WHITE PAPER

RDX® PowerEncrypt

RDX PowerEncrypt Datenverschlüsselung schützt auf RDX-Medien gespeicherte Daten während des Transports oder der Archivierung außerhalb des Betriebsgeländes vor unbefugten Zugriffen.

Was ist RDX PowerEncrypt?

Die RDX PowerEncrypt-Datenverschlüsselung kann zu jedem RDX-Medium hinzugefügt werden. Die auf das RDX-Medium geschriebenen Daten werden mithilfe von AES-256 XTS-Standards verschlüsselt und der Datenzugriff wird mit einem über die RDX-Manager-Software bereitgestelltem Passwortschlüssel gesichert. Ohne den Passwortschlüssel kann ein unbefugter Nutzer nicht auf die Daten, die auf dem RDX-Medium gespeichert sind, zugreifen und somit sind sowohl das Medium als auch die Daten nutzlos. Mit RDX PowerEncrypt können Sie sicher sein, dass Ihre Daten geschützt sind.

Die Voraussetzung für den Zugriff auf das verschlüsselte RDX-Medium ist die Installation der RDX-Manager Software. Der RDX-Manager ermöglicht sowohl den Zugriff auf das Medium als auch auf die Daten und bietet Tools zum Löschen, Partitionieren und Formatieren der Daten. Außerdem wird das sichere Löschen von Medien durch die Nutzung des RDX-Managers zur Entfernung der Verschlüsselung automatisch ausgeführt.

Die aktuellste RDX-Manager Software, einschließlich der RDX PowerEncrypt-Funktionalität, steht auf der RDX QuikStor Produkt-Website zum Download bereit. Die Installation des RDX-Managers ist für die Nutzung von RDX nachdrücklich zu empfehlen, da es einfachen Zugriff auf alle RDX-Funktionen einschließlich der Medienauswurfsicherheit, Modus-Änderungen, Medienvorbereitung, Diagnostik, Firmware-Upgrades und jetzt auch RDX PowerEncrypt-Funktionen erlaubt.

Der Nutzen von PowerEncrypt

Das ins RDX QuikStor SATA III-Laufwerk eingebaute RDX PowerEncrypt stellt einen zusätzlichen Nutzen ab der Firmware Version 0253 dar, und wird bald im Zuge unseres intensiven Produktentwicklungsvorhabens für andere RDX-Produkte verfügbar sein.

RDX PowerEncrypt wird über das FIPS 140-2 validierte RDX SATA III-Laufwerk bereitgestellt. So können jetzt Daten auf RDX-Medien für jeden Anwendungsfall, der Datensicherheit verlangt, vertraulich verschlüsselt werden. Kunden, die das RDX SATA III-Laufwerk im FIPS 140-2-Modus betreiben müssen, können ein Set mit manipulationssicheren Siegeln für die RDX Medien bei Overland-Tandberg bestellen.

Betriebsmodi und Optionen

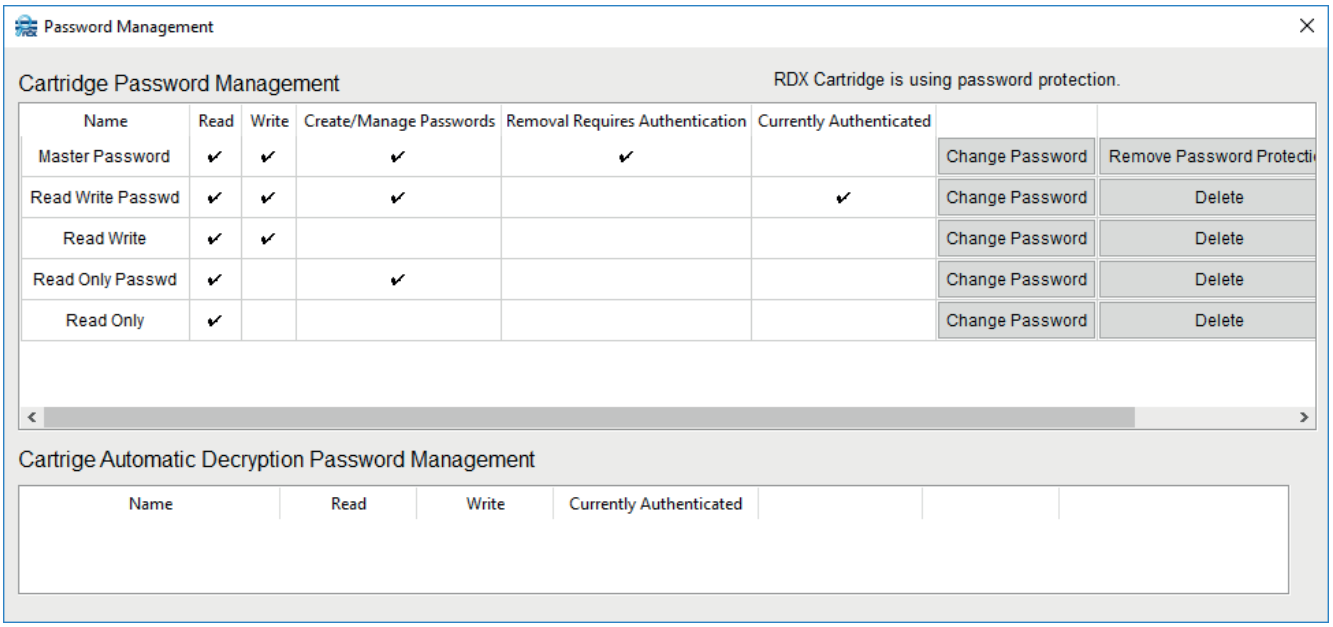
RDX PowerEncrypt bietet zwei Modi der Datensicherheit – den Passwortschutz und den Passwortschutz mit Verschlüsselung.

