

**SEP**  
G Suite

**protectionnow.**

SEP Cloud Application Protection Service  
für G Suite

[www.sep.de/sepcaps](http://www.sep.de/sepcaps)

# Warum Ihre G Suite-Daten Backup benötigen:

## Auch in der Cloud gehen Daten verloren

Wenn Unternehmen wichtige Geschäftsdaten in die Cloud migrieren, entstehen bei der Umsetzung der Datensicherheit neue Herausforderungen.

Laut einer Cybercrime Umfrage von PwC\* wurden in den letzten 12 Monaten 7 von 10 Unternehmen von einem Cyberangriff getroffen. Die durchschnittlichen Kosten der Datenrettung betragen dabei 150.000 US\$. Menschliche Fehler, wie versehentliches Löschen sind nach wie vor der Hauptgrund für Datenverlust.

On-Premise Daten werden in Unternehmen und Organisationen selbstverständlich gesichert. Erfolgt die Nutzung als SaaS-Anwendung existiert aber keine Sicherung von G Suite Daten. Tatsache ist, dass die Wiederherstellung von, in der Cloud gespeicherten Daten - ohne eine regelmäßige Sicherung - unmöglich ist.

## Sind Ihre G Suite Daten gefährdet?

G Suite beinhaltet kein automatisches Backup & bietet nur minimalen Datenschutz. G Suite deckt keinen Datenverlust ab, der durch eigene interne Fehler, böswillige Handlungen, Ransomware oder andere Cyberkriminalität verursacht wird. Wenn Sie beispielsweise einen Benutzer löschen, werden alle Daten, die mit dem Konto des Benutzers verbunden sind, aus Google entfernt. Sich ausschließlich auf Google als Backup der G Suite zu verlassen, bedeutet, das Risiko einzugehen, dass Ihre kritischen G Suite Daten für immer verloren gehen können.

## Compliance mit Google Vault?

Abhängig von Ihren spezifischen gesetzlichen Anforderungen können Sie Google Vault verwenden, um die Anforderungen an die gesetzliche Datenspeicherung zu erfüllen, da Vault so konzipiert ist, dass es die Anforderungen an eDiscovery & Compliance erfüllt. Vault ist jedoch nicht für Backup- und Wiederherstellungsanforderungen konzipiert - um dies zu gewährleisten, benötigen Sie zusätzlich zu Google Vault eine zweite Anwendung.

## Datensicherung: wer ist verantwortlich?

### Kunde

#### User Errors

Versehentliches Löschen & Überschreiben

#### Sicherheitsangriffe

Katastrophen, Malware, Hacking-Ereignisse, böswillige Insider

#### Datenkorruption

Synchronisationsfehler

### SaaS Provider

#### Betriebsstörungen

Stromausfall, Infrastrukturausfälle, Naturkatastrophen

*“Cloud-to-Cloud-Backup ist die einzige praktische Option für SaaS-Datensicherung.”*

*Forrester Research, Dezember 2017.*

## Gründe für Datenverlust:

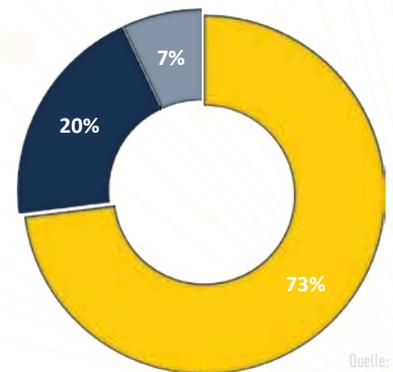
### 73% Menschliche Fehler

- Versehentliches Löschen & Überschreiben 63%
- Accounts löschen 10%

### 20% Hacking & Insider

- Hacker 13%
- Böswilliges Löschen 7%

### 7% Software von Drittanbietern



Quelle: Aberdeen Group

## Die Probleme mit Google Vault Restore

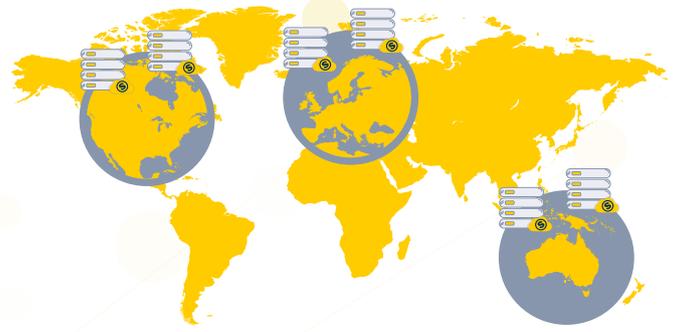
Vault stellt die Daten nicht in Google wieder her, sondern ermöglicht nur den Export von Daten. Um die Daten in das Benutzerkonto zu konvertieren und hochzuladen, ist manuelle Arbeit erforderlich und in den meisten Fällen geht jedes zuvor angebrachte Label verloren. Im Falle von Ransomware kann Vault frühere Versionen von Dateien wie MS Word, PPT oder Excel nicht wiederherstellen, sondern sucht nur nach den neuesten Versionen der Drive-Datei, ohne gelöschte Dateien einzubeziehen. Weitere manuelle Arbeiten folgen mit dem Herunterladen, Importieren in Drive, etc. Der Datentransfer zwischen Google Vault-Benutzern ist zeitaufwändig und komplex; Google Vault ermöglicht keine schnelle granulare Wiederherstellung.

