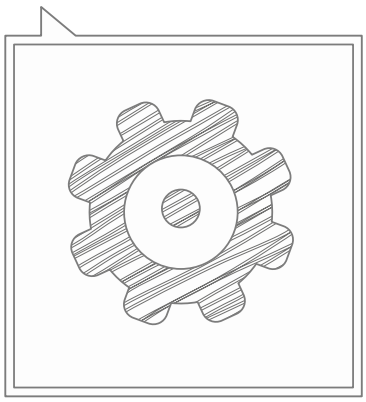
TABLE OF CONTENTS



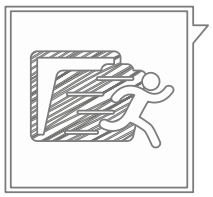
KEEPITSAFE DR: ADVANCED DATA PROTECTION

Robust and reliable, **KeepItSafe® DR** is a fully managed service supporting Windows and Linux environments. It is also application-aware, thereby effectively protecting your mission-critical Microsoft Exchange, Microsoft SQL, and Microsoft SharePoint applications.

KeepItSafe DR protects not only physical platforms but VMware ESX, VMware ESX(i), and Microsoft Hyper-V virtual platforms via a single user interface, recovering application data from a block level to an individual file locally in just minutes.

KeepItSafe DR is an all-in-one online backup and IT disaster-recovery solution that backs up and restores not just data but the entire OS and all the applications required to access your data. If the entire local server crashes, the KeepItSafe off-site server is instantly turned on, and the original server's data, complete OS and applications are available for use, as though they never left. It is push button data recovery of your entire environment in minutes not days.

KEY FEATURES



RAPID RECOVERY

What It Does:

- ✓ Enables near-zero downtime.
- ✓ Data and applications on non-system volumes are instantly available and accessible during recovery-
  - Rapid recovery instantly runs or resumes physical or virtual machines on any virtual platform (including VMware vSphere ESX(i), Microsoft Hyper-V, Citrix XenServer or Virtual Box) directly from the backup file.
  - When a non-system volume is being restored, KeepItSafe DR presents the volume metadata to the operating system instantly, and makes data available on demand.

How It Works

- ✓ You initiate restoration of a non-system volume from the KeepItSafe DR core console.
- ✓ The KeepItSafe DR agent on the target machine quickly begins to restore the metadata (directory structure, security descriptors, NTFS file attributes, free space map, etc.) of the target volume.
- ✓ Once metadata is restored, the volume and its contents become available to the system.
- ✓ The agent then begins restoring data blocks from the KeepItSafe DR core server, and writing the blocks to the target volume.
- ✓ Requests for data are prioritized, and blocks are immediately restored and delivered to the requesting program or system.
- ✓ Requestor is unaware that data was just recovered, ensuring a seamless recovery.
- ✓ Agent continues restoring all of the data in the background while prioritizing data requests as received, until the restore is complete.

BACKUPS AND ARCHIVING

KeepItSafe DR Backup Options:

- ✓ Minimizing RPOs with scheduled backups and retention policies-
  - KeepItSafe DR's scheduled backups can capture the entire system as often as every five minutes. This enables you to achieve a five-minute recovery point objective, which ensures minimal data loss when recovery is required. Backups can be restored down to the individual file level.
  - Retention rules ensure that backups are kept for the correct amount of time (defined in minutes, hours, days, weeks, months or years), and that backups no longer needed are automatically deleted to reduce storage requirements.
- ✓ Minimizing RTOs with Rapid Recovery or a virtual standby-
  - KeepItSafe DR Rapid Recovery helps you meet tight RTOs by making data and applications on nonsystem volumes instantly available and accessible during a recovery. Specifically, it presents the volume metadata to the operating system, putting the volume, with its data, applications and services, back in production. It then restores the data in the background, prioritizing the restoration of any specific data requested by users.
  - Using the KeepItSafe DR virtual standby feature ensures high availability of your mission-critical servers at all times. With a virtual standby, you can significantly improve business continuity with highly granular, five-minute RPOs and near-zero RTOs. Any machine protected with KeepItSafe DR can be converted automatically to a virtual machine on VMware (either in ESX(i) or workstation), on Microsoft Hyper-V, or on Virtual Box. The virtual standby will be continuously updated with the block-level changes from the source server on a scheduled basis. If your protected machine should go down, simply fire up the virtual standby.

