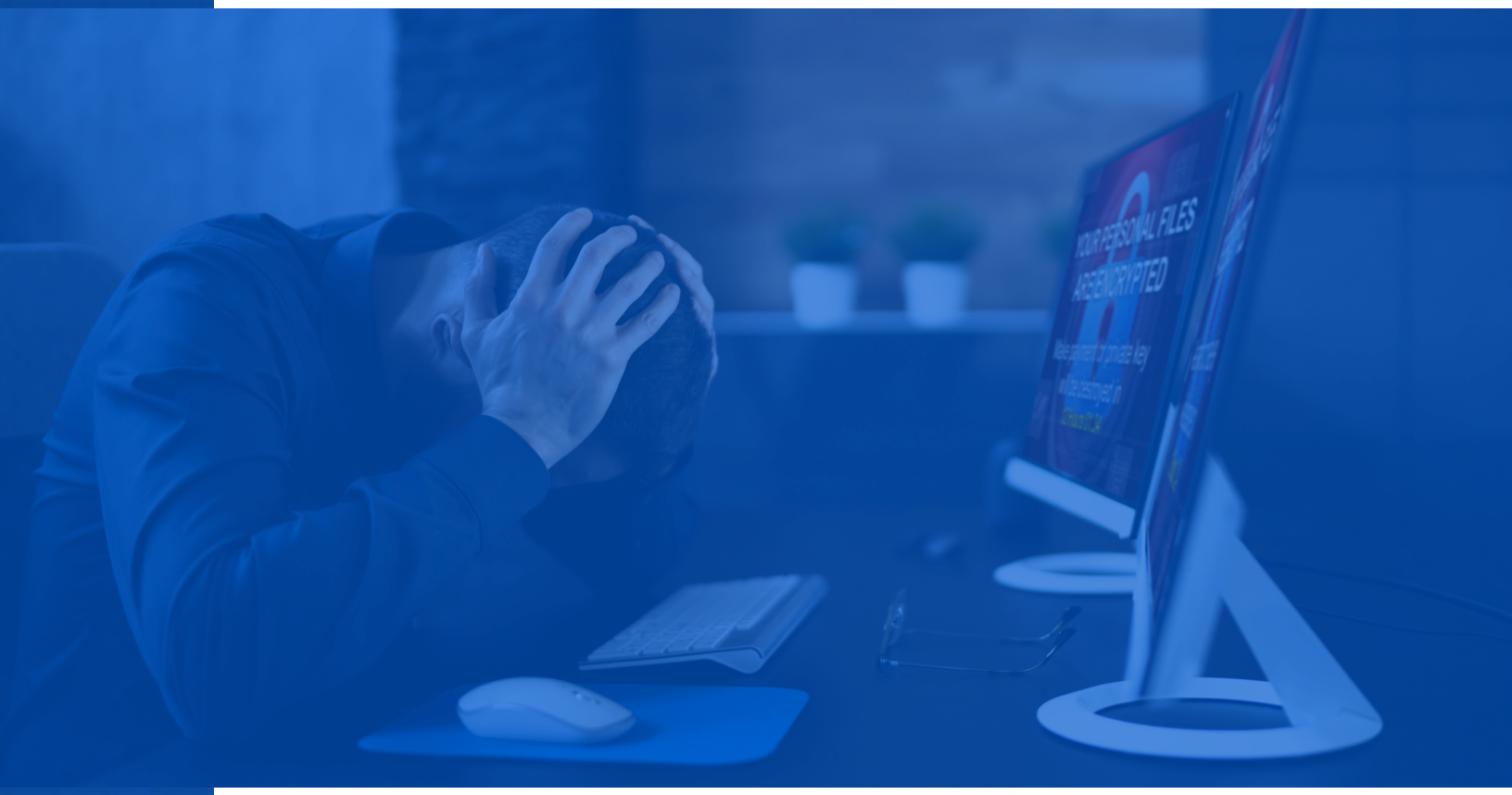
EBOOK

NovaBACKUP



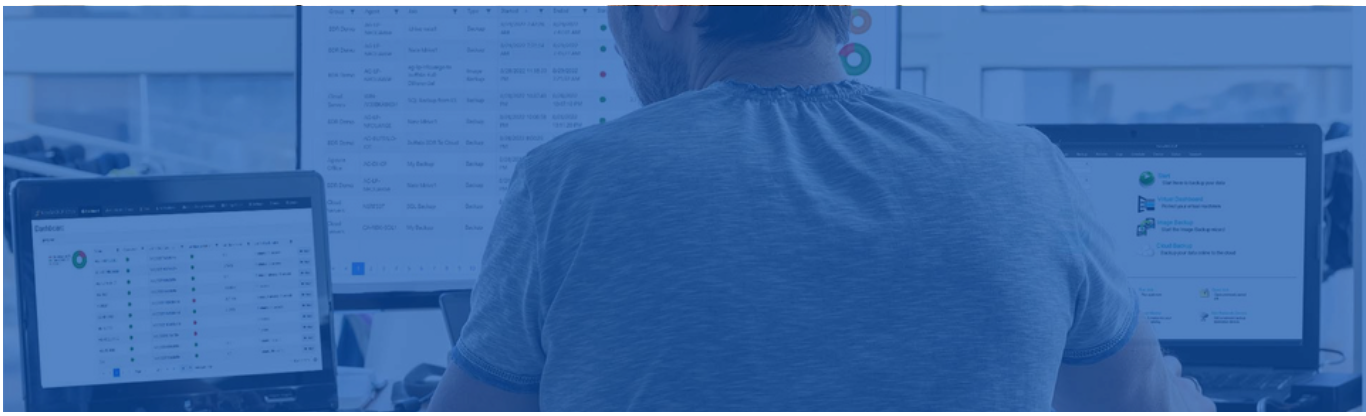
HOW TO PROTECT YOUR BACKUPS FROM RANSOMWARE

A Practical Guide with NovaBACKUP

Ransomware has long shifted from a rare, headline-grabbing event to a daily operational risk for organizations of all sizes—especially for small and midsize businesses. Attackers now leverage automation and AI to scale up both the volume and sophistication of their attacks, making it increasingly difficult for traditional defenses to keep pace.

> As of 2023, over 72% of businesses worldwide were affected by ransomware attacks.[1] SMBs, in particular, are targeted nearly four times more often than large organizations. [2]

While endpoint and network security remain essential, backups are your last line of defense when ransomware strikes. If your backup data is compromised, whether encrypted, deleted, or otherwise rendered unusable, recovery becomes nearly impossible without paying a ransom, which is unreliable and often ineffective.



This guide focuses specifically on protecting your backups from ransomware. We'll cover practical strategies, technical configuration examples in NovaBACKUP, and operational best practices to ensure your backups remain resilient and recoverable, even in the face of advanced attacks.

WHY PROTECTING BACKUPS FROM RANSOMWARE MATTERS

When ransomware hits, backups are your ultimate safety net. But modern ransomware actively targets backup files and repositories to block recovery. Protecting your backups becomes increasingly important as organizations with clean, recoverable backups were able to restore operations within a week, while those forced to pay ransom often faced months of downtime.

> 31% of organizations hit by ransomware needed one to six months to recover. In contrast, 45% of those using backups recovered within a week.[3]

If both your production data and your backups are encrypted or deleted by an attacker, your safety net is gone. Paying the ransom is unreliable and costly. Even after paying, there's no certainty of data recovery, and the process often drags on for months.

> Only 54% of organizations that paid a ransom were able to recover their data.[4]

Clean, recoverable backups are the only guarantee of business continuity. They are the key to minimizing downtime and preventing catastrophic data loss.

CORE PRINCIPLES FOR A RESILIENT BACKUP STRATEGY

Simply running regular backups of files and systems is no longer enough. Your backups need the same level of attention as your production systems. The following principles form the foundation of a resilient backup strategy, helping you protect critical data and maintain business continuity even under attack.

