keepit®

Why compliance and continuity is good business for healthcare organizations

– and how secure backup of Microsoft 365 data gets you there

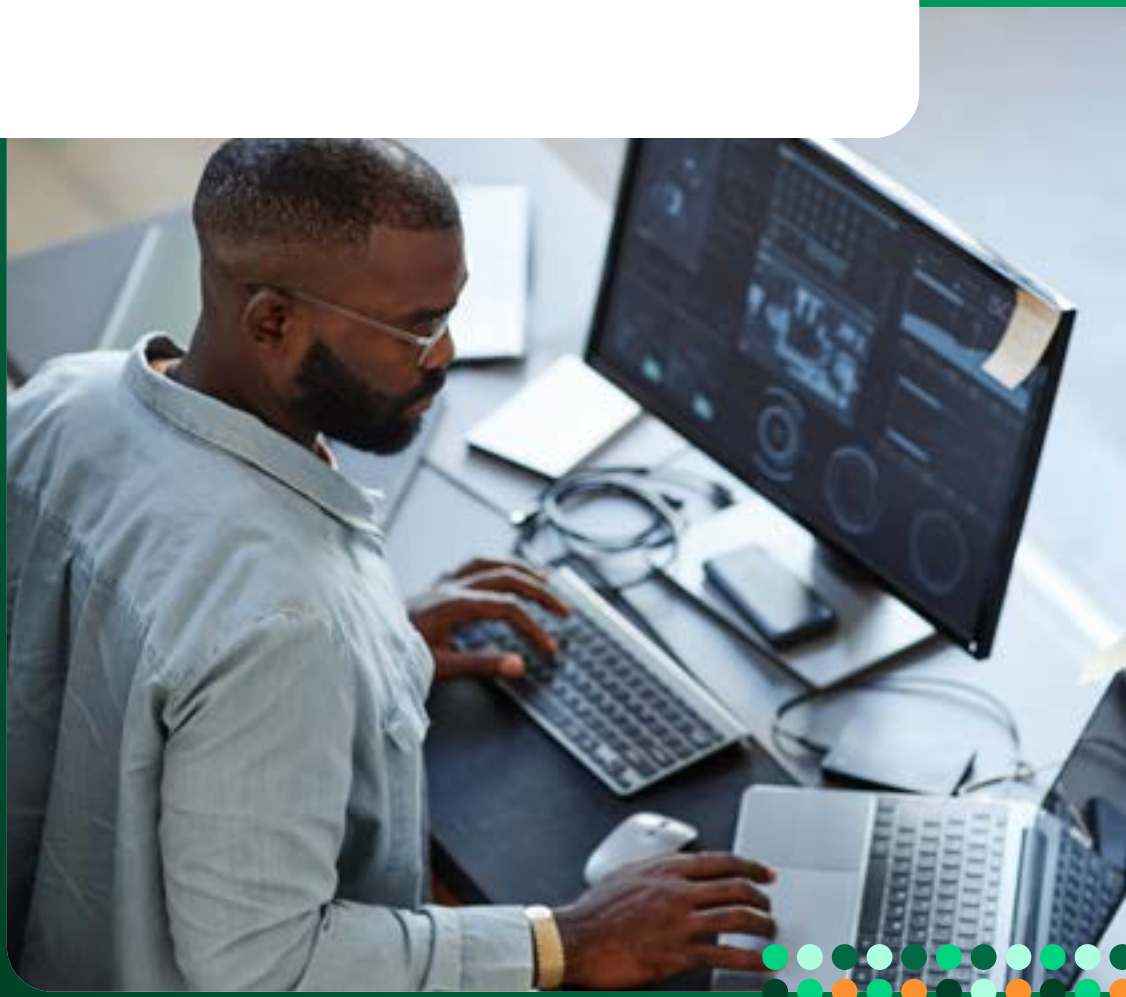


Table of contents

keepit

Introduction

This guide is for Operations, Security, and Technology leaders and decision makers within hospitals, clinics, and other healthcare delivery organizations (HDOs) using the Microsoft 365 (M365) line of subscription services.

By reading this guide and completing the short exercises within, you will learn:

- Why backups of SaaS data are essential to your organization
- Why those backups must be provided by a dedicated third party
- Your SaaS data risk and protection readiness
- How to strengthen your budget requests and win the support of senior leadership
- What to look for in a dedicated backup solution

While some of the specifics within this guide pertain to the United States, and the focus is on M365, the general guidance is applicable to any healthcare organization using any software-as-a-service (SaaS) application.

If you only take one thing away from this guide, please let it be that it is your organization's responsibility to protect your SaaS data – not your SaaS vendors'.

The SaaS vendors are very clear about this point in their terms and conditions, but their customers often don't realize the truth. Here's what Christophe Bertrand, Senior Analyst at ESG Research has to say:

it is your organization's responsibility to protect your SaaS data – not your SaaS vendors'

"Thirty-five percent of the market thinks that their SaaS vendor – for example, Salesforce or Microsoft 365 — is responsible for data protection. That's not true at all. People are confusing the availability of the service itself with the recoverability of the service's data.

Aside from that 35%, a good portion of the rest of the market believes it's a shared responsibility. But the truth is that they're totally, solely responsible. And only 13% of the businesses we surveyed understood that fact.

It is concerning how many organizations are totally disconnected from the reality that they are responsible for protecting this data.

Using a SaaS application doesn't absolve them from having to do the backups."

7 out of 8 IT professionals in North America don't know who is responsible for data protection

Source: ESG Master Survey Results: 2021 Data Protection Cloud Strategies

Part 1

Why backing up SaaS data is essential

There are two major reasons why backing up SaaS data is essential for HDOs:

1. Regulatory requirements:

HDOs are legally obligated to preserve certain types of information for periods of time that exceed the SaaS service's built-in capabilities.

