TABLE OF CONTENTS

SECURE CLOUD BACKUP AND RECOVERY

Information is one of your company's most valuable assets, and it gets more difficult to manage every day. **KeepItSafe® Online Backup** securely stores in the KeepItSafe Cloud the data you generate from servers, databases, enterprise applications, mobile devices, cloud applications, and virtual machines.

Should you ever need to recover your data, KeepItSafe Online Backup combines the rapid recovery time of a private cloud application with the cost savings, compliance, and scalability of a public solution.

Plus, it requires no on-site equipment, and integrates all data-protection into a secure, accountable, off-site solution for the setup, monitoring, and management of all you data backups.

KEY FEATURES

AGENTLESS SOLUTION

One installation backs up your entire network. Agentless architecture is secure because it does not need to be installed on each machine, eliminating the need for open ports on your firewall and dramatically enhancing security by removing points of attack withinagent-basedarchitectures.

Online Backup software is able to eliminate the need for locally installed agents because it leverages the protocols, APIs, methods, and functionality that platform, operating system, database, and other application vendors use for remotely accessing and managing their own systems.

While other backup/restore solutions require a unique backup agent for each type of system and application (installed on every target server, workstation, and laptop), the Online Backup architecture integrates support for all major platforms and applications into a single, optimized software system consisting of just two major components: the DS-Client (just one installed at each remote site) and the DS-System (installed at the vaulting location).

DS-Client software installed at either a local or remote site captures data from target backup machines; the DS-Client then conducts several data-reduction processes, compresses, encrypts, and transmits the data via an IP WAN to the DS-System at the central location.

FAST BACKUP & RESTORE

After a full initial backup, achieving fast backup and restore performance requires using Changed Block Tracking (via APIs) and/or Online Backup's incremental forever technology.

During a backup operation, common files are de-duplicated both locally and globally. Then incremental delta block changes of data are compressed and encrypted prior to transport over the WAN. Data remains encrypted in-flight and at-rest. The backup data is only unencrypted by the original client when the original client has retrieved the encrypted data from the data center for a restore.

Online Backup uses de-duplication, compression, and delta blocking to cut down on backup traffic, as well as the software's ability to counter data theft through strong AES encryption.

24/7 CORRUPTION DETECTION

Our 24/7 Corruption Detection tool guarantees data integrity with zero corruption for successful restores. It runs seamlessly in the background, constantly scanning for corrupted or problematic files. This can include files with data corruption or logical inconsistencies caused by third-party technologies (such as faulty RAID controllers, file systems, operating systems, disk subsystems, network packet loss, etc.). As Corruption Detection checks backup files, it automatically corrects file and directory ID duplications without the need for human intervention. When Corruption Detection finds a problematic file that it cannot fix at the central-site location, it automatically triggers the software at the remote site to re-synchronize and resend any corrupted files during the next scheduled backup — all without human intervention.

DATA SECURITY

Communication between the DS-Client and DS-System is always initiated by the DS-Client. This communication is secured by a **5-layer protection** system:

1. **Network Access Protection**
   This layer ensures that the only TCP ports that need to be enabled are those used by the DS-System and DS-Client services.

2. **Configuration Layer Protection**
   This layer ensures that the DS-Client must pass its customer account and DS-Client number(s) to the DS-System, which ensures the connection is from a legitimate party.

3. **Registration Layer Protection**
   Each time a DS-Client communicates with the DS-System, it sends a unique identifier, called a hardware cookie, to register with the DS-System. This identifier is based on the DS-Client's operating system and hardware configuration (partitions, memory, CPUs, etc.).

4. **Encryption Authentication**
   Encryption authentication validates access to backed up data. A one-way hash of the DS-Client's encryption key is performed to create two encryption cookies. This hash is used to ensure that data being backed up or restored is encrypted with the same key.

5. **Communication Encryption**
   By default, all of the following communications are encrypted with a randomly generated, 256-bit encryption key:

- ✓ Between the GUI and service/daemon (e.g., DS-User to DS-Client).
- ✓ Between service/daemon and service/daemon (e.g., DS-Client to DS-System).
- ✓ This ensures that a 3rd-party cannot decrypt the communication between Online Backup software components. Even if the communication method is unencrypted, customer data always remains encrypted with customer encryption keys.

BANDWITH OPTIMIZATION

One of the biggest challenges with protecting remote sites is managing WAN bandwidth costs. For service providers, managing bandwidth costs is an essential factor in delivering a profitable backup service. Service providers' WAN costs are based on the amount of bandwidth consumed across all customers at peak times. Optimizing the amount of band width being consumed in the data center mitigates steep fluctuations, which lowers the operational costs associated with bandwidth for service providers.

The combination of deduplication of data, continuous deltas, and data compression changes the economics of protecting data in the service providers' favor, enabling them to reduce the amount of WAN bandwidth used (minimizing operational costs) and reduce the amount of storage capacity required to deliver the service. This combination is not a one-time cost savings but an ongoing requirement in ensuring the economic viability of the service. Bandwidth throttling functionality enables bandwidth management, as well.

