Netzwerkfähige RDX Systeme für sensible Umgebungen

Einsatz von Wechselmedien unter Einhaltung von Sicherheitsbestimmungen

Viele Unternehmen führen Sicherheitsbestimmungen ein, die den Anschluss externer Speichergeräte wie USB-Festplatten und Speichersticks an Laptops, Desktops oder Servern untersagen, um sich vor Viren oder Malware-Angriffen zu schützen.

Abwehr von Bedrohungen

USB-Peripheriegeräte haben sich zu einem attraktiven Tor für Cyber-Angriffe entwickelt. Die unkontrollierte Verwendung externer Speichergeräte gefährdet vertrauliche Unternehmensinformationen oder führt zur Blockierung von Computersystemen, die das gesamte Unternehmen lahmlegen kann. Daher werden lokal angeschlossene Speichergeräte oft nicht akzeptiert und Administratoren blockieren USB-Anschlüsse an Laptops, Desktops oder Servern.

Off-Site Datenschutz

Viele Unternehmen möchten jedoch nicht auf Wechselmedien verzichten, da sie Daten aus Compliance- und Datenschutzgründen extern speichern müssen.

Für maximale Datensicherheit ist es wichtig, Kopien der Sicherungsdaten außerhalb des Standorts aufzubewahren. Gemäß der 3-2-1-Sicherungsstrategie werden 3 Kopien der Sicherungsdaten auf 2 verschiedenen Medien gespeichert, wobei 1 Kopie außerhalb des Standorts gespeichert wird, wobei Medienrotation implementiert werden sollte. Dies bietet Schutz vor lokalen Katastrophen und schütz vor Viren- oder Ransomware-Angriffe.

Gesetzliche Bestimmungen schreiben vor, dass Daten über einen längeren Zeitraum aufbewahrt werden. Diese Daten sollten auch an einem entfernten Ort gespeichert werden.

Herausforderungen

- USB-Anschlüsse sind aus Sicherheitsgründen deaktiviert
- Unternehmen müssen aus Gründen der Compliance und der Sicherheit Daten auslagern
- Unternehmen benötigen eine kostengünstige und sichere Datenschutzlösung
- Backups müssen vor Viren- und Ransomware-Angriffen geschützt werden

Vorteile

- Einfach zu installieren und zu bedienen
- Keine besondere sorgfalt erforderlich
- Bietet Schutz vor Viren und Ransomware-Angriffe
- Transparente Integration in Sicherungs- und Archivierungsanwendungen
- Bietet umfassenden Schutz für vertrauliche Daten mit ausgelagerten Kopien
- Bietet WORM Funktionalität für die konforme Datenarchivierung
- Flexible Skalierbarkeit mit verschiedenen Medienkapazitäten und unbegrenzter Kapazität außerhalb des Standorts

Das netzwerkfähige RDX

Als etablierter Standard mit Eigenschaften, die über andere einfache Datenspeicherprodukte hinausgehen, ist RDX die vertrauenswürdige Technologie für Wechseldatenträger. Das robuste, widerstandsfähige Design stellt einen zuverlässigen und wertigen Datenspeicher bereit. Durch die Auslagerungsmöglichkeit ist RDX ideal für die Notfallwiederherstellung von Geschäftsdaten.

Kundenvorteile

- Nahtlose Integration in bestehende Umgebungen; Keine Änderung des Arbeitsablaufs
- Offsite-Speicherfunktionen mit umfassendem Datenzugriffsschutz
- Erschwingliche und niedrige Gesamtbetriebskosten
- Erfüllt die gesetzlichen Anforderungen für elektronisch gespeicherte Daten
- Benutzerfreundlichkeit
- Zukunftssicher durch vollständige Vorwärts- und Rückwärtskompatibilität

Die netzwerkfähige RDX-Lösung bietet mehr Flexibilität. Das System lässt sich problemlos in die vorhandene Ethernet-Umgebung integrieren und bietet eine erweiterte Benutzerfreundlichkeit, unabhängig von Einschränkungen der USB-Anschlüsse. Es bietet austauschbaren Speicher über das Netzwerk und gewährleistet die normale Datensicherung und -wiederherstellung sowie den vollständigen Datenschutz bei Desastern oder Viren- und Ransomware-Angriffen. RDX ist eine wesentliche Komponente für jede Backupstrategie in einer virtuellen, physischen oder hybriden IT-Infrastruktur.

