keepit®

Version 2 | 二版
www.version-2.com

Recovery for SaaS Apps

When Disaster Strikes

How Keepit enables business continuity and disaster recovery by safeguarding SaaS data in 7 steps

keepit®

Recovery for SaaS Apps When Disaster Strikes

Every day, businesses shift critical operations into cloud-based software-as-a-service (SaaS) applications; at the same time, cyber criminals are directing more effort toward cloud services, putting businesses at risk.[1]

Most businesses have some form of continuity and disaster recovery (DR) plan,[2] but these plans often take for granted that the crucial SaaS data needed to maintain or recover operations will be available—quickly, easily, and completely. Moreover, even experienced IT professionals often don't know that backing up data is their responsibility, rather than their SaaS providers'.

SaaS Provider's Responsibility	
Application	Harware Failure
Operation System	Software Failure
Virtualisation	Naturial Disaster
Hardware	Power Outage
Network	Physical Intrusion

Your Data — Your Responsibility	
Users	Human Errors
Data	Programmatic Errors
Administration	Malicious Insiders
	Ransomware Attacks
	Viruses/Malware

Unfortunately, many will learn the hard way that relying on SaaS providers to safeguard data introduces risk: according to Gartner, by 2022, 70% of organizations will have suffered a disruption due to unrecoverable data loss in a SaaS application.[3]

According to ESG, the most common reasons for data loss are service outages, accidental deletion, and external malicious deletion such as ransomware attacks (Figure 2).

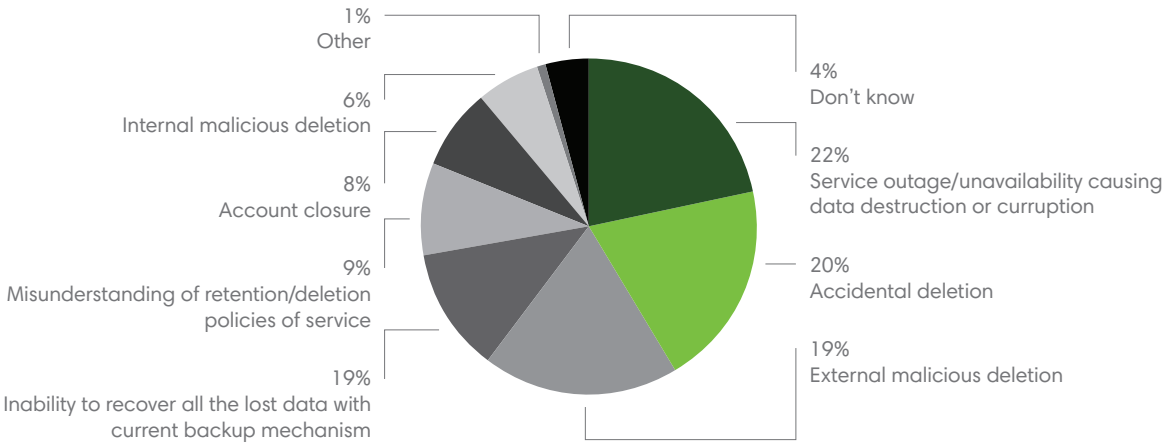
[1] In January 2021, the United States' Cybersecurity and Infrastructure Security Agency (CISA) warned of the increasing threat, in Analysis Report (AR21-013A): Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services [CISA]

[2] See Only 54% of organizations have a company-wide disaster recovery plan in place [Security Magazine]

[3] Gartner, Assuming SaaS Applications Don't Require Backup Is Dangerous, Nik Simpson & Michael Hoeck, 5 August 2021

Other reasons include problems with backup mechanisms and retention/deletion policy misunderstandings. Additionally, ESG uncovered that 81% of Microsoft Office 365 users had to recover data, but only 15% were able to recover 100% of their data.[4]

Figure 2: Top Causes of SaaS Data Loss
What is the top cause of data loss for the SaaS-based applications your organization uses? (Percent of respondents, N=344)



Preserving Access to Essential Data

Keepit's mission is to protect data in the cloud. Since 2013, we have worked tirelessly to purpose-build an efficient and secure data protection solution that provides simple, reliable, cost-effective, and vendor-neutral backup and recovery for SaaS workloads.

