Ransomware Protection and Recovery

What's New in NAKIVO Backup & Replication

INTRODUCTION

Ransomware remains a significant cybersecurity challenge in 2024. While organizations are now less likely to pay the ransom, the overall threat landscape is concerning. Total ransomware payments nearly doubled in 2023 to $1.1 billion, with attacks increasing from 2,581 in 2022 to 4,399 in 2023[1].

NAKIVO Backup & Replication goes beyond basic data protection to keep your infrastructure safe against ransomware-related data loss. Protection starts at the source and extends comprehensively to secure the data within the storage repository, ensuring backup data integrity throughout its lifecycle. This holistic defense against ransomware attacks allows you to recover data locked by ransomware and swiftly resume business operations.

The following is an overview of the latest ransomware resilience capabilities available in NAKIVO Backup & Replication v11.

EXPANDED RANSOMWARE PROTECTION ACROSS PLATFORMS

NAKIVO continuously enhances the solution's capabilities to protect data against ransomware attacks, extending cyber resilience to cover backups of Microsoft 365, file share and Proxmox VE data.

Ransomware protection for Microsoft 365 backups

Microsoft 365 has always been a prime target for ransomware attacks. NAKIVO Backup & Replication has consistently offered users full control over their Microsoft 365 data through onsite backups. This functionality allowed customers to maintain a copy of their Microsoft 365 backups on-premises and offline, ensuring protection against cybersecurity threats like ransomware.

The latest version of NAKIVO Backup & Replication supports immutable storage for Microsoft 365 backups. You can leverage immutable storage in local Linux-based repositories, public cloud platforms (Amazon S3, Wasabi, Azure Blob, Backblaze B2) and other S3-compatible storage. With immutability enabled, your recovery points become unalterable, safeguarding them from encryption by ransomware and unwanted modifications.

For added protection, you can use the Backup Copy feature to create additional offline copies on air-gapped storage (tape, NAS, USB drives, etc). These physically isolated backups remain inaccessible to ransomware operators, even during a network breach.

Moreover, you can implement the industry-recommended 3-2-1-1 backup strategy to reap the benefits of hybrid storage, protect against cybersecurity threats and ensure data availability in any scenario.

THE 3-2-1-1 BACKUP STRATEGY

3 copies of your data

2 different media types

1 offsite copy

1 immutable and/or air-gapped copy

[1] The State of Ransomware

Ransomware protection for Proxmox VE backups

The agent-based backup for Proxmox functionality allows you to create immutable and air-gapped backups of Proxmox VM data to protect them from ransomware encryption.

You can store backups locally, in public clouds and on other S3-compatible storage platforms, enabling immutability against ransomware and accidental changes. You can also create air-gapped backups on tape and other detachable devices and apply the 3-2-1-1 backup strategy to ensure multi-layered availability and complete data recoverability.

Hybrid storage for file share backups

Backup of unstructured data in SMB/NFS shares hosted on NAS devices and Windows/Linux machines can be sent to cloud platforms, S3-compatible storage, local folders, other NFS/SMB shares and deduplication appliances. Selecting a local or cloud-based repository as the destination allows you to benefit from the immutability feature and protect backups against ransomware attacks and unauthorized deletions.

You can also leverage the Backup Copy and Job Chaining functionalities to create air-gapped backups on tape, ensuring a multi-tiered approach to data availability and recoverability per the 3-2-1-1 backup strategy.

CYBERSECURITY CAPABILITIES IN NAKIVO BACKUP & REPLICATION

Hackers constantly exploit software and network vulnerabilities to gain unauthorized access to sensitive data systems and deploy ransomware.

Source-side backup encryption

NAKIVO Backup & Replication builds upon its built-in security features with the introduction of Backup Encryption. This feature complements the existing security capabilities, which include:

- Network and backup repository encryption: Encrypts the network to protect backup data in flight and the backup repository to protect data at rest, rendering backups unreadable to unauthorized users.
- Role-Based Access Control (RBAC): Customizes permissions to user roles, ensuring only authorized personnel can access backup data.
- Two-Factor Authentication (2FA): Adds an extra layer of security, requiring a second form of verification beyond just a password.

The new feature extends encryption capabilities directly to the data source. Now, backups, backup copies, and self-backups, including system configurations, can be encrypted before they are transmitted over the network. Source-side backup encryption is designed to be universally applicable across all supported environments and platforms. Whether your backups reside in local folders, on public cloud platforms, within S3-compatible storage, on SMB/NFS network shares, tape, or deduplication appliances, they are protected with a robust layer of encryption.

This layered approach ensures the highest level of data security, exceeding compliance requirements and industry security standards.