## Sie sind für Ihre G Suite

## Datensicherheit verantwortlich

Die G Suite verfügt nur über eine begrenzte Datensicherung und -wiederherstellung. Als Kunde der Google G Suite sind SIE dafür verantwortlich, den notwendigen Schutz Ihrer G Suite Daten zu gewährleisten, nicht Google. Sie müssen sicherstellen, dass alle Ihre kritischen Daten vor Verlust durch versehentliches Löschen, Hackeraktivitäten, böswillige Insider und Synchronisationsfehler geschützt sind.

# SEP Cloud Application Protection Service (CAPS) für G Suite:



## Vollständiger Schutz Ihrer Cloud-Daten

SEP CAPS Cloud-to-Cloud-Backup gewährleistet den vollständigen Schutz Ihrer G Suite Daten. Mit dem automatisierten Backup von SEP CAPS an einem physisch unabhängigen und sicheren Ort können Sie jederzeit auf Ihre Daten zugreifen - auch wenn Ihre SaaS-Anwendung Ausfallzeiten hat.



## Täglich automatische Backups

Einmal eingerichtet, führt SEP CAPS mehrmals täglich Sicherungen Ihrer G Suite Daten durch. SEP CAPS garantiert ein Minimum von einem Backup pro Tag, führt aber in der Regel 4-6 Backups pro Tag durch. Mit SEP CAPS können Sie sicher sein, dass Ihre Daten gesichert und sicher sind.



## Individuelle Aufbewahrung

Standardmäßig speichert SEP CAPS Ihre G Suite Daten für 1, 5 oder 10 Jahre. Gerne bieten wir Ihnen auch benutzerdefinierte Aufbewahrungszeiten, die Ihre Anforderungen erfüllen. Es fallen keine extra Speicherkosten an. SEP CAPS ist ein skalierbarer Backup-Service, der auf Ihre Bedürfnisse zugeschnitten ist.



## Aktivierung Ihres SEP CAPS Accounts

In 3 einfachen Schritten wird Ihr SEP CAPS-Backup für G Suite eingerichtet. Sie werden automatisch über den aktuellen Systemstatus per E-Mail informiert - es ist ein sehr benutzerfreundliches Set-and-Forget. SEP CAPS erkennt neue Benutzer und fügt diese automatisch zum Backup-Set hinzu.



## Was gesichert wird:

SEP CAPS sichert automatisch alle Ihre Daten auf Ihrer G Suite-Plattform:

- Gmail
- Google Drive
- Google Team Drive
- Kalender
- Google Sites
- Aufgaben



## Schnelles Finden & Wiederherstellen

Mit den Funktionen Search & Restore können Sie jederzeit alle Ihre G Suite Daten finden und wiederherstellen. Browsen oder durchsuchen Sie G Suite Daten und finden Sie in Sekundenschnelle die gesuchten Backups.

Mit SEP CAPS sind alle Ihre Daten über alle Snapshots hinweg jederzeit verfügbar. Einzelne E-Mails, Dateien oder Objekte von einem einzelnen Benutzer bis hin zu einem vollständigen Benutzerkonto können nun einfach und schnell wiederhergestellt werden. SEP CAPS ermöglicht auch die benutzerübergreifende Wiederherstellung von Daten von einem Benutzer zum anderen.

