RDX® RansomBlock

Virus and Ransomware protection of business data stored on RDX media

Ransomware has emerged as the most dangerous cyber threat for 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 files are encrypted, deleted or inaccessible.

Threat to all kind of businesses

Ransomware attacks harm small businesses as well as large enterprises. They are typically carried out in an email attachment or download link, using a Trojan that is disguised as a legitimate file like invoices, order confirmations or notifications. Another threat are links on already infected websites, where users are asked to click on an imbedded download link diverting the systems to automatically download the Ransomware and infect your computer and all other computers on the same network.

RDX RansomBlock

RansomBlock is an additional feature for RDX WORM media of the rdxLOCK software. It allows write operations for granted applications and processes similar to a personal FireWall. Therefore, backup applications are able to use RDX WORM media like a regular RDX backup target.

Protected backups

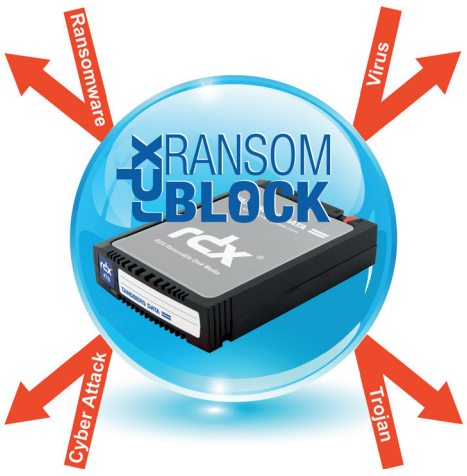
An effective protection against virus and ransomware attacks is to store data off-site and keep it outside the network, which can be perfectly done with RDX. However, during backups, or if backups of business critical data are performed continuously or frequently during the day, they might be no opportunity to place the backup media off-site or off-line. Backup strategies like media rotation or the 3-2-1 backup method, are difficult to implement. In this case, backup data is threatened by virus or ransomware attacks.

Cloud storage could be a preferred solution. It is a good way for data protection especially when it is not used as a primary backup target and it is used for infrequent data access. Primary backup or disaster recovery however might be difficult. Furthermore, cloud storage or backup data are threatened by virus and ransomware attacks if they are permanently connected and online.

The RansomBlock feature allows only authorized applications, like backup software, to perform modifications to the data, while defending data access from cyber-attacks. It secures backups against virus and ransomware attacks automatically and doesn‘t need any security software updates to ensure full data recovery in case of infected data or blocked computer systems.

Key Benefits

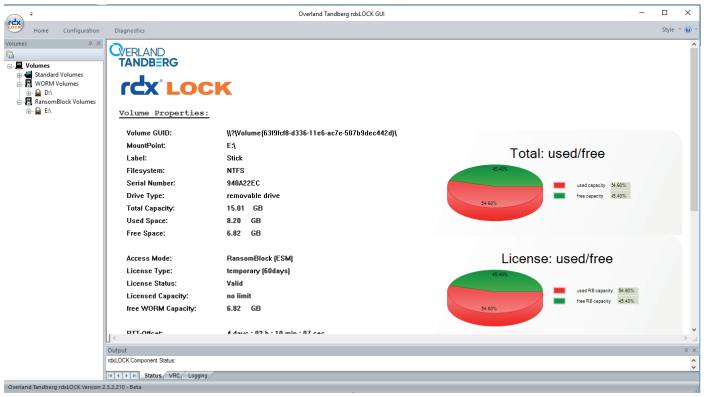
- Full data protection against virus and ransomware attacks
- Blocks unauthorised write access with RDX WORM Media
- Ensures business continuity without ransom payments
  Backups will not be infected, just restore and continue
- Transparent backup application integration
- Whitelist and blacklist capabilities for applications
- Real-time access control
- Automatic whitelisting for initial setup and configuration simplification
- 60-day free trial
  *Full functionality can be tested for 60 days**



*Data will not be accessible after 60 days unless a valid RDX WORM media with licence will be purchased and installed.

