

BackupAssist ER protects your business from:

- traditional outages such as natural disasters and damaged hardware, and
- modern threats like ransomware and hacking.

Protection is achieved with Disk to Disk to Cloud backup jobs that create both local backups (onsite) and secure, cloud backups (offsite).

With BackupAssist ER, all backups are recoverable from any machine and can be used for both full system recoveries and granular recoveries. The backups will always be there for you, as its CryptoSafeGuard feature shields your backups directly from attack while also preventing them from being polluted with corrupted data.

These core features work together to protect your business and provide a clear path to a predictable, successful recovery



FEATURES AT A GLANCE

Ransomware protection

- › Shield backups from attack
- › Scan for signs of ransomware
- › SMS notification of alerts

Fast local imaging

- › Disk to disk to cloud
- › Application consistent backups
- › Reverse incremental imaging

Image to the cloud

- › Zero-knowledge encryption
- › Deduplication & compression
- › Bandwidth throttling

Recovery capabilities

- › Bare-metal recovery
- › Fast recovery to a VM
- › File and application recovery

With **multiple layers** of protection, BackupAssist ER makes it easy to achieve **predictable** and **successful recoveries** from local and cloud backups

LAYERED PROTECTION

Ransomware protection

CryptoSafeGuard protects your backups from ransomware in 3 ways. Backup Shield prevents unauthorized processes from creating, deleting or updating your back up data. The Detector feature scans the back up data for any signs of a ransomware infection and blocks jobs from running, effectively maximizing the availability of good backups for recovery. CryptoSafeGuard sends a fast SMS to let alert you of any detected risks.

Disk-to-disk-to-cloud

Create fast local image backups that are replicated to the cloud. They are application-consistent so your SQL and Exchange databases and other VSS-aware applications are protected. The backup format is a reverse-incremental chain of VHDX files, with optional AES 256 CBC encryption, providing backup history while improving reliability and speed of access for the latest backup.

Our new cloud technology sends the image to your choice of Microsoft Azure Blob Storage or Amazon S3, providing a safe, offsite copy of your data, well protected from cyber attacks. For transmission and storage, the data is deduplicated by data chunks within files, then compressed and encrypted for privacy and efficiency. This achieves zero-knowledge encryption while ensuring every next backup is incremental. Further, BackupAssist ER supports bandwidth throttling to minimize impact on your network.

Recovery capabilities

With BackupAssist ER bare metal backups, you can perform a granular recovery, an instant recovery, or a full recovery to dissimilar hardware, cloud or VM from any backup, from any installation. Creating a single Lifeline Recovery media as a bootable drive or ISO gives you a specialized boot environment supporting bare metal recoveries to larger or smaller disks, and with control over the target disk per volume. With VM Instant Boot you can quickly recovery by booting a new Hyper-V VM from the backup, which minimizes downtime and gets your business back online within minutes. And granular recoveries of files, folders, individual SQL and Exchange databases, or even recoveries of individual Exchange mailboxes, mail and calendar items and contacts are easy with BackupAssist ER's built-in recovery capabilities.

TECHNICAL CONSIDERATIONS

VM INSTANT BOOT

VM Instant Boot allows you to boot a backup as a Hyper-V guest. This minimizes downtime and gets your business back online within minutes.

CLOUD VM DISASTER RECOVERY (VMDR)

If your local backup and server are lost, download from your cloud backup to a new install, then use VM Instant Boot to recover to Hyper-V.

SUPPORTED PLATFORMS

BackupAssist ER supports the following OS:

- > Windows Server 2019
- > Windows Server 2016
- > Windows Server 2012 r2
- > Windows 10

32-bit and core versions of Windows are not supported.

RANSOMWARE PROTECTION

- > **Direct backup protection:** CryptoSafeGuard Shield prevents unauthorized modification of backups
- > **Scanning for ransomware:** the CryptoSafeGuard Detector doesn't let ransomware-effected content pollute backups
- > **Notifications:** configurable, sent by email and SMS

LOCAL BACKUP

- > **Supported destinations:** any locally mapped disk (USB, iSCSI) or network share (including NAS).
- > **Backup file format:** VHDX file chain. Can be opened using standard Windows tools.
- > **Past versioning:** historical backups are stored using a reverse incremental system.
- > **Retention:** specify the number of backups that you want to keep.
- > **Encryption:** option to encrypt using AES-256 CBC encryption.
- > **Resilience to failure:** supports automatic recovery if a previous backup was interrupted.

CLOUD BACKUP

- > **Supported destinations:** Amazon S3 bucket, Microsoft Azure blob storage container.
- > **Backup file format:** proprietary deduplicated, compressed and encrypted data chunks.
- > **Past versioning:** forever incremental.
- > **Retention:** specify the number of backups that you want to keep.
- > **Encryption:** data is encrypted using AES-256.
- > **Deduplication and compression:** achieves typical space savings of 50% to 75%.
- > **Resilience to failure:** supports automatic recovery if a previous backup was interrupted.

RECOVERY

- > **Lifeline Recovery media creation:** create the media using any BackupAssist ER supported platform.
- > **Lifeline Recovery media size:** approximately 512MB.
- > **Bare-metal Disaster Recovery (BMDR) options:** P2P, P2V, V2P, V2V, P2C, V2C, C2P, C2V, C2C.
- > **Supported media:** USB drive or ISO.
- > **Exchange Granular:** requires a local backup. If you need to restore from a cloud backup, you can download the Exchange database first.

VM INSTANT BOOT

- > **Backup type:** supports local and cloud backups of a full server (BMR-capable). Support for encrypted local backups will be added in an upcoming release.
- > **Hyper-V support:** recover your server on any BackupAssist ER supported platform running Hyper-V (including Windows 10).
- > **Original backup:** changes made while running the recovered VM are saved separately, and the original backup is not touched.