Einfacher Passwortschutz (ohne Verschlüsselung)

RDX PowerEncrypt unterstützt bis zu acht Passwörter mit je vier verschiedenen Zugriffsrechten und Verwaltungsoptionen. Diese vier Zugriffsrechte sind:

- Schreibgeschützter Zugriff
- Schreibgeschützter Zugriff mit Passwortverwaltung
- Lese- und Schreibzugriff
- Lese- und Schreibzugriff mit Passwortverwaltung

Außerdem wird ein Masterpasswort mit Lese- und Schreibzugriff und Passwortverwaltung automatisch zur Verfügung gestellt. Dieses Masterpasswort wird zur Verwaltung des RDX-Medienschutzes verwendet.



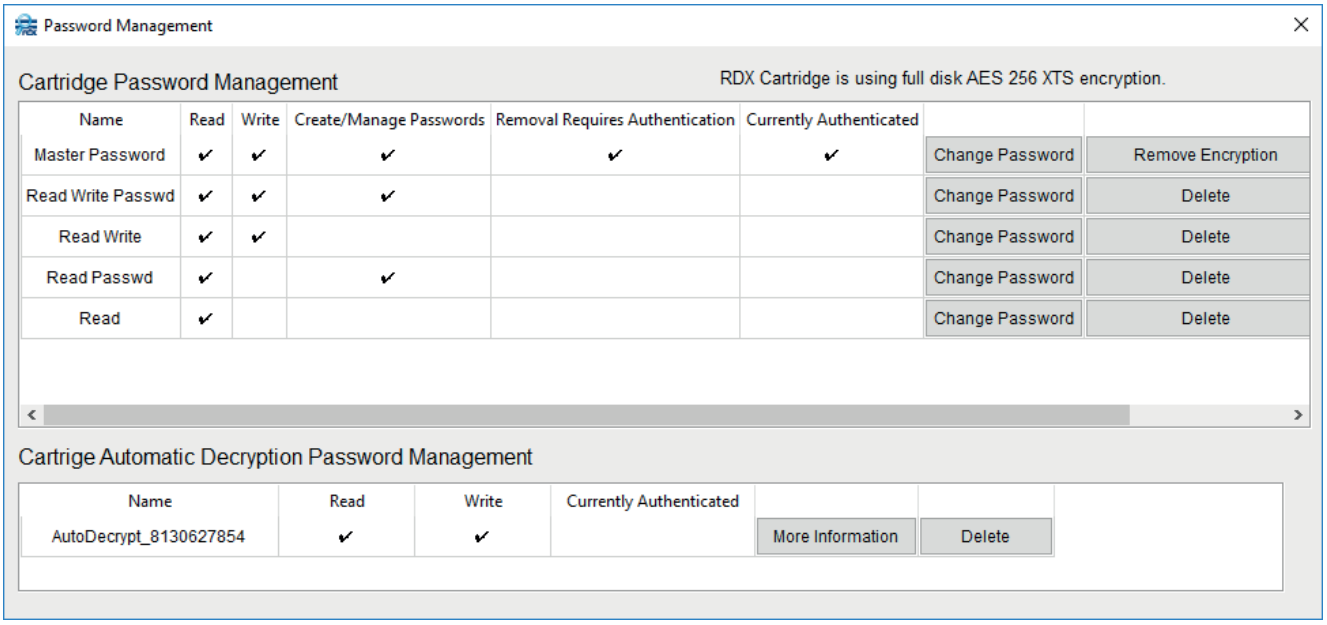
Die Abbildung zeigt Passwortkombinationen für den einfachen Passwortschutz