2. Organizational continuity / business operations:

HDOs depend on the information stored in SaaS systems to maintain business/ organizational continuity; if the information becomes unavailable, then disruption is the result.

There are a few other reasons (which we'll touch upon), but those are probably he biggest.

In recent decades, the healthcare sector has undergone a digital transformation that has fundamentally altered how services are delivered. Timely access to information has always been an important element of effective healthcare, but the scale and scope of that information has expanded tremendously.

As a result, the operations of today's HDOs depend upon a range of digital data types — many of which are considered sensitive.

Examples of digital data categories HDOs depend on

Personally identifiable information (PII), such as name, address, and contact information, plus government identification like Social Security Number (SSN) or driver's license.

Financial information, including credit card and insurance details.

Protected health information (PHI), including patient medical history, demographic data, test results, and other confidential data collected to identify a patient and deliver care.

Intellectual property and proprietary/non-public information, like patents, trade secrets, process details, research and development (R&D) program information, and other business documents.

Today, much of this sensitive data required for continued operations is stored within SaaS applications. For example, countless HDOs rely on Microsoft 365 for a range of services, including email (Outlook), collaboration and sharing (SharePoint and Teams), and storage (One Drive).

There are two consequences of this digital transformation that relate to the need for dependable data backups.

First, healthcare organizations are governed by multiple regulations that require them to retain certain types of data, including records housed in SaaS applications.

Second, if any of this information becomes unavailable, then disruption – to patient care, to business operations, and IT operations – quickly follows.

Compliance considerations

As HIPAA Journal explains, each state has its own laws governing the retention of patients' medical records; plus, those retention periods can vary considerably depending on the nature of the records and towhom they belong.

In the U.S., state laws govern the retention of patient's medical records, while HIPAA imposes requirements on how long HIPAA-related documents must be retained. Requirements in both cases regularly exceed what SaaS applications deliver.

For example (quoting from HIPAA Journal),"In Florida, physicians must maintain medical records for five years after the last patient contact, whereas hospitals must maintain them for seven years.

In North Carolina, hospitals must maintain patients' records for 11 years from the date of discharge, and records relating to minors must be retained until the patient has reached 30 years of age."

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) doesn't pre-empt these state-level laws but does impose an additional requirement covering how long HIPAA-related documents should be retained. The relevant section stipulates the documents must be retained for a minimum of six years from when the document was created or – in the event of a policy – from when it was last in effect.

Needless to say, these retention requirements go well beyond what SaaS applications typically deliver

Continuity considerations

Unfortunately, there are several things that can go wrong with SaaS data. For example, even a simple misconfiguration can cause primary sources of data to become unavailable, making accidental deletion a real risk (and may not be discovered until it's too late to recover from the SaaS app).

In fact, according to ESG Research, the most common reasons for data loss are service outages and accidental deletion (see Figure 1).Unfortunately, accidents, misconfigurations, and other 'innocent' causes aren't the only ways data can be lost and continuity harmed.

