SOLUTION BRIEF

Data Protection Solutions with Acronis Cyber Backup and RDX®

Overland-Tandberg and Acronis provide an easy, fast and flexible backup solution for small and medium businesses.

Acronis Cyber Backup

Small and medium businesses are suffering from lack of regular backups of their critical business data. Very often there are no dedicated IT personnel and office staff available to take care of data management. As office staff have to concentrate on their daily business, backups are either performed rarely or are not done at all.

Because of this, they need easy to use solutions that can be handled by non-IT personnel. RDX and Acronis Cyber Backup are a perfect fit for this environment.

Solution Benefits

- Complete data protection solution with media rotation and off-site storage for SMB environments
- Compliance: enable business to meet regulatory and GDPR requirements
- Future proof: easily scales as your data grows
- Simplicity: easy to install and use
- Security options: protects against virus and ransomware attacks as well as against unauthorized data access

Why backup is important

Businesses data is the most important asset of a company. Data protection is essential in order to continue after a catastrophic data loss event. Data loss could mean the loss of information which can never be recovered or rebuilt. There are endless reasons for data loss or a partial data loss. For example, a ransomware attack could lock your data, a user could accidentally or purposely delete data that is important to continue with your business, and hardware and/or software solutions and updates can cause data loss or delay in business continuity. A good backup strategy is vital for business stability and should be incorporated into every business continuity plan.

Overland-Tandberg RDX

Overland-Tandberg's RDX technology is a removable disk system which simply attaches to laptops, desktops and servers via USB, SATA or iSCSI. It consists of a QuikStor system and a media. RDX is ideal for use in regular office environments. Because of its rugged design, there is no special care necessary. Unlike tape, there is no need for media replacements, maintenance and cleaning.

RDX combines the benefits of tape (like removability) and disk (like random access). This enables RDX to be used in backup scenarios with deduplication and compression features. Removability allows media rotation with off-site storage for full disaster protection.

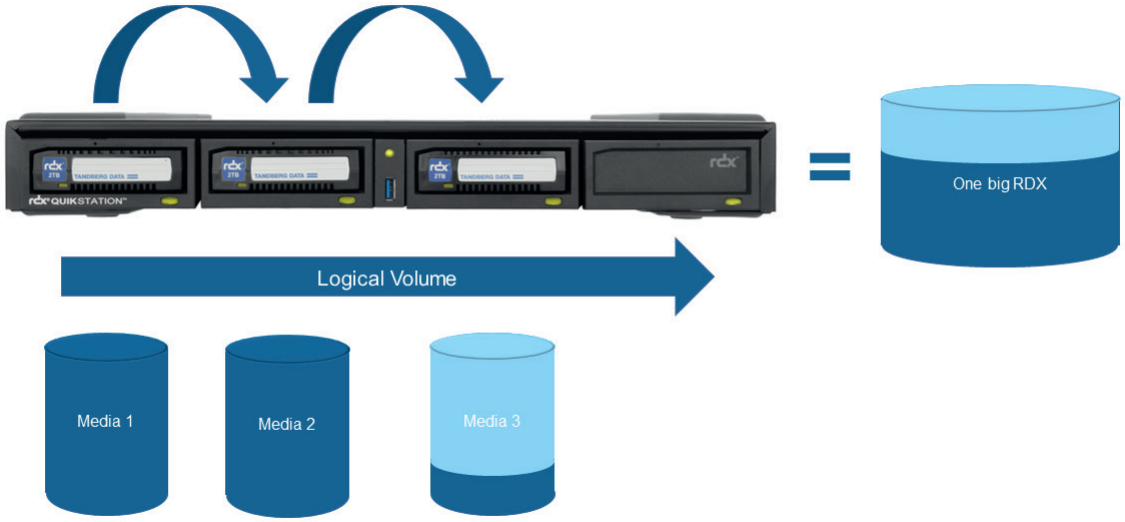
RDX QuikStor systems and RDX QuikStation appliances

Overland-Tandberg's RDX QuikStor single systems are available as external devices with USB 3.0 interface and simply attach to desktops, laptops and servers and are ready for immediate use. The internal RDX systems are available with USB 3.0 or SATA III interface and are ideal for system integrators to offer a comprehensive data protection solution with a built-in removable backup target.

The Overland-Tandberg RDX QuikStation is an iSCSI network-attached removable disk appliance designed to provide a flexible platform for data protection and off-site disaster recovery for physical or virtual SMB and SME environments. The RDX QuikStation family offers two models with either four or eight integrated RDX systems to fit varying capacity and feature requirements.

Providing multiple operation modes for disk, removable disk, tape automation* or a combination* of disk and tape, results in a versatile data protection solution. Building a logical volume by spanning RDX docks together, extends the capacity limitation of one single RDX media volume, but still maintain all RDX benefits of removability and protection of customer's data. The RDX QuikStation can be configured with 1 or 2* logical volumes in either protected or unprotected mode.