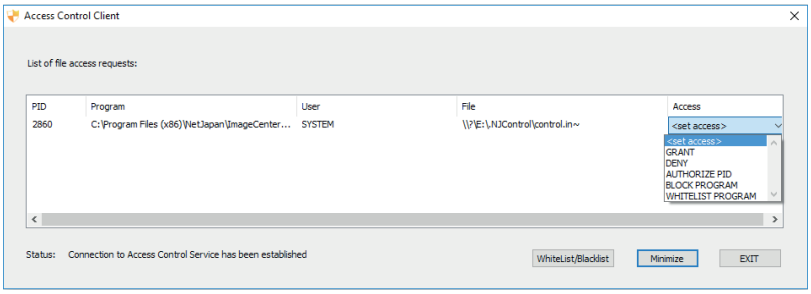
rdxLOCK and Access Control Client

rdxLOCK is a software solution for Windows® systems that enables RDX WORM media to be used for compliance archiving with WORM or ransomware protection with RansomBlock features. rdxLOCK is used to set the RDX media into the desired mode, to manage licenses and to view and gather statistics. rdxLOCK can be downloaded from the Tandberg Data website for free. A 60-day trial period allows testing with full functionality. Afterwards, a licensed RDX WORM media needs to be purchased. With rdxLOCK, users are able to asssociate the license with the media.



Data cannot be accessed by other systems without rdxLOCK software installed. So data is protected during transit or off-site storage.

The Access Control Client monitors all read and write operations, which are performed to the RDX media that have been set into RansomBlock mode and manages all access rights previously defined. For a predefined time period of max 24hrs, access rights can be granted automatically for simplifying intial setup of write tasks of applications. Administrators can also manually set permissions during runtime. In this case, the Access Control Client window pops up with a dialog, where users decide whether access operations should be denied or granted just for this occurrence, or put onto a white- or blacklist for future access.



Administrators are also able to verify the black and white listed applications and remove them if desired, or to manually add applications in advance.

Specifications

Media			
Models	8868-RDX: 1TB WORM Cartridge	8869-RDX: 2TB WORM Cartridge	8870-RDX: 4TB WORM Cartridge
Reliability & Data Integrity			
Unrecoverable Error Rate	1 error in 10^{14} bits read		
Cartridge Drop Shock (Non-operating)	1m (39.4in.) drop to tile over concrete floor		
Load-/ Unload (Minimum)	5,000 insertion / removal cycles (media), 10,000 insertion / removal cycles (drive)		
Archival Environmental			
Cartridge Archive Storage Life	> 10 years (HDD) offline storage in archival environment		
Archival Storage Environment	5° to 26°C (41° to 78°F), 5% to 95% relative humidity		
Maximum Wet Bulb	25°C (77°F) (non-condensing)		
WORM Functionality			
Software	rdxLOCK		
System Requirements			
Operating Systems Server	Windows Server 2008 SP2 Standard & Enterprise Edition, 32-bit, 64-bit MS Windows Server 2008 R2 SP2 Standard & Enterprise Edition, 64-bit MS Windows Server 2012 Standard & Enterprise Edition, 32-bit, 64-bit MS Windows Server 2012 R2 Standard & Enterprise Edition, 64-bit MS Windows Server 2016		
Operating Systems Desktop	MS Windows 7, 32-bit, 64-bit, MS Windows 8, 32-bit, 64-bit, MS Windows 8.1, 32-bit, 64-bit, MS Windows 10 Itanium based systems are not supported		
Hardware	RDX QuikStor internal SATA, SATA III, USB 2.0 und USB 3.0, RDX QuikStor external USB 2.0 und USB 3.0 RDX QuikStation, iSCSI (RDX single drive mode and disk autoloader mode only)		

Sales and support for Overland-Tandberg products and solutions are available in over 90 countries.
Contact us today at sales@overlandstorage.com or sales@tandbergdata.com

DS_v4_Nov13_2017