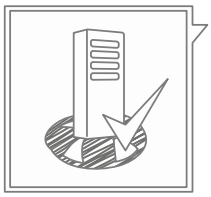
BACKUP, REPLICATION, AND RECOVERY

What It Does

- ✓ Continuously protects the workloads on your VMs, physical servers, or cloud severs with KeepItSafe DR's incremental forever snapshots (up to 288 times a day), which guarantees up to five-minute recovery point objectives (RPOs).
- ✓ For aggressive recovery time objectives (RTOs), Rapid Recovery allows you to access data directly from backup files almost instantly, until the production machine is restored.

How It Does It

- **Verified Recovery** - Perform automated recovery testing and verification of backups for Microsoft Exchange and SQL Server. KeepItSafe DR performs automated nightly mount checks of file systems, Microsoft Exchange and SQL Server instances. If a problem is found with corrupt data or application data that will prevent these from being mounted, you are alerted. This gives you time to correct the issues before you need to restore the data after an incident. Identify data corruption early and prevent maintenance or transfer of corrupted data blocks during the backup process (mountability checks).
- **Rapid Recovery** - Leverage near-instant recovery technology for protected virtual machines or servers. Access the damaged server's application and data directly from the backup image if there's an outage, so users remain productive and your IT team meets stringent RTOs and RPOs.
- **Universal Recovery** - Restore backups from physical to virtual, virtual to virtual, virtual to physical, or physical to cloud, as well as carry out bare-metal restores to dissimilar hardware.
- **Virtual Standby** — Continuously export data from a protected machine to a virtual machine (VMware, Hyper-V, or VirtualBox), creating a highly-available bootable copy of the protected machine.
- **Global Deduplication and Compression** - Inline deduplication and compression eliminates redundant data to save storage costs while optimizing backups for WAN replication.
- **FIPS Certification** - Ensure enterprise-class security compliance with FIPS 140-1 and 140-2 cryptographic modules.



CONFIRMED RECOVERY (MOUNTABILITY CHECKS)

Confirmed Recovery tests your backups automatically to ensure your Microsoft applications can be fully recovered at any time. Production machines aren't affected by the testing process, which takes place on a separate core. After the first full backup, KeepItSafe DR runs incremental-forever backups for much greater speed and efficiency.

How It Works

- **Integrity Check** - Backup of all servers, including Exchange, SQL Sever, and SharePoint, quickly checks for catastrophic corruption. This takes only a few seconds to enumerate the files located in the backup and ensures that files are accessible and not severely damaged.
- **SHA-256 Checksum** — When enabled, checksum is executed automatically by the KeepItSafe DR smart agent on Microsoft Exchange, SharePoint, and SQL servers.
    - For Exchange servers, KeepItSafe DR performs nightly checksums on the Exchange database (EDB). Every Exchange database page has a field that contains a checksum of that page, which is calculated every time the page is modified. KeepItSafe DR automatically calculates the checksum of the backed-up EDB pages and then compares the values to the ones stored in the EDB pages themselves to ensure the integrity of the backed-up page. By performing a checksum verification on the EDB, KeepItSafe DR enables administrators to easily adhere to Microsoft's best practices of performing checksum verification before log truncation.

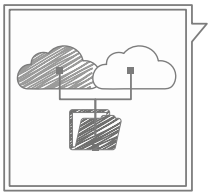
- We have identified no other backup and recovery product on the market that allows log truncation only if the checksum is successful. This is important because without a successful Exchange backup or the presence of transaction logs, Exchange recovery becomes impossible. To ensure that checksums are done quickly, KeepItSafe DR will perform a checksum only on EDB pages that have changed since the last checksum analysis.

