OVERLAND TANDBERG

RANSOM BLOCK

Virus and ransomware protection of data stored on RDX® media

Key Benefits

- Data protection against virus and ransomware attacks
- Blocks unauthorized write access with RDX WORM Media
- Ensures business continuity without ransom payments
- Transparent backup application integration
- Whitelist and blacklist capabilities for applications
- Real-time access control
- Automatic whitelisting for initial setup and configuration simplification

Ransomware has emerged as the most dangerous cyber threat for organizations. Ransomware is a type of malicious software that blocks access to the victim's data until a ransom is paid. After a ransomware attack, systems might be locked, or files are now encrypted, deleted or inaccessible.

Threats to all kinds of businesses

Ransomware attacks harm small businesses as well as large enterprises. A 2020 cybersecurity global report revealed the average cost to recover or remediate a ransomware attack could range from $150K to $2M USD. Ransomware can infiltrate business IT networks in countless ways – from an email attachment, download links or Trojans disguised as legitimate files like invoices.

RDX RansomBlock for peace of mind

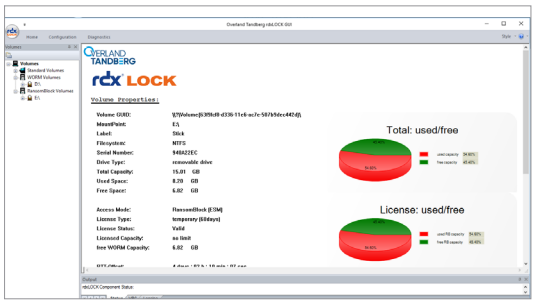
The RansomBlock functionality sets all data on the RDX® WORM media into a read-only mode. In addition, it only allows write operations to RDX media to granted applications and processes, like a FireWall. Therefore, backup applications can use RDX WORM media like a regular RDX backup target. For RDX supported backup applications see our compatibility matrix.

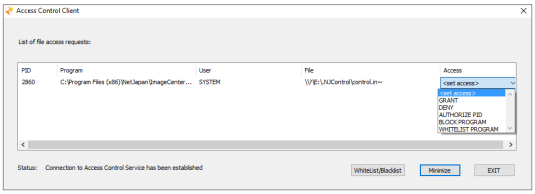
Protected backups

Security experts are now counseling that effective protection against virus and ransomware attacks needs to include new backup 3-2-1-1 strategies where one backup copy is stored in an unalterable state, and another copy is air-gapped or stored outside the network. However, during backups, or if backups of business-critical data are performed frequently during the day, there might be no opportunity to take the backup media off-line or off-site. In such cases, backup data may still be at risk from virus or ransomware attacks via the network.

Cloud archived storage is also a proven solution for data protection, when it is not used as a primary backup target, and it is used for infrequent data access. However, cloud storage or backup data are still at risk from virus and ransomware attacks if they are permanently connected and online.

The RDX RansomBlock feature is a smart supplement to Cloud backups. RDX RansomBlock allows only authorized 'whitelisted' applications, like backup software, to perform modifications to the data. It secures backups against virus and ransomware attacks because these are automatically blocked or 'blacklisted'.





Access Control Client

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.

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 initial 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 white and blacklisted 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 (system)		
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	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 and USB 3.0, RDX QuikStor external USB 2.0 and USB 3.0 RDX QuikStation, iSCSI (RDX single system mode, logical volume mode and disk autoloader mode only)		

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.