In the pre-SaaS paradigm, organizations could often perform a full disaster recovery on their own, but the move to the cloud has introduced new complications and dependencies:

- Full SaaS application restoration requires the tenant to be restored and repopulated with data.
- Maintaining continuity in the meantime requires accessing SaaS data.

While Keepit does not replicate the SaaS application and all its functionality, the solution provides controlled, convenient—and instant—access to SaaS data in a usable format, so organizations can maintain continuity; plus, Keepit's secure backups ensure SaaS data can be restored once the application returns to a healthy status.

[4] ESG, Technical Validation, Keepit: Dedicated Data Protection for SaaS Workloads, Kerry Dolan, October 2021

Consequences of the Cloud

In the on-premises model, meeting a Recovery Time Objective (RTO) is largely dependent upon backup and restoration of systems and associated customer data. Over time, organizations have addressed their continuity and recovery needs by investing in hardware and software solutions.

However, in the SaaS world, things are quite different. Maintaining continuity during — and recovering from — a disaster involving SaaS applications both depend upon:

- How completely and quickly data can be *accessed*, regardless of the SaaS application's state.
- How completely and quickly data can be *restored*, once the application tenant is operational.

Therefore, achieving DR objectives as an organization requires accounting for both:

- Cloud *data availability*, which is largely the customer's responsibility, and
- Cloud *application availability* (e.g., M365), which is controlled by the application vendor.

For the majority of organizations — i.e., those lacking the specialized skill sets and extensive resources required — the most reliable and cost-effective way to ensure availability of SaaS data is to use a third-party data protection service.

An all-too-common threat: ransomware

To illustrate the distinction between access and restoration, and to show how the Keepit Cloud plays a key role in enabling both business continuity and quick, safe disaster recovery, we'll use an example of a ransomware incident. Today's most devastating ransomware attacks employ a two-pronged approach to maximize disruption and apply pressure. Frequently, attackers:

- Use a compromised administrator account to impede recovery options (e.g., by turning off versioning, flushing out recycle bins, deleting/encrypting data).
- Detonate ransomware on one or more endpoints to encrypt local copies of data; these copies subsequently get synchronized in cloud repositories, resulting in the online data estate becoming encrypted and inaccessible.

Such attacks threaten organizations worldwide, large and small, and — powered by a vicious cycle in which proceeds fuel increased cybercrime operations[5] — they are occurring with increasing frequency.[6]

[5] Research from Palo Alto suggests the average ransom in the first half of 2021 is $570,000 USD, an increase of 171% over the year prior; see Average Ransomware Payment Hits $570,000 in H1 2021 [Dark Reading]

[6] Research from Check Point reports that ransomware incidents increased 93% year over year; see Ransomware attacks increase dramatically during 2021 [Computer Weekly]

