# Networked RDX Systems in sensitive environments

## Utilising removable storage while maintaining security regulations


Many companies are introducing security regulations that prohibit the connecting of external storage devices, such as USB hard drives and memory sticks, to company laptops, desktops or servers, to avoid virus infection or malware attacks.

## Ward off threats

USB peripherals have become an attractive tool for launching cyber-attacks. Uncontrolled use of external storage devices threaten sensitive company information or result in blocking computer systems which can paralyze the whole business. Therefore, local attached storage devices are not accepted, and administrators block USB ports at laptops, desktops or servers.

## Off-site storage is essential

However, many companies do not want to overlook removable storage because they need to store data off-site for compliance and data protection reasons.

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 prevents against virus or ransomware attacks.

Legal regulations prescribe the retention of data over a longer period of time. This data should also be stored in a remote location.

## The networked RDX solution

As an established standard, with attributes beyond other simple data storage products, RDX is the trusted removable disk technology. The tough, armoured design provides a reliable and valuable data repository. On the go capability makes it ideal for off-site disconnected storage for disaster recovery, and builds the lifeline for all business data.

### Challenges

- USB ports are disabled due to security reasons
- Businesses need removable storage for off-site compliance and data protection reasons
- Companies need a cost-effective and secure data protection solution
- Backups need to be protected against virus and ransomware attacks

### Benefits

- Easy to install and easy to use
- No special care required
- Offers protection against virus and ransomware attacks
- Transparent integration into backup and archive applications
- Provides full disaster protection for sensitive data with off-site copies
- Offers WORM for compliant data archiving as well as backup for disaster recovery using one technology
- Flexible scalability with various media capacities plus unlimited off-site capacity

## Customer benefits

- Removability for data security and to meet compliance requirements
- Seamless integration into existing environments; no change in workflow
- Off-site storage capabilities with full data access protection
- Affordable and low TCO
- Meets compliance requirements for electronically stored data
- Ease of use
- No compatibility issues and future-proof due to full forward and backward compatibility

The network connected RDX solution offers greater flexibility. The device easily integrates into the existing ethernet environment and offers extended usability, independently from connectivity limitations of USB ports. It provides removable storage over the network and ensures normal data backup and restore operation as well as full data protection in case of either disaster or virus and ransomware attacks. RDX is an essential component for every business continuity strategy in either a virtual, physical or hybrid IT infrastructure.

## Enhanced security with RDX RansomBlock*

RDX creates the Air-Gap between the network and the storage device. When storage devices are disconnected from the network, backup data is safe and cannot be threatened by malware attacks.

However, in some cases, the RDX media cannot be ejected after a backup job has finished. Often, companies perform multiple backups per day because they can not afford to lose data over a dedicated period of time. So, the RDX media stays inserted and the backup data is at risk.

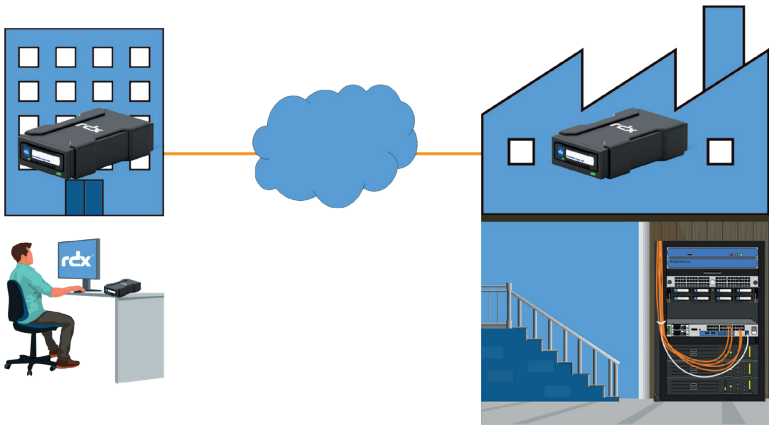
In this case, RDX RansomBlock should be introduced to protect data stored on RDX while online. RansomBlock allows only authorized applications, like backup software, to perform modifications to the data, while defending data access from cyber-attacks. RDX RansomBlock doesn't require security software updates and ensures full data recovery in case of infected data or blocked computer systems.

## Off-Site data protection

In addition to disaster and cyber-attack protection capabilities, RDX also provides data theft protection for media which are stored off-site or are in transit. Built-in password protection makes it difficult for unauthorised personnel to access the data on the RDX media, even if an RDX system is available.

## RDX simplifies data management

Overland-Tandberg's RDX QuikStor is an affordable system with a low total cost of ownership. It simplifies backup, archiving and data transportation tasks with important security features. Optional software provides data security and meets compliance requirements, and with media-capacities from 500GB to 5TB, it fulfils the majority of backup, storage and archiving requirements.



*optional feature

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

UC_v2_nov28_2019