios para ayudar a las organizaciones a atender sus necesidades de infraestructura de TI de forma rentable, que incluye soluciones sólidas de almacenamiento de datos para habilitar un almacenamiento fiable y siempre activo, así como la recuperación tras desastre. Como las necesidades de negocio van cambiando, las soluciones de IBM se centran en la interoperatividad y la integración de nuevos casos de uso o enfoques, desde la analítica hasta la copia de seguridad de varios sitios o la recuperación prácticamente al instante. Con IBM, las organizaciones pueden crear una infraestructura de almacenamiento flexible, sólida y resiliente para dar soporte a las operaciones más importantes y garantizar así un funcionamiento fluido y la conformidad con la normativa.

Las ofertas de IBM Storage e IBM Security están diseñadas para trabajar conjuntamente y proporcionar una solución completa para la prevención, la detección y la recuperación de ciberataques.

Más información

Visite nuestra página de soluciones para obtener más información sobre la familia de sistemas de datos FlashSystem o póngase en contacto con su representante o Business Partner de IBM. Si prefiere que contactemos con usted, rellene este formulario para programar una consulta con un experto en almacenamiento de IBM.

Asimismo, IBM Global Financing ofrece numerosas opciones de pago que le ayudarán a adquirir la tecnología que necesita para hacer crecer su negocio. Ofrecemos gestión integral del ciclo de vida de los productos y servicios de TI, desde la adquisición hasta la retirada del servicio. Visite: https://www.ibm.com/financing/flash

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.