RDX Removable Disk in the Public Sector

Easy to use backup solutions for municipalities

USE CASE

Most municipalities consist of small offices and remote departments, like administrative services, education facilities, citizen office, building department or car registration. Beside paper forms, most of the information and data generated in these departments are held in digitised format, which results in a rapid data growth.

Backup challenge for distributed infrastructure

Securing all these data is essential. Because of the distributed infrastructure, it is often difficult to gather all data from the different offices and consolidate them into one backup source. In addition, network bandwidth could be an issue to be able to transfer backup data in an adequate timeframe. Modernising existing network infrastructures could be very cost-intensive, so alternative data security strategies must be found.

RDX takes on this challenge

The RDX removable disk systems fit ideally into these environments. The RDX family provides easy to use standalone RDX QuikStor drives for use in smaller offices and remote departments and RDX QuikStation appliances for centralized data storage. As an additional advantage, RDX is both easy to use and integrate as most public institutions do not have dedicated IT staff.

The rugged design of the RDX media provides shock and drop resistance and is ideal for secure data transportation by mail or courier services. This overcomes network bandwidth limitations and easily enables data seeding of remote office data to the central data storage repository.

Challenges

- Sensitive citizen data needs to be protected and secured
- Distributed infrastructures make data management difficult
- Lack of IT skills makes daily data backup tasks a nightmare
- Limited network bandwidth complicates data transfer
- Data and system protection against ransomware attacks for business continuity
- No backup automation
- Backup islands make backup data consolidation impossible

Benefits

- Data protection against data loss as well as virus and ransomware attacks
- Easy to install and easy to use
- Reliable and affordable
- Rugged design, no special care needed
- One storage technology for data protection across all offices and departments
- Long-term data retention

The right solution for every location

To satisfy the different requirements of each department and office, dedicated elements of the RDX family of removable disk systems can be implemented. Smaller offices and remote locations are equipped with the RDX QuikStor drive. This device easily connects via USB 3.0 or SATA III (internal version) into servers, desktops or laptops. Here, local backups are performed for each remote location. For the main or the central office, RDX QuikStation is implemented. With its iSCSI connectivity, it easily integrates into existing network infrastructures and both physical and virtual environments. Different operational modes allow flexible utilization of the RDX QuikStation. Tape automation modes* even allow easy replacement of existing legacy tape systems.

* QuikStation 8 only

Customer benefits

- Business continuity and security
- Seamless integration into existing environments, no change in workflow
- Affordable and low TCO – fits almost any budget
- Overcomes data transfer problems due to network bandwidth limitations
- High transfer rates and instant data access
- Flexible scalability with various media capacities, unlimited off-site capacity
- No compatibility issues and future proof due to full forward and backward compatibility of drives and media

3-2-1 backup and media rotation

For maximum data security, it is important to keep off-site copies of the backup data. According to the 3-2-1 backup strategy, 3 copies of backup data are held on 2 different media where 1 copy is stored off-site with media rotation implemented. This provides protection against local disasters and virus or ransomware attacks.

At remote departments and small offices, RDX media is rotated between the remote location and the central office, where the backup data is incorporated into the central backup set. For media rotation, at least three pieces of media are used, to ensure that one media is at the remote location, one media at the central location and another media is on transit to or from the remote location.

Two-tiered backup

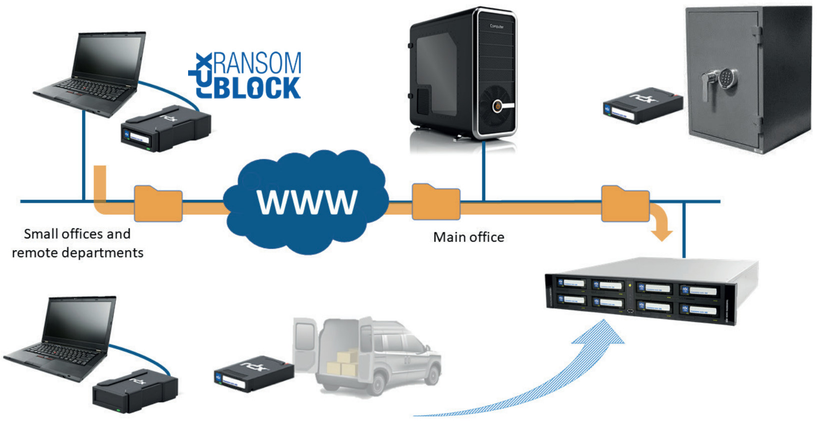
If network bandwidth is not an issue at remote sites, a two-tiered backup approach can be implemented. In this case, a primary backup job saves the data to the local RDX QuikStor drive. Hereafter, a secondary job - mostly replication job - transfers the backup data to the centrally installed RDX QuikStation over the network. So, two copies exist on two sites for maximum protection.

A two-tiered backup strategy can also be implemented at the main office with QuikStation. In this case, a backup replication job is performed to a second RDX media in the QuikStation. This replica should then be rotated as described above.

Security considerations

Ransomware has emerged as the most dangerous cyber threat for all organisations. Ransomware is a type of malicious software that blocks access to the victim's data until a ransom is paid. After a ransomware attack, system might be locked, or the files encrypted, deleted or inaccessible. A distributed environment is one good solution to protect against these attacks, as not all systems will be harmed at a time. In case of an incident, several departments are still able to work.

If a remote department or remote office has been infected, the local backup helps to recover from such an attack in a short timeframe. But as malware is also affecting backups, media rotation or the 3-2-1 backup strategy needs to be implemented, because at least one media copy was off-site during the malware attack and can be used for total system restore without the need of paying ransom.



In environments, where off-site vaulting of backups is not always possible, e.g. because of lack of personal or multiple backup runs per day, backups are threatened as well. In this case, **RDX RansomBlock*** should be introduced, to protect data stored on RDX as it allows only authorized applications, like backup software, to perform modifications to the data, while defending data access from cyber-attacks. RDX RansomBlock doesn't need any security software updates and ensures full data recovery in case of infected data or blocked computer systems.

* optional feature, separate software licence required

Sales and support for Overland-Tandberg products and solutions are available in over 90 countries.
Contact us today at salesemea@overlandtandberg.com

UC_v2_nov25_2019