NAKIVO

RESUMEN DE LA SOLUCIÓN

SÓLIDA PROTECCIÓN DE DATOS DE RECURSOS COMPARTIDOS DE ARCHIVOS DE NAKIVO

A medida que aumenta la dependencia de los recursos compartidos para almacenar y gestionar datos, también lo hacen los riesgos de pérdida de datos, fallos de hardware y ataques de ransomware, áreas en las que los métodos tradicionales de backup suelen quedarse cortos.

NAKIVO NAS Backup ofrece una protección completa para los datos no estructurados en recursos compartidos SMB/NFS alojados en dispositivos NAS y servidores de archivos Windows y Linux. De **backups incrementales** y **opciones de recuperación granular** a **funciones avanzadas de ciberseguridad** para garantizar que los datos permanezcan **seguros, accesibles** y **resilientes** frente a posibles amenazas.

VENTAJAS

2 VECES
más rápido con seguimiento de cambios, aceleración de la red y mucho más.

49%
del costo de otros proveedores

4000
puntos de recuperación ofrecen los RTO y RPO más ajustados.

4.8 ESTRELLAS
valoración media del ahorro de tiempo y dinero

5 MINUTOS
para instalar la solución y lanzar un primer job

PRINCIPALES FUNCIONES DE NAKIVO NAS BACKUPS

Backups rápidos: Utilice el seguimiento de cambios para crear backups incrementales copiando sólo los archivos nuevos o modificados desde el último backup, ahorrando tiempo y requisitos de almacenamiento.

El backup directo en la nube: Haga backup de sus recursos compartidos de archivos en plataformas en la nube como Amazon S3, Wasabi, Azure Blob y Backblaze B2, así como en otros destinos compatibles con S3, y acceda a ellos desde cualquier lugar.

Destinos de backups flexibles: Envíe backups de archivos compartidos y copias de backup a carpetas locales, nubes públicas, almacenamiento compatible con S3, otros recursos compartidos SMB/NFS y appliance de desduplicación además de cintas.

Backups a prueba de ransomware: Proteja los backups de recursos compartidos frente al ransomware y otras actividades maliciosas con almacenamiento inmutable en repositorios locales y en la nube, así como almacenamiento aislado de la red en cintas u otros soportes sin conexión.

Recuperación en cualquier escenario: Garantice una rápida recuperación operativa y la disponibilidad de los datos en varios escenarios con opciones de recuperación completas y granulares a partir de sus backups de recursos compartidos.

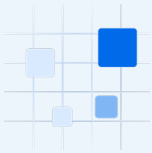
Ajustes de retención flexibles: Establezca políticas de retención a medida para garantizar el cumplimiento de la normativa y facilitar recuperaciones de datos precisas, con hasta 4.000 puntos de recuperación disponibles para realizar reversiones eficientes.

Herramientas de ciberseguridad: Proteja su entorno de backups frente a diversas actividades sospechosas o infracciones mediante el control de accesos basado en roles (RBAC), la autenticación de dos factores (2FA) y el cifrado AES-256.

Gestión optimizada: Gestione las operaciones de protección de datos desde cualquier lugar con la interfaz basada en web. Automatice y mejore la eficacia de las copias de seguridad y la recuperación mediante el panel de control Calendario, el encadenamiento de jobs y la aceleración de la red.

Cumplimiento normativo: Utilice las funciones de ciberseguridad de la solución para reforzar la protección de datos, la seguridad y las estrategias de recuperación, al tiempo que cumple las normas y reglamentos del sector.

Instalación rápida: Instale rápidamente la solución en Windows, Linux, NAS o como appliance virtual preconfigurado para VMware o Nutanix.



2024 Gartner© Magic Quadrant™

Mención honorífica en la categoría de soluciones empresariales de backup y recuperación

CLIENTES DE TODOS LOS SECTORES CONFÍAN EN NOSOTROS

> **7 veces más rápida en el backup**
>
> *La solución es más rápida que nuestros productos anteriores y admite muchas configuraciones diferentes.*
>
> Praful Soni, responsable informático sénior de Transpek

PROTEGE SUS RECURSOS COMPARTIDOS NAS

PROBAR GRATIS

DEMOSTRACIÓN GRATUITA

PROTECCIÓN CONTRA LOS ATAQUES DE RANSOMWARE

Almacenamiento de respaldos por niveles: Almacene copias de backups de recursos compartidos en diferentes ubicaciones -in situ, externas y en la nube- para garantizar que sus datos estén disponibles para su recuperación en caso de ataque.

Almacenamiento inmutable: Backups de archivos compartidos seguros en almacenamiento inmutable a prueba de manipulaciones a nivel local, en la nube y en sistemas de almacenamiento NEC HYDRAstor para evitar modificaciones no autorizadas y el cifrado de ransomware.

Almacenamiento aislado de la red: Cree y envíe copias de backups a dispositivos de cintas para asegurarse de que están aislados de amenazas basadas en la red como ransomware, malware y accesos no autorizados.

Cifrado multicapa: Proteja los datos de los recursos compartidos en cada etapa con cifrado AES-256: en el origen, en vuelo y en reposo, para garantizar que permanezcan seguros frente a accesos no autorizados.

AMPLÍE SU OFERTA DE SERVICIOS MSP

Consola para MSP: Proporcione servicios BaaS/DRaaS escalables y personalizables y gestione entornos de clientes con instancias independientes como inquilinos remotos junto con inquilinos locales.

Arrendamiento múltiple avanzado: Gestione hasta 100 inquilinos aislados en una única instancia con control granular de la asignación de recursos. Acceda a entornos de inquilinos remotos de forma segura a través de un único puerto, eliminando la necesidad de complejas configuraciones VPN.

Panel de control Visión general del inquilino: Obtenga información y alertas en tiempo real sobre las infraestructuras de los clientes, incluido el estado de los nodos, los recursos disponibles, las actividades programadas y la información de inventario.

Portal de autoservicio: Permita a los inquilinos crear sus propios jobs de backups y recuperación de forma independiente y ahorre tiempo y recursos valiosos.

¿POR QUÉ NECESITA EL BACKUP NAS DE NAKIVO?

Los recursos compartidos de archivos suelen almacenar grandes volúmenes de datos críticos y colaborativos no estructurados que son propensos a diversos riesgos:

Prevención de la pérdida de datos: Los borrados accidentales o los fallos de hardware podrían causar la pérdida permanente de datos e interrumpir los flujos de trabajo operativos.

Protección antirransomware: El ransomware se dirige a los recursos compartidos de la red debido a los datos críticos que contienen, que pueden interrumpir las operaciones si se cifran o bloquean.

Control de versiones y recuperación: Unas políticas de retención adecuadas permiten hacer reversiones a versiones anteriores de los archivos y recuperar con precisión los que se necesiten.

Cumplimiento normativo: Muchos sectores imponen estrictas medidas de conservación y seguridad de los datos compartidos o en colaboración.

nakivo.com | +1 408 335 7367 | 4894 Sparks Blvd., Sparks, NV USA 89436-8202