

# Mitigate the threat of Ransomware with QNAP Snapshots

Ransomware is a threat that cannot be ignored. Recent studies suggest there is a ransomware strike every 10 seconds, with affected businesses and individuals potentially losing critical data (payment of the ransom provides no promise of the data's safe return and is never recommended). Having a well-planned backup strategy is the best foundation of disaster recovery, but what is the best way to protect these backups?



Snapshots are an advanced data protection method that records the state of files and data at the block level. If these files/data are deleted, modified, or tampered with, then their content can easily be reverted back to a previously-recorded state.

## Your NAS must have Snapshot Protection

QNAP have made great strides to empower every QNAP NAS with snapshot protection. With only 1GB RAM needed for snapshot protection on QNAP NAS, there is no excuse for not using snapshots.

TS-1253BU	TS-431X2	TS-228A
Intel Celeron J3455 4-core 1.5 GHz, up to 2.3 GHz	Annapurna Labs AL-314 4-core 1.7 GHz	Realtek RTD1295 4-core 1.4 GHz
4GB/8GB RAM	2GB/8GB RAM	1 GB RAM
256 Snapshot Per Volume/LUN	32/64 Snapshots Per Volume/LUN	16 Snapshots Per Volume/LUN
1024 Snapshots Whole NAS	64/256 Snapshots Number Whole NAS	32 Snapshots Number Whole NAS



# What makes QNAP Snapshots so special?

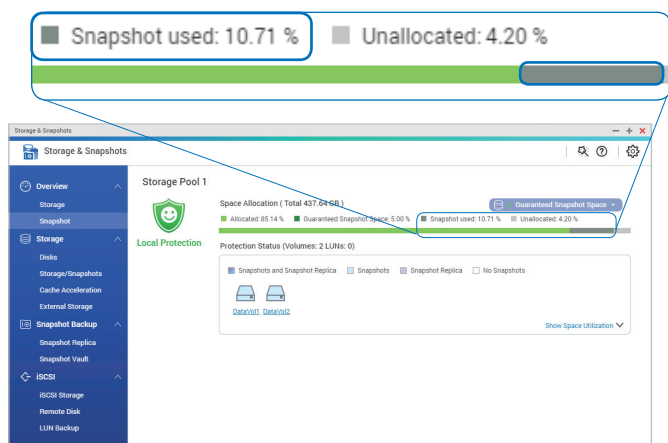
## Negligible impact on NAS performance

Unlike the open-source BTRFS snapshot technology used by competitors, QNAP NAS uses a proprietary ext4-based snapshot technology that enables snapshot protection for both volumes and iSCSI LUN with minimum performance impact.



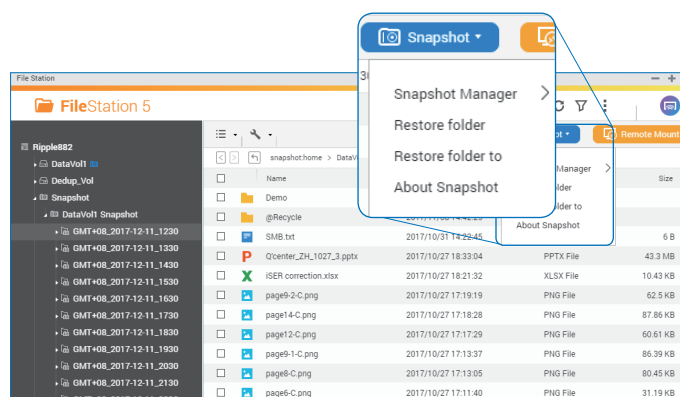
## Easily monitor snapshot space usage with the "Outside of Volume" Snapshot design

QNAP provides easy-to-use management tools to monitor and allocate storage space used by snapshots. This assists in preventing snapshots from affecting NAS storage and application services by using too much storage space.



## Fully integrated with QNAP NAS, user-friendly operation

Snapshots are directly built into the QNAP NAS operating system. The contents of snapshots can be easily viewed, compared, and restored in File Station. Windows users can even integrate them with Windows' "Previous Version" functionality for convenient data recovery.



# Back up Snapshots for Ultimate Disaster Recovery Planning

QNAP NAS provides Snapshot Replica for users to back up snapshots to another QNAP NAS. By utilizing multiple backup plans and a Snapshot Vault on a remote NAS, IT staff can recover snapshot content directly at the remote NAS. As QNAP has made snapshots available to more NAS, it is now ideal to use a high-capacity QNAP NAS to store snapshots from various other QNAP NAS.

## Mitigating the threat of ransomware in 6 easy steps

1. Create a dedicated volume and share folder to store backup files while retaining 20% of unallocated space for snapshots.
2. Use the free QNAP NetBak Replicator for Windows and Time Machine for Mac to regularly back up files to the NAS.
3. Set up a scheduled snapshot for the dedicated volume.
4. If ransomware strikes, immediately remove the connection between the infected computer and NAS.
5. Login to the QNAP NAS and check to see if NAS data has been affected.
6. Browse through the snapshots and revert the whole dedicated volume to its most-recent and uninfected normal version.

## QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAX : +886-2-2641-0555 Email: qnapsales@qnap.com  
Address : 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

QNAP may make changes to specification and product descriptions at any time, without notice.  
Copyright © 2018 QNAP Systems, Inc. All rights reserved.  
QNAP ® and other names of QNAP Products are proprietary marks or registered trademarks of QNAP Systems, Inc.  
Other products and company names mentioned herein are trademarks of their respective holders.



51000-024422-RS  
201801(EN)A