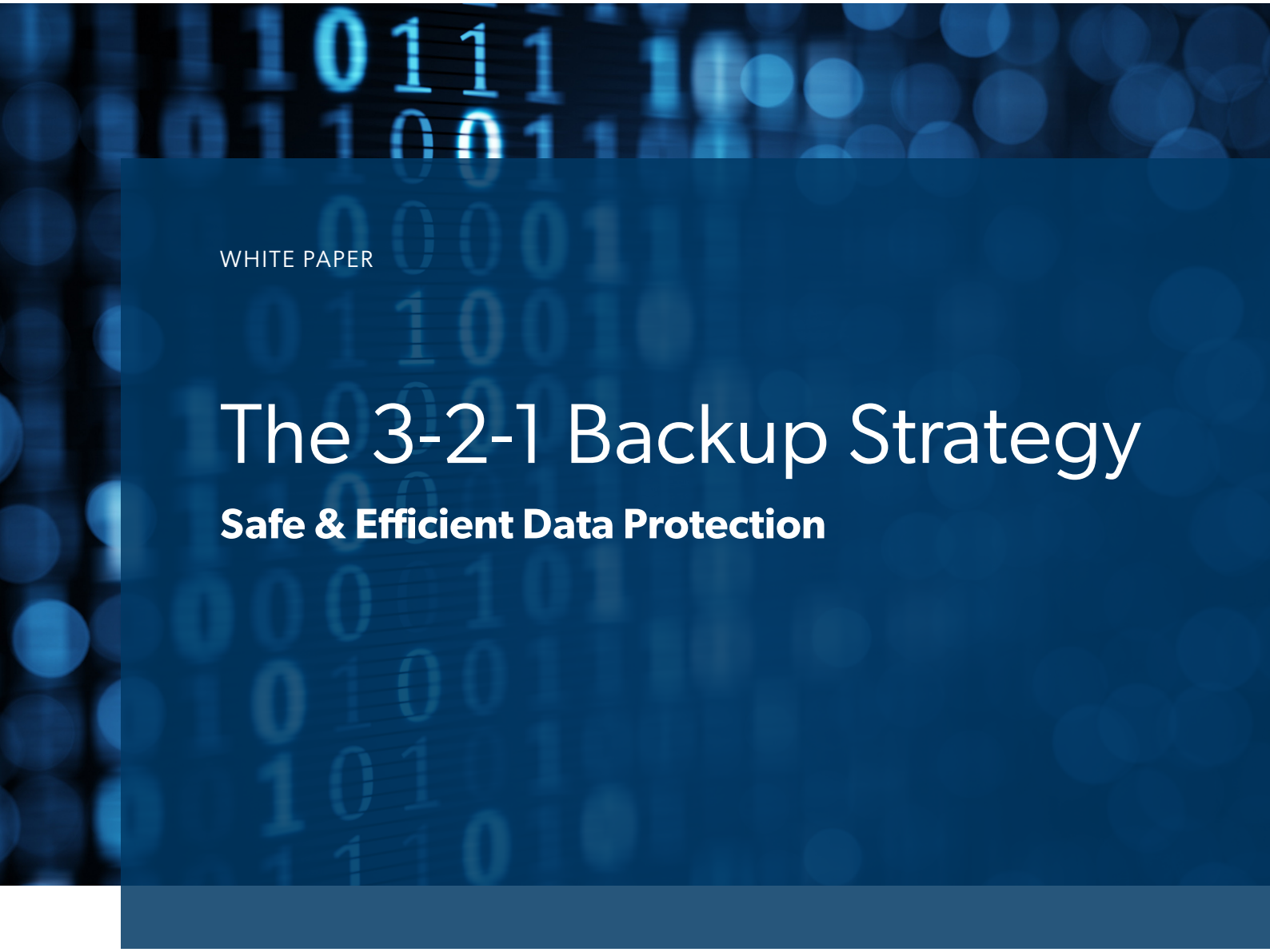


WHITE PAPER

The 3-2-1 Backup Strategy

Safe & Efficient Data Protection

Abstract

Alongside employees, business data is one of the most important assets of a company. Data protection and business continuity is essential for organizations to continue operations 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:

- Local disasters could destroy the backup on your local device
- Ransomware attacks could lock your data
- A user could accidentally, or purposely delete data that is important to continue with your business
- Hardware and/or software solutions and updates can cause data loss or delay in business continuity

This White Paper describes effective methods for how data should be protected to minimize business downtime and outage cost in case of a data loss incident. It shows best practices for small, medium and enterprise environments for implementing a disaster recovery strategy.