TOP CAUSES OF SAAS DATA LOSS

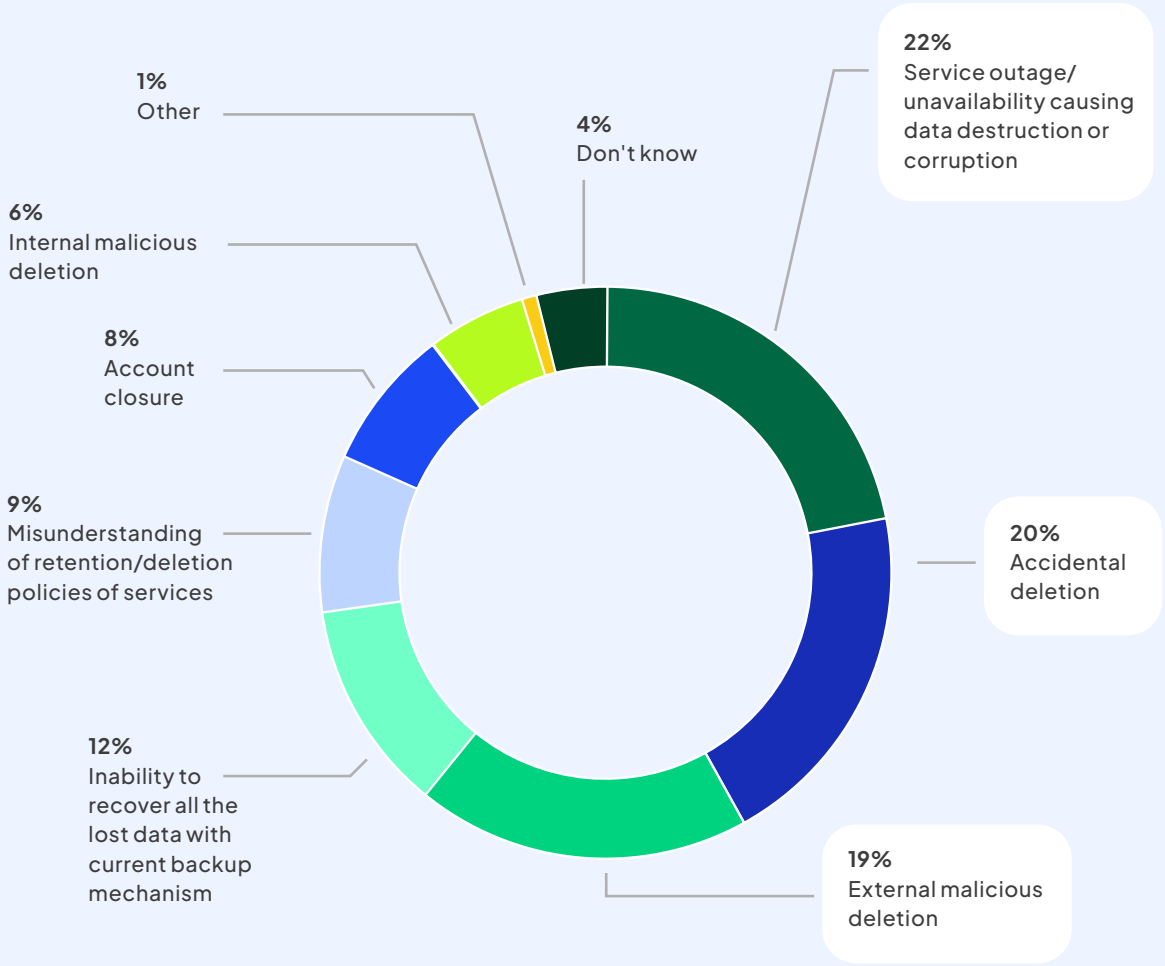
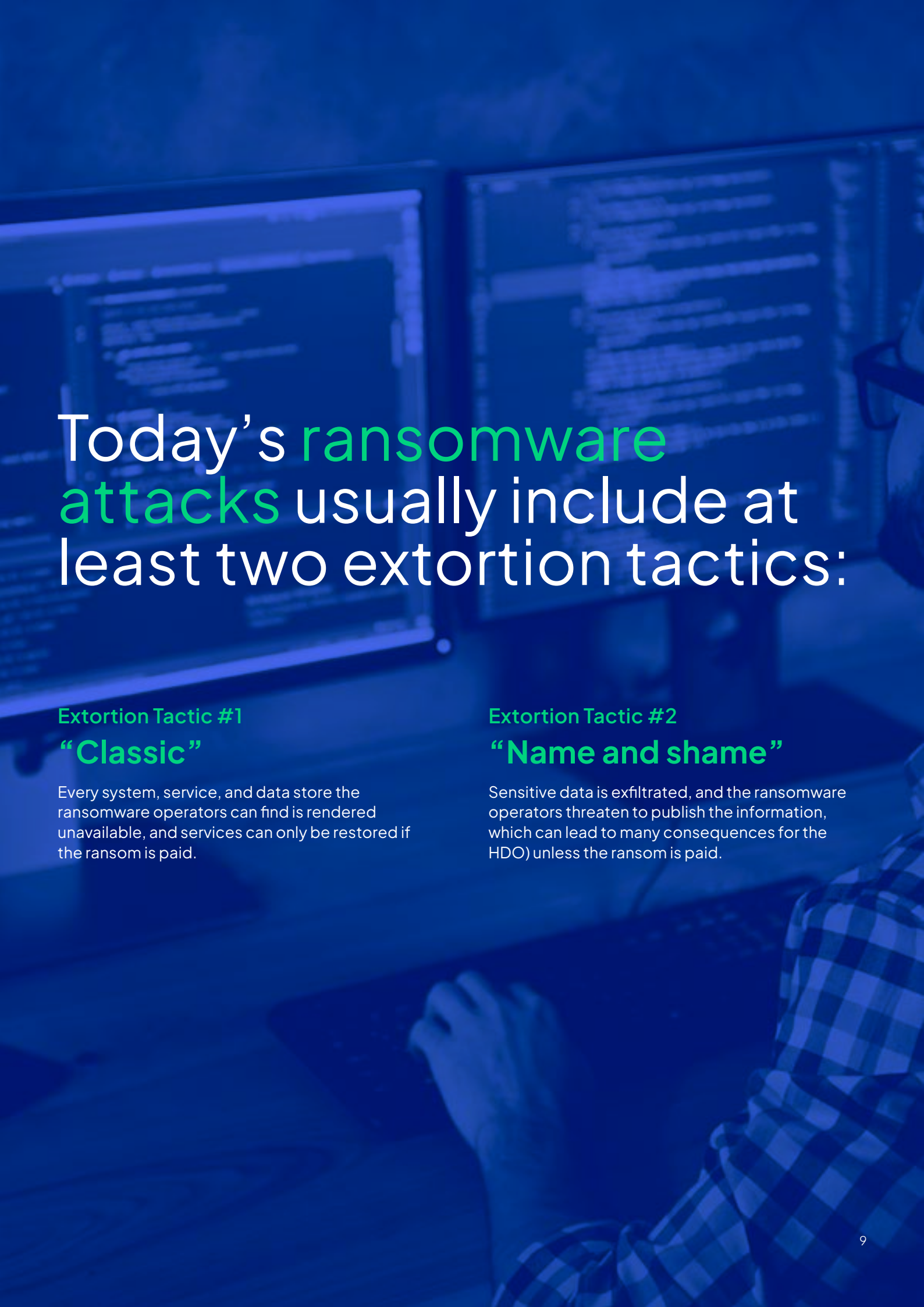


Figure 1: Top causes of SaaS data loss, as found by ESG Research

According to ESG Research, the three most common causes of data loss are:

- Service outages/unavailability causing data destruction or corruption (22% of incidents)
- Accidental deletion (20%)
- External malicious deletion (19%)



Today's ransomware attacks usually include at least two extortion tactics:

Extortion Tactic #1

"Classic"

Every system, service, and data store the ransomware operators can find is rendered unavailable, and services can only be restored if the ransom is paid.

