

¿Por qué elegir NAKIVO como protección contra el ransomware?

¿Cuánto le costaría a su empresa que los sistemas dejaran de funcionar debido a una filtración de datos, un pirateo informático o, peor aún, un ataque de ransomware? NAKIVO Backup & Replication proporciona una protección fiable contra el ransomware para los datos de backup almacenados localmente, en la nube o en cinta, lo que le permite reanudar rápidamente las operaciones comerciales normales y recuperar cualquier dato bloqueado por el ransomware.



VENTAJAS CLAVE RESPALDADAS POR DATOS

RÁPIDA

2 veces

Más rápida en el backup de máquinas virtuales. Recuperación instantánea completa y granular para cualquier cosa. 2 minutos para la instalación y ejecución del primer job.

ASEQUIBLE

49%

Menos de TCO, desde **2.10 € per la máquina virtual/mes** con una suscripción o indefinidamente desde **199 € /zócalo** de CPU en las licencias perpetuas.

LA MEJOR VALORADA

4,8

Por las principales comunidades de TI (Gartner Peer Insights, Spiceworks, Trustradius y Capterra) por su excepcional experiencia de usuario y funciones.

«Gracias a NAKIVO Backup & Replication, **mejoramos el rendimiento, ahorramos tiempo en la gestión y permitimos la inmutability** para proteger nuestros datos contra el ransomware.»

Diano Tura, fundador de Dorelan

Nosotros **sufrimos un ciberataque**, y el equipo de ingeniería de NAKIVO nos proporcionó una compatibilidad excelente para **restaurar todos nuestros servidores afectados muy rápidamente tras el incidente del ransomware.**

Jesus Alfonso Rangel Diaz
Coordinador informático de Foxconn BC

«NAKIVO Backup & Replication es una solución estable de backups de máquinas virtuales, que proporciona **backups inmutables que le protegen contra el ransomware** y le permite recuperar máquinas virtuales enteras en cuestión de minutos.»

Gabriel Palafox,
Director General de Sensanet

ESTÁS EN BUENA COMPAÑÍA

1 La compatibilidad multiplataforma

Proteja todas las cargas de trabajo desde un único panel de cristal: VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Amazon EC2, Windows/Linux, Microsoft 365, recursos compartidos y Oracle Database.

2 Backups inmutables en la nube

Haga backups de inmutable en la nube (Amazon S3, Wasabi, Azure Blob, Backblaze B) y otros medios compatibles con S3 con Object Lock activado. Ningún usuario o tercero puede sobrescribir o modificar los datos del backup hasta que expire el periodo especificado.

3 Backups locales inmutables

Crear backups inmutables en repositorios locales de Linux durante el tiempo que sea necesario. Sólo el usuario root puede modificar la configuración de inmutabilidad del backup, garantizando backups a prueba de manipulaciones hasta que transcurra el periodo de retención predefinido.

4 Backups aislados de la red

Cree copias de backups en cinta y otras unidades extraíbles (NAS desconectados, unidades USB, etc.) a partir de los backups existentes para bloquear eficazmente las posibles amenazas de ransomware.

5 Almacenamiento avanzado de backups por niveles

Aplicar la estrategia de backup 3-2-1-1 (distribuir los backups en varios dispositivos de almacenamiento para mitigar los riesgos: in situ, en la nube y en cinta) con una copia adicional que sea inmutable.

6 12 opciones de recuperación

Recuperación instantánea de VM - Recuperación granular - Recuperación completa - P2V/V2V - Recuperación bare-metal - Recuperación desde cintas - Recuperación de Microsoft 365 - Conmutación por error de VM e instancias en la nube y más...

7 Recuperación del ransomware mediante la replicación

Cree y mantenga réplicas idénticas de cargas de trabajo en un sitio remoto para garantizar operaciones empresariales eficaces y una inactividad mínima incluso después de un evento de ransomware.

8 Recuperaciones seguras

Verifique instantáneamente los backups y las réplicas para garantizar la recuperabilidad. Integre la solución con software antimalware para analizar los backups en busca de malware o ransomware antes de la recuperación para aislar posibles amenazas.

9 Ciberseguridad

La solución ofrece sólidas medidas de seguridad, como la autenticación de dos factores (2FA) y el cifrado AES-256 estándar del sector, que garantizan la protección e integridad de los datos desde su creación hasta su recuperación.

10 Administración sencilla

Garantice la protección y la resiliencia a escala con una única solución compatible con todas las cargas de trabajo, nubes y arquitecturas, con paneles intuitivos y asistentes paso a paso.

¿TODO LISTO PARA EMPEZAR?

PROBAR GRATIS

DEMOSTRACIÓN GRATUITA