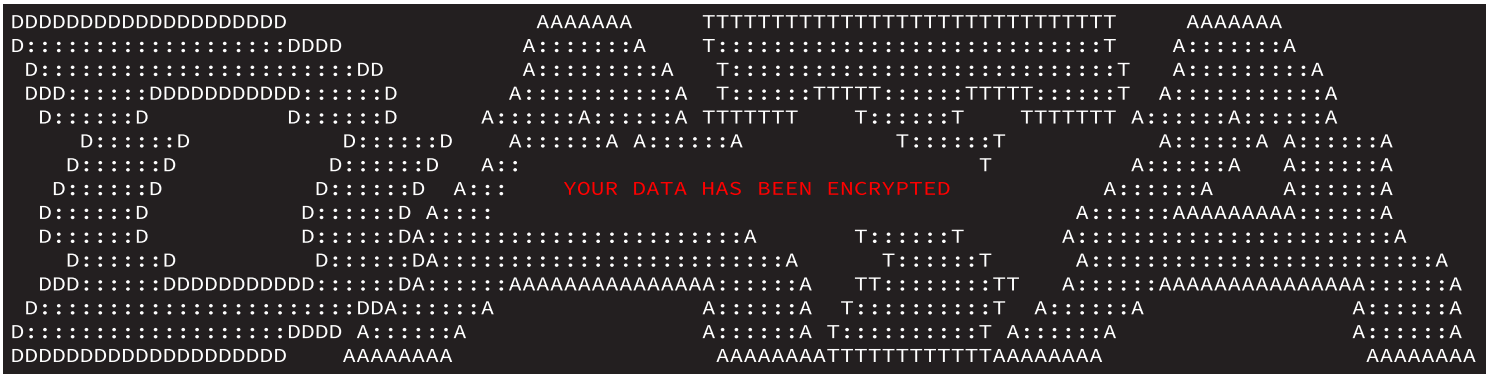
Disaster Strikes Acme: Ransomware and Recovery

Acme is a global IT services consultant with 6,500 employees. They handle sensitive client data and their business depends upon safeguarding private information and ensuring service availability.

Detonation

One holiday weekend, a threat actor detonates ransomware within Acme's environment. To disrupt Acme's operations, all email has been encrypted and the message from the attacker warns that OneDrive data will be encrypted if a ransom isn't paid within 72 hours.

Ransomware disrupts Acme's operations



Upon learning of the attack, Acme's leaders enact their:

- Incident Response (IR) plan, which includes guidance for: business decisions; threat investigation, containment, and response; regulatory and contractual obligations; internal and external communications; procedures for engaging with law enforcement, etc.
- Disaster Recovery plan, which focuses on quickly and safely restoring operations (e.g., data and services) in a prioritized manner.

Microsoft OneDrive Recovery

Acme's DR plan refers to Microsoft's documentation page, Recover from a ransomware attack in Microsoft 365.[7] The purpose for this Microsoft article is to ensure customers understand the activities involved in SaaS recovery scenarios compared to on-premises application scenarios.

Step 1: Verify your backups

Microsoft advises that, *"If you have offline backups, you can probably restore the encrypted data after you've removed the ransomware payload (malware) from your environment,"* and adds, *"If you don't have backups, or if your backups were also affected by the ransomware, you can skip this step."*

Two points concern Acme:

- Microsoft offers no guarantee ("probably") that restoration is possible.
- Acme is aware that many ransomware families are adept at infecting backups,[8] which now has the IT staff worrying if their backups are impacted.

With Keepit

Keepit is a dedicated SaaS data protection solution completely separated from the Microsoft environment. Even an attack against the Azure ecosystem will not impact the backups.

Data stored in Keepit is completely immutable—and therefore cannot be encrypted or changed—and is always accessible regardless of the state of the SaaS application tenant.

Step 2: Disable Exchange ActiveSync and OneDrive sync

To *"stop the spread of data encryption,"* Microsoft's guidance is to *"temporarily disable user access to mailboxes,"* and to pause OneDrive sync to *"help protect your cloud data from being updated by potentially infected devices."*

With Keepit

Because Keepit's backups are separate from the Microsoft environment and completely immutable, data can be accessed completely independent of SaaS application availability.

[6] All excerpts from this page are as they appeared in October 2021

[7] In response to these developments, the United Kingdom's National Cyber Security Centre (NCSC) updated their malware guidance; see Updating our malware & ransomware guidance [NCSC]

Continued
While Acme's IT team understands the intention and necessity of these actions, they also recognize that disabling ActiveSync and OneDrive sync will prevent users from accessing their data—severely impeding many aspects of the Incident Response plan, especially those relying upon communication and collaboration.

