rewind

Protecting SaaS data in the face of *rising risks*

The importance of SaaS backups for data resilience

rewind

Table of Contents

How safe is your SaaS data?

What would happen to your organization if all the data, workflows, processes, and institutional knowledge stored in SaaS platforms disappeared tomorrow?

Now, ask yourself the same question but assume you have secure backups of all that data and you can restore it with a few clicks.

That's why data resilience matters, and that's why a bulletproof backup strategy is important.

Data resilience starts with understanding the risks. Every business needs a SaaS backup strategy to ensure it can recover quickly from any disruption.

SAAS DATA IS AT RISK

SaaS adoption is only becoming more widespread; in fact, Gartner[1] predicts that end-user SaaS spending will reach $300 billion this year. Threats are also growing and evolving at an unprecedented pace: as of 2025, cybercrime costs the global economy $10.5 trillion annually according to Cybersecurity Ventures[2]. And of course, human error remains an ever-present risk.

DATA LOSS HAPPENS

Data loss in SaaS platforms is not an *if* proposition but a *when*. It could come in the form of a sophisticated ransomware attack, or something as simple as an accidental deletion. Whatever the cause, the fallout can be catastrophic.

There's a common misconception that the SaaS platforms organizations rely on can recover data in the event of a data disaster at the user account level. They can't.

Organizations must face the facts: their SaaS data is vulnerable and proactive risk mitigation is a must.

The good news is that word is getting out about the importance of backups: in 2024, 15% of organizations already saw backing up SaaS data as a priority and by 2028, that number is expected to grow to 75% according to Gartner[1].

And as organizations awaken to the risks of SaaS data loss, the important work of building up defences against disaster and creating data recovery strategies falls to IT leaders and their teams.

MITIGATING SAAS DATA RISKS

This eBook will walk you through the current landscape of SaaS data threats, the steep cost of inaction, and the essential steps for building resilience into your data protection strategy. We'll explore the Shared Responsibility Model for SaaS data and how to incorporate a bulletproof backup strategy while meeting data security and other compliance requirements.

Whether you're an IT, engineering, or software development leader, this guide will equip you with the knowledge you need to protect your organization's most valuable digital assets.

1 Choubey, Sonika. "Gartner Predicts 75% of Enterprises Will Prioritize Backup of SaaS Applications as a Critical Requirement by 2028." Gartner, Aug. 27, 2024.

2 Morgan, Steve. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Cybercrime Magazine, Nov. 13, 2020.

SaaS data threats: ransomware and malicious attacks

Ransomware attacks are one of the most pervasive threats facing businesses today, and these attacks have evolved into highly sophisticated operations. As organizations have moved away from on-premise systems and toward cloud-based platforms and SaaS applications, so too have attack vectors changed to target data stored in the cloud.

Ransomware attacks can take many forms, but fundamentally, malicious actors encrypt critical business data then demand exorbitant ransoms for the key that will unlock that data. Organizations that choose to pay the ransom often discover that it's no guarantee they'll get their data back. Turns out there's no honor among thieves.

There are many ransomware horror stories (and many more attacks that go unreported) but take this example: Change Healthcare, a subsidiary of UnitedHealth, is among the biggest medical claim payments processors in the U.S. A data breach in 2024[3] saw 4TB of sensitive patient data compromised and held for ransom. The reported $22 million ransom was perhaps the least of the organization's worries. The cost of reputational damage and lost trust, exacerbated by an investigation under the Health Insurance Portability and Accountability Act (HIPAA), is harder to measure in dollars and cents but is no less real and has a longer-term impact.

That is just one example. With the annual cost of cybercrime topping $10.5 trillion, the scale of the threat is staggering today and it's only getting worse. By 2031, Cybersecurity Ventures estimates[4] that a ransomware attack will happen every two seconds.

While external threats loom, internal risks also put critical data at risk, making data loss not an *if* but a *when*. And the cost of data loss to an organization can be astronomical.

Data resilience isn't just about prevention, it's about recovery. A comprehensive backup strategy ensures you have clean, restorable data to fall back on.

3 Change Healthcare. "Change Healthcare Cyberattack Support." UnitedHealth Group, Jun. 20, 2024.

4 Morgan, Steve. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031." Cybercrime Magazine, Jul. 7, 2023.

SaaS data threats: from AI to simple accidents

As organizations come to grips with artificial intelligence (AI) and go about finding ways to implement this new technology into their work, so too do the bad actors[5]. Cybercriminals are using AI to automate and enhance their attacks