Online Backup software runs with negligible impact on servers, workstations, and laptops, eliminating the CPU-cycle hits associated with agent-based solutions. Delta blocking, common file elimination, and compression technologies also minimize impact on bandwidth and storage resources.

EXCHANGE BACKUPS

Our cloud backup provides you with multiple features to ensure that your enterprise information assets in Microsoft Exchange are protected in the most efficient and effective manner:

Single-pass Microsoft Exchange backup
Recover data to the level of granularity that you choose from a single backup of your Microsoft Exchange database.

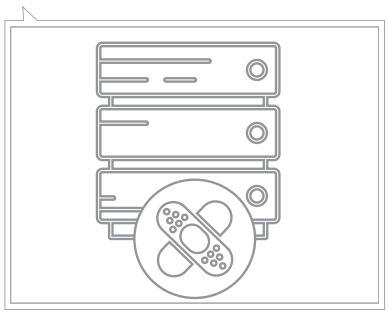
Granular recovery
Restore the complete database, individual accounts, or just a single email based on the need of the hour.

Restore location flexibility
Have the ability to recover the information to the same location that you back it up from, or to an alternative location of your choice.

Non-disruptive backups
Back up your large, all-important email repository without affecting the performance of the application.

Enterprise scalability
Protect everything from single instances to large Microsoft Exchange clusters in physical and virtual implementations.

Automated and efficient
Automate your backup operations through features that include scheduling options and automated inclusions of new mailboxes, reducing the need for manual intervention.

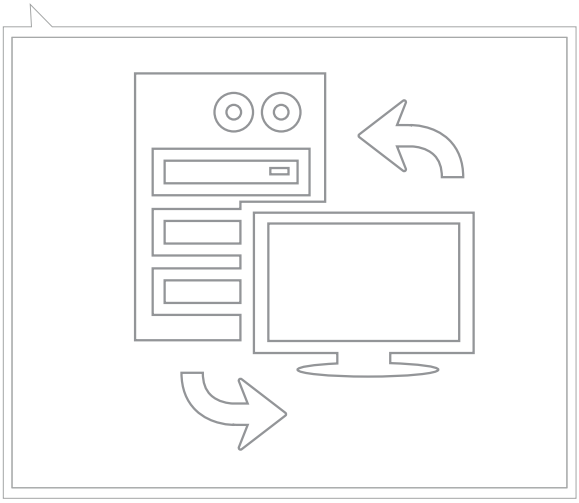


LONG TERM ARCHIVING

Retention allows long-term archival of DS-System backup data:

1	To save money while still offering data protection by archiving obsolete generations, deleted data, and old data.
2	To enable compliance with backup regulations by allowing periodic copy archiving, and to provide data destruction (with certificate).
3	To provide optional off-site replication for additional redundancy and compliance.

KeepItSafe Online Backup BLM Archive is for data that changes infrequently, if at all, and for data that does not need to be available for immediate restores. Once data is backed up to BLM it will not change. BLM Archive packages are searchable and browsable so individual files and folders can be restored via the Web. BLM makes it possible to keep older data, and older generations of data, protected and recoverable at a lower cost. If you need to restore a large amount of data, we can ship it to you free on a portable drive (encrypted).



FEATURE-BENEFIT SUMMARY

Item	Category	Feature	Description	Benefit
1	Assurance/ Service	System monitored by trained engineers	Available 24/7 to help by phone, email or chat.	We'll take care of the backups, allowing you to focus on the rest of your business. Plus, enjoy simplified data recovery with single-source accountability across the enterprise.
2	Flexible Set up	Multi-model implementation with choice of public, private, or hybrid cloud architecture	We can set up your backup in such a way that you can back up solely off-site (public or private), or back up through a combination of on-premise backup (to a KeepItSafe appliance) and off-site backup.	
3	Security Certificates	NIST FIPS 140-2 security certification	Is a U.S. government computer security standard used to accredit cryptographic modules. The title is "Security Requirements for Cryptographic Modules".	Our encryption standards are so high that they've attained the seldom-issued FIPS 140-2 certificate.
4	Security Certificates	ISO 27001 certification	The ISO 27000 family of standards helps organizations keep information assets secure. Using these standards we manage the security of assets such as financial information, intellectual property, employee details, or information entrusted to us by third parties such as yourself.	We go the extra mile to ensure that our processes and procedures provide the maximum assurance to your organization.
5	Redundancy or Security	Data securely backed up at multiple off-site data centers	For redundancy.	Redundancy lowers the likelihood that data can ever be lost.