1 Keep Multiple Copies, Including Offsite and Air-Gapped Backups

Maintain at least three sets of your data. The first set is your primary data aka your production environment. In addition, make sure you have:

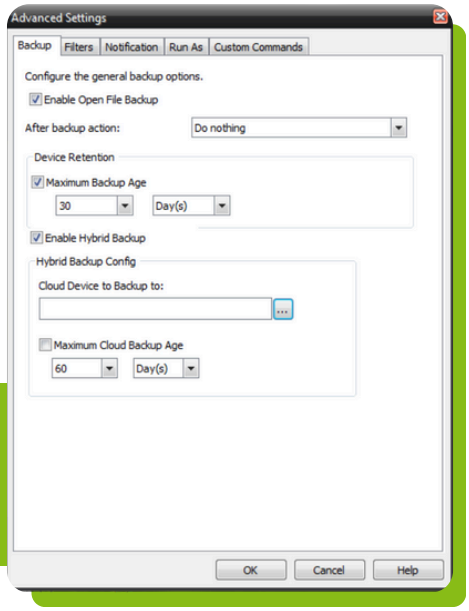
- **Copies on local storage:** Local backups are often the first target for ransomware because they are accessible from within the network. However, being onsite makes them ideal for quick recovery.
- **Copies on offsite or air-gapped storage:** Examples include cloud storage or removable drives that aren't continuously connected. Cloud backups in particular are a critical component of a ransomware-resilient strategy because they isolate data from your network, ensuring recovery even if ransomware spreads. However, proper configuration is essential for true isolation and security (see point #4).

With NovaBACKUP:

Hybrid Backup Jobs and Load-Balanced Restore

NovaBACKUP automates hybrid backup jobs, writing to local and cloud storage in sequence to keep both copies current.

Create a local backup job, set a 30-day retention for local backups. Then check the hybrid backup function and select the cloud storage with a 60-day retention.



Hybrid backups with staggered retention and an incremental-forever backup scheme (see #2) address ransomware's tendency to remain dormant for weeks. Keeping only the latest backup risks restoring infected data. **Versioning** ensures multiple restore points across locations, so you can roll back to a clean state.

And there's an added advantage: thanks to hybrid backups, NovaBACKUP optimizes **recovery speed**. When restoring data, it pulls from the fastest source, starting with local storage and falling back to cloud if needed, so you can get systems back online quickly.

2 Adopt Incremental Forever Backups

Traditional backup methods—full, incremental, and differential—served their purpose for decades, but they fall short in today's fast-paced IT environments. Each of these comes with their own challenges, either juggling large data sets, long backup windows, or inefficient storage use.

With NovaBACKUP:

Incremental Forever for Resilient Backups

NovaBACKUP's incremental forever approach solves these challenges. Instead of repeating full backups, this approach captures the initial full copy once and then tracks only changes going forward. At the same time, all increments are linked, enabling restores from any point in time.

The result? Faster backups, more efficient storage use (often with lower costs), and a more resilient foundation for today's data protection needs.

Explore the technical details of NovaBACKUP's incremental forever approach in our blog post.

3 Focus on Immutable Backups

Immutability typically refers to cloud storage features that prevent data deletion for a set period of time, say, 90 days. Storage-level immutability (for example, Wasabi Object Lock) blocks deletion or modification at the storage layer, making it a strong defense against ransomware by preventing encryption or other changes to files on that storage.

With NovaBACKUP:

Job-Level Immutability Plus Integrity Checks

Unlike solutions that rely on third-party storage features, NovaBACKUP provides job-level immutability built directly into the backup process, ensuring data cannot be deleted or altered during the retention period.

Storage-level immutability adds another layer of security, but NovaBACKUP's job-level immutability achieves the same result: backup data cannot be deleted or modified until retention expires, unless the job settings are explicitly changed.

For example, with a 30-day retention, every version of your selected files—including all changes—remains protected for the full retention period.