* QuikStation 8 only



A logical volume spans the data across multiple RDX media to build one big RDX

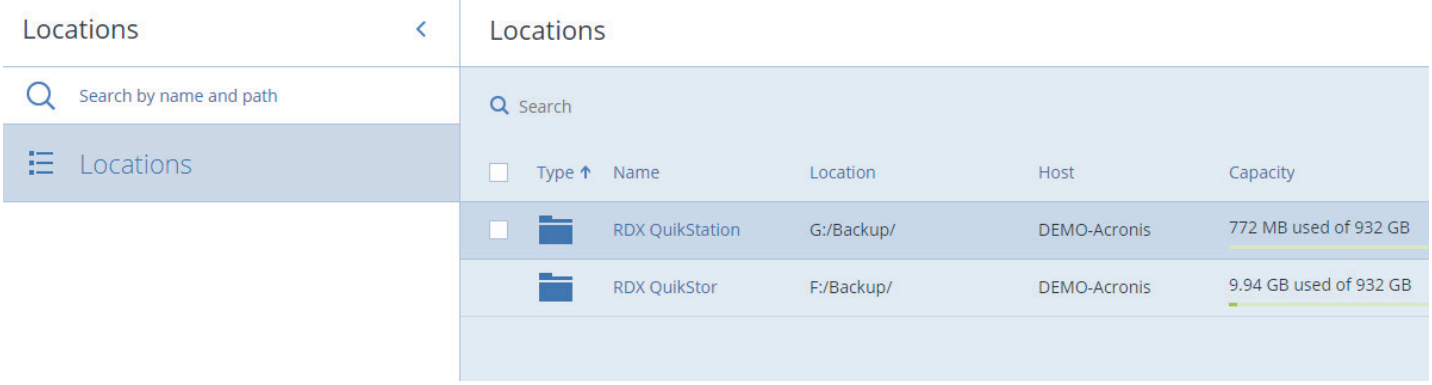
Acronis Cyber Backup

Acronis Cyber Backup is an easy and fast backup solution that protects everything across 21 platforms. With just a few simple steps, backups can be performed to on-premises storage and the Acronis Cloud. Individual files, application data, or a complete system can be recovered in seconds. In case of a system crash, recovery can be performed to bare metal, whether it is the same or dissimilar hardware from different vendors. Windows server can be migrated by recovering an image to the cloud or a virtual environment.

Acronis Cyber Backup allows to store backups in up to five different locations whether on-site or off-site to ensure full disaster protection. It improves IT productivity by restoring folders, files, databases, documents, mailboxes, and individual emails directly from your complete image backup and enjoy granular recovery of Oracle databases, Microsoft Exchange, Microsoft SQL, and Microsoft SharePoint.

RDX integration in Acronis Cyber Backup

RDX removable disk systems and media are fully compatible with Acronis Cyber Backup. The RDX appears as a regular drive letter and can be easily added as a new backup location during the initial setup of Acronis Cyber Backup. This enables RDX to be used as a backup target for backup plans.



Integration of RDX QuikStor and RDX QuikStation as a backup location for Acronis Cyber Backup

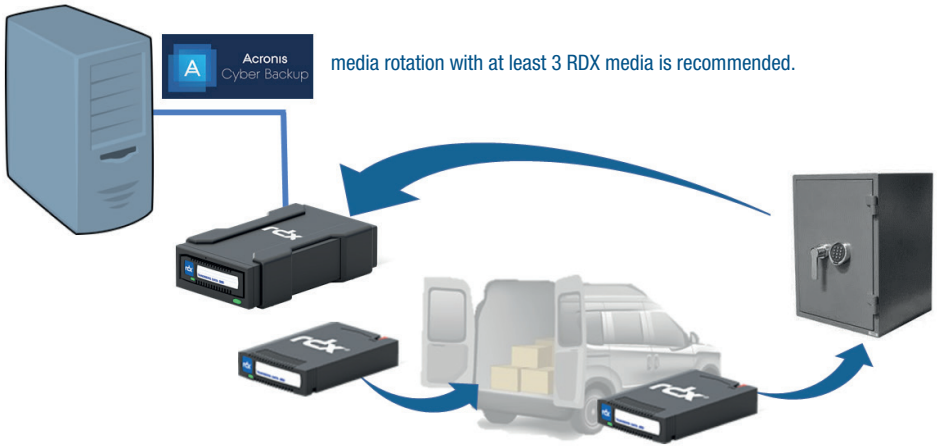
Backup scenario examples

Backup to RDX with media rotation

Backups are usually done to local disks devices or network attached storage (NAS) systems. This might work as long as there are no local disasters or virus and ransomware attacks. Local disasters could also destroy the backup on the local device. Virus and ransomware attacks can infect backup sets regardless of their location on the computer or network.

In both cases, backups should be kept off-site to have at least one copy of the backup accessible to recover from unforeseen events. Therefore, a set of multiple backup media should be used to be sed to rotate the media between the datacenter, being in transit and the off-site location.

Backup software that targets a drive letter can continue with the backup job. The RDX connection keeps the drive letter, regardless of the inserted media. If a new media is inserted, an initial full-backup is performed. Incremental or differential backups will continue on each RDX media according to the desired backup plan.



