RDX® RansomBlock

Schutz vor Viren und Ransomware von auf RDX-Medien gespeicherten Geschäftsdaten

Ransomware hat sich zur größten Cyberbedrohung für Unternehmen entwickelt. Hierbei handelt es sich um eine schädliche Software, die den Datenzugriff blockiert, bis ein Lösegeld (engl. ransom) bezahlt wurde. Nach einem Ransomwareangriff sind die Systeme meistens gesperrt und Daten gelöscht, verschlüsselt oder nicht mehr zugänglich.

Eine Bedrohung für jedes Unternehmen

Ransomwareangriffe können kleine und große Unternehmen gleichermaßen schädigen. Ransomware wird typischerweise über E-Mail-Anlagen oder Download-Links durch Trojaner in die Systeme eingeschleust, die sich als normale Dateien wie Rechnungen, Bestätigungen oder Benachrichtigungen tarnen. Weitere Gefahren stellen Links auf bereits infizierten Websites dar, die nach der Anwahl automatisch Ransomware herunterladen und nicht nur den PC des Verursachers, sondern alle Computersysteme im gleichen Netzwerk infizieren.

RDX RansomBlock

RansomBlock ist eine zusätzliche Funktion der rdxLOCK-Software für RDX WORM-Medien. Sie erlaubt Schreiboperationen für auswählbare Anwendungen, ähnlich einer Firewall. Somit können Backupanwendungen RDX WORM-Medien als ein reguläres Backupziel nutzen.

Geschütze Backups

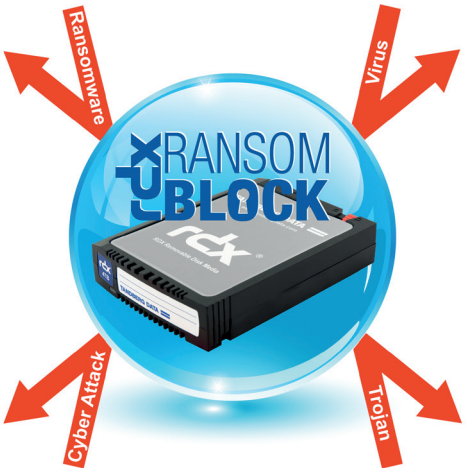
Einen effektiven Schutz gegen Viren- und Ransomwareangriffe bietet die externe Speicherung von Daten außerhalb des Netzwerkes, für die RDX perfekt geeignet ist. Während laufender Backups oder wenn Backups von unternehmenskritischen Daten kontinuierlich oder regelmäßig im Laufe des Tages durchgeführt werden, ist es jedoch eventuell nicht möglich, die Backupmedien extern auszulagern oder offline zu setzen. Somit sind Backupstrategien wie Medienrotation oder das 3-2-1-Backupverfahren schwierig umzusetzen. In diesen Fällen sind Backupdaten durch Viren- oder Ransomwareangriffe bedroht.

Cloudspeicherung könnte eine bevorzugte Lösung sein. Sie ist eine gute Möglichkeit des Datenschutzes, insbesondere, wenn sie nicht als primäres Backupziel genutzt und für seltenen Datenzugriff verwendet wird. Primäres Backup oder Notfallwiederherstellung könnten jedoch problematisch sein. Zudem sind Cloudspeicher oder Backupdaten durch Viren- und Ransomwareangriffe bedroht, wenn sie permanent verbunden und online sind.

Die RansomBlock-Funktion erlaubt nur autorisierten Anwendungen, wie Backupsoftware, die Ausführung von Datenänderungen und wehrt den Datenzugriff durch Cyberattacken ab. Sie schützt Backups automatisch vor Viren- und Ransomwareangriffen und benötigt keine Updates der Sicherheitssoftware, um die vollständige Datenwiederherstellung im Falle von infizierten Daten oder blockierten Computersystemen zu gewährleisten.

Vorteile

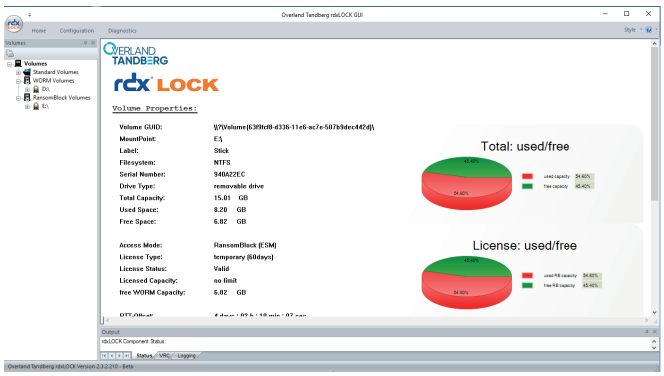
- Umfassender Datenschutz gegen Viren- und Ransomwareangriffe
- Blockiert nicht autorisierten Schreibzugriff auf RDX WORM-Medien
- Gewährleistet Geschäftskontinuität und vermeidet Lösegeldzahlungen
  Backups werden nicht infiziert und ermöglichen einfaches Wiederherstellen
- Transparente Integration in Backup-anwendungen
- Erstellen einer Whitelist und einer Blacklist für erlaubte und abgelehnte Anwendungen
- Zugriffskontrolle in Echtzeit
- Automatische Erstellung einer Whitelist zur Vereinfachung der Erstkonfiguration
- 60 Tage kostenlose Testversion
  *Die volle Funktionalität kann 60 Tage getestet werden**