RDX PowerEncrypt erlaubt die Bereitstellung auswählbarer Features und Funktionen an verschiedene Benutzer im Unternehmen oder an Kunden für einen sicheren Datenaustausch. Abhängig von den verschiedenen Berechtigungsstufen sind Features möglicherweise grau unterlegt und nicht auswählbar.

Die Anwendung des schreibgeschützten Datenzugriffs schützt die Daten sowohl vor Viren- als auch vor Ransomwareangriffen. Der schreibgeschützte Modus bedeutet, dass Daten nur von Personen mit entsprechendem Passwort verändert, verschlüsselt oder gelöscht werden können.

Festplattenverschlüsselung mit AES-256 XTS-Verschlüsselung

Zusätzlich zum einfachen RDX-Medien Passwortschutz ist RDX PowerEncrypt fähig, die Daten mit AES-256 XTS-Verschlüsselung zu verschlüsseln. Die Verwendung dieser Verschlüsselung ist nachdrücklich zu empfehlen, falls die RDX-Medien außerhalb des Betriebsgeländes gelagert oder an einen anderen Ort transportiert werden sollen. Wie beim Feature des einfachen RDX-Passwortschutzes können bis zu acht verschiedene Passwörter mit dedizierten Datenzugriffsrechten und einer Vielzahl von Funktionen für verschiedene Zugriffsberechtigungen zugewiesen werden.



Die Abbildung zeigt Passwortkombinationen für die AES-256 XTS-Verschlüsselung

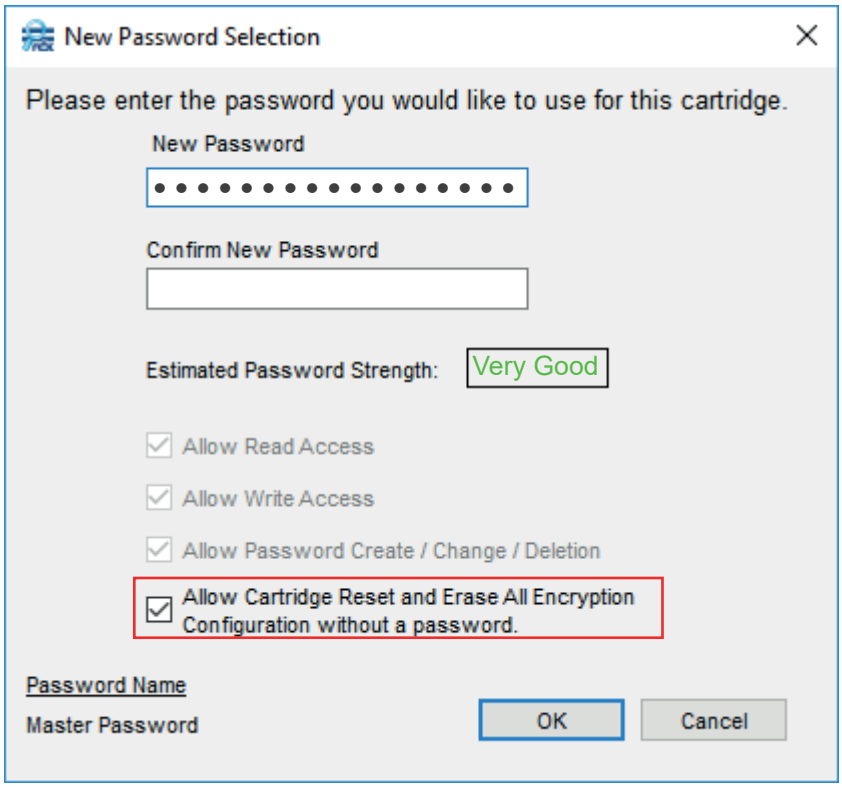
Die Benutzerfreundlichkeit wird durch die automatische Passwortoption für das RDX-Laufwerk und -Medien erhöht. Diese Option erlaubt den Datenzugriff ab dem Moment, an dem die Kassette in ein mit dieser Option konfiguriertes Laufwerk eingeschoben wird. Diese Funktionalität ist sowohl für Sicherungsszenarien einschließlich Medienrotation als auch für Bare-Metal-Recovery Zwecke ideal, also immer dann, wenn der RDX-Manager nicht für den Datenpasswortschutz zur Verfügung steht. Das Passwort wird auf dem Laufwerk abgelegt und kann mit verschiedenen Arten von RDX-Medien verwendet werden, wodurch Wiederherstellungen über eine Vielzahl von RDX-Kassetten verteilt werden kann. Das Passwort kann, falls nötig, zu jedem Zeitpunkt sicher vom Laufwerk entfernt werden.

