keepit®

When disaster strikes

A guide to data recovery and business continuity

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 overlook crucial SaaS app data needed to maintain or recover operations — thereby representing an essential gap in organizations' preparedness levels. Even experienced IT professionals aren't aware that backing up data is their responsibility, rather than their SaaS providers'.

SaaS provider's responsibility

Application	Hardware failure
Operating system	Software failure
Virtualization	Natural 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). In fact, ESG found that in 2023, 75% of organizations experienced at least one successful ransomware attack. Out of the organizations attacked, 84% lost some of their data, showing that recovery capabilities currently are not where they need to be to combat the growing threat.[4]

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.[5]

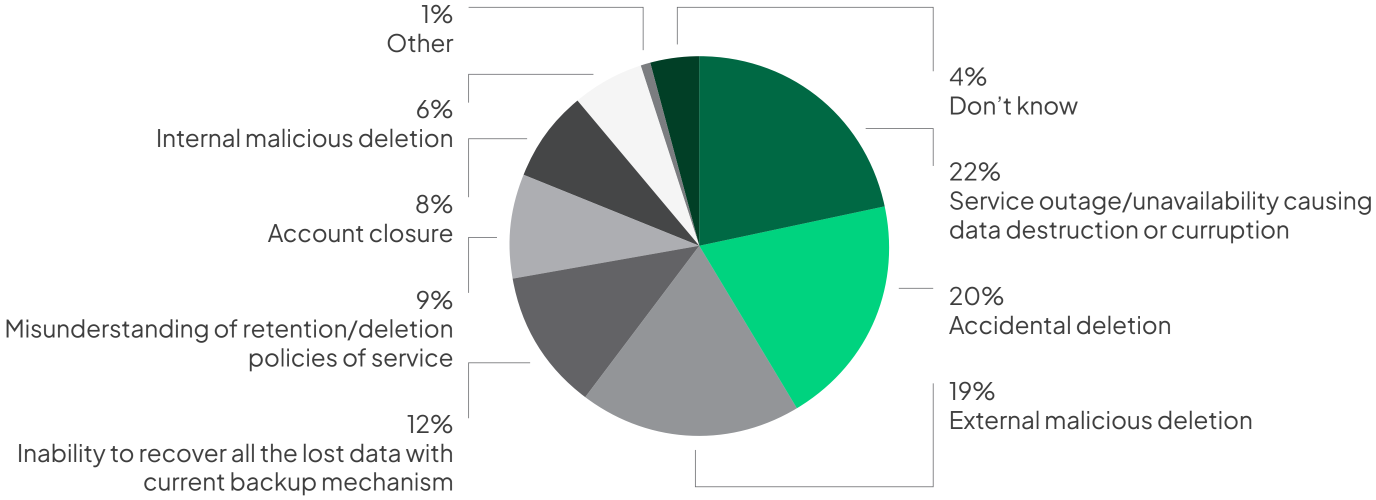

Figure 2: Top causes of SaaS data loss: What is the top cause of data loss for the SaaS-based applications your organization uses? (Percent of respondents, N=344)

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.

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:

1. How completely and quickly data can be accessed, regardless of the SaaSapplication's state.
2. How completely and quickly data can be restored, once the application tenantis 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 copiesof data; these copies subsequently get synchronized in cloud repositories,resulting in the online data estate becoming encrypted and inaccessible.

Such attacks threaten organizations worldwide and are powered by a vicious cycle in which proceeds fuel increased cybercrime operations.[6]

According to the World Economic Forum, cybercrime is now the world's largest economy, only behind USA and China.[7] They are occurring with increasing frequency Gartner research estimates that in 99% of attacks, backups and security products are targeted, as attackers are trying to take out organizations' defensive capabilities.[8]

Disaster strikes Acme: Ransomware and recovery

"Acme" (a fictional company used for this example), 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.

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 contractualobligations; internal and external communications; procedures for engagingwith law enforcement, etc.
- Disaster recovery plan, which focuses on quickly and safely restoringoperations (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.[9] 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 imspossible.
- Acme is aware that many ransomware families are adept at infecting backups,[11] which now hasthe IT staff worrying if their backupsare impacted.

With Keepit:

Keepit is a dedicated SaaS data protection solution that operates on an independent logical infrastructure completely separate from Microsoft’s environment. Attacks on the Azure ecosystem pose no threat to backups stored in Keepit as they are securely stored in our air-gapped cloud.

Data within Keepit remains entirely immutable, impervious to encryption or modification, ensuring constant accessibility irrespective of the SaaS application tenant’s status

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.*”

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.

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. 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.[10]

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 encryptor delete the backup versions, soyou can’t use File History or System Protection to restore files.”
- “If a folder is synchronized to OneDrive and you aren’t using thelatest version of Windows, there mightbe some limitations using File History.”

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

With Keepit:

After an application resumes service, Keepit streamlines data restoration, ensuring swift recovery.Our granular restore functionality fits seamlessly into customers’ disaster recovery plans, letting them prioritize critical data for faster restoration, minimizing downtime.

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

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 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.

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. Moreover, our "restore in place" feature preserves metadata and hierarchies, crucial for reinstating emails in a usable format, allowing seamless resumption of previous functionalities.

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 synchroniza-tion — 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.

Establishing priority users or data to be recovered first to ensure continuity. With granular, prioritized restores, organizations can return to operation while the full restoration is still underway.

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 granular restoration of data into the application tenant in a useable format.

Manage risk and recover with confidence

To help enterprises avoid disruption due to lost or inaccessible SaaS data, Keepithas architected a dedicated, vendor-neutral SaaS data backup solution that isresilient, secure, and easy to use — after all, what good is a backup if you can'tfind what you're looking for or if it takes a long time to recover? Plus, Keepit is fast to implement and has simplicity baked into the platform. No training is needed — 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, providing even greater efficiency and customization options.

This granular, prioritized recovery is crucial for reducing costly downtime and ensuring seamless business continuity. Our software seamlessly integrates into your existing disaster recovery processes, fitting into your business workflow effortlessly.

About Keepit

Keepit provides next-level SaaS data protection for companies with data stored in the cloud. Keepit's vendor-independent cloud dedicated to SaaS data protection is based on a blockchain-verified solution. Keepit protects data in key business applications including Microsoft 365, Microsoft Azure AD, Google, and Salesforce.Headquartered in Copenhagen with offices and data centers globally, Keepit is trusted by thousands of companies worldwide to protect and manage their cloud data.For more information visit www.keepit.com or follow Keepit on Linkedin.

End notes

[1] In January 2021, the United States' Cybersecurity and Infrastructure Security Agency (CISA) warned of the increasing threat, in Analysis Raeport (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

[4] ESG 2023 Ransomware Preparedness: Lighting the way to readiness and mitigation

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

[6] 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]

[7] Moschetta, et al., 2023. Cybersecurity in this era of polycrisis (https://www.weforum.org/agenda/2023/02/cybersecurity in an-era-of-polycrisis/)

[8] Research from Check Point reports that ransomware incidents increased 93% year over year; see Ransomware

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

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

[11] 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]