✓ **Mountability Check (Exchange backups only)**

- While the checksum ensures the integrity of Exchange data, it alone cannot guarantee that a backup is recoverable, so KeepItSafe DR also performs a mountability check on every Exchange snapshot.
- An EDB that passes a checksum for the integrity of its pages can fail the mountability check if it is missing data — for example, if it has incomplete volume groups or if its EDB, log or, file paths are not in the location specified by metadata.
- Mountability checks work by simulating a real mount of the Exchange database to the KeepItSafe DR core server, using technology from KeepItSafe and from Microsoft (ESUTIL) to mount the volumes containing the EDB, system, and log paths.

✓ **Attachability Check (SQL and SharePoint backups only)**

- Due to the nature of their databases, Microsoft SQL and SharePoint use an attachability check rather than the mountability check employed by Exchange.
- The databases are attached to an off-production SQL instance installed on the KeepItSafe DR Core server.
- This check automatically determines whether highly transactional and business-critical databases are thoroughly backed up and tested prior to recovery, running as if the database was restored. If the database fails to attach to SQL then KeepItSafe DR will fail the job and send you an alert.



BIDIRECTIONAL REPLICATION

KeepItSafe DR offers two replication strategies – multi-hop replication and chained replication. This gives organizations flexibility to deal with limits on bandwidth, replication window constraints, and restrictions on the number of incoming and outgoing replication tasks.

✓ **Multi-Hop** - A protected agent is replicated to multiple KeepItSafe DR cores:

- One of the most important aspects of a good disaster recovery plan is maintaining up-to-date copies of vital data in multiple locations to minimize downtime and data loss. KeepItSafe DR makes it easy for organizations to replicate their data to multiple sites quickly and efficiently.
- By replicating their protected machines to multiple sites simultaneously, company XYZ can be assured that if one site goes down, the Web and database servers can be brought up at a secondary site in a matter of minutes.

✓ **Chained Replication** - With KeepItSafe DR, a company can choose a chained replication approach in which core server A replicates all of

its data to core server B, and in turn core server B replicates its data, along with the data from core server A, to the core server C site.

- This replication approach is useful if, for example, the Los Angeles site has significantly more bandwidth capabilities than the San Diego site, making replication to Houston faster.

KEEPITSAFE DR: BEYOND BACKUP

Key advantages of KeepItSafe DR protection:

- ✓ **Rapid and Flexible Recovery:** KeepItSafe DR shines on recoveries too, delivering aggressive, near-zero application recovery time objectives (RTO), and over-performs when it comes to the granularity of its recovery point objectives (RPO). You can specify snapshots as frequently as every five minutes to effectively eliminate the potential for data loss. Legacy backup system users who are limited to being able to back up only once a week, or once a day, will find KeepItSafe DR's highly granular recovery time flexibility a welcome revelation.
- ✓ **Reliable Recovery:** Integrated replication and daily verification of both data and application integrity through KeepItSafe DR's backup verification technology. It validates recoverability of critical data in the event of disaster.

Innovative KeepItSafe DR Core Technologies:

- ✓ **Global Deduplication and Compression:** Save storage costs through integrated, inline deduplication and compression while optimizing backups for WAN replication. It eliminates redundant data from your backups not just locally, but across your entire network.
- ✓ **Universal Recovery™ to any VM or Server:** KeepItSafe DR was built from the ground up for virtual and physical environments, enabling one of the fastest and most flexible recovery procedures possible – in minutes, not hours or days, with a near-zero RPO. KeepItSafe DR provides full bare-metal recovery to dissimilar hardware and VM servers in seconds as well as granular recovery of individual objects, applications, files, or messages in just minutes.
- ✓ Combined, these technologies deliver fast, reliable, and secure local recoveries and cloud-enabled disaster recovery. With its scalable object store, KeepItSafe DR is uniquely capable of handling exabytes of data, or more, rapidly, with built-in global deduplication, compression, encryption, and replication to any private or public cloud nfrastructure. Flexible enterprise data-retention policies are supported for recovery and compliance purposes.

Data Off-Siting and Disaster Recovery:

- ✓ **WAN Optimized Replication:** KeepItSafe DR offers new WAN-optimized, deduplication-aware replication for off-siting data to public or private clouds.
- ✓ **SmartAgent with Incremental-Forever Approach for VMs and Physical Servers:** SmartAgents use an incremental-forever, changed-block-tracking approach that tracks, captures, and transmits the changed blocks from the protected disk volume to the KeepItSafe DR core at preconfigured intervals. They are fully application-aware and lie dormant when not in use. Even when they're hard at work, the ultra-light SmartAgents tread lightly.

