WHITE PAPER

Backup and Restore Strategies with Off-Site Capabilities

How to identify the appropriate life insurance for your data

At home, you safeguard against incidents to protect your family, your life, your property – everything that is valuable to you. You buy insurance to have peace of mind. But, what about your data? Data is the most valuable asset of your company. Is it safeguarded? If not, consider a tailored insurance which covers your requirements for protecting your data.

Analyzing your data

What are my requirements? At home, you might have insurance for different assets, and some are more relevant than others. This also applies for your data. Some of them are business critical, others are rarely accessed. Ask yourself: Where does my data reside, is it stored locally or in the Cloud? Most importantly ask: How long can I continue without it and how much will it cost me if it is lost?

Analyzing possible incidents

To find the right insurance for your data, you need to be aware of the threats in your environment. Hardware failures are responsible for data loss and human errors are also a threat. Nowadays, data corruption due to virus and ransomware attacks ranges in the top three reasons for data loss. Also, analyze your environment for possible incidents such as floods, earthquakes or tornadoes, and consider unforeseen events like fire or water damage.

Cost considerations

After analyzing your data and possible threats, next look at the cost of possible data insurances. For example, Cloud might offer an affordable entry level price point, but cost increases dependent on capacity and retention time. Tape might be the most cost-efficient solution for big data. Consider initial costs, but also perform a TCO analysis for long term cost.

Checking your environment

We learned that selecting the right insurance is dependent on data importance and cost. In addition, you should consider your amount of data regardless of the size of your business. Finally, you should take a look at your IT environment. Does your business consist of laptop users or do you utilize servers? Do you operate physical or virtual environments or a mix? Do you have multiple locations or branches?

Choosing the right software

The first step to choosing the right insurance for your data is the selecting the appropriate backup software. According to your needs, you should ask some of the following questions:

- **Does this backup software support my entire IT environment?**
  (Physical, virtual, servers, desktops, branches, home office users, etc.)
- **Does this backup software support multiple backup jobs?**
  (You can define separate jobs for more important and less important data)
- **Can I perform backup copies to a second backup target?**
  (Have an additional backup copy on another media, removable media is preferred)
- **Does this backup software support media rotation?**
  (With this, SOHOs and small SMBs are able to implement a full disaster protection strategy)
- **Does this backup software support backup to the Cloud?**
  (Cloud is ideal for weekly and monthly backups as a supplement for local backups)

The 3-2-1-1 backup strategy

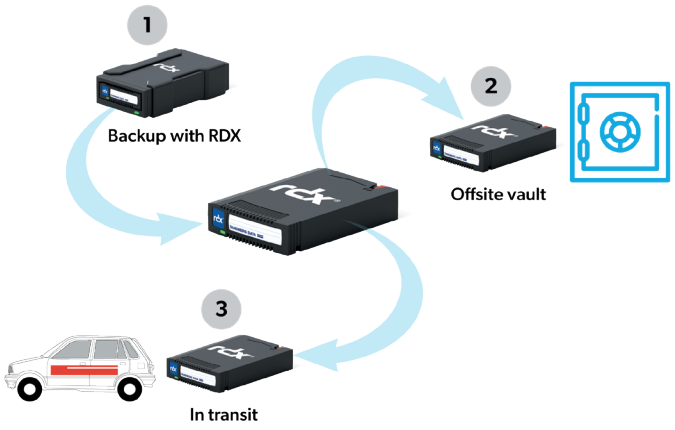
Whether your business is in the SMB environment or your company is a large enterprise, you should implement a 3-2-1-1 backup strategy, which means to create three copies of your data on two different media, store one copy off-site and create one immutable copy.

Almost all backup applications enable you to perform a copy job of the backup after the primary backup job is finished. You should plan to utilize two different media: one media for primary backup and another one as a secondary backup target. If one media fails, the other media is still available for recovery tasks. As a primary backup target, disk is the best choice. In addition, another copy should be stored on a removable media to place this copy off-site. This ensures the ability to perform a full data recovery in case of a disaster at the business site. An immutable copy, like WORM, protects your backup from malware and ransomware attacks.

Media rotation

For smaller environments with single server infrastructure, laptop users or single NAS implementations, media rotation is an ideal method to be fully protected against data loss due to a disaster.

Media rotation is building an Air-Gap between storage devices and the network; the backup data is safe and cannot be threatened by malware attacks. In this case, a single backup target with removable media, like RDX, should be implemented. Using multiple media enables you to alternate the media after the backup has finished. As media can be ejected manually, most backup applications allow ejecting the media when backup is complete.