Falls die automatische Entschlüsselung nicht aktiviert ist, ist ein Passwort für den Zugriff der Daten auf dem RDX-Medium nötig

Alternativ würde für den Datenaustausch zwischen verschiedenen Orten der Zugriff auf die RDX-Laufwerke mit aktivierter Passwortoption automatisch erlaubt werden, während er auf die anderen RDX-Laufwerke mit nicht-aktivierter Passwortoption automatisch verweigert wird. So bleiben die Daten auf Ihrem RDX-Medium weiterhin sicher und verschlüsselt. Ein weiterer praktischer Vorteil ist, dass Nutzer bei aktivierter Option kein Passwort eingeben müssen und so schnellen Zugriff auf die Daten erhalten. Falls die automatische Entschlüsselung nicht aktiviert ist, ist ein Passwort für den Zugriff der Daten auf dem RDX-Medium nötig.

Anmerkungen zu Passwörtern

Aus Sicherheitsgründen wird für den Zugriff auf die Daten, die auf dem RDX-Medium gespeichert sind, ein Passwort verlangt. Falls das Passwort für ein verschlüsseltes RDX-Medium verloren geht oder vergessen wird, kann niemand auf die Daten zugreifen.



Ist das markierte Kästchen nicht aktiviert und das Passwort wurde vergessen, wird das Medium nutzlos.

Falls **Allow Cartridge Reset and Erase All Encryption Configuration without a password** box ***nicht aktiviert ist*** und Sie Ihr Passwort vergessen, sind nicht nur die Daten unzugänglich, sondern das RDX-Medium kann nicht neu formatiert werden, wodurch das Medium nicht länger verwendbar ist. Wir weisen Sie darauf hin, dass das Vergessen Ihres Passworts nicht unter die RDX-Medien-Garantie fällt.

Die Passwortstärke ist der Schlüssel zur Absicherung der Daten. Falls Hacker versuchen, das Passwort zu knacken, ist die Verwendung eines sehr starken Passworts wichtig. Um Ihnen dabei zu helfen, ein starkes Passwort zu kreieren, analysiert RDX PowerEncrypt das vorgeschlagene Passwort und zeigt die geschätzte Stärke an (Sehr schwach, Schwach, Okay, Gut oder Sehr gut).

RDX PowerEncrypt evaluiert die Entropie eines Passworts auf Grundlage einiger Algorithmen einschließlich gemeinsamer Worte, wiederholter Zeichen, Datumsformate, Nummersubstitution (Leet) und Tastaturlayout.

Für die Verwendung eines starken Passworts für RDX PowerEncrypt empfehlen wir die Verwendung folgender Eigenschaften:

- Die gemeinsame Verwendung von mindestens sechs nicht zusammenhängenden Worten
- Zufällig platzierte Großbuchstaben in den Wörtern (z. B. der zweite Buchstabe in jedem Wort)
- Symbole und Nummern als Wortteilung

Im Optimalfall sollten Sie einen Satz mit 6 oder mehr Wörtern verwenden.

Aufgrund von Fortschritten in der Technologie (wie schnellere CPU-Geschwindigkeiten, Brute-Force-Angriffen und Wörterbuchangriffen) wird das Knacken von Passwörtern einfacher. Die schnellsten Computer heutzutage können um die 1014 Schlüssel pro Sekunde verschicken; dies wird sich in Zukunft weiter erhöhen. Um dem entgegenzuwirken, erlaubt RDX PowerEncrypt nur einen Versuch pro Sekunde und verringert so die Gesamtanzahl der Versuche, ein Passwort zu knacken, auf langsame 60 Versuche pro Minute. Hierdurch wird die Wahrscheinlichkeit, dass ein sicheres Nutzerpasswort erraten wird, wesentlich verringert. Außerdem wird die Software so robust, dass sie sogar den parallelen Hacking-Techniken, die zur Reduzierung der Zeit für das Knacken von Verschlüsselungen verwendet werden, standhält.