- An RMW algorithm is tightly coupled with deduplication; the two cores match keys before transferring data, then replicate only the unique blocks that are compressed- encrypted- deduplicated across the WAN. This can result in up to a 10X reduction in bandwidth requirements. All data in-flight is replicated over SSL connections.

✓ **Virtual Standby:** Create and maintain an up-to-date virtual standby machine for fast disaster recovery for all of your Windows workloads, including Exchange, SharePoint, and SQL. The bootable virtual machine is an exact clone of the production server as of the last snapshot.

✓ **Failover and Fail-Back:** If the worst occurs and you do suffer a data disaster, KeepItSafe DR supports failover and fail-back in replicated environments. In case of a comprehensive outage, the target core in the secondary site can recover instances from replicated machines and immediately commence protection on the failed-over machines. Once the primary site is restored, the core can "fail-back" protection to the machines at the primary site.

✓ **Retention Policies:** KeepItSafe DR offers highly flexible and granular backup retention policies that can be easily customized for different business and compliance requirements without compromising availability or the integrity of the backups. Customers with Big Data can now rely on KeepItSafe DR to retain very large amounts of data with complex retention policies by using metadata operations to perform roll-up operations for aging.

Virtualization and Cloud:

✓ **VMware, Hyper-V, and XenServer Support:** KeepItSafe DR can export any protected or replicated machine to VMware, Hyper-V, or XenServer. Exports can be ad hoc or continuous. With continuous exports, the virtual machine is incrementally updated after every snapshot. The incremental updates are very fast, so standby clones are ready to power up with a click of a button. The formats for export are VMware Workstation/Server on a folder, direct export to Vsphere/VMware ESX(i) host, Microsoft Server 2008/R2 Hyper-V and Citrix XenServer.

✓ The hot standby (Virtual Standby, see above) option is the best way to ensure the fastest recovery times. When you set up in continuous mode, it will make (and update after every snapshot) a virtual machine to a vCenter or Hyper-V host of your choice. This can allow you to stand up a downed server as a Virtual Machine in a matter of minutes. The virtual standby function allows you to minimize the down time of a failure by ensuring that rather than running a complete export of the latest backup at the time of the crash, you will already have the data exported (or in process of being exported) to a virtual environment where you can then manually boot the machines and bring them back online. What we will need to find is a balance between the interval of snapshots and the speed at which your core can actually run the exports. As long as the core is simply taking incremental snapshots and exporting incrementals then it shouldn't be an issue. For larger servers, VMware does not support larger than 2TB volumes unless you are on ESXi 5.5, otherwise export to Hyper-V 2012 will allow for virtual disks larger than 2TB using VHDX format.

UNDERSTANDING RETENTION POLICY AND ROLLUP

- When protecting your data using KeepItSafe DR, backup snapshots are taken frequently (according to the protection policy defined) and are saved to the repository specified by the core. These recovery points are deduplicated before they are committed, and each represents the ability to restore the agent machine as of the point when the snapshot was taken. The more frequently an agent is backed up, the more granular the recovery point. Whether one agent or many are backed up to a core, they proliferate quickly in the repository. To conserve resources over time, this data is then generally rolled up to an incrementally less-granular series of recovery points.
- For disaster recovery purposes, you must also back up system metadata (which includes information about file-set attachment points, storage pools, volumes, and policies) separately.

BACKUP AND RESTORE KEEPITSAFE APPLIANCE SETTING

You can back up KeepItSafe's appliance-setting information to a file, and later restore these settings if you have problems with the core machine or if you want to migrate the settings to a different machine. Backed-up information includes:

- Repository metadata (e.g., repository name, data path, and metadata path).
- Machines protected in the core.
- Replication relationships (targets and sources).
- Machines configured for virtual standby.
- Information about encryption keys.

Contact **KeepItSafe DR** at **888 965 9988** to schedule a free Network Evaluation and Data Protection Assessment.