RDX® RansomBlock

La protection des données d'entreprise stockées sur les supports RDX contre les virus et les rançongiciels

Les rançongiciels constituent aujourd'hui la plus grande cybermenace pour les entreprises. Il s'agit de logiciels malveillants qui bloquent l'accès aux données de la victime jusqu'au versement d'une rançon. Une attaque par rançongiciel peut avoir pour effet de verrouiller le système, de chiffrer des fichiers, de les supprimer ou de les rendre inaccessibles.

Une menace qui plane sur toutes les entreprises

Les rançongiciels attaquent indifféremment les petites ou les grandes entreprises. Ils sont généralement diffusés sous forme de pièce jointe ou de lien de téléchargement contenant un cheval de Troie déguisé en fichier légitime tel qu'une facture, une confirmation de commande ou une autre notification. Les liens vers des sites déjà infectés constituent une autre menace : les utilisateurs sont invités à cliquer sur un lien de téléchargement intégré, par lequel le système télécharge automatiquement le rançongiciel qui contamine alors l'ordinateur, ainsi que tous ceux du réseau

RDX RansomBlock

RansomBlock est une fonctionnalité complémentaire du logiciel rdxLOCK destinée aux supports RDX WORM. À la manière d'un pare-feu personnel, elle permet uniquement les opérations d'écriture par les applications et processus autorisés. Les applications de sauvegarde peuvent ainsi utiliser les supports RDX RansomBlock comme n'importe quel support de sauvegarde RDX classique.

Des sauvegardes protégées

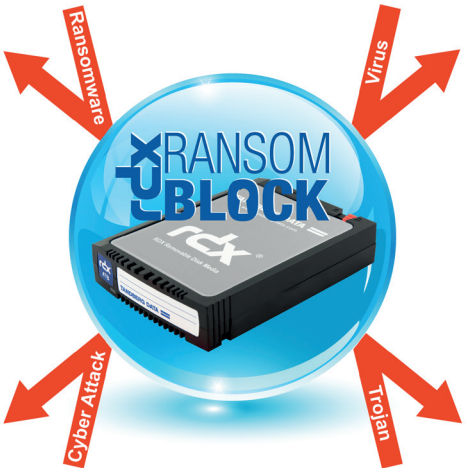
Une protection efficace contre les virus et les rançongiciels consiste à stocker les données hors site, à l'extérieur du réseau, ce que permet parfaitement la technologie RDX. Toutefois, il n'est pas toujours possible, durant les sauvegardes ou en cas de sauvegardes continues ou fréquentes des données stratégiques tout au long de la journée, de mettre le support de sauvegarde hors site ou hors ligne. Des stratégies de sauvegarde telles que la rotation des supports ou la méthode des 3-2-1 sont difficiles à mettre en œuvre. En effet, les données de sauvegarde se trouvent alors exposées aux attaques par virus ou rançongiciels.

Le stockage dans le cloud peut dans ce cas être la solution préconisée. C'est notamment le cas si elle ne fait pas office de cible de sauvegarde principale et qu'elle est réservée aux données peu utilisées. Le stockage lié aux sauvegardes principales et les reprises après sinistre peuvent toutefois se révéler difficiles. En outre, les données de stockage dans le cloud ou de sauvegarde restent exposées aux virus et rançongiciels si elles restent connectées et en ligne en permanence.

En réservant à des applications autorisées, telles que les logiciels de sauvegarde, la possibilité d'apporter des modifications aux données, la fonction RansomBlock préserve les données de toute cyberattaque. Cette protection des sauvegardes contre les virus et rançongiciels s'effectue automatiquement et sans mise à jour des logiciels de sécurité, et permet une récupération complète des données en cas d'infection ou de blocage des systèmes informatiques.

Avantages clés

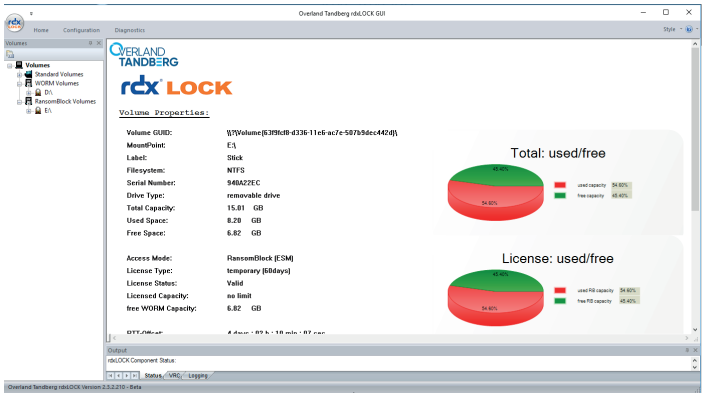
- Protection complète des données contre les virus et rançongiciels
- Blocage des accès en écriture non autorisés
- Assurance de poursuite de l'activité sans risque de demande de rançon
  Les sauvegardes ne pouvant être infectées, il suffit de restaurer les données et de continuer
- Intégration transparente aux applications de sauvegarde
- Listes noire et blanche d'applications
- Contrôle d'accès en temps réel
- Liste blanche automatique pour simplifier la mise en œuvre initiale et la configuration
- 60 jours d'essai gratuit
  *Toutes les fonctionnalités en essai gratuit pendant 60 jours**



*Au-delà de 60 jours, les données ne seront plus accessibles hors achat et installation d'un support RDX WORM sous licence.