Backup and NAS

Most NAS systems offer a built-in backup application which is able to perform a backup to an external device which is connected via USB3.0. In this case, RDX QuikStor® is the ideal solution. In conjunction with media rotation, RDX offers full disaster protection with off-site storage capabilities.

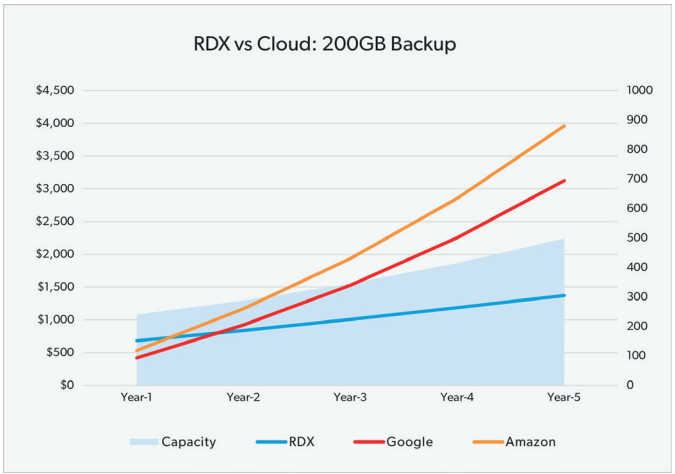
If using a NAS system as a backup device, you should complete this solution by adding a secondary backup target. Consider media like RDX or tape to overcome failures of the primary backup target.

Backup and Cloud

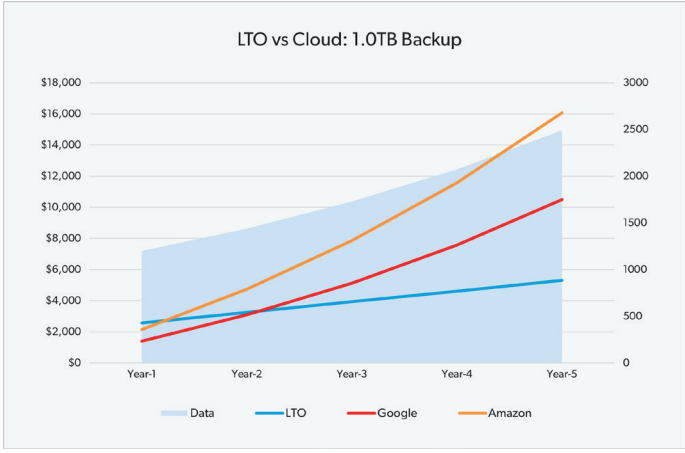
Backup to Cloud is now more popular than ever. SMBs especially are using this option to protect their data in the public Cloud. The advantage is that backups are stored off-site and are available even in case of a disaster at the primary location. Users can implement the off-site part of the 3-2-1-1 backup strategy. But you should not only rely on Cloud backup alone. If you have a total breakdown, your network might be broken too. In addition, take a look at your bandwidth. Is your network strong enough to get your data back?

Furthermore, consider the cost of a backup to Cloud solution. Many Cloud providers attract with low entry level fees. This might be less expensive as the deployment of a local hardware-based solution, but if data is growing, the price increases rapidly, and you will reach the break even point pretty fast. Also, most Cloud providers charge a fee for accessing data. These costs must be included in your TCO calculation as well.

Backup to Cloud is a good solution for keeping data copies off-site. Backup to Cloud protects your data against any event which could happen at your data center. In addition, Cloud protects your data against virus and ransomware attacks. Cloud is recommended for weekly and monthly backups. It can also
be used for daily backups as a supplement
for local backups. Local backups ensure full restore capabilities even if the network connection to the Cloud has failed. If network bandwidth is a problem, local backups allow fast restores and enable you to be back in business much earlier.



Cost comparison: RDX vs Cloud



Cost comparison: LTO vs Cloud

Think about restore, then plan your backup

Before you plan your backup strategy, think about the importance of your data. As previously mentioned, data should be analyzed according to the importance of your business. Ask the following questions:

- What is the maximum downtime my business can tolerate?
- What is the maximum amount of data loss my business can tolerate?
- Which data do I need first?
- Which data can be restored afterward?

Local backups ensure fast restores and reduce business downtime. Local backups should be done to disk, like NAS or RDX. In case of RDX, label your media to pick the right cartridge in case of a restore. The local backup should also include the system information and applications.