Extortion Tactic #2

"Name and shame"

Sensitive data is exfiltrated, and the ransomware operators threaten to publish the information, which can lead to many consequences for the HDO) unless the ransom is paid.

Forgive us if we're repeating what you already know, but the actual stats are pretty astounding. For example:

of organizations experienced at least one successful ransomware attack in 2023

ESG Report: 2023 Ransomware Preparedness

of attacks on healthcare where the attack type is known were ransomware

IBM Security X-Force Threat Intelligence Index 2022

19 days

is the average length of a ransomware incident

United States Department of Health and Human Services (HHS)

And when disruption results, the impact spans the entire organization. The 2021 HIMSS Healthcare Cybersecurity Survey reported that the most significant security incidents caused disruption to:

32%
of survey respondents

Systems/devices impacting business operations

26%
of survey respondents

IT Operations

21%
of survey respondents

Systems/devices impacting clinical care

Why HDOs are particularly vulnerable to ransomware attacks

Other than the goldmine of valuable data and enormous leverage gained by shutting down potentially life-saving services, there are many other reasons why ransomware gangs target healthcare organizations:

Comparatively weak defenses

HDOs are focused on providing healthcare services, and rarely have the dedicated budget needed to build and maintain an especially strong cybersecurity posture.

Lack of cybersecurity specialists

There's a reason why the world's largest enterprises either have staff dedicated security teams or work closely with third-party specialists. Security is a specialized field, and HDOs typically lack the same resources, or the experts they have are already overburdened.

An ever-expanding attack surface

The IT environment within most HDOs is a complex and expanding mix of legacy systems, traditional on-premises equipment, specialized devices, and hybrid clouds, creating plenty of opportunity for attackers to find and exploit vulnerabilities to gain entry, establish persistence, and escalate their intrusions.

A large employee base

Many (perhaps even most) ransomware attacks begin with a successful phishing email – phishing campaigns that target HDO employees are executed with skill, and it only takes one mistake from one employee to bypass defenses.

Poor detection, response, and remediation capabilities

Again, security is a very specialized field, and many HDOs lack these skills in house and haven't proactively engaged third-party providers.

While backups can't prevent ransomware attacks (and can't prevent the attackers from publishing what they steal), they have proven to reduce the impact by minimizing service disruption.

Once again, the backup features built into SaaS applications are woefully inadequate to support a disaster recovery process like the one needed after a ransomware detonation.

Part 2

Protecting SaaS data is your responsibility

As noted in the introduction, backing up cloud SaaS data is the responsibility of the SaaS customer, not the vendor.

For example, Figure 2, on the right on this page, comes from Microsoft directly (see "Division of Responsibility" in the Shared responsibility in the cloud documentation) and shows the areas of responsibility between you and them for the deployment of their SaaS application.

Note that "information and data" fall under "Responsibility always retained by the customer." And if that wasn't clear enough, Section 1d of the Microsoft online subscription agreement says that:

"You are solely responsible for the content of all Customer Data [...] Microsoft does not and will not assume any obligations with respect to Customer Data."

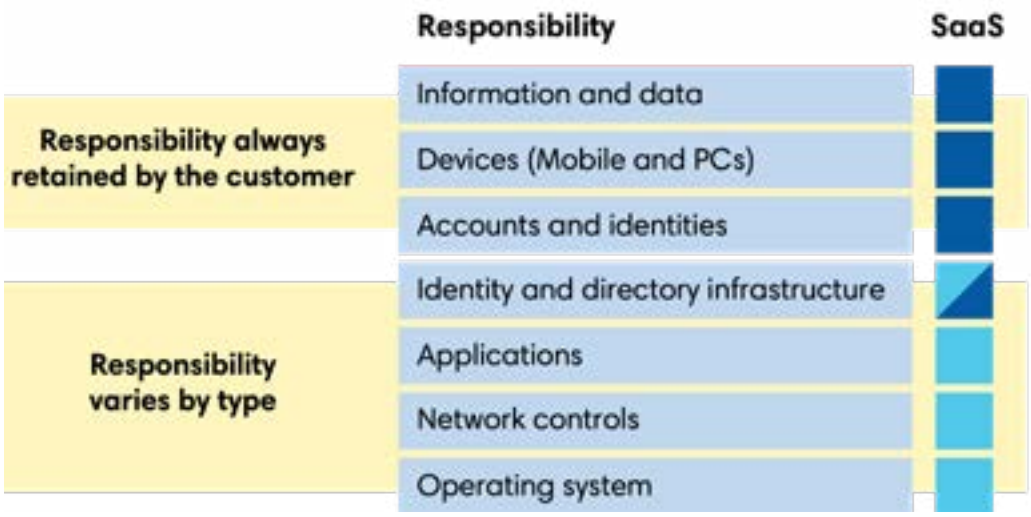


Figure 2: Microsoft's own guidance is very clear that protecting "information and data" is your responsibility.

The Recovery Gap

ESG Research found that 81% of Microsoft 365 users had to recover data. Unfortunately, only 15% were able to recover 100% of their data.

Learn more about the realities of the SaaS shared responsibility model

While SaaS apps may provide recycle bins, those still put your data at risk because they have varying storage durations and can be emptied or bypassed with hard deletes.

Putting items on retention or legal hold can preserve data longer but using an e-discovery search to find missing or deleted data won't allow you to do a direct restore. Plus, the data you export may or may not be in a usable format.

At the end of the day, the responsibility for data loss across your SaaS applications — OneDrive, Teams, SharePoint, Exchange, Azure AD, Salesforce, Google Workspace, or practically any other service from any other vendor — is yours.