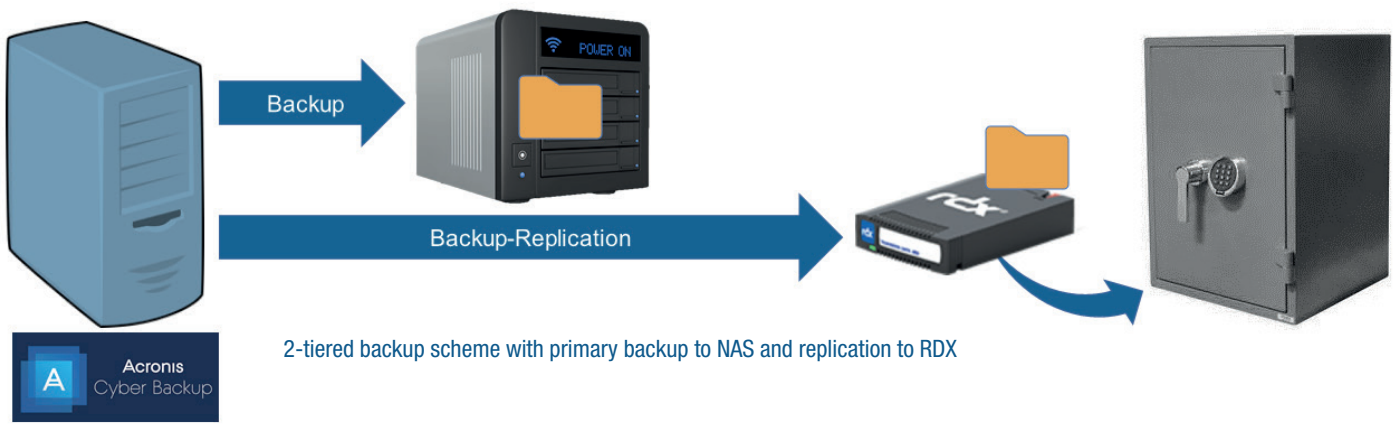
media rotation with at least 3 RDX media is recommended.

2-Tiered backup with NAS and RDX

Backup to Network Attached Storage (NAS) system is very common. Acronis Cyber Backup easily supports NAS systems as a backup target. But users should consider that a backup to NAS is not sufficient in terms of protection against local disasters or virus and ransomware attacks, as they also affect NAS backups.

Therefore, backup to NAS should be supplemented by a backup to the removable media system RDX. A secondary backup copy should be issued by the end of the day or the end of the week to store backup copies off-site for full disaster protection.

Acronis Cyber Backup allows such a backup strategy to be implemented. A primary backup plan to NAS can be created that either performs one daily backup or multiple backups per day according to the requirements of the business. Hereafter, a replication plan copies the backup to RDX for off-site storage. Fast recoveries can be performed from the NAS system. In case of a disaster or malware attack, RDX builds the last line of defense.



2-tiered backup scheme with primary backup to NAS and replication to RDX

Ransomware protection with RDX RansomBlock

In cases where the media cannot be rotated immediately after the backup job has been finished, like multiple backups per day or a backup media that is rotated only once per week or month to reduce the number of media, the backup data is exposed to the risk of being infected by virus or malware attacks.

Overland-Tandberg optionally offers a security software for Windows systems called RDX RansomBlock which protects data on RDX media against virus and ransomware attacks while they are in use for backup. The RansomBlock feature allows only authorized applications, like backup software, to perform modifications to the data, while defending data access from cyber-attacks. It secures backups against virus and ransomware attacks automatically and doesn‘t need any security software updates to ensure full data recovery in case of infected data or blocked computer systems.

Securing backup data kept off-site and meet GDPR requirements

Media stored off-site or media in transit are at risk of being stolen and data might be accessed by an unauthorized person.

There are new regulations being implemented like General Data Protection Regulation (GDPR). GDPR regulates how the personal data of customers, suppliers and employees must be handled, processed and secured in our digitized world to ensure privacy.

Article 23 of GDPR speaks about limiting the access to personal data to only those supporting data processing. In that, data needs to be secured against unauthorized access. Article 32 paragraph 1 describes the security of personal data by using encryption.

In Article 34 paragraph 3 of GDPR the communication of a data breach is described. Data breaches must be communicated immediately, unless the data is encrypted. In this case, no communication needs to take place.

For internal RDX systems with a SATA III interface, Overland-Tandberg offers RDX PowerEncrypt hardware encryption. This can be added to all RDX media. Data written to RDX media is encrypted with AES-256 XTS standards. Data access is restricted to only those having a password key deployed with the RDX Manager software. With this, data is secured at any media rotation stage.

Acronis Cyber Backup and RDX

Acronis Cyber Backup and RDX removable disk systems from Overland-Tandberg build a comprehensive and flexible data protection solution for small and medium businesses. They are easy to install and easy to use and ideal for operation even for non-IT personnel. The removability of RDX offers full protection against local disasters and malware attacks. Further security features can be implemented by additional software like RDX RansomBlock or RDX PowerEncrypt.

SB_v3_jul10_2020