BackupAssist™ ER

Vollautomatisiertes Disk-to-Disk-to-Cloud-Backup

DATENBLATT

BackupAssist ER schützt vor:

- Ausfällen durch Naturkatastrophen und beschädigte Hardware sowie
- modernen Bedrohungen wie Ransomware und Hackerangriffen.

Schützen Sie Daten mit Disk-to-Disk-to-Cloud-Backups, mit denen lokale Backups (Onsite) und sichere Cloud-Backups (Offsite) erstellt werden.

Stellen Sie mit BackupAssist ER Daten von jedem Rechner aus wieder her, egal ob granular oder vollständig. Die CryptoSafeGuard-Funktion schützt Ihre Backups vor Angriffen und Verunreinigung durch korrupte Daten.

Mehrere Schutzschichten ermöglichen schnelle und zuverlässige Wiederherstellungen von Onsite- und Offsite-Backups.

AUF EINEN BLICK

Ransomware-Schutz
- Schutz der Backups vor Ransomware
- Scannen nach Anzeichen von Ransomware
- SMS-Benachrichtigung bei Warnungen

Schnelle lokale Sicherung
- Von Festplatte zu Festplatte in die Cloud
- Anwendungskonsistente Backups
- Umgekehrte inkrementelle Sicherung

Sicherung in der Cloud
- Zero-Knowledge-Verschlüsselung
- Deduplizierung und Komprimierung
- Bandbreitenoptimierung

Wiederherstellungsfunktionen
- Bare-Metal-Restore
- Schnelle Wiederherstellung auf einer VM
- Restore von Dateien und Anwendungen

Mehrschichtiger Schutz

BackupAssist ER schützt Ihre Backups auf drei Arten vor Ransomware:

- **Backup-Schutz:** verhindert, dass nicht autorisierte Prozesse Daten erstellen, löschen oder aktualisieren
- **Detector-Funktion:** scannt die Daten auf Anzeichen einer Ransomware-Infektion und blockiert die Ausführung von Jobs
- **CryptoSafeGuard:** sendet im Falle eines erkannten Risikos sofort eine Warnung per SMS

Disk-to-Disk-to-Cloud

Erstellen Sie schnelle lokale Image-Backups, die in die Cloud repliziert werden. Sie sind anwendungskonsistent, sodass Ihre SQL- und Exchange-Datenbanken sowie andere VSS-fähige Anwendungen geschützt sind.

BackupAssist ER erstellt wahlweise bei Microsoft Azure, Microsoft Azure Blob Storage, Amazon S3 sowie EL storage / Wasabi und weiteren S3-kompatiblen Speichern eine geschützte Offsite-Kopie. Für die Übertragung und Sicherung werden die Daten zwecks Effizienz und Datenschutz komprimiert sowie verschlüsselt. Inkrementelle Backups sowie Bandbreitenoptimierung sorgen für minimale Belastung Ihres Netzwerks.

Wiederherstellungsmöglichkeiten

Dank Bare-Metal-Backups führen Sie granulare oder vollständige Restores auf abweichender Hardware, in der Cloud oder auf einer VM von jedem Backup und von jeder Installation aus durch. Mit VM Instant Boot können Sie eine neue Hyper-V-VM aus dem Backup booten und so die Ausfallzeit im Notfall minimieren. Auch granulare Wiederherstellungen von Dateien, Ordnern, einzelnen SQL- und Exchange-Datenbanken oder sogar einzelnen Exchange-Postfächern, E-Mail- und Kalendereinträgen sowie Kontakten sind problemlos möglich.

BackupAssist™ ER

DATENBLATT

Technische Daten

VM Instant Boot

VM Instant Boot ermöglicht das Booten eines Backups als Hyper-V-Gast. Dies minimiert die Ausfallzeit und bringt Ihr Unternehmen innerhalb weniger Minuten wieder online.

Cloud VM Disaster Recovery (VMDR)

Wenn Ihr lokales Backup und Ihr Server verloren gehen, laden Sie Ihre Cloud-Sicherung auf eine neue Installation herunter und verwenden Sie dann VM Instant Boot zur Wiederherstellung auf Hyper-V.

Unterstützte Betriebssysteme

- **Windows Server 2022**
- **Windows Server 2019**
- **Windows Server 2016**
- **Windows 10**
- **Windows 11**

32-Bit- und Core-Versionen von Windows werden nicht unterstützt.

Ransomware-Schutz

- **Direkter Backup-Schutz:** CryptoSafeGuard Shield verhindert die unbefugte Veränderung von Backups.
- **Scannen nach Ransomware:** Der CryptoSafeGuard Detector lässt nicht zu, dass von Ransomware betroffene Inhalte Backups verunreinigen.
- **Benachrichtigungen:** Mitteilungen sind konfigurierbar und können per E-Mail und SMS versendet werden.

Lokale Sicherung

- **Unterstützte Ziele:** jede lokal zugeordnete Festplatte (USB, iSCSI) oder Netzwerkfreigabe (einschließlich NAS)
- **Backup-Dateiformat:** VHDX-Dateikette, Öffnung mit Standard-Windows-Tools
- **Versionierung:** Speicherung vergangener Backups mit einem inkrementellen System
- **Aufbewahrung:** Anzahl der Backups, die aufbewahrt werden sollen
- **Verschlüsselung:** Option zur AES-256 CBC-Verschlüsselung
- **Ausfallsicherheit:** automatische Wiederherstellung bei Unterbrechung einer vorherigen Sitzung

Cloud-Backup

- **Unterstützte Ziele:** Microsoft Azure, Microsoft Azure Blob Storage, Amazon S3 sowie EL storage / Wasabi und weitere S3-kompatible Speicher
- **Sicherungsdateiformat:** proprietäre, deduplizierte, komprimierte und verschlüsselte Datenchunks
- **Vergangene Versionierung:** jederzeit inkrementell
- **Aufbewahrung:** Anzahl der Backups, die aufbewahrt werden sollen
- **Verschlüsselung:** AES-256
- **Deduplizierung und Komprimierung:** erzielt typische Speicherplatzeinsparungen von 50 bis 75 %
- **Ausfallsicherheit:** automatische Wiederherstellung bei Unterbrechung einer vorherigen Sitzung

Wiederherstellung

- **Erstellung von Lifeline Recovery-Medien:** Erstellung von Medien mit einer beliebigen von BackupAssist ER unterstützten Plattform
- **Größe der Lifeline Recovery-Medien:** etwa 512 MB
- **Bare-Metal Disaster Recovery (BMDR)-Optionen:** P2P, P2V, V2P, V2V, P2C, V2C, C2P, C2V, C2C
- **Unterstützte Medien:** USB-Laufwerk oder ISO-Datei
- **Exchange Granular:** lokales Backup erforderlich, Wiederherstellung aus Cloud-Sicherung nach Download der Exchange-Datenbank möglich

VM Instant Boot

- **Backup-Typ:** unterstützt lokale und Cloud-Backups eines kompletten Servers (BMR-fähig)
- **Hyper-V-Unterstützung:** Wiederherstellung Ihres Servers auf jeder von BackupAssist ER unterstützten Plattform mit Hyper-V (einschließlich Windows 10)
- **Original-Backup:** separate Speicherung von Änderungen während des Betriebs der wiederhergestellten VM, gleichzeitig bleibt das Original-Backup unangetastet