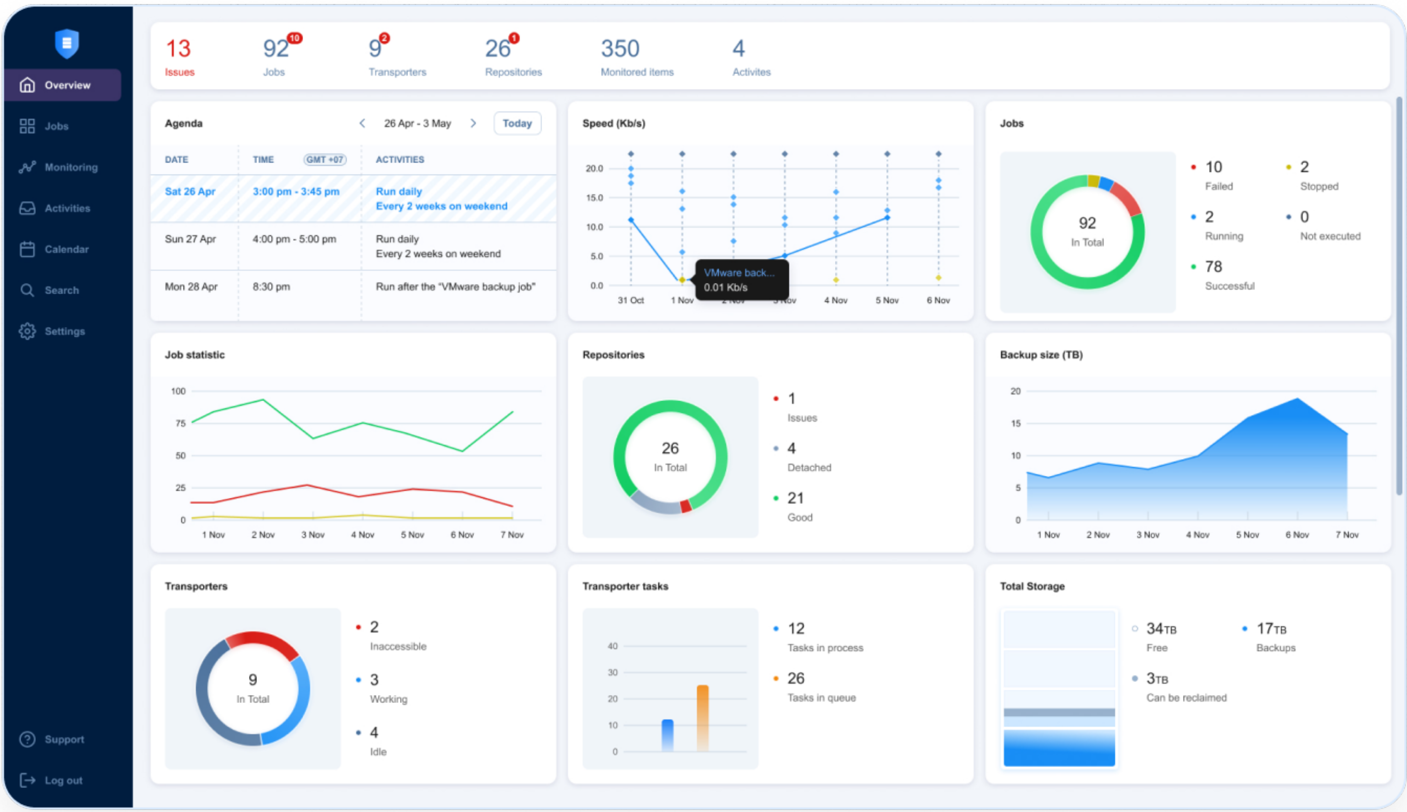
LATEST FEATURES AND ENHANCEMENTS

Immutable storage on deduplication appliances

NAKIVO Backup & Replication takes data protection a step further by offering immutable storage on the NEC HYDRAstor deduplication appliances. This powerful feature leverages the WORM technology to ensure backups remain unalterable, regardless of threat. Once data is written to the NEC HYDRAstor, it cannot be modified or deleted, enabling swift recovery of data, minimizing downtime and maintaining business operations.

Backup malware scan

We've also extended the ransomware recovery capabilities of NAKIVO Backup & Replication with the Backup Malware Scan feature to help organizations ensure the recovery of clean data. You can integrate external anti-malware software and scan backups for malware and ransomware before recovery to prevent infections in your infrastructure. If malware is detected, choose to fail the recovery or recover to an isolated network.



DATE	TIME GMT +07	ACTIVITIES
Sat 26 Apr	3:00 pm - 3:45 pm	Run daily Every 2 weeks on weekend
Sun 27 Apr	4:00 pm - 5:00 pm	Run daily Every 2 weeks on weekend
Mon 28 Apr	8:30 pm	Run after the "VMware backup job"

START PROTECTING YOUR DATA AGAINST RANSOMWARE

DOWNLOAD FREE TRIAL

Free for 15 days.
No feature limitations.

SCHEDULE A DEMO

Get answers on features,
pricing and more.

NAKIVO®

This publication has been prepared for general guidance and does not constitute professional advice, a public offer or an undertaking. No representations or warranties (express or implied) are given as to the accuracy or completeness of the information contained in this document, and, to the extent permitted by law, NAKIVO, Inc., its affiliates, employees, contractors and agents do not accept or assume any liability, responsibility or duty of care for any consequences of anyone acting, or refraining to act, in reliance on the information contained in this document or for any decision based on it. All third party trademarks and trade names are the property of their respective owners.

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