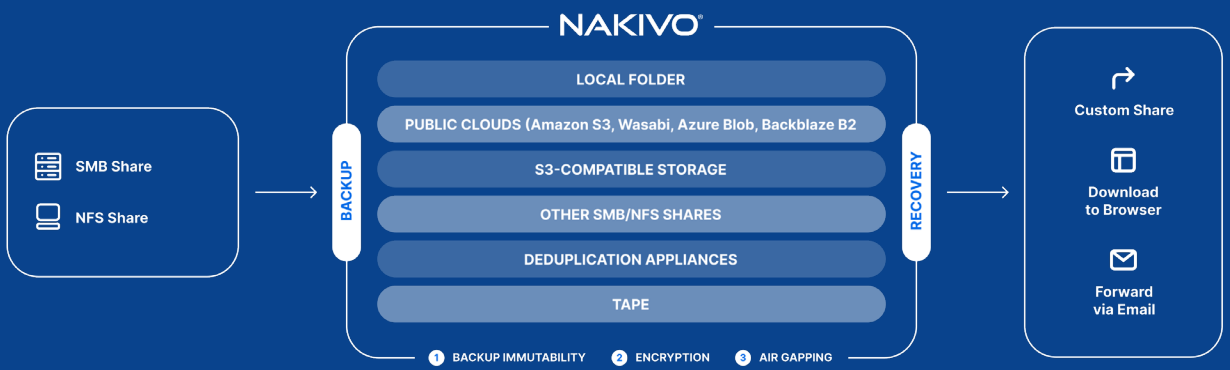
NAKIVO

SOLUTION BRIEF

ROBUST FILE SHARE DATA PROTECTION FROM NAKIVO

As reliance on file shares to store and manage data grows, so do the risks of data loss, hardware failures, and ransomware attacks — areas where traditional backup methods often fall short.

NAKIVO NAS Backup delivers comprehensive protection for unstructured data in SMB/NFS shares hosted on NAS devices and Windows and Linux file servers. From **incremental backups** and **granular recovery options** to **advanced cybersecurity capabilities** to ensure data remains **secure, accessible**, and **resilient** in the face of potential threats.



BENEFITS

2X
faster with change tracking, network acceleration and more

49%
recovery points deliver the tightest RTOs and RPOs

4,000
recovery points deliver the tightest RTOs and RPOs

4.8 STARS
average rating for saving time and money

5 MINUTES
to deploy and run your first job

KEY CAPABILITIES OF NAKIVO NAS BACKUP

Fast backups
Use change tracking to create incremental backups by copying only new or modified files since the last backup, saving you time and storage requirements.

Direct backup to cloud
Back up your file shares to cloud platforms such as Amazon S3, Wasabi, Azure Blob, and Backblaze B2, as well as other S3-compatible destinations and access them from anywhere.

Flexible backup targets
Send file share backups and backup copies to local folders, public clouds, S3-compatible storage, other SMB/NFS shares, and deduplication appliances in addition to tape.

Ransomware-proof backups
Protect file share backups against ransomware and other malicious activities with immutable storage in local and cloud repositories as well as air-gapped storage on tape or other offline media.

Recovery for every scenario
Ensure swift operational recovery and data availability in various scenarios with full and granular recovery options from your file share backups.

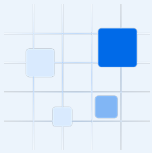
Flexible retention settings
Set tailored retention policies to ensure compliance and facilitate precise data recoveries, with up to 4,000 recovery points available for efficient rollbacks.

Cybersecurity tools
Protect your backup environment against a variety of suspicious activities or breaches with role-based access control (RBAC), two-factor authentication (2FA), and AES-256 encryption.

Streamlined management
Manage data protection operations from anywhere with the web-based interface. Automate and enhance backup and recovery efficiency using Calendar Dashboard, Job Chaining, and network acceleration.

Regulatory compliance
Use the solution's cybersecurity features to strengthen data protection, security, and recovery strategies while meeting industry standards and regulations.

Quick deployment
Swiftly deploy the solution on Windows, Linux, NAS, or as a pre-configured virtual appliance for VMware or Nutanix.



2024 Gartner© Magic Quadrant™

Honorable Mention in Enterprise Backup and Recovery Solutions Category

TRUSTED BY CUSTOMERS ACROSS INDUSTRIES

> **7X faster backups**
>
> *The solution is faster than other products I have used and supports many different configurations.*
>
> Praful Soni, Senior IT Manager at — Transpek

START PROTECTING YOUR NAS FILE SHARES!

TRY FOR FREE

GET FREE DEMO

PROTECT AGAINST RANSOMWARE ATTACKS

Backup data tiering: Store file share backup copies in different locations — onsite, offsite, and in the cloud — to ensure your data is available for recovery in the event of an attack.

Immutable storage: Secure file share backups in tamper-proof, immutable storage locally, in the cloud and in NEC HYDRAstor storage systems to prevent unauthorized modifications and ransomware encryption.

Air-gapped storage: Create and send backup copies to tape devices to ensure they are isolated from network-based threats like ransomware, malware, and unauthorized access.

Multi-layered encryption: Protect file share data at every stage with AES-256 encryption — at the source, in flight and at rest to ensure it remains secure from unauthorized access.

EXPAND YOUR MSP SERVICE OFFERING

MSP console: Deliver scalable and customizable BaaS/DRaaS services and manage client environments with standalone instances as remote tenants alongside local tenants.

Advanced multi-tenancy: Manage up to 100 isolated tenants in a single instance with granular resource allocation control. Access remote tenant environments securely through a single port, eliminating the need for complex VPN setups.

Tenant overview dashboard: Get real-time insights and alerts on client infrastructures, including node status, available resources, scheduled activities, and inventory information.

Self-Service portal: Enable tenants to create their own backup and recovery jobs independently and save valuable time and resources.

WHY DO YOU NEED NAKIVO NAS BACKUP?

File shares often store large volumes of critical and collaborative unstructured data that are prone to various risks:

Data Loss Prevention: Accidental deletions or hardware failures could cause permanent data loss and disrupt operational workflows.

Ransomware Protection: Ransomware targets network file shares due to the critical data they contain, which can disrupt operations if encrypted or locked.

Version Control and Recovery: Proper retention policies allow rollbacks to previous file versions and precisely recover needed.

Regulatory Compliance: Many industries mandate strict data retention and security measures for shared or collaborative data.

nakivo.com | +1 408 440 5605 | 4894 Sparks Blvd., Sparks, NV USA 89436-8202