If backup files are deleted or altered on the storage, NovaBACKUP detects the issue through built-in integrity checks. At the start of every backup job, it checks the integrity of all backup files for both local and cloud backups along with the locally stored indexes. If a file is missing or corrupt (for example, maliciously deleted from a NAS), NovaBACKUP automatically re-adds it during the next backup, ensuring full recoverability.

4 Isolate and Secure Your Backup Storage

One of the most important aspects of protecting your backups from ransomware is to keep the backup storage—both for local and offsite backups—separate from the production environment. **Never map backup storage as a network drive** on production systems and use backup destinations exclusively for backup data, not for file sharing, collaboration, or production workloads.

Any backup storage should only be accessible from the backup server or agent, not from other machines on the network. This prevents ransomware from spreading to backup files via compromised endpoints.

Avoid using services like OneDrive or Google Drive for backups, as they're tied to daily workflows. This reduces the risk of accidental deletion, overwriting, or ransomware exposure through synced endpoints.

On top of that, create a dedicated backup user specifically for backup operations on your backup storage (including NAS, USB, cloud etc.) and apply the principle of least privilege.

> As of 2025, human error is involved in up to 95% of data breaches. Isolating backup credentials minimizes the risk of accidental exposure.[5]

With NovaBACKUP:

Encrypted Credentials and Controlled Access

When configuring the backup storage in NovaBACKUP, any credentials used to access the backup storage are encrypted and stored within the application, thus not exposed to users or endpoints.

For local storage like a NAS, you can assign a dedicated backup user for all backup operations. NovaBACKUP then stores those credentials in an encrypted format inside its configuration files, ensuring they cannot be accessed or reused by ransomware or unauthorized users.

For NovaBACKUP's integrated cloud storage, credentials are generated and managed exclusively for backup operations. This storage cannot be used for any other purpose, and only the backup agent has access, eliminating unnecessary exposure.

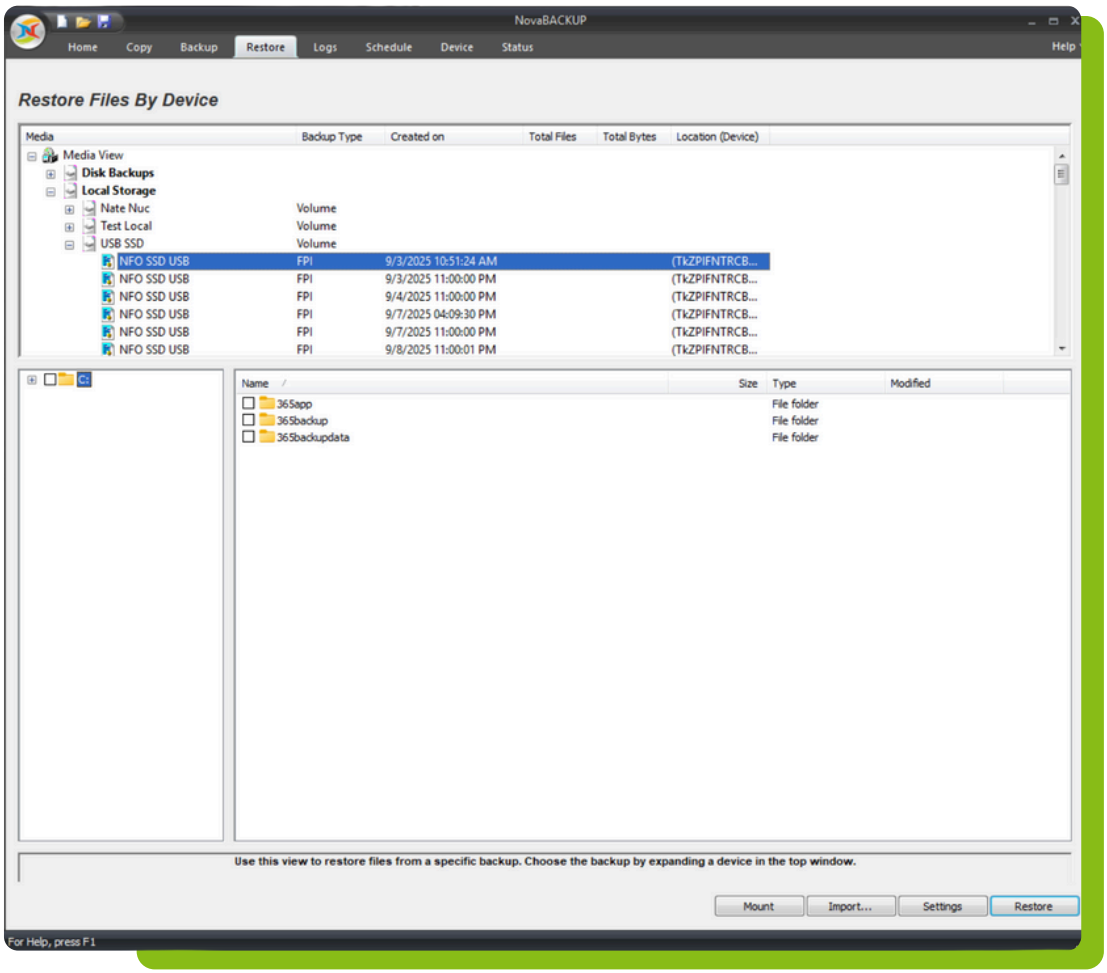
5 Test Restores and Verify Integrity Regularly