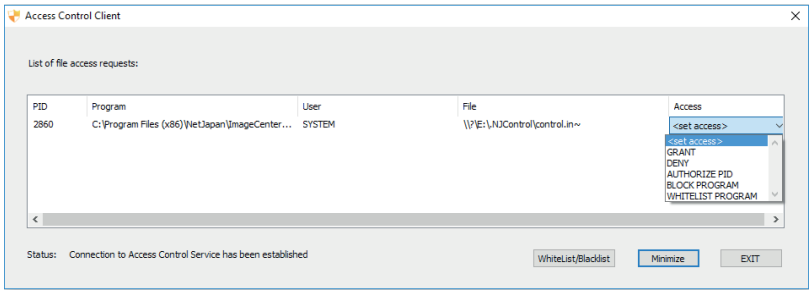
rdxLOCK et contrôle d'accès client

rdxLOCK est une solution logicielle pour Windows® permettant d'utiliser les supports RDX WORM à des fins d'archivage de conformité avec WORM ou d'assurer la protection contre les rançongiciels avec les fonctionnalités RansomBlock. rdxLOCK permet de mettre le support RDX dans le mode souhaité, de gérer les licences et de consulter et recueillir des statistiques. rdxLOCK peut être téléchargé gratuitement sur le site web de Tandberg Data. Une période d'essai de 60 jours permet de tester toutes les fonctionnalités. Un support RDX WORM sous licence doit être ensuite acheté. rdxLOCK permet aux utilisateurs d'associer la licence au support.



Les autres systèmes ne peuvent accéder aux données que si le logiciel rdxLOCK est installé. Les données sont ainsi protégées pendant leur acheminement ou une fois stockées hors site.

Le contrôle d'accès client surveille toutes les opérations de lecture et d'écriture effectuées sur les supports RDX en mode RansomBlock et permet de gérer tous les droits d'accès préalablement définis. Pendant une durée prédéfinie maximale de 24 heures, les droits d'accès peuvent être accordés automatiquement afin de faciliter la configuration initiale des tâches d'écriture des applications. Les administrateurs peuvent également définir manuellement les autorisations durant l'exécution. Dans ce cas, la fenêtre de contrôle d'accès client affiche une boîte de dialogue permettant aux utilisateurs d'interdire ou d'autoriser les opérations d'accès sur le moment, ou de mettre en place une liste de blanche ou noire pour les accès ultérieurs.



Les administrateurs ont également la possibilité de vérifier les applications inscrites sur liste blanche ou noire et de les supprimer le cas échéant, ou d'ajouter manuellement des applications à l'avance.

Caractéristiques techniques

Supports			
Modèles	8868-RDX : Cartouche WORM 1 To	8869-RDX : Cartouche WORM 2 To	8870-RDX : Cartouche WORM 4 To
Fiabilité et intégrité des données			
Taux d'erreur irrécupérable	1 erreur par lecture de 10^{14} bits		
Cartouche résistance aux chocs (hors fonctionnement)	Chute de 1 m sur un sol en carrelage ou béton		
Chargement/déchargement	5 000 cycles d'insertion/retrait (supports), 10 000 cycles d'insertion/retrait (lecteur)		
Environnement d'archivage			
Durée de vie du stockage d'archives de la cartouche	> 10 ans (stockage hors ligne dans l'environnement d'archivage sur disque dur)		
Environnement de stockage d'archives	5 à 26 °C, 5 à 95 % d'humidité relative		
Température max. de thermomètre humide	25 °C (sans condensation)		
Fonctionnalité WORM			
Logicie	rdxLOCK		
Configuration requise			
Systèmes d'exploitation serveur	Windows Server 2008 SP2 Standard et Enterprise Edition, 32 bits, 64 bits MS Windows Server 2008 R2 SP2 Standard et Enterprise Edition, 64 bits MS Windows Server 2012 Standard et Enterprise Edition, 32 bits, 64 bits MS Windows Server 2012 R2 Standard et Enterprise Edition, 64 bits MS Windows Server 2016		
Systèmes d'exploitation bureautique	MS Windows 7, 32 bits, 64 bits, MS Windows 8, 32 bits, 64 bits, MS Windows 8.1, 32 bits, 64 bits, MS Windows 10 Les systèmes basés sur Itanium ne sont pas pris en charge.		
Matériel	RDX QuikStor SATA interne, SATA III, USB 2.0 et USB 3.0, RDX QuikStor USB 2.0 et USB 3.0 externes RDX QuikStation, iSCSI (mode lecteur RDX unique et chargeur automatique de disques uniquement)		

Les services de vente et d'assistance pour les produits et solutions d'Overland-Tandberg sont disponibles dans plus de 90 pays.
Contactez-nous dès aujourd'hui à l'adresse salesemea@overlandtandberg.com.

DS_v5_Nov21_2019