In fact, in their documentation about preventing and recovering from malware infections, Microsoft explicitly instructs customers to back up their data:

> **"Backup files. Follow the 3-2-1 rule: make 3 copies, store in at least 2 locations, with at least 1 offline copy."**

We couldn't agree more!

Ransomware operators are targeting backups

Ransomware gangs aren't dumb, and they don't lack resources. They operate like Fortune 500 enterprises, are funded by the proceeds of their crimes, are supported by a shockingly well-developed ecosystem of specialized services, and often enjoy the protection of nation-states.

Ransomware-as-a-service is becoming a huge business, and according to the World Economic Forum (WEF), cybercrime has emerged as the world's third-largest economy, trailing only the United States and China.

They're also constantly evolving their Tactics, Techniques, and Procedures (TTPs) to find new ways to get into IT environments, inflict maximum damage, and gain maximum leverage.

One outcome in recent years is that ransomware operators have begun to specifically target backups, leading Microsoft to warn in its 2021 Digital Defense Report that, "information disruptors and attackers aggressively search for backup facilities."

For example, the Conti ransomware deletes Windows Volume Shadow Copies prior to encryption and disables 146 Windows services related to backup, security, and database capabilities.

The Conti gang and their affiliates also routinely employ multi-week dwell times, both as part of the strategy to maximize discovery and to find and corrupt backups.

These TTPs are just part of why their ransom message confidently states:

"(...) all the data that has been **encrypted by our software** cannot be recovered by any means without contacting our team directly."

As a result of these ever-evolving tactics, the CISA Alert DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks recommends "ensuring that backups are implemented, regularly tested, and isolated from network connections."

"information disruptors and attackers aggressively search for backup facilities."

Microsoft, 2021 Digital Defense Report

Part 3

Test your SaaS data risk and protection readiness

Completing the following short assessment will help you to better understand your SaaS data risk and protection readiness.

For both risk and protection readiness, add up the number of times you answered “No.”

Quick self-assessment:

SaaS data risk	Yes	No
We have strong IT defenses in place, including endpoint, cloud, and network protection, and robust logging.	☐	☐
We have a Security Operations (SecOps) team, Managed Detection and Response (MDR) service, or similar real-time security function to contain threats that bypass our defenses.	☐	☐
We understand our threat surface, including legacy systems and hybrid IT environments.	☐	☐
We have a robust vulnerability discovery and management program.	☐	☐
All our employees undergo regular, healthcare domain-specific Phishing and Security Awareness Training (PSAT).	☐	☐

If you scored 2/5 or higher on the risk assessment, then your SaaS data is at high risk.

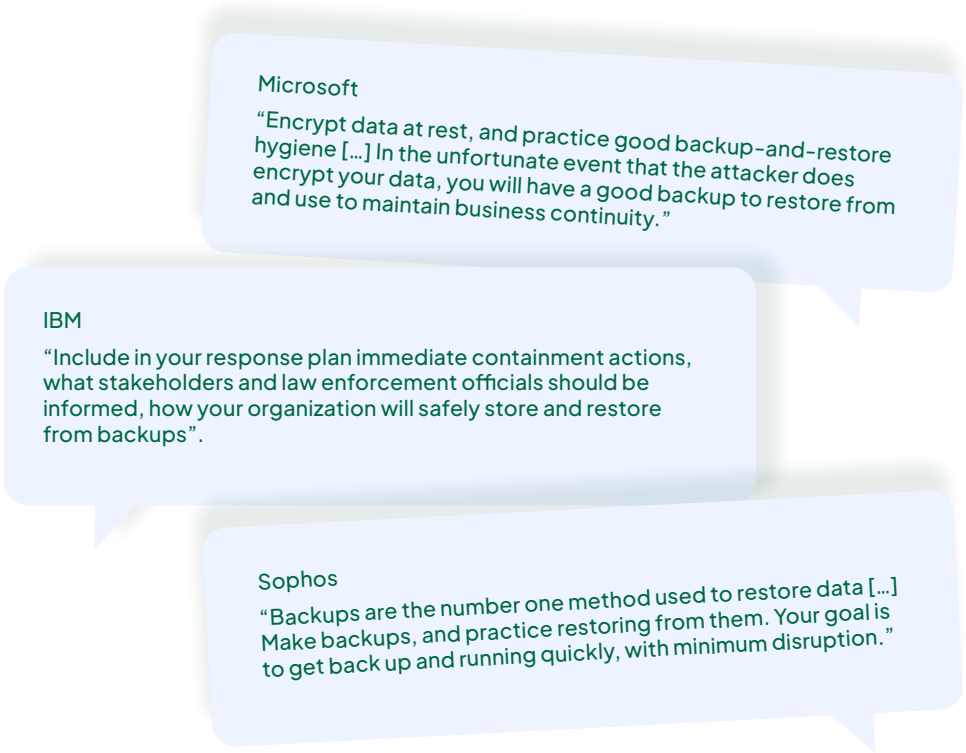
SaaS data protection readiness	Yes	No
We have a backup and recovery solution in place for our M365 application data beyond the limited functionality included within M365.	☐	☐
We can access our data 24/7, even if primary systems are unavailable.	☐	☐
We have a retention policy in place and regularly verify that the policy is followed.	☐	☐
We comply with HIPAA and other regulatory requirements that apply to our region.	☐	☐
We have tested our M365 restoration processes, and are confident that we can fully restore any of our M365 data if it were to be lost.	☐	☐
We are satisfied with the time it takes to restore data, whether we need to restore a specific file or perform a full disaster recovery.	☐	☐
We are satisfied with the time it takes to offboard employees.	☐	☐
We stop paying SaaS licensing for departed employees.	☐	☐
We can remotely monitor the status of our SaaS applications' backups.	☐	☐
We can easily get an overview of the total body of data backed up from our SaaS applications.	☐	☐
We are satisfied with the number of resources we apply to backup and related IT tasks.	☐	☐
We understand that cybercrime operators specifically target healthcare delivery organizations and that their TTPs specifically target backups.	☐	☐

If you scored 3/12 or higher on the data protection readiness assessment, then it is likely you will encounter serious problems recovering data in the event of a disruption.

