OBJECT FIRST

Lista de comprobación

Lista de comprobación de resiliencia frente a ransomware

Identificar el almacenamiento de las copias de seguridad con inmutabilidad absoluta

Los ataques de ransomware son cada vez más sofisticados. El 66% de las organizaciones han sufrido como mínimo un ataque en los últimos dos años y el 96% de estos tenían como objetivo los datos de las copias de seguridad*.
Por lo tanto, cuando se produce —no si se produce— una vulneración y su empresa, su reputación y su carrera profesional están en riesgo, el almacenamiento inmutable de las copias de seguridad es su mejor y definitiva línea de defensa.

No obstante, si los datos "inmutables" los puede sobrescribir un administrador de copias de seguridad o de almacenamiento, un proveedor o un atacante, entonces no cuenta con una solución de almacenamiento con inmutabilidad absoluta.

Use esta lista de comprobación de 3 pasos para ver si su solución de copia de seguridad actual (o futura) está a prueba de ransomware.

* ESG Research 2025

Prepararse

Paso 1. Uso de almacenamiento de objetos S3

- ☐ Utiliza su solución de almacenamiento el Bloqueo y versionamiento de objetos S3 para reforzar la inmutabilidad y proteger el historial de copia de seguridad?
- ☐ Aplica el Modo de cumplimiento (no gobernanza) y admite cifrado de extremo a extremo desde el momento en que se crean los datos?
- ☐ Se puede verificar de forma independiente la inmutabilidad mediante estándares abiertos y pruebas de penetración de terceros?

Solo el almacenamiento de objetos S3 proporciona una seguridad inherente, con inmutabilidad nativa integrada directamente en su protocolo y sus API. Este diseño de base asegura que, una vez grabados los datos, no se pueden alterar ni eliminar. El almacenamiento de objetos S3 se basa en una arquitectura estándar de la industria y abierta que está conforme a las mejores prácticas de seguridad informática y permite pruebas de terceros.

Paso 2. Asegurar la inmutabilidad instantánea

- ☐ Su solución garantiza que los datos de copias de seguridad sean inmutables desde el momento en que se graban, sin ninguna demora ni "zona de reposo"?
- ☐ Evita la inmutabilidad basada en instantáneas o en la capa de deduplicación, que aplica protecciones solo después de que el trabajo finaliza?
- ☐ Se graban los datos de copia de seguridad directamente en el almacenamiento de objetos con el bloqueo de objetos S3 habilitado?

Asegurar que los datos de copia de seguridad sean inmutables desde el momento en que se graban es fundamental para evitar alteraciones no autorizadas, mantener la integridad de los datos y defenderse contra el ransomware. La manera comprobada y más segura de lograrlo es a través del versionamiento S3 combinado con el Bloqueo de objetos, lo cual refuerza la inmutabilidad cuando se crea un objeto en el sistema de almacenamiento.

Paso 3. Usar un dispositivo de destino integrado a medida

- ☐ Su configuración separa estrictamente el software de copia de seguridad del almacenamiento de las copias de seguridad, limitando el radio de alcance de una vulneración?
- ☐ Está utilizando un dispositivo de destino dedicado y gestionado por el proveedor en lugar de una configuración de almacenamiento propia que requiere actualizaciones, parches y supervisión manuales?
- ☐ Es su solución segura de forma verificable, o depende de un sistema de archivos propio de un proveedor, lo que impide las pruebas independientes y oculta cómo se aplica la inmutabilidad?

El almacenamiento de copia de seguridad diseñado específicamente consta de un dispositivo de almacenamiento autónomo que está configurado y optimizado para almacenar datos de copia de seguridad. Hay dos tipos: Dispositivos integrados, que combinan software de copia de seguridad y almacenamiento en un único sistema, y dispositivos de destino, que proporcionan un dispositivo de almacenamiento llave en mano para software de copia de seguridad externo como Veeam. Solo un dispositivo de destino S3 de copia de seguridad integrado a medida y llave en mano proporciona una resiliencia de datos de confianza cero al separar adecuadamente el software y el almacenamiento, y permitir pruebas de seguridad independientes.

Inmutabilidad absoluta: La defensa definitiva contra el ransomware

Si no puede marcar cada casilla, es posible que sus copias de seguridad sean vulnerables a ataques de ransomware. Inmutabilidad absoluta significa cero accesos a acciones destructivas. Nadie —ni siquiera el administrador con más privilegios ni el atacante con acceso al almacenamiento de copia de seguridad— puede modificar ni eliminar datos.

Lograr la inmutabilidad absoluta mediante cero accesos exige ceñirse **a tres principios fundamentales:**

1. **Almacenamiento de objetos S3:** Un estándar completamente documentado y abierto con inmutabilidad integrada que permita pruebas de penetración y verificación independientes.
2. **Inmutabilidad instantánea:** Los datos de copia de seguridad deben ser inmutables desde el momento en que se graban.
3. **Dispositivo de almacenamiento de destino:** Un dispositivo de almacenamiento de destino dedicado separa el almacenamiento del software de copia de seguridad y elimina los riesgos asociados con el almacenamiento de copia de seguridad autogestionado durante las operaciones.

Descargue nuestro documento técnico y descubra por qué la **Inmutabilidad absoluta** es la resiliencia definitiva contra el ransomware.

Descargue nuestro documento técnico ↗

Acerca de Object First

Object First proporciona un software de copia de seguridad seguro, sencillo y potente que está integrado a medida para Veeam y es absolutamente inmutable. Con la defensa definitiva contra el ransomware, usted y su organización pasan a ser Sencillamente resilientes.

Solicitar una demo ↗