Business continuity

In many cases, companies cannot afford any downtime. Whether they provide their total IT infrastructure over the private Cloud to their employees and third parties or if they offer online services to their customers, every minute of downtime might cost thousands of dollars. In worst case, these companies won't be able to recover from this downtime.

These companies would benefit from implementing a business continuity solution by deploying a second disk system at a remote location, either inside or outside their campus. As an ideal solution, nearly all NAS systems provide a replication feature which continuously copies data to a second system at the remote location.

Use cases and recommendations

SOHO and small SMBs

Most SOHO or small SMB environments don't perform backups at all. They are not aware that losing data might result in losing business. Windows and Mac users can benefit from backup applications built into the operating system. Windows Backup and Time Machine offer scheduled backups to removable disk like RDX QuikStor with the capability of media rotation for full disaster protection with off-site storage.

RDX QuikStor attached to laptop

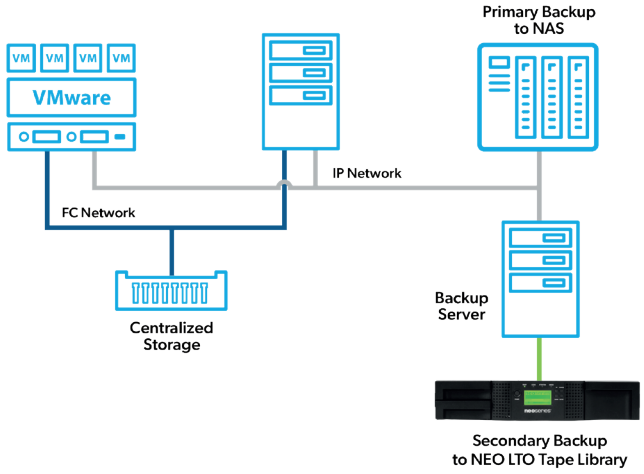
NAS users should utilize the integrated backup app of their systems. Most NAS vendors offer scheduled backups to RDX QuikStor with media rotation.

RDX QuikStor attached to NAS

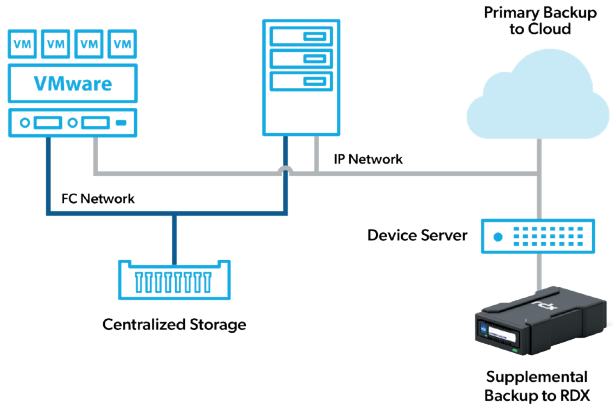
Midrange to large SMBs

Most SMBs only use one backup target which is mainly disk. To implement 3-2-1-1 backup strategy, they should implement a secondary backup to tape or Cloud. The primary backup to NAS systems ensures fast backups and restores.

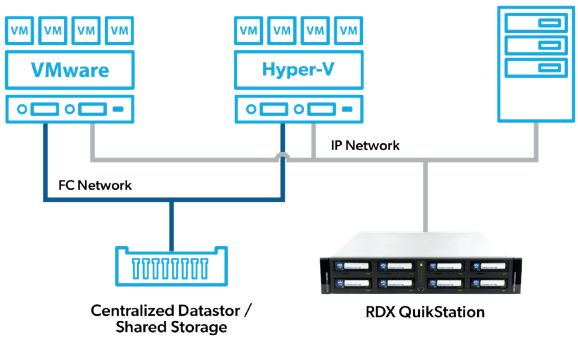
A secondary backup to removable media like RDX or NEO tape automation products ensures full disaster protection with off-site storage.



Companies should not rely on backup to Cloud implementations. A supplemental backup to NAS or networked RDX is important to be protected against network breakdowns and slow network bandwidth. Important business data should reside on a local backup device to speed up restore operations and back to business.