Part 4

Making the business case for dedicated SaaS backup and recovery

IT and security vendors couldn't be more adamant that they consider backups to be essential:



Of course, the truth is that practically all healthcare organizations are already backing up data. Unfortunately, the current approaches have major flaws, for example:

Inadequate protection

One particularly sobering fact revealed in the 2021 HIMSS Healthcare Cybersecurity Survey is that "Only 28% of respondents have implemented data loss prevention comprehensively (100%) across the enterprise."

Hidden costs

Many HDOs operate from a traditional data center environment – owning and managing the hardware and software that handles backups. This approach carries large costs, many of which may be 'hidden' in larger budgets.

In our experience, by switching from the traditional data center to cloud backup, healthcare organizations can substantially slash associated expenses. However, as any IT professional knows, just because something is a good idea doesn't mean a board will see things the same way and approve a budgetary request.

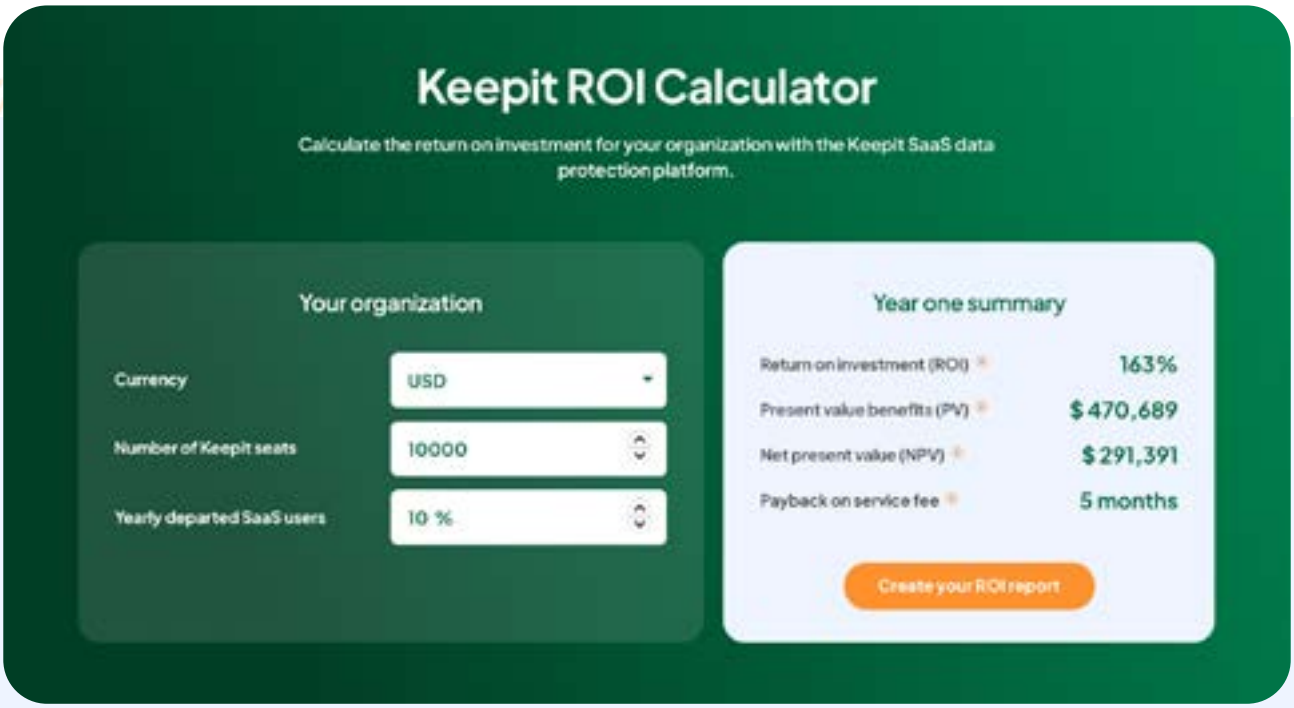
Fortunately, there are many factors that contribute to the business case for a dedicated SaaS backup and recovery solution, including:

- Fulfilling regulatory bligations
- Protecting organizational continuity
- Reducing response and recovery costs
- Avoiding Ransom Payments
- Filling cyber insurance gaps

If you need more ways to make the case, take a look at:

What's the Return on Investment (ROI) of a cloud backup solution?

or try our ROI Calculator on our website to find out what return on investment your company could realize when deploying Keepit.



Try our ROI Calculator

Find out what return on investment your company could realize when deploying Keepit.

Calculate ROI

Fulfilling regulatory obligation

Few people like being told what to do, but it turns out that governments do have the authority to compel action.

