



# protectionnow.

SEP Cloud Application Protection Service  
for Microsoft 365

[www.sepsoftware.com/sepcaps](http://www.sepsoftware.com/sepcaps)

# Why your Microsoft 365 Data needs Backup:

*"Cloud-to-cloud backup is the only practical option for SaaS data protection.*

*Forrester Research, December 2017.*

## Data in the Cloud also gets lost

As companies move vital business data from on-premises to the cloud, new challenges in enforcing IT security arise.

According to a recent Cybercrime Survey from PwC, \*7 out of 10 companies have been hit by a cyberattack during the last 12 months – with the average data recovery cost at \$150,000. Human errors such as accidental deletion continue to be the number one reason for data loss.

Before SaaS applications such as Microsoft 365, most businesses had a local exchange server that was always backed up and secured. Likewise, your Microsoft 365 cloud data needs protection. The hard fact is that you can also lose data stored in the cloud – and data restoration can be quite a costly affair without an independent backup of your data.

## Are your Microsoft 365 Data at Risk?

Microsoft 365 is a great productivity solution operated under stringent security controls. Unfortunately, Microsoft 365 doesn't have native backup and flexible recovery capabilities for user data. Rather, Microsoft 365 relies on recycle bins and file version histories as recovery mechanisms, which are not true backup functionalities. It has many limitations for organizations recovering from serious internal and external attacks and can incur additional costs for data retention.

Built-in tools do not offer the clear separation of the backup from the production environment, as recommended as data protection best practice. Relying solely on Microsoft as your Microsoft 365 backup, means risking that your valuable sales and customer data could be lost forever.

## Reasons for Data Loss:

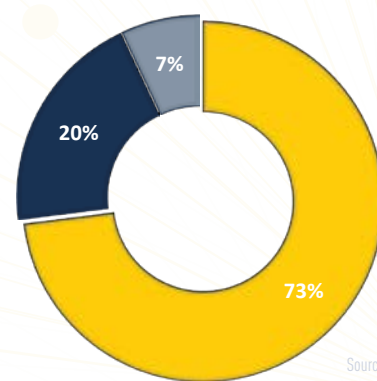
### Human Error 73%

- Accidental deletion & overwrites 63%
- Closing accounts 10%

### Hacking & Insider Threats 20%

- Hackers 13%
- Malicious deletes 7%

### 3rd Party Software 7%



## The Problems with Recovery via Microsoft

Microsoft 365 comes with limited backup and restore options. Microsoft relies on recycle bins and file versions as the main recovery mechanisms with many limitations for recovering from serious internal or external attacks. The native restore options are also very cumbersome, as they don't offer the ease of use or reliability of data. Finally, it may just be too late to restore your data: If, for instance, a user accidentally deletes an important email or file, and realizes this too late, there are no restore options with Microsoft, and your data is lost.

## Data Protection: Who is responsible?

### Customer

#### User errors

Accidental deletion & overwrites

#### Security attacks

Hacking events, Malware  
Malicious insiders

#### Data corruption

Sync errors

### SaaS Provider

#### Operational failures

Power outage  
Infrastructure failures  
natural disaster

## You are responsible for your Microsoft 365 Data Security

As a Microsoft 365 customer, YOU are responsible for ensuring the necessary protection of your Microsoft 365 data, not Microsoft. For example, in the event that data is lost due to accidental deletion – the number one reason for data loss – you are responsible for restoring the lost data. Microsoft will not cover any data loss caused by your own internal errors, malicious actions, ransomware or any other cybercrime event. In other words, the main reasons for losing data in the cloud are not covered by Microsoft.

# SEP Cloud Application Protection Service (CAPS) for Microsoft 365:

## Full Protection of Your Cloud Data

SEP CAPS cloud-to-cloud backup ensures full protection of your Microsoft 365 data across Exchange, SharePoint, and OneDrive. With SEP CAPS's automated backup to a physical independent and safe location, you can access your data anytime – even if your SaaS application is experiencing downtime.

## Daily Automated Backup

Once set up, SEP CAPS will run a daily back-up of your Microsoft 365 data every day, all year long. SEP CAPS guarantees a minimum of 1 daily backup, but normally runs 4-6 backups a day. With SEP CAPS, you can rest assured that your data is backed up and safe.

## Customized Retention

By default SEP CAPS offers unlimited retention for your Microsoft 365 data or according to individual requirements. This way, you don't need to worry about storage costs running out of control. SEP CAPS is a scalable backup service, customized to your needs.

## Activating Your SEP CAPS Account

In 3 easy steps, your SEP CAPS backup to Microsoft 365 is connected to Microsoft and running. SEP CAPS will automatically notify you in case of any backup problems via e-mail – it's a simple set-and-forget. SEP CAPS automatically detects and adds new users to the backup set too.