Today's threats

Data loss incidents can happen at any time. Whether hardware errors, human errors or viruses and malware attacks or local disasters, businesses must be prepared to establish business continuity and data availability. The following statements show a selection of possible causes and effects of data loss.

Product and technology challenges:

- 21% of all data loss is caused by hardware failures
- 1 out of 3 laptops fail within three years
- 390,000+ malware programs are discovered every day
- Ransomware attacks cause an average of 16.2 days of downtime
- 43% of cyber attacks are aimed at small business, only 14% are prepared to defend themselves

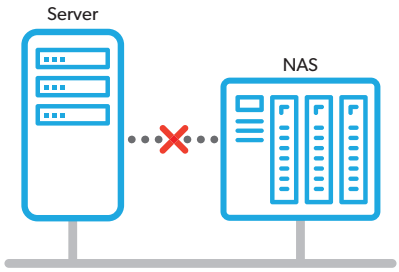
A business that shuts down due to data loss faces a number of consequences. There is a risk of lost sales that affect the balance sheets. Financial obligations can no longer be met, which means higher interest rates, annoys suppliers and banks and limits creditworthiness and claims for damages by third parties. Employees can no longer carry out their tasks. All this can damage the reputation of the business for a long time.

Financial and economic challenges:

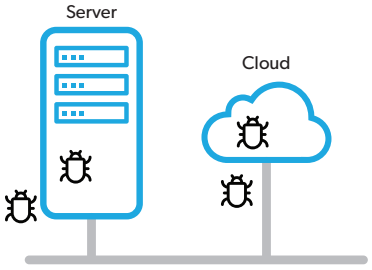
- Small businesses suffer especially hard. 98% are closing after being hacked
- 93% of companies without a disaster recovery plan had closed within one year of a data attack
- 60% of companies close within 6 months of a data loss
- 1 hour of downtime costs:
  - $8,000 for a small company
  - $74,000 for a medium company
  - $700,000 for a large enterprise

The Challenge

Many businesses are not prepared to ensure business continuity. Backups are usually performed on just one storage device, such as local disks devices or network attached storage (NAS) systems or Cloud. This is a viable solution but fails to take into consideration 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 either on the computer or network or Cloud.



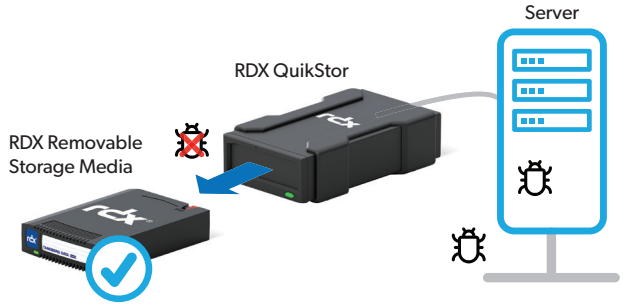
In both cases, it might be impossible to restore the data and recover from these incidents. Perhaps some data can be reconstructed from letters, invoices, or other paper documents. Maybe customers can help to provide lost information, but most of the information is lost.

In case of a ransomware attack, there may be no other choice other than paying the ransom to have the data decrypted. Regardless the cause of the data loss, businesses will suffer in terms of revenue, investments, reputation, trust and loss of customers.