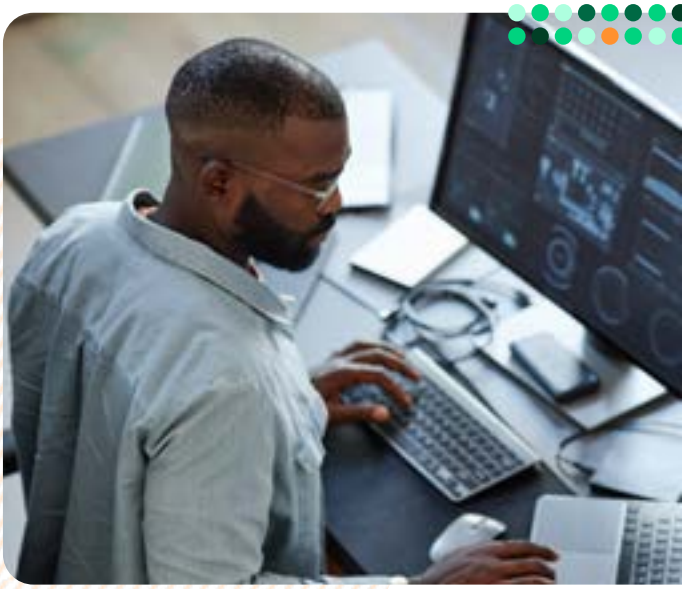
Focusing on the United States, the simple fact is that both federal and state laws impose strict requirements around data retention for different types of healthcare records and information. Plus, regulations are subject to change, adding more pressure to comply to avoid a regulatory audit and heavy fines.

Failure to comply can lead to financial and legal exposure such as lawsuits, fines, settlements, and certification losses, while also increasing the risk of data breaches.

For HDOs committed to minimizing or avoiding these risks, having a proper backup and recovery practice in place is inextricably linked to compliance. For example, passing an audit with missing data would be extremely tedious, time-consuming, and unnecessarily expensive.

Third-party backup and recovery help you stay compliant by ensuring your data remains immutable and tamperproof. Immutable data and metadata make it possible for you to document and recover not just all data but all data processing, ensuring that auditors have full visibility of everything that has impacted the data.

If complying with laws (and avoiding potentially hefty fines) isn't enough to secure the budget, there are other reasons to invest in SaaS backup.



The Costs of Non-Compliance

Some estimates say compliance failures cost businesses nearly $1.5 billion annually and growing.

Learn more in Data Compliance Makes Third-Party Security a Must

Protecting organizational continuity

In a presentation called Conti Ransomware and the Healthcare Sector, the United States Department of Health and Human Services (HHS) relayed that the average length of a general ransomware incident is 19 days.

As a second data point, Sophos reported that 25% of healthcare organizations disrupted by ransomware took up to a month to restore operations.

Whether an HDO is run for profit or not (and setting aside the patient impacts of disruptions) keeping services operational is essential for maintaining the revenue that keeps an organization running – and having reliable backups that can be quickly restored is vital for returning to partial or complete service.

When disaster strikes

In the real world, data outages are a matter of when, not if, making your ability to recover essential data quickly an important part of business continuity planning.

Learn more in Recovery for SaaS Apps: When Disaster Strikes

Reducing response and recovery costs

The shorter the outage, the lower the recovery and remediation costs, making loss avoidance a compelling part of the value proposition.

Recovery processes and costs can also include Digital Forensics and Incident Response (DFIR) activities, whether mandated by cyber insurance coverage, necessary for root cause analysis, driven by a motivation to prosecute, or some other reason. Third-party backups assist DFIR activities by providing trustworthy information that extends much farther back in time than what can be pulled from SaaS applications.

But being able to restore services quickly from a dedicated SaaS backup doesn't just protect revenue and minimize recovery costs, it also means you don't have to pay the ransom.

Rising remediation costs

Research by Sophos suggests that the average remediation cost for healthcare organizations soared to $1.85M USD in 2021 (up from 'only' $1.27M USD in 2020).

Avoiding ransom payments

Here are additional sobering ransom statistics from Sophos. First, 61% of healthcare organizations disrupted by ransomware in 2021 paid the ransom. This statistic suggests that no matter how many times the board or the finance team says, "We won't pay the ransom," there's a better-than-even chance that when faced with a brutal reality they will.

And it turns out that paying the ransom isn't even a guarantee that services will be fully restored. Even ignoring buggy ransomware decryptors (unfortunately a real thing), Sophos' investigations revealed that "On average, in 2021, healthcare organizations that paid the ransom got back only 65% of their data."

And in case you're feeling lucky, the Sophos report went on to note that "Only 2% of those that paid the ransom in 2021 got ALL their data back."

That's a poor return for ransoms that typically range from $1M USD to $25M USD.

Those ransom amounts also mean that even if the business case is made entirely on ransom avoidance, it's a good bet that a dedicated SaaS backup solution will pay for itself in the very first ransomware incident.

Also, as the United States government focuses more attention on ransomware and the criminal enterprises behind it, paying a ransom may constitute a violation of federal laws.

"But wait," you may be thinking, "we have cyber insurance…"

To that we say:
"Maybe you do, but probably not really..."

"Only 2% of those that paid the ransom in 2021 got ALL their data back."

"On average, in 2021, healthcare organizations that paid the ransom got back only 65% of their data."

You don't get what you pay for

61% of healthcare organizations disrupted by ransomware in 2021 paid the ransom

Ransom demands typically range from $1M — $25M USD

Only 2% that paid the ransom recovered all their data

Filling cyber insurance gaps and meeting coverage requirements

The cyber insurance market is in a state of explosive growth, with written premiums expected to reach $20B USD globally by 2025, representing a four-fold increase over 2016.

But as cyberattacks have become more frequent and severe, insurers are crunching the numbers, resulting in stricter coverage requirements, more restrictive policy terms, and significantly higher premiums. Consider that:

- A 2021 report by MDR provider eSentire found that only 60% of security professionals whose organizations have cyber insurance indicated that their insurer covers costs of lost business.
- Sophos' State of Ransomware in Healthcare 2022 reports that only 78% of healthcare organizations have ransomware coverage, and 46% of those note that there are exclusions or exceptions in their policies.
- Sophos also noted that 51% of healthcare organizations reported that the level of cybersecurity capabilities they need to qualify for coverage in the first place has risen.
- In The Long Road Ahead to Ransomware Preparedness, ESG Research reported that only 66% of organizations with cyber insurance were covered for ransoms.