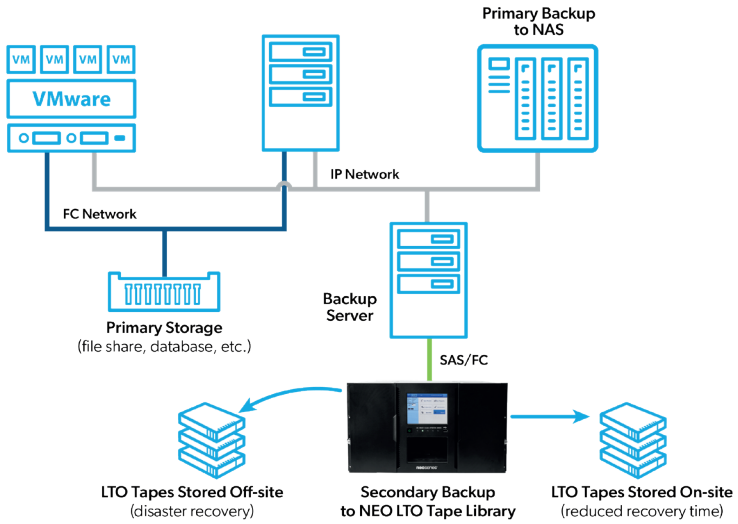
RDX QuikStation® is the ideal device for virtual environments. It provides easy integration with iSCSI connectivity. So VMs can utilize their own RDX device for individual applications. Multiple operational modes allow backup to disk and backup to removable disk/tape in one system.



Enterprises

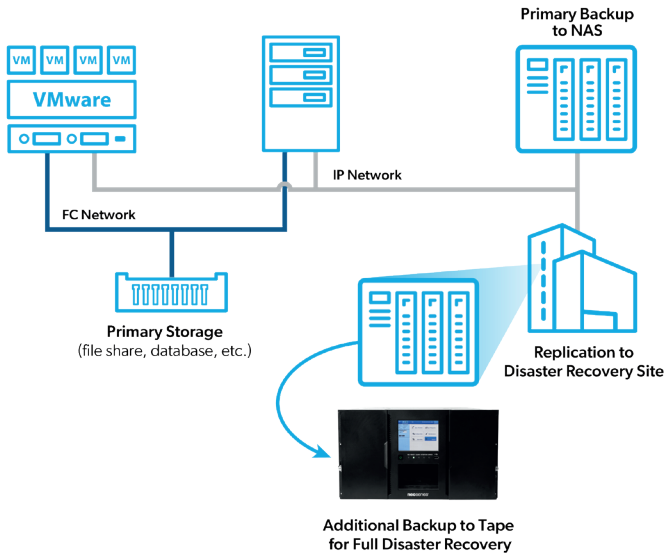
Larger companies should think about their data protection environment in terms of restore as well. What is the maximum business downtime they can afford? They should consider the 3-2-1-1 backup strategy.

Primary backup to a NAS server ensures fast backups and restores and are available at different capacity points. Secondary backup to NEO LTO tape libraries ensures full disaster protection with off-line and off-site storage.



Most enterprises have to provide 24/7 data and application availability. In this case, business continuity must be ensured by implementing a secondary data center. Most NAS systems provide continuous replication between remote locations and offers data availability in case of a disaster at the primary location.

But even here, Tape should be added to the backup concept as virus/malware could be replicated and destroy also the replica backup at the remote site.



Ransomware Protection

An effective protection against virus and ransomware attacks is to store data off-site and keep it outside the network, which can be done perfectly with our LTO based NEO or RDX product lines. However, during backups, or if backups of business-critical data are performed continuously or frequently during the day, there might not be an opportunity to place the RDX backup media off-site or offline. 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.

To tackle this problem for RDX solutions, users should consider 3rd party backup-solutions which offer inside ransomware protection.

Conclusion

Business data is the crown jewel of a company. Losing data will result in losing business. Before implementing a backup solution, analyze your data, your IT and your natural environment. Consider all incidents which could happen, including human errors, hardware failures, virus and ransomware attacks as well as natural disasters. Get an idea on which data must be recovered first in case of a disaster. This will shorten downtime and get you back to business much faster.

Implement the 3-2-1-1 backup strategy to be protected against hardware failures and malware intrusion. If your company is a SOHO or small SMB, use media rotation. Watch costs and availability especially if you plan to use cloud backup and be aware of which backups you put in the cloud. Combine it with an on-premise backup solution for your daily restore tasks.

Last, but not least, perform restore tests and practice the disaster recovery process, get prepared and be ready for any data recovery tasks to keep your business alive and ensure business continuity.

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

WP_v5_jul18_2022