COHESITY

UNA GUÍA EJECUTIVA PARA EVALUAR LAS BÓVEDAS CIBERNÉTICAS

Resumen ejecutivo: Por qué el uso de bóvedas cibernéticas es esencial para la resiliencia cibernética

Ninguna empresa es inmune a los ciberataques, por lo que una respuesta y recuperación eficaces son esenciales para todas las organizaciones. Los atacantes harán todo lo posible para obligarlo a pagar rescate, incluso apuntando a los mismos sistemas destinados a proteger sus datos. Las estrategias de copia de seguridad tradicionales, diseñadas para proteger contra fallas de hardware y desastres naturales, hacen poco para proteger a su organización contra ataques cibernéticos dirigidos de múltiples etapas. Cuando el ransomware ataca, las copias de seguridad de los datos que están conectadas a redes de producción pueden cifrarse o eliminarse, haciendo casi imposible lograr una recuperación limpia y rápida. Para los líderes de TI, no es cuestión de si ocurrirá un ataque, sino de cuándo. ¿Su organización está lista para recuperarse de manera confiable cuando llegue ese ataque?

A medida que organizaciones como la suya se replantean cómo proteger y recuperar sus datos, una bóveda cibernética se ha convertido en una parte fundamental de la estrategia moderna de resiliencia cibernética. Una bóveda cibernética garantiza que tendrá una copia intacta de sus datos para recuperarse cuando todo lo demás falle. El uso de bóvedas cibernéticas proporciona la separación, la verificación y el control necesarios para garantizar datos limpios y recuperables, incluso ante ataques cibernéticos destructivos. Es por eso que sus pares están adoptando la bóveda cibernética como un imperativo para la resiliencia.

El desafío: La recuperación cibernética es mucho más compleja que la recuperación ante desastres

Durante años, las organizaciones han diseñado sistemas de respaldo para abordar las fallas de hardware, las eliminaciones accidentales y los desastres naturales. Estos sistemas han sabido cumplir bien su propósito. Pero no son suficientes para proteger los datos contra los ataques cibernéticos destructivos que son dominantes en la actualidad.

Como resultado, ha surgido un factor de riesgo crítico: los datos de respaldo pueden ser tan vulnerables como los datos de producción. Los actores de amenazas ya no se centran únicamente en cifrar los datos de producción. Se infiltran en repositorios de copias de seguridad, deshabilitan las programaciones de instantáneas, instalan malware y corrompen metadatos para eliminar las rutas de recuperación.

Estos riesgos existen incluso si cuenta con una plataforma moderna de protección de datos.

Por qué su patrimonio de datos está en riesgo

Tal vez esté pensando: "Tengo una plataforma de datos segura para todas mis copias de seguridad, con todos los complementos de seguridad habilitados". ¿No es suficiente?". Respuesta corta: No.

Dicha plataforma reduce significativamente su riesgo y su superficie de ataque. Pero por sí sola no elimina la exposición.

Este es el motivo:

- **Conectividad compartida**: La mayoría de los sistemas de respaldo permanecen conectados a la red de producción. Si ese entorno de producción se ve comprometido, los atacantes ya tienen un camino hacia los datos de respaldo.
- **Superposición de credenciales**: Las credenciales administrativas a menudo se comparten entre entornos. Cuando un atacante obtiene acceso privilegiado, puede eliminar o cifrar copias de seguridad con la misma facilidad que los datos de producción.
- **Falsa inmutabilidad**: Algunas copias de seguridad "inmutables" solo están bloqueadas por software. Si se vulnera el plano de control de almacenamiento o la API, la marca de inmutabilidad puede revertirse.
- **Las amenazas latentes pueden permanecer**: Muchas organizaciones efectúan la restauración a partir de copias de seguridad sin validar la integridad de los datos o escanear malware latente, lo que aumenta el riesgo de reinfección durante la recuperación.

El impacto en el negocio

El resultado es una brecha de confianza: la integridad percibida de los datos de respaldo es mucho más alta que la realidad. Las consecuencias negativas se encadenan:

- **Tiempo de inactividad prolongado**: Las copias de seguridad no verificadas o comprometidas prolongan la recuperación, de horas a días o semanas.
- **Presión operativa**: Los equipos pasan tiempo recreando sistemas o conjuntos de datos en lugar de ejecutar planes de recuperación.
- **Costos acumulativos**: Cada hora de tiempo de inactividad aumenta la pérdida de ingresos, la exposición regulatoria y el daño a la marca.
- **Erosión de la confianza**: Cuando TI no puede ofrecer una recuperación rápida y limpia, la confianza de los ejecutivos y de la junta directiva en la resiliencia organizacional disminuye.