Continued
This timely, secure, and restricted access — achieved through unique Keepit functionality called "Public Links" — ensures personnel can execute essential tasks while the wider IR and DR efforts are underway.[9]

Step 3: Remove the malware from the affected devices

Microsoft advises, *"Run a full, current antivirus scan on all suspected computers and devices to detect and remove the payload," and reminds the reader, "Don't forget to scan devices that are synchronizing data, or the targets of mapped network drives."*

Acme's staff know that every moment of downtime is harming their business, but they also know that they cannot rush this crucial step — which will take a long time, even with automation tools — without running the risk of reintroducing the ransomware into their environment.

With Keepit
Keepit's ability to provide access to SaaS data before application restoration allows organizations to maintain elements of continuity — and to execute on their DR and IR plans — during this potentially lengthy recovery step.

Access can even be scripted in advance utilizing powerful APIs, speeding up recovery efforts and simplifying continuity.

Step 4: Recover files on a cleaned computer or device

With the ransomware removed, it is now safe to *"use File History … or System Protection … to attempt to recover your local files and folders."* However, Microsoft's directions include two significant caveats:

- *"Some ransomware will also encrypt or delete the backup versions, so you can't use File History or System Protection to restore files."*
- *"If a folder is synchronized to OneDrive and you aren't using the latest version of Windows, there might be some limitations using File History."*

At this point, Acme is hoping to avoid these complications.

With Keepit
Once an application has returned to service, Keepit makes data restoration quick and simple.

Plus, unlike all-or-nothing services, Keepit's users can choose exactly what data from what time period to recover.

[9] To learn more about this valuable feature—demonstrated with a short tutorial video—see Share data with a public link [Keepit]

Step 5: Recover your files in your OneDrive for Business

For those files that can't be recovered using File History or System Protection, Microsoft offers that, *"Files Restore in OneDrive for Business allows you to restore your entire OneDrive to a previous point in time within the last 30 days."*

Acme's IT staff expected to encounter limitations, but the 30-day window was an unwelcome surprise. At this early point in the incident investigation, they have not yet determined when the attacker gained initial access into the environment — so there's a very real possibility that at least some files will need recovery from a point beyond the 30-day limit.

With Keepit

The 30-day access capabilities presumes the Microsoft tenant was healthy and configured correctly — but what if there was a problem with the tenant or the data has been compromised?

In an attack scenario, there are no assurances that any tenant data can be used. In contrast, all data stored in Keepit is immutable and instantly accessible. The business can allow users to access data from any point in time across the backup set — dating back as far as is needed.

Step 6: Recover deleted email

The encryption of their emails is a major problem for Acme — just as the attackers hoped. Unfortunately, Microsoft's instructions are clear that recovery is not a sure thing, saying *"In the rare case that the ransomware deleted all your email, you can probably recover the deleted items,"* before pointing to additional resources.

Acme's IT staff assure the C-level executives that their critical correspondence can "probably" be recovered.

With Keepit

Keepit's backups ensure organizations can fully recover data at any granularity — including individual items and mailboxes to entire SharePoint sites and OneDrive repositories, to entire tenants — from any point in time.

Step 7: Re-enable Exchange ActiveSync and OneDrive sync

After endpoints and other devices have been cleaned and data has been recovered, *"you can re-enable Exchange ActiveSync and OneDrive sync."*

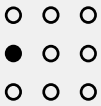
Only after recovery and synchronization — which can easily take many days — can Acme's team access their data and restore some level of normal operations.

With Keepit

If Acme was a Keepit customer, then their staff and trusted third-parties could have had access to data the entire time—maintaining some level of continuity and aiding in both IR and DR efforts.

Key Takeaways

While this example used Microsoft 365 as the SaaS service, the same concepts apply to others (e.g., Google Workspace, Salesforce, etc.). No matter the vendor, and no matter the reason for needing to access your data and backups:



Accessing data (i.e., finding and using it) is typically a more urgent need for your organization than full restoration (i.e., reloading data into services and applications).

"Recovery" for the SaaS vendor means making the infrastructure and application available — whether or not your data is there.