*Daten sind nach 60 Tagen nicht mehr lesbar, bis ein RDX WORM-Medium mit gültiger Lizenz erworben und installiert wurde.

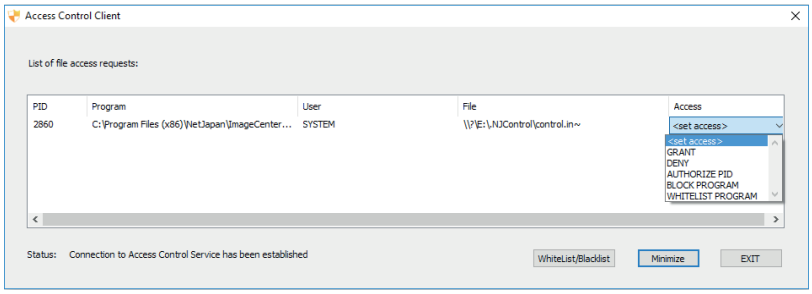
rdxLOCK und Access Control Client

rdxLOCK ist eine Windows® - basierte Softwarelösung für die Nutzung von RDX WORM-Medien als Speicher für die revisionssichere Archivierung mit WORM oder für den Schutz vor Ransomware mit RansomBlock-Funktionen. rdxLOCK wird verwendet, um das RDX-Medium auf den gewünschten Modus einzustellen, Lizenzen zu verwalten und Statistiken anzuzeigen und zu erfassen. rdxLOCK kann kostenlos von der Tandberg Data-Website heruntergeladen und mit vollem Funktionsumfang für 60 Tage getestet werden. Anschließend muss ein lizenziertes RDX WORM-Medium erworben werden. rdxLOCK erlaubt die Verknüpfung der Lizenz mit dem Medium.



Systeme ohne rdxLOCK-Software können nicht auf die Daten zugreifen, sodass die Daten während des Transports oder der Speicherung an einer externen Lokation geschützt sind.

Der Access Control Client überwacht alle Lese- und Schreibvorgänge, die auf den RDX-Medien ausgeführt werden, die zuvor in den RansomBlock-Modus gesetzt wurden. Er verwaltet alle vorab festgelegten Zugriffsrechte. Zugriffsrechte können für einen vorgegebenen Zeitraum von maximal 24 Stunden automatisch gewährt werden, um die erste Einrichtung von Schreibvorgängen für Anwendungen zu erleichtern. Administratoren können außerdem manuell während der Laufzeit Berechtigungen festlegen. In diesem Fall erscheint das Dialogfenster des Access Control Client, in dem die Anwender entscheiden, ob Zugriffe für dieses eine Ereignis verweigert bzw. gewährt oder für zukünftige Zugriffe auf eine White- oder Blacklist gesetzt werden sollen.



Administratoren können zudem die Anwendungen auf der Black- und Whitelist überprüfen und sie entfernen oder vorab Anwendungen manuell hinzufügen.

Spezifikationen

Medien			
Modelle	8868-RDX: 1TB WORM-Medium	8869-RDX: 2TB WORM-Medium	8870-RDX: 4TB WORM-Medium
Zuverlässigkeit und Datensicherheit			
Nicht wiederherstellbare Fehlerrate	1 Fehler in 10^{14} gelesenen Bits		
Medium Falltest	1m Fall auf Betonboden		
Lade-/Endladezyklen (Minimum)	5.000 bei Medium, 10.000 bei Laufwerk		
Archiv-Umgebung			
Archivierungszeit des Mediums	> 10 Jahre Offline Storage in Archiv-Umgebung		
Umgebungsbedingungen	5° to 26°C, 5% to 95% relative Luftfeuchtigkeit		
Maximum Wet Bulb	25°C (nicht kondensierend)		
WORM Funktion			
Software	rdxLOCK		
Systemvoraussetzungen			
Betriebssysteme 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		
Betriebssysteme 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 Keine Itanium basierten Systeme und Windows Core Installationen		
Hardware	RDX QuikStor internal SATA, SATA III, USB 2.0 und USB 3.0, RDX QuikStor external USB 2.0 und USB 3.0RDX QuikStation, iSCSI (Nur im RDX Drive Modus und Disk Autoloader Modus)		

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