FEATURE-BENEFIT SUMMARY

Item	Category	Feature	Description	Benefit
6	Security	AES 256 bit encryption in transit and at rest	The Advanced Encryption Standard (AES), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192, and 256 bits. 256-bit requires the most cycles and thus is the least likely to be vulnerable to an attack today or far into the future.	Impenetrable.
7	Security	Customer-empowered dual-key encryption and authentication	This ensures that the data you transfer to us during backups is encrypted by both the sender (you) and the recipient (us).	Yet another security measure we take to ensure that your data is safe from the moment you send it off-site.
8	Security	5-step authentication process	We follow a strict number of steps to ensure that only authorized personal can access your data. These steps include Network Access Protection, Configuration Layer Protection, Registration Layer Protection, Encryption Authentication, and Communication Encryption.	
9	Customized Backup Process	Customizable archive and data retention policies configured to match business needs	This basically means that we can custom-design your backup frequency and version retention policies in accordance with your exact requirements.	Enables your team to access data within seconds after a loss.

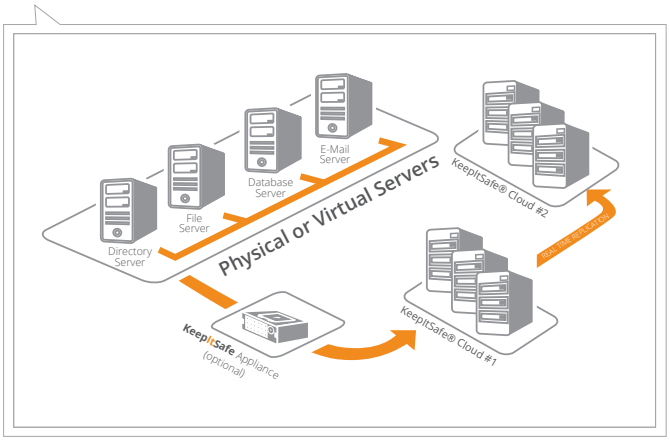
FEATURE-BENEFIT SUMMARY

Item	Category	Feature	Description	Benefit
10	Data Integrity	Systemic remediation	Guarantees data integrity with zero corruption for successful restores. This tool runs seamlessly in the background, constantly scanning for corrupted or problematic files. This can include files with data corruption or logical inconsistencies caused by third-party technologies.	
11	Deployment Efficiency	Agentless	If we are backing up 100 servers, an agent-based backup and recovery solution would require 100 application installs, whereas the agentless software requires only one installation for the same 100 servers.	Simple and efficient.
12	Operational Efficiency	Incremental forever	After an initial full backup, fast backup and restore performance is achieved either by leveraging changed block tracking (via APIs) and/or Online Backup's incremental forever technology.	
13	Operational Efficiency	Bandwidth optimization	We can throttle bandwidth and time backup to fit in perfectly with your bandwidth constraints. This, in conjunction with deduplication, continuous deltas, and compression, makes KeepItSafe a cost-effective solution.	Our backup solution will never overwhelm your organization's bandwidth, and our throttling functionality makes bandwidth management a breeze.
14	Operational Efficiency	Exchange backups flexibility	We can offer both message-level restores or database-level restores of your exchange data.	This flexibility simplifies recovering precisely the data you need. (Other services can only restore the DB, which makes finding a single email near-impossible.)

FEATURE-BENEFIT SUMMARY

Item	Category	Feature	Description	Benefit
15	Operational Efficiency	BLM archive	If your data changes infrequently then we have affordable backup and archiving solutions for you that provide the same high standard of security and service that our other products do, but at a lower cost.	
16	Assurance/ Service	Data validation	Virtualized data-recovery simulations ensure data is restorable whenever needed.	
17	Recovery	Virtualized disaster recovery	Failover path in near real-time.	Enables your team to access your data within seconds after a loss.
18	Service/User Experience	Unified dashboard for cloud, server and mobile endpoint data	This basically means that you can manage both your server backups and mobile endpoint backups from a single interface with at a glance dashboard.	We'll manage your backups, but if you want to see what is happening at a glance, our unified server backup and endpoint backup dashboards can help.
19	Tracking/ Documentation	Audit trail of all system backup and recovery activities	Every byte of data that is backed up or recovered is recorded by our system, and audit reports can be created whenever needed.	
20	Compliance	Our set-up is designed to comply with EU data protection regulations, HIPAA, FINRA and GLBA	We have processes and procedures in place that make us your ideal business associate, and we can sign documentation you need to substantiate this.	

HOW IT WORKS



1. When your scheduled data backup begins, data is transferred to the server with the installed Online Backup software.

2. When data reaches this server it is analyzed for data blocks that have changed or are new since the last backup. Those blocks are compressed and encrypted using military-grade encryption.

3. This compressed and encrypted data is transmitted over the Internet to one of our secure KeepItSafe data centers, where it will remain encrypted at all times.

4. Your encrypted data is replicated to a secondary, secure data center in the KeepItSafe network. This secondary location ensures your data is safe and can be restored in any type of emergency.

SYSTEMS SUPPORTED BY ONLINE BACKUP

Contact **KeepItSafe Online Backup** at **888 965 9988** to schedule a free Network Evaluation and Data Protection Assessment, plus a free software trail.