USE CASE

RDX® Removable Disk Systems in Finance Environments

Challenges

- Financial sector is the most cyber-attacked industry
- Backups need to be protected against virus and ransomware attacks
- Banks and financial offices aren't allowed to utilize removable disks
- USB ports are disabled for security reasons
- Financial data is extremely sensitive and needs to be encrypted
- Branch offices need a cost-effective and secure data protection solution

Solution Benefits

- Easy to install and easy to use
- No special care required
- Provides FIPS 140-2 validated hardware encryption
- Offers protection against virus and ransomware attacks
- Meets government regulation, like GDPR
- Transparent integration into finance applications
- Provides full disaster protection for sensitive financial 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

Finance environments have specialized security requirements. Their sensitive data needs to be protected against unauthorized access, viruses and cyber-attacks. Therefore, data backup by system administrators is extremely important. Most finance environments will not accept USB devices attached to their systems and block or disable these ports. In addition, data must be encrypted for protection against unauthorized access.

Regular backups and off-site storage

Regular backup of business-critical data is essential for finance businesses. However, this is not enough. Backups need to be stored off-site to ensure full disaster protection.

Off-site vaulting also protects against virus and ransomware attacks. Virus and ransomware attacks can infect backup sets regardless of their location, both on the computer and network.

According to IBM's X-Force threat intelligence index from 2019, the finance and insurance sector has been the most-attacked industry for three years in a row, with 19 percent of total attacks and incidents in 2018.

The RDX technology – rugged, reliable, removable, secure

Overland-Tandberg's RDX QuikStor® combines the benefits of tape's removability and long archival life, as well as the benefits of disk's fast data access and high throughput. The rugged design of the RDX media ensures data integrity. QuikStor system and media are fully backward and forward compatible, which reduces operational costs and eliminates compatibility issues.

FIPS 140-2 validated encryption

RDX QuikStor is available with a SATA III interface and is easy to integrate into servers or desktop PCs. This allows the use of a removable disk device for backup and transfer of backup data off-site, even if USB ports are not usable due to compliance and security policies.

While the RDX media is in transfer or stored off-site, the backup data is jeopardized and can be accessed by unauthorized personnel or be stolen. To mitigate this danger, the data must be encrypted.

The RDX QuikStor system with SATA III interface offers RDX PowerEncrypt FIPS 140-2 validated hardware encryption. RDX media are offered from 500GB to 8TB capacity.

Customer Benefits

- **Business continuity and security**
- **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 RDX QuikStor systems with SATA III interface offer RDX PowerEncrypt hardware encryption. RDX PowerEncrypt data encryption can be added to any RDX media. It is FIPS 140-2 validated and encrypts the data written to the RDX media using AES-256 XTS standards. Access to the data is secured by a password key.

PowerEncrypt can manage several user passwords with different data access levels. So users can be granted permission to read and write, or just to read data from the cartridge according to their role inside the company.

With this feature, backup data is secured at any time. Without the password key, the data that resides on the RDX media cannot be accessed by an unauthorized user making both the media and data useless. RDX PowerEncrypt is fully compatible with Overland-Tandberg's additional security features like WORM.

Compliance archiving with WORM

With RDX WORM*, RDX QuikStor can also be used as storage for regulatory compliance archiving. Its compliance has been assessed by KPMG AG Wirtschaftsprüfungsgesellschaft, Frankfurt am Main. RDX WORM is transparent for archiving applications and provides an affordable and easy to integrate archive solution for finance environments. Even files that are copied to the media via drag and drop are secured immediately by the WORM functionality.

Air Gap protection against ransomware

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 utilize removable storage media. RDX 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.

RDX simplifies data management tasks

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 for the finance environment. Software features provide data security and meet compliance requirements, and with media-capacities from 500GB to 8TB, it fulfills the majority of backup, storage and archiving requirements.

* optional feature

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.