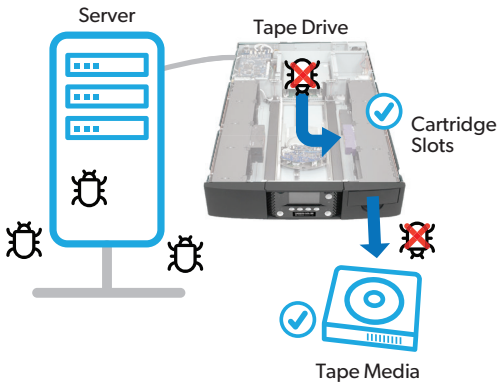
The Solution – Building the Air Gap

When storage devices are no longer connected to the network, the backup data is safe and cannot be threatened by malware attacks. Therefore, businesses should utilise removable storage media. Removable disk systems can detach the storage media from the network to ensure data accessibility after a local disaster or a ransomware attack.

This can be done either by taking the storage device off-line or removing the storage media and transporting it to a safe location outside the campus (off-site). Eject operations can be configured or scripted with most backup software.



The same applies for the data stored on tape. It is protected against virus and ransomware attacks. As the tape format - with the exception of LTFS and object storage - is not a file system, crypto lockers and viruses do not have a chance to infect the data, even if a tape media is in the drive. However, local disasters should also be taken into consideration, where tapes will be destroyed as well. Therefore, tapes should also be stored off-site outside the datacentre. When tape libraries with hundreds or thousands of tape media are used, they should be located in a separate datacentre or archive facility.



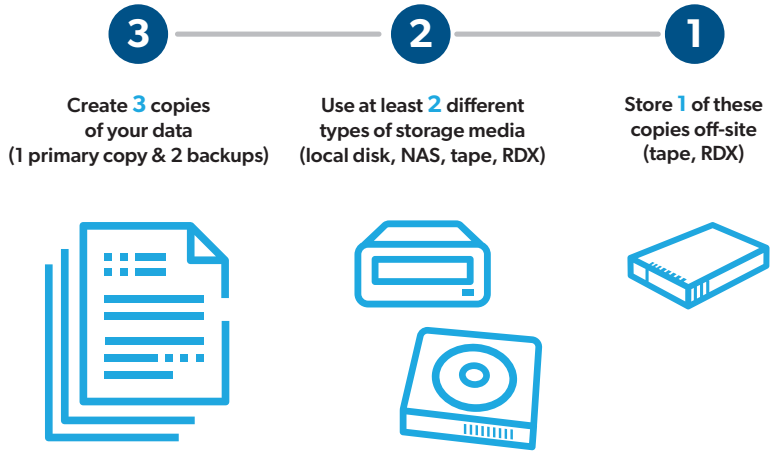
The 3-2-1 Backup Strategy

Whether your business is in the SMB environment or a large enterprise, you should implement the 3-2-1 backup strategy, which means to keep three copies of your data on two different media and store one copy off-site.

Almost all backup applications enable you to perform a copy job or additional backup jobs after the primary backup job is finished. Usually, companies use disk, either NAS, DAS or SAN as a primary backup target. This ensures fast restore in case of a data loss. It provides short downtime and rapid return to business.

For the secondary backup target, a storage system with another media type should be implemented. If the primary media – disk in this case – fails, the other media is still available for recovery tasks. Depending on the amount of data, tape or RDX should be used. If companies have to backup a large amount of data, tape autoloaders or tape libraries are best practice. They allow full automation and media handling for fast recovery.

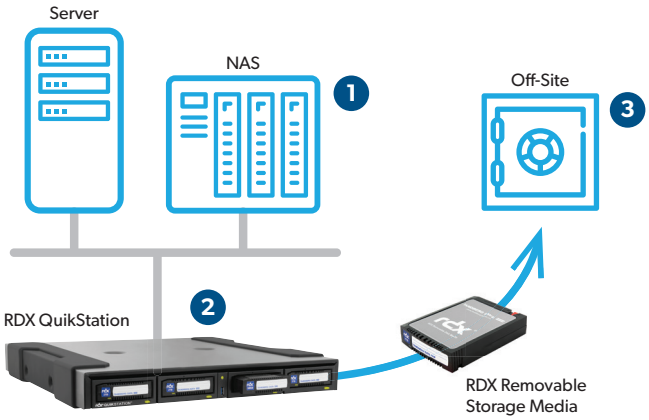
The tertiary backup target must be a removable storage media device. This media should be placed off-site at a save location and builds the last line of defence, in case of a local disaster where the primary and secondary backup is not available any more or in case of a virus or ransomware attack, which makes these backup unusable. For the tertiary backup, tape or RDX are the recommended choice.