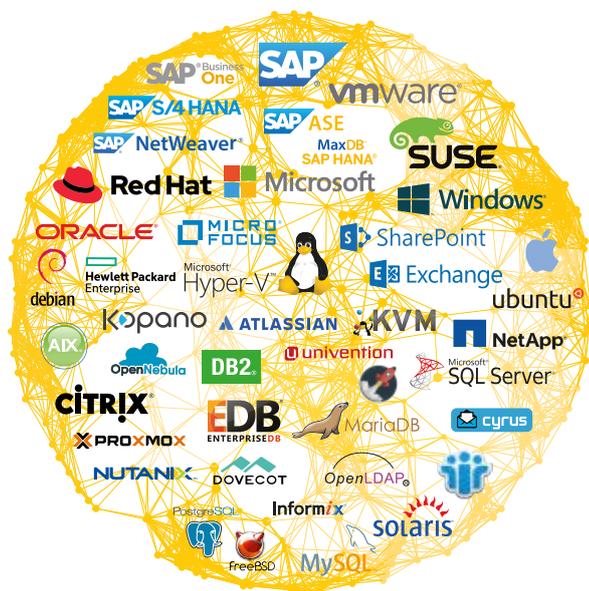


## Einzigartig Manipulationssicher

Bei SEP CAPS erlaubt keine Funktion das Überschreiben von vorhandenen Daten. Der zum Patent angemeldete Blockchain-Algorithmus macht Manipulationen auf niedriger Ebene unmöglich.

## SEP CAPS gibt Ihnen:

- ✓ Automatisiertes, tägliches Backup zu einer unabhängigen Lokation
- ✓ Die breiteste Abdeckung auf dem Markt
- ✓ Alle Backups sind rund um die Uhr verfügbar.
- ✓ Schnellsuchfunktion mit granularen Features
- ✓ Einfache granulare und In-Place-Wiederherstellung
- ✓ Einzigartige Point-in-Time Wiederherstellung
- ✓ Backup - Suche - Wiederherstellen: Eine Komplettlösung aus einer Hand
- ✓ Individuell angepasst bis zu unbegrenzter Aufbewahrung
- ✓ Freigabefunktion für Benutzer
- ✓ Einfachheit und Benutzerfreundlichkeit der Lösung
- ✓ Einhaltung der regulatorischen Anforderungen
- ✓ Option zum Hinzufügen eines vollständigen Backups Ihrer Endgeräte



## Das Unternehmen - mehr als 25 Jahre Erfahrung in Datensicherung & Wiederherstellung

SEP macht die Welt jeden Tag ein wenig sicherer. Mit den Hybrid Backup- und Disaster Recovery-Lösungen werden die Daten von Unternehmen und Organisationen rund um die Uhr gesichert und im Katastrophenfall vollständig wiederhergestellt.

Unser Anspruch: Es dürfen keine Daten verloren gehen. Deshalb werden alle Komponenten nach der Entwicklung ausgiebig getestet und ständig verbessert.

SEP entwickelt und vertreibt seit 1992 unternehmensweite Datenschutzlösungen mit Sitz in Holzkirchen bei München. SEP verfügt über ein starkes Partnernetzwerk und setzt beim Vertrieb zu 100% auf Reseller.

## DSGVO ready - gesetzeskonforme Datensicherung und Wiederherstellung

SEP sesam sichert absolut zuverlässig businesskritische Informationen, Applikationen, Datenbanken und Systeme, welche alle Arten an Informationen von Sales- und Kundenbeziehungen über Produktion und Verwaltung bis hin zu Finanz- und Businesstransaktionen beinhalten. Aufgrund dieser Wichtigkeit wird eine umfassende Business Continuity Strategie benötigt, die sich auf Recovery Point Objectives (RPOs) und Recovery Time Objectives (RTOs) fokussiert, welche essentiell bei einem Disaster Recovery Szenario sind.

SEP sesam ist für die Sicherung von virtualisierten und physikalischen Umgebungen optimiert und ermöglicht die Einhaltung von gesetzlichen Anforderungen in heterogenen IT-Umgebungen. Verschlüsselung gehört zu den zentralen technischen Elementen.

Die sichere Datenaufbewahrung wird durch die Verschlüsselung des SEP Si3-DedupStores eingeführt. Nach Zerlegen des Datenstroms in Blöcke und der Komprimierung jedes Blocks, lässt sich nun jeder einzelne Block durch einen beliebig definierbaren Key verschlüsseln.

Zur Wiederherstellung der Daten kann der Key in der Datenbank des Backupserver hinterlegt werden oder der Dateneigentümer muss eine Rücksicherung mit seinem persönlichen Key autorisieren. Diese Verschlüsselung garantiert BSI-Konformität.

## Persönlicher Kontakt

SEP AG  
Konrad-Zuse-Straße 5  
83607 Holzkirchen  
Deutschland

+49 8024 46331-0

[info@sep.de](mailto:info@sep.de)

1.

## Jetzt 30-Tage-Vollversion testen!



Die SEP sesam 30-Tage-Vollversion beinhaltet alle Funktionen zur optimalen Datensicherung & Wiederherstellung, sowie einen persönlichen Demo Support.

2.

## SEP sesam Support Matrix



SEP sesam unterstützt ein großes Portfolio an Betriebssystemen, Datenbanken, Virtualisierungsplattformen, Anwendungen und Hardware Snapshots.

3.