Erweiterte Sicherheit mit RDX RansomBlock*

RDX ermöglicht das Loslösen des Speichersystems vom Netzwerk. Sobald Speichergeräte nicht mehr mit dem Netzwerk verbunden sind, sind die Backupdaten auf dem RDX Medium geschützt und können nicht durch Malware-Angriffe bedroht werden.

In einigen Fällen kann das RDX-Medium jedoch nach Abschluss eines Sicherungsjobs nicht ausgeworfen werden. Sehr oft führen Unternehmen mehrere Sicherungen pro Tag durch, da sie es sich nicht leisten können, Daten über einen bestimmten Zeitraum zu verlieren. Das RDX-Medium bleibt also eingelegt und die Sicherungsdaten sind gefährdet.

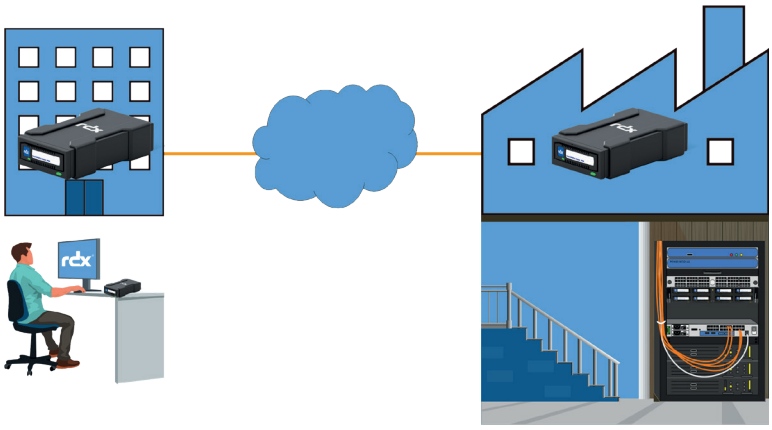
In diesem Fall sollte RDX RansomBlock eingeführt werden, um die auf RDX gespeicherten Daten online zu schützen. Mit RansomBlock können nur autorisierte Anwendungen wie z.B. Backupsoftware Änderungen an den Daten vornehmen und gleichzeitig den Datenzugriff vor Cyberangriffen schützen. RDX RansomBlock benötigt keine Sicherheitsupdates und stellt die vollständige Datenwiederherstellung bei infizierten Daten oder blockierten Computersystemen sicher.

Datenschutz auch beim Auslagern

Zusätzlich zu den Funktionen zum Schutz vor Desastern und Cyberangriffen bietet RDX auch Schutz vor Datendiebstahl für Medien, die außerhalb des Standorts gespeichert oder unterwegs sind. Durch den integrierten Passwortschutz ist es für nicht autorisiertes Personal schwierig, auf die Daten auf dem RDX-Medium zuzugreifen, selbst wenn ein RDX-System verfügbar ist.

Einfaches Datenmanagement

RDX QuikStor von Overland-Tandberg ist ein erschwingliches System mit niedrigen Gesamtbetriebskosten. Es vereinfacht alle Aufgaben im Bereich Datenmanagement. Optionale Software bietet Datensicherheit und erfüllt die Compliance-Anforderungen. Mit einer Speicherkapazität von 500 GB bis 5 TB erfüllt sie die meisten Anforderungen für Sicherung, Speicherung und Archivierung.



*Optionales Feature