Overland Tandberg

WHITE PAPER

The Last Line of Defense

Building effective business continuity solutions

December 13, 2023

Background

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
- 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

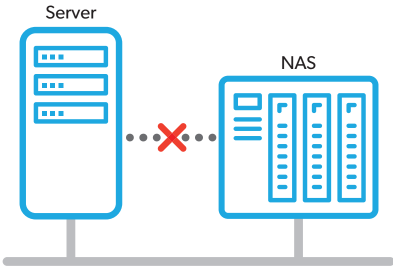
A business shutdown due to data loss faces a number of consequences. There is a risk of lost sales that affect the balance sheets. Financial obligations can no longer be met, which means higher interest rates and claims for damages by third parties. Employees can no longer carry out their tasks and are therefore in default.

It can also damage reputation. Delays in assisting clients may cause them to switch to the competition. The temporary liquidity shortage annoys suppliers and banks and limits creditworthiness.

Here are some financial and economic challenges:

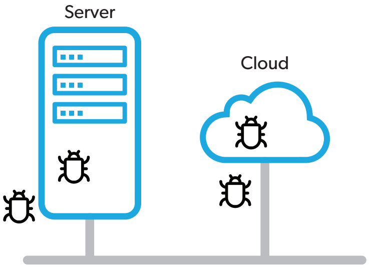
- 1 hour of downtime costs small businesses $100k – Gartner
- Cyber attack incident costs businesses of all sizes $200k – Hiscox Business Insurance
- 98% of small businesses close after being hacked
- 60% of companies close within 6 months of a data loss

The Problem



Many businesses are not prepared to ensure business continuity. Backups are usually performed on 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. However, businesses will suffer in terms of revenue, investments, reputation, trust and loss of customers.

The Solution – Building the Last Line of Defence

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.

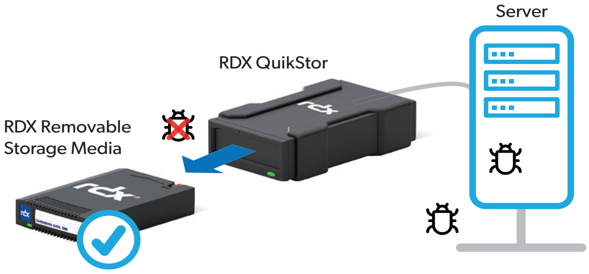
This can be done either by setting the storage device off-line or removing the storage media and transporting it to a safe location outside the campus (off-site). Eject operations can be configured or scripted with most backup software.

The same applies for the data stored on tape. A tape media in a cartridge slot secures data written on it.

The RDX® Technology

RDX is a proprietary removable disk technology owned by Overland-Tandberg. It consists of removable disk systems and removable disk appliances. The tough, rugged design provides a reliable and valuable data repository. The portability makes it ideal for off-site disconnected storage to build the Air Gap for disaster recovery and ransomware protection.

The **RDX QuikStor** is the ideal solution for remote/home office users and branch offices as well as SMB environments. Due to the removable data cartridge,

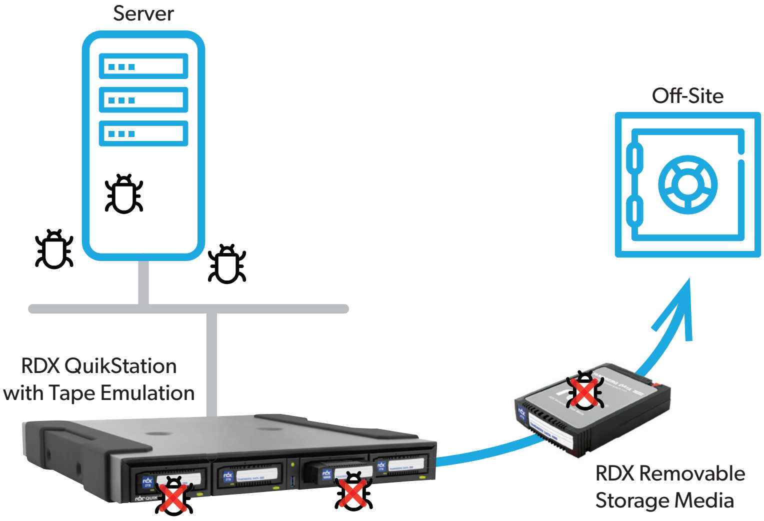


an air gap is built and backups can be stored off-line and off-site and are securely protected against ransomware attacks.

We recommend establishing a media rotation scheme with at least three data cartridges, where one cartridge is off-site, one is in transit and one on the QuikStor system, ready for the next backup.

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, logical volumes across all RDX, disk autoloader, tape autoloader and tape library emulations.

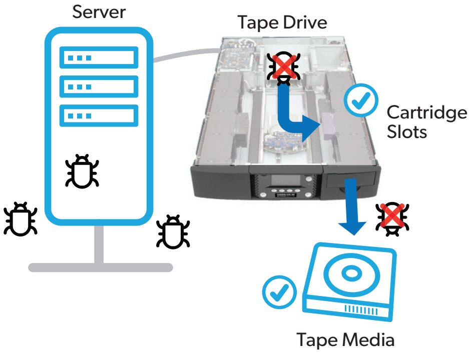
The disk modes provide the same functionality as described in the QuikStor section. When put in disk autoloader mode, only one cartridge is physically assigned to a RDX dock, the others are air gapped as they reside in a logical disk slot. In tape automation emulation modes, the media is treated as a LTO-tape and offers full virus and ransomware protection.



However, local disasters should also be taken into consideration, where media will be destroyed as well. Therefore, the RDX media should also be stored off-site outside the datacentre.

The NEO® Tape Libraries

Overland-Tandberg's LTO tape and LTO tape automation systems are based on 40 years of expertise in high-capacity data storage. Utilising industry leading LTO tape technology, the NEO Series tape family provides reduced cost of ownership, improved data availability, improved reliability, ease of data management and protection from cyber-attacks.



Overland-Tandberg offers tape solutions for every use case and business size. Starting with a stand-alone tape drive to autoloaders and small libraries to scalable tape-libraries of the NEOxl family, every request on capacity and performance will be covered.

The cartridge slots and I/O-ports of Overland-Tandberg's tape autoloaders and tape libraries build an air gap by providing off-line and off-site storage capabilities. As long as a LTO tape media resides in a cartridge slot or even outside the tape system, ransomware has no chance to harm the data.

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.

Building a last line of defence using removable media is essential for keeping businesses running and eliminate downtime. Removable media storage systems like Overland-Tandberg's RDX and NEO tape library solutions ensure accessibility of your data after an attack.

We are recommending to regularly perform a backup and store them even off-site to be not only protected against malware attacks but also against local disasters.

Further Information

If our White Paper has not answered all your questions about your backup challenges, Overland-Tandberg storage specialists are available globally to offer you help in finding the best solution for your business. Visit our contacts page to reach out to a specialist in your region.

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.