Filling the Gaps

As premiums rise and insurers' requirements for pre-existing controls and protections increase, third-party backup has an ever-more-important role to play in managing costs.

Part 5

Finding the right dedicated SaaS data backup solution

To meet your compliance and continuity needs as a healthcare delivery organization — including keeping your data available 24/7 and recovering from disruptions within minutes — consider only cloud backup vendors whose solutions offer:

- **Cost efficiency**
  Enterprise scalability and a fixed pricing model which include data consumption, zero hidden costs, and free data retention of departed users for free

- **3-2-1 principle of backup**
  This principle mandates that you must have three copies of data (one primary and two backups), two copies stored at separate locations, and one on an off-site storage such as a secure private cloud.

- **Scalability**
  Unlimited data storage, automatic daily backup with two copies in two data centers that are physically and logically independent from the SaaS application provider (i.e., not in the public cloud), data residency options, and built-in redundancy.

- **Vendor Neutrality**
  Independent cloud that runs in the vendor's own data center regions and operates on their own hardware to avoid the risk linked to keeping your primary data and backups in the same place.

- **Quick and easy data recovery**
  Comprehensive Microsoft 365 coverage, extensive search capabilities, live document preview, point-in-time navigation/restore, and recovery from single item to tenant level.

- **Granularity**
  Granular data restores are widely preferred as a best practice over full rollback restores, as it enables quick and precise restoration of options of any data object, including the metadata.

- **Ease of use**
  Intuitive and easy to use: products that require little or no training actually get used. With simple and efficient search, file previews, backup management and configuration and flexible retention policies, admins and users can ensure all backup and recovery capabilities are utilized.

- **Security**
  Immutable blockchain-verified technology storage, data encryption at rest and in transit, configurable admin permissions, multi-geo configuration, secure role-based access controls (RBAC) including SSO and MFA, ISO/IEC 27001 certified platform and data centers, and ISAE 3402-II certifications.

- **Air-gapped backup**
  Backups are regularly tested and isolated from network connections as recommended by experts such as the security agency, CISA.

- **Provides immutable data storage**
  Immutable data storage based on the strictest data policies like GDPR regulatory compliance.

- **Feeds your disaster recovery and business continuity strategies and plans**
  Fast restore for a single record or bulk restore for full disaster recovery, API- or UI-driven, covering retention policies and the need for long-term or unlimited data retention.

Part 6

Start protecting your critical SaaS data today

While we can't speak for the other backup services, we can share the experiences of our customers:

Keepit customers realized a 163% Return on Investment over three years, by profiting from the following benefits:

- **Faster and more accurate recovery from a ransomware attack:**
  Through fast and granular recovery functionality, customers were able to achieve a 90% reduction in time needed for priority restore, and a 57% reduction in time needed for a full restore.
  Total savings year three: $819,149

- **Reduced SaaS Licensing Costs:**
  Customers can retain data as long as needed while eliminating license costs for departed users – this means 3 months of saved licensing cost for each offboarded employee.
  Total savings year three: $351,446

- **On-premises backup cost avoidance:**
  A 91% reduction in time needed to manage Keepit vs. an on-premisessolution, as well as the associated maintenance and hardware costs, translates into
  Total savings year three: $133,944

- **SaaS user productivity impact:**
  Less admin time spent on finding and restoring data – our customers were able to save half an hour on every restore task.That's a big chunk of time your IT team can spend on bigger priorities.
  Total savings year three: $21,380

Data is based on a composite company with 10.0000 SaaS users, a turnover rate of 10%, and a growth of 1000 SaaS users every year.

Source: The Total Economic Impact Of Keepit Dedicated Software-As-A-Service Data Protection, Forrester, January 2024

Want to know what ROI your company could realize when deploying Keepit for data protection and recovery? Try our ROI Calculator to see for yourself.

Take the next step toward protecting your Saas data

Request a demo

Deploy Keepit, the world's only independent cloud dedicated to SaaS data protection, to protect your data in key business applications including Microsoft 365, Microsoft Entra ID, Google and Salesforce. Tamper-proof data storage in an isolated, independent cloud means data availability 24/7. With this solution, you tick off your checklist, and can ensure compliance and continuity for your business.

Keepit is trusted by thousands of companies worldwide to protect and manage their cloud data.

To learn more, visit our website.

To start a conversation with our data protection experts, please get in touch.

keepit®

Keepit provides next-level SaaS data protection for key business applications, ensuring business continuity and access to data. Keepit is the world's only independent backup and recovery solution and keeps data resilient to cyberattacks and human error. Headquartered in Copenhagen with offices and data centers globally, Keepit is trusted by companies worldwide.

HQ – Copenhagen
Denmark
Keepit A/S
Per Henrik Lings Allé 4, 7.
2100 København, Denmark
CVR: 30806883
+45 8987 7792
sales@keepit.com

Dallas, Texas
United States
Keepit USA Inc.
3232 McKinney Avenue Suite 820
Dallas TX 75204, USA
TIN: 85-358 6335
+1 469-461-4892
sales@keepit.com

London
United Kingdom
Keepit Technologies UK, LTD.
Warnford Court
29, Throgmorton Street
London EC2N 2AT, UK
Company reg. no.: 13785045
sales@keepit.com

Munich
Germany
Keepit Germany GmbH
Maximiliansplatz 22
380639 München
Amtsgericht München,
HRB 270094
Geschäftsführer Morten Felsvang
sales@keepit.com