Solutions for Secondary and Tertiary Backup

RDX® QuikStation®

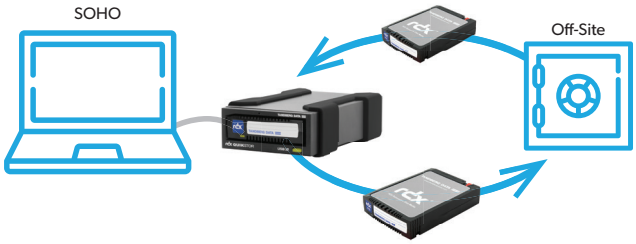
The RDX QuikStation is an iSCSI attached removable disk appliance designed to provide a flexible platform for hybrid cloud data protection and off-site disaster recovery for physical or virtual environments. It provides multiple configurations from single disk targets, disk autoloader to tape autoloader and tape library emulations and logical volumes across all RDX targets with RAID 5 or RAID 6 fault tolerance. As RDX QuikStation includes hard-disk based media, it offers the same performance advantages as the primary backup target on the secondary side.



Due to its removable media design, QuikStation can also play the role of the tertiary backup device. A backup copy to a second RDX media can be ejected and placed off-site after the backup job is finished.

RDX® QuikStor®

The RDX QuikStor is a removable disk system, which easily integrates into most environments and applications. As a tertiary backup repository, it complements the 3-2-1 backup strategy with off-site storage for medium businesses.



For smaller environments, with single server infrastructure, laptop users or single NAS implementations which cannot afford multiple storage systems, a media rotation scheme with RDX QuikStor and three RDX media is the best solution. This depicts the 3-2-1 backup strategy in a simple way:

- One media is in the office, ready for the next backup job
- A second media is off-site at a safe location
- The third one is in transit to or from the off-site location

Using media rotation enables you to alternate the media after the backup has finished. For media rotation it is very convenient if the media is ejected after the backup job is completed. For that, most backup software offer a built-in media eject or allow integration of pre- and post-scripts commands during the configuration of backup jobs, which initiate a media eject.

NEO Series® Tape Products

Overland-Tandberg standalone LTO tape drives and NEO Series automated tape libraries are based on 30+ years of expertise in high-capacity data storage. Reduced cost of ownership, improved data availability, improved reliability, ease of data management and protection from viruses are the foundation of the NEO platform. The NEO family of tape and tape automation products are excellent for use as a secondary and tertiary backup target. With LTO tape technology, the NEO tape products are recognized as the standard for final data protection processes.

As a secondary backup target, the NEO tape libraries offer automated backup processing on a second media beside disk. As already mentioned, backups are already protected against crypto lockers and viruses even if an LTO tape media resides in the drive. To build the final stage of the 3-2-1 backup strategy, a third backup copy should be created on a second LTO media which should be ejected after the backup is complete to store off-site.

The NEO products should be integrated into the 3-2-1 backup strategy especially in environments with high capacities and enterprise environments. The scalability in capacity and performance satisfies the requirements of future adaption.

Conclusion

Ensuring Business Continuity is the most important task for companies of any size. Data loss and business downtime results in financial loss and even leads to business closure.

The 3-2-1 backup concept has established itself as one of the safest and most proven backup methods to be protected against hardware failures and malware intrusion. If your company is a SOHO or small SMB, media rotation is a necessity.

Sales and support for Overland-Tandberg products and solutions are available in over 100 countries. Contact us today at salesemea@overlandtandberg.com. Visit OverlandTandberg.com.