FIPS 140-2 Validierung

FIPS Federal Information Processing Standard) 140 wurde vom NIST (National Institute of Standards and Technology) herausgegeben, um die Anforderungen und Standards für Kryptografie-Module, die sowohl Hardware- als auch Software-Komponenten enthalten, zu koordinieren.

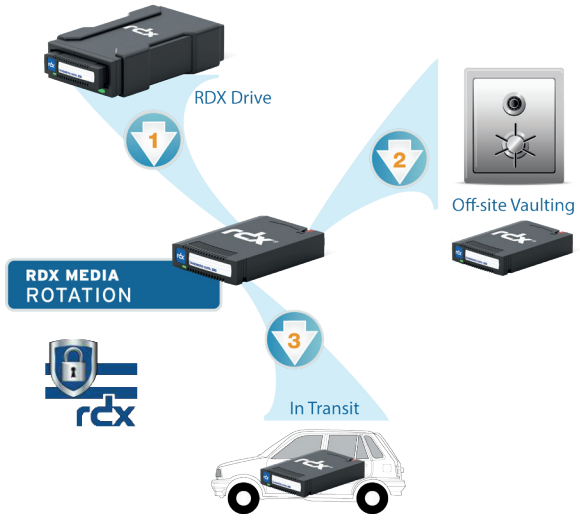
Die RDX PowerEncrypt-Software verwendet das FIPS 140-2 validierte RDX SATA III-Laufwerk, um die Standards für Kryptografie-Module zu erfüllen. Mit dieser Validierung erfüllen das RDX SATA III-Laufwerk und RDX PowerEncrypt die rechtlichen Beschaffungsanforderungen und erhalten die Vertraulichkeit und Integrität der Informationen, geschützt durch das Modul.

Die Validierung durch den FIPS 140-2 Standard stellt sicher, dass das RDX SATA III-Laufwerk und RDX PowerEncrypt solide bewährte Sicherheitspraktiken und starke Verschlüsselungsalgorithmen und -methoden verwenden. Sie legt außerdem fest, wie Einzelpersonen oder andere Prozesse zur Verwendung des Produkts autorisiert sein müssen und wie Module oder Komponenten designed sein müssen, um sicher mit anderen Systemen zu interagieren. Um als FIPS 140-2 validiert zu gelten, mussten sich das RDX SATA III-Laufwerk und RDX PowerEncrypt an die genannten Design- und Implementierungsanforderungen halten und von einem der 13 unabhängigen, durch NIST-akkreditierte Labore getestet und genehmigt werden.

Anwendungsfälle

Backup und Archivierung

RDX PowerEncrypt eignet sich großartig für jegliche Sicherungs- und Archivierungsanwendungen. Das Entfernen der RDX-Medien erlaubt die Lagerung von Sicherungen für Notfallwiederherstellungen und zu Archivierungszwecken außerhalb des Betriebsgeländes und kann einem Medien-Rotationsschema folgen.



Um die Sicherungen während der Lagerung an einem anderen Ort gegen unautorisierte Zugriffe zu schützen, bietet RDX PowerEncrypt den höchsten Datenschutz und Sicherheit für das Backup-Set und

das Archiv. Das automatische Passwortzugriffsfeature erleichtert die Verwendung verschlüsselter Medien, falls ein Bare-Metal-Restore nötig ist.

RDX-Medien demonstrieren eine langfristige Archivierungslebensdauer von 10+ Jahren und sind somit eine ideale Lösung zur Archivierung unter Einhaltung regulatorischer Vorgaben und Compliance.

Mit RDX PowerEncrypt sind Daten sicher und können nicht durch unbefugten Zugriff gelesen, verändert oder gelöscht werden.

Neue Regulierungen seitens der Regierungen für Datenschutz

Aktuell werden neue Regulierungen wie die Datenschutz-Grundverordnung (DSGVO) eingeführt. Die DSGVO reguliert, wie die persönlichen Daten von Kunden, Anbietern und Mitarbeitern in unserer digitalisierten Welt zur Sicherung von Privatsphäre gehandhabt, verarbeitet und gesichert werden müssen.