Bóveda cibernética: Su última línea de defensa cuando todo lo demás falla

Una bóveda cibernética aborda esta brecha de confianza. Una bóveda cibernética es un repositorio seguro, aislado e inmutable que almacena copias limpias de datos críticos. La bóveda está deliberadamente desconectada de las redes de producción y de los sistemas de respaldo primarios.

Adoptar una bóveda cibernética actualiza la regla de copia de seguridad 3-2-1: conservar tres copias de los datos en dos tipos de medios diferentes, con una copia fuera del sitio, aislada e inmutable.

En la práctica, las organizaciones implementan esta regla moderna de copia de seguridad de la siguiente manera:

- **Las tres copias de los datos deben ser inmutables:** Las copias deben protegerse mediante almacenamiento de tipo write-once, read-many (WORM) o bloqueo a nivel de objeto, y validarse continuamente mediante detección de anomalías basada en IA y análisis periódicos de amenazas para confirmar que los datos estén limpios.
- **Dos medios diferentes significa almacenar datos en dos plataformas diferentes o límites de confianza:** Las copias deben residir en sistemas distintos que no compartan el mismo plano de control ni la misma superficie de ataque. Esto puede incluir combinaciones de disco, cinta o almacenamiento en la nube, diseñadas para el aislamiento de datos.
- **Se debe aislar una copia fuera del sitio:** La copia final debe estar separada por un aislamiento lógico o físico y protegida por un modelo de seguridad aislado y custodia de terceros. Esta copia también debe protegerse con autenticación multifactor (MFA), quórum y verificaciones de integridad de datos.

Juntos, estos avances transforman la regla 3-2-1 en un pilar fundamental de la resiliencia cibernética. La bóveda cibernética sirve como el punto de recuperación final y limpio para los datos críticos. Al combinar la inmutabilidad, el aislamiento, los diversos dominios de almacenamiento y una rigurosa validación de la integridad, la bóveda cibernética permite a las organizaciones recuperarse de manera segura de un ataque cibernético destructivo, incluso en el peor de los casos en el que su ecosistema de respaldos se haya visto comprometido.

Evaluación de las soluciones de bóveda cibernética

Al seleccionar una solución de bóveda cibernética, los líderes de TI deben evaluar tanto la arquitectura de seguridad como la preparación operativa. Según los comentarios de cientos de líderes de TI, los siguientes cinco pilares son capacidades críticas:

1. **Aislamiento y control de acceso:** Los datos de la bóveda deben ser inaccesibles desde las redes de producción. Busque aislamientos físicos impuestos, dominios de identidad independientes, MFA y aprobaciones administrativas basadas en quórum.
2. **Inmutabilidad e integridad:** Los datos deben ser a prueba de manipulaciones, con almacenamiento WORM y políticas de bloqueo de retención que eviten la modificación o eliminación, incluso por parte de los administradores.
3. **Automatización y orquestación:** La replicación, validación y recuperación de la bóveda deben automatizarse. La orquestación basada en políticas reduce el error humano y acelera la recuperación.
4. **Protección contra amenazas:** La detección de anomalías y el escaneo de malware basados en IA señalan posibles amenazas en las instantáneas para ayudar a garantizar que solo se almacenen y restauren datos limpios y no comprometidos.
5. **Cumplimiento e informes:** Los registros de auditoría inmutables, el cifrado y la gestión de retención deben alinearse con marcos como NIST SP 800-209, ISO 27040 y DORA para demostrar la capacidad de recuperación y la preparación para la resiliencia.

Tarjeta de puntuación de evaluación: use esta tarjeta de puntuación durante sus conversaciones con proveedores.

Instrucciones:

1. Para cada categoría, asigne un puntaje de 1 a 5 para cada proveedor, donde 1 no cumple con el requisito y 5 cumple completamente con el requisito.
2. Multiplique el puntaje de cada proveedor por el **Peso** para esa categoría y registre el resultado en la celda de puntaje ponderado correspondiente.
3. Para cada proveedor, sume todos los **Puntajes ponderados** de la columna y registre el total en la fila **Total ponderado** en la parte inferior de la tabla.
4. Utilice el **Total ponderado** para comparar a los proveedores en general y registrar cualquier observación cualitativa o riesgo por separado.