## GDPR

SEP CAPS is EU-GDPR-compliant and a data processor that works exclusively on the instructions of the data owner. This distinction is important in that SEP does not collect or store data that is not expressly designated by the data owner. No actions are taken without the instruction of the data owner.



## What Is Backed Up:

SEP CAPS will automatically backup all your data across your Microsoft 365 platform:

- Mails and Shared Mails
- In-Place Archives
- Calendar – Tasks – Contacts
- Groups (conversations, plans, files, sites, calendar)
- SharePoint Sites
- OneDrive
- Teams



## Quickly Find & Restore

With the Search & Restore functions, you can find and restore any of your Microsoft 365 data at any time. Browse or search across Exchange, SharePoint, and OneDrive, and locate specific backups of your data in a second. You may even scroll back and forth in time with the granular snapshot feature.

With SEP CAPS, all of your data across all snapshots is available at all times. Quickly restore anything from a single email or file from a single user to a complete user account. SEP CAPS also allows for cross-user restoration of data from one user to another as well as from one Microsoft 365 account to another.

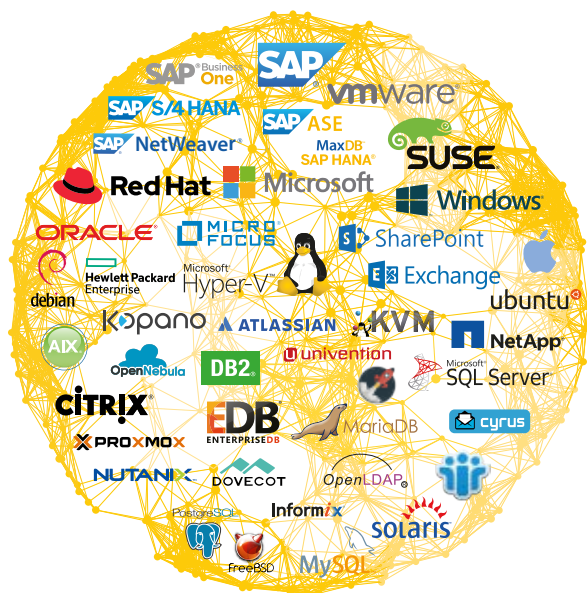


## Uniquely Tamper-Proof

With SEP CAPS no function allows overwriting of any existing data. The patent-pending blockchain algorithm makes low-level tampering impossible.

### SEP CAPS gives you:

- ✓ Automated daily backup to an independent location
- ✓ The broadest coverage in the market
- ✓ All backup is available 24/7
- ✓ Quick search function including granular feature
- ✓ Easy granular and in-place restore
- ✓ Unique point-in-time restore
- ✓ Backup – Search – Restore: An all-in-one solution
- ✓ Customized up to unlimited retention
- ✓ Sharing feature between users
- ✓ Simplicity and a user-friendly solution
- ✓ Compliance with regulatory requirements
- ✓ Option to add full backup of your endpoints
- ✓ Data retention even as long CAPS is no longer used i.e. when no new backup data is added



## The Company - more than 25 Years of Data Protection & Recovery Experience

SEP makes the world a little safer every day. With the hybrid backup and disaster recovery solutions, the data of companies and organizations are backed up around the clock and completely restored in the event of a disaster.

Our ambition: No data should be lost. This is why all components are extensively tested and constantly improved after development.

SEP has been developing and selling enterprise-wide data protection solutions since 1992, based in Holzkirchen near Munich. SEP has a strong partner network and relies 100% on resellers for sales.

## GDPR ready - compliant data protection and recovery

SEP sesam secures absolutely reliable business critical information, applications, databases and systems, which contain all kinds of information from sales and customer relations, production and administration up to financial and business transactions. Because of this importance, a comprehensive business continuity strategy is needed that focuses on Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs), which are essential in a disaster recovery scenario.

SEP sesam is optimized for securing virtualized and physical environments and enables compliance of legal requirements in heterogeneous IT environments. Encryption is one of the central technical elements.

Secure data retention is introduced by the encryption of the SEP Si3-DedupStore. After splitting the data stream into blocks and compressing each block, each individual block can now be encrypted with an arbitrarily definable key.

To restore the data, the key can be stored in the database of the backup server or the data owner must authorize a restore with his personal key. This encryption guarantees BSI conformity.

## Personal Contact

SEP AG  
Konrad-Zuse-Straße 5  
83607 Holzkirchen  
Germany



+49 8024 46331-0

info@sep.de

1.

## Try the 30-day full version now!



The SEP sesam 30-day full version includes all functions for optimal data backup & recovery, as well as a personal demo support.

2.

## SEP sesam Support Matrix



SEP sesam supports a large portfolio of operating systems, databases, virtualization platforms, applications and hardware snapshots.

3.