A backup is only valuable if it can be restored successfully. That's why regular restore tests are essential to confirm data integrity and measure recovery speed. Don't rely solely on automated verification—errors happen. Always perform manual restore tests alongside automated checks. This also ensures that you and your team then know how a restore would actually work. Finally, don't forget to document your restore procedures so any team member can execute them under pressure.

With NovaBACKUP:

Built-In Verification and Easy Manual Checks

Beyond the built-in verification described in #3, NovaBACKUP lets you mount backups for manual integrity checks. You can browse and verify files without performing a full restore. This feature also allows you to quickly make data accessible, so users can keep working while you restore full systems and networks.



BONUS TIP

Encryption Is Non-Negotiable

While backup encryption won't stop ransomware from locking your backup files, it ensures the data inside remains secure against exfiltration. Always encrypt all your local and cloud backups both at rest and in transit to prevent unauthorized access if files are stolen or intercepted.

FINAL THOUGHTS

To protect your backups against ransomware, backup strategies must evolve. It's not just a single checkbox that makes your backup ransomware resilient. It's a combination of features, strategy, and ongoing maintenance, including regular reviews of configurations, retention policies, and access controls.

Equally important: test restores frequently to verify data integrity and ensure recovery procedures are documented and executable by any team member.

Don't wait for an incident to reveal gaps in your backup isolation or recovery process. Take immediate action and check your backup jobs, confirm your retention and versioning, and validate that both local and cloud backups are protected and recoverable.

Ready to strengthen your backup strategy? Request a NovaBACKUP trial or schedule an expert review of your setup today.

ABOUT NOVABACKUP

NovaBACKUP provides robust hybrid backup solutions designed specifically for small businesses and the MSPs that support them, giving you fast local restores, secure offsite cloud storage, and responsive expert support—all in one easy-to-manage solution.

Schedule a call with one of our backup experts today!

Our Service Promise

We promise to treat the protection and safety of your data like we do our own. Our job it to make data protection as simple and reliable as possible. You can count on us to provide professional, knowledgeable support that meets your data protection needs. Feel free to reach out to our team if you need assistance with your backup and recovery needs.

NovaBACKUP

SOURCES:

1 https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

2 https://www.verizon.com/business/resources/reports/dbir/

3 https://www.sophos.com/en-us/content/state-of-ransomware

4 https://securitybuzz.com/cybersecurity-news/ransomwares-dirty-secret-paying-doesnt-guarantee-recovery/

5 https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

NovaBACKUP
29209 Canwood Street
Agoura Hills, California
91301

Tel.: (805) 579-6700
Fax: (805) 579-6710
M-F 9am-5pm PT

Email: ols@novabackup.com
www.novabackup.com