		Proveedor 1		Proveedor 2		Proveedor 3		Proveedor 4	
Categoría	**Peso**	**Puntaje**	**Puntaje ponderado**	**Puntaje**	**Puntaje ponderado**	**Puntaje**	**Puntaje ponderado**	**Puntaje**	**Puntaje ponderado**
Aislamiento/Aislamiento físico	10								
Inmutabilidad/WORM	10								
Separación de los controles de acceso	10								
Autenticación fuerte (MFA/quórum)	8								
Detección de amenazas/anomalías	8								
Bloquear la recuperación de instantáneas infectadas	8								
Coordinación de la recuperación	8								
Sala limpia/Validación	8								
Cumplimiento/Auditabilidad	8								
Simplicidad SaaS/TTV	7								
Flexibilidad híbrida/multinube	8								
TCO/Gastos generales operativos	7								
Total ponderado									

La bóveda cibernética moderna ofrece resultados comerciales medibles:

- **Resiliencia**: Una copia de recuperación aislada física o lógicamente que permanece intacta incluso cuando las plataformas de respaldo se ven comprometidas.
- **Continuidad**: Las copias de seguridad en bóveda garantizan que las organizaciones tengan una copia de los datos para recuperar, independientemente del alcance del ataque.
- **Cumplimiento**: El almacenamiento inmutable y la aplicación de la retención proporcionan evidencia auditable de la protección de datos y la preparación para la recuperación.
- **Confianza**: Los puntos de recuperación se conservan fuera del radio de impacto operativo y se pueden validar antes de su uso, lo que garantiza que los datos restaurados estén limpios y no estén comprometidos.

La bóveda cibernética conecta las operaciones de TI, la seguridad y el cumplimiento, por lo que, cuando ocurre una crisis, se garantiza una recuperación limpia, no una apuesta.

Desde la dependencia de copias de seguridad hasta la recuperación resiliente: Bethany Children's Health Center

Muchas organizaciones están integrando la bóveda cibernética como un componente estándar de su estrategia de protección de datos. Un ejemplo es el Bethany Children's Health Center de Oklahoma, que brinda atención a niños con necesidades médicas complejas. Para permitir una atención ininterrumpida, el centro debe proteger los datos de salud confidenciales y restaurarlos rápidamente en caso de un ataque cibernético o un desastre. Bethany cumple con estos requisitos al almacenar copias de seguridad inmutables tanto en las instalaciones como en Cohesity FortKnox, una bóveda en la nube aislada.

Para mayor resiliencia, Bethany sigue el principio 3-2-1, manteniendo tres copias de datos en dos medios diferentes, con una copia almacenada fuera de las instalaciones. Se mantienen dos copias de seguridad inmutables en las instalaciones, y la tercera se almacena en Cohesity FortKnox.

Cohesity FortKnox proporciona un servicio de bóveda cibernética gestionado disponible para entornos de DataProtect y NetBackup, ofrecido en AWS, Azure y GCP, y como soluciones en las instalaciones para los entornos más seguros. FortKnox combina aislamiento, inmutabilidad y automatización para ofrecer una recuperación rápida, limpia y verificada a escala empresarial.

FortKnox agrega una nueva capa de defensa: una bóveda segura y aislada físicamente que garantiza que los datos críticos permanezcan seguros, conformes y recuperables.

Próximos pasos para evaluar su resiliencia cibernética

Su plan de resiliencia no puede basarse en suposiciones que ya no se aplican. A medida que los ataques cibernéticos se vuelven más agresivos, la continuidad del negocio depende cada vez más de la solidez de su última copia, la más segura, de los datos. La bóveda cibernética representa un enfoque proactivo que fortalece la recuperación cibernética y reduce el tiempo de inactividad.

Comience por evaluar:

- **¿Hace copias de seguridad de sus datos SaaS, en las instalaciones y en la nube desde todas sus fuentes de datos en una única plataforma moderna?**
- **¿Ha fortalecido su plataforma con MFA, inmutabilidad y control de acceso basado en roles (RBAC)?**
- **¿Cumple con la regla de respaldo 3-2-1?**
- **¿Qué medidas de aislamiento separan sus datos de respaldo de las redes de producción?**
- **¿Con qué frecuencia escanea sus copias de seguridad en busca de amenazas?**
- **¿Con qué frecuencia prueba su plan de respuesta cibernética?**
- **Durante su última prueba de respuesta cibernética, ¿con qué rapidez logró recuperarse?**

Este es el momento de elevar la resiliencia cibernética de un objetivo técnico a un imperativo estratégico. La preparación, no las suposiciones, es la máxima ventaja competitiva.

Vea cómo las bóvedas cibernéticas modernas pueden proteger sus datos, fortalecer su postura de recuperación y proporcionar la confianza para operar de manera segura, sin importar la amenaza. Obtenga más información en https://www.cohesity.com/es-es/platform/fortknox/

COHESITY

cohesity.com/es-es
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500065-001-ES 2-2026