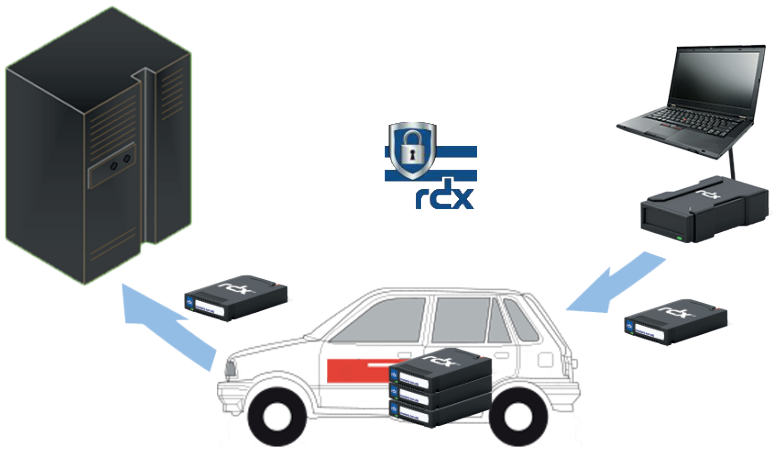
Artikel 23 der DSGVO behandelt die Limitierung des Zugriffs auf persönliche Daten auf diejenigen Einzelpersonen, die die Datenverarbeitung unterstützen und fordert folglich, dass die Daten gegen unbefugte Zugriffe geschützt sein müssen.

Artikel 32, Paragraf 1 der DSGVO beschreibt die Sicherheit persönlicher Daten durch die Verwendung von Verschlüsselung.

Artikel 34, Paragraf 3 beschreibt wie Datenschutzverletzungen sofort kommuniziert werden müssen, außer die Daten sind verschlüsselt. Im Fall von Verwendung der RDX-Verschlüsselung ist keine Kommunikation erforderlich.

RDX PowerEncrypt bietet all diese Funktionalitäten. Zugriffskontrolle wird durch die verschiedenen Stufen an Zugriffsrechten gesichert, mit Passwortschutz und Datenverschlüsselung als höchste Datensicherheit.

Datentransport und Datenaustausch



Das robuste Design der RDX-Medien erleichtert den Transport. RDX hält Vibrationen und harschen Bedingungen stand und kann von bis zu einem Meter aus ohne Folgen auf Zementboden fallen gelassen werden. RDX-Medien können ganz einfach auf regulärem postalischem Weg oder über Transportdienstleister verschickt werden. Große Datenmengen unter Verwendung von aktuellen Netzwerktransfergeschwindigkeiten an Cloud-Ressourcen zu senden oder zu empfangen ist eine Herausforderung. Eine Alternative zu langsamen Transfergeschwindigkeiten über ein lokales oder umfassendes Netzwerk wäre die Verwendung von RDX, angeschlossen an einen lokalen Server für einen schnelleren Transfer.

Außerdem stellt die hohe Kapazität von RDX-Medien für die Konsolidierung großer Datenmengen von Zweigstellen einer Organisation zum zentralen Datenzentrum eine bessere Lösung dar als Netzwerktransfers.

Während des Transports können unverschlüsselte Daten auf dem Medium missbraucht werden, falls RDX-Medien gestohlen werden. Sensible Daten von Unternehmen oder Regierungen müssen geschützt werden.

RDX PowerEncrypt bietet eine starke Lösung für den Schutz solcher Datenbestände.

Zusamenfassung

Durch seine einfache Verwaltung und volle Funktionalität kann RDX PowerEncrypt in einer Vielzahl von persönlichen, kleingewerblichen oder unternehmerischen Anwendungen implementiert werden. Die eingebaute Passwortschutz-Funktionalität für RDX QuikStor SATA III-Laufwerke ist ein zusätzlicher Pluspunkt. RDX PowerEncrypt sichert höchste Vertraulichkeit für Datenschutz mit branchenführender und regulierungskonformer AES-256 XTS-Verschlüsselung zusammen mit Zugriffskontrolloptionen.

Konform mit und validiert unter FIPS 140-2 Standards für Kryptografie, stellt RDX PowerEncrypt eine akzeptable Lösung für Regulierungsbehörden internationaler Industrien im Auftrag von Datensicherheit dar. RDX PowerEncrypt ist mit einer Reihe von Anwendungen wie Sicherung und Wiederherstellung, Archivierung, Datentransport und Datenaustausch kompatibel.

RDX PowerEncrypt ist aktuell für interne RDX QuikStor SATA III-Laufwerke mit Firmware-Level 0253 oder neuer zusammen mit dem neuen RDX-Manager Software-Dienstprogramm erhältlich. Im Einklang mit unserem intensiven Produktentwicklungsvorhaben wird es bald auch für andere RDX-Produkte verfügbar sein.