Recovery timelines can easily bloat to days, weeks, and even months.

Therefore, it is essential that you have a data backup solution—independent of the SaaS vendor's infrastructure—that allows users to access data instantly, as needed, and that enables quick, easy, and complete restoration of data into the application tenant.

Manage Risk and Recover with Confidence

To help enterprises avoid disruption due to lost or inaccessible SaaS data, Keepit has architected a dedicated, vendor-neutral SaaS data backup solution that is resilient, secure, and easy to use — after all, what good is a backup if you can't find what you're looking for or if it takes a long time to recover?

Plus, Keepit is fast to implement and has a predictable, all-inclusive pricing structure that doesn't require capital outlays — so you can get started right away.

Maintaining continuity

While Keepit doesn't replicate the application and all its functionality, it ensures SaaS data is always instantly accessible, in a usable format, so personnel can keep working even before applications and services become available.

Administrators can provide each user with a specific link, giving them secure access to all or parts of their data (or someone else's data, as required) within the entire backup history. Administrators can also include additional safety measures, like granting access only for a configurable amount of time.

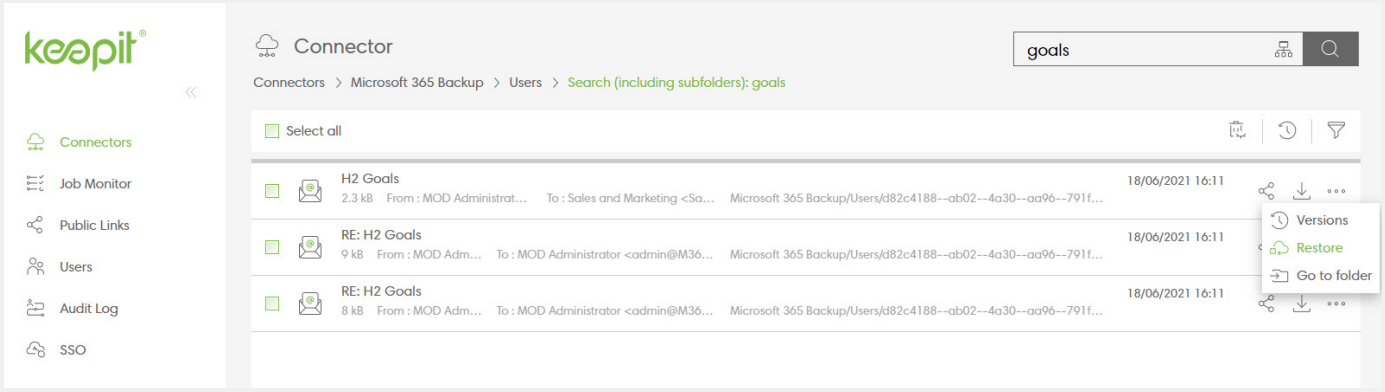
These operations can be performed via the UI, but for disaster recovery and other bulk activities we recommend scripting them and leveraging the API.

Restoring from a backup

The efficiency of Keepit's restore process is unparalleled in the market. To restore from a backup, simply search for or browse to the data you need and click "Restore." All your data with all your history is readily available for you in a modern web-based user interface that offers not only live browsing but also provides previews, downloads, and restores of your data elements.

And that's it — there are no extra steps. Plus, to enable fast and tiered recoveries (e.g., C-level and IT first, then operations, then support, etc.), data restoration can be scripted through our API.

Maintain business continuity with Keepit



Ready to protect your business?

If you would like to learn more about Keepit or start a free trial, please visit www.keepit.com or reach out to us at sales@keepit.com

Recommended by leading analysts and loved by customers globally, Keepit is the world's only independent cloud dedicated to SaaS data protection.

keepit®

Recovery for SaaS Apps

When Disaster Strikes

Version 2 | 版二
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore
Tel : (65) 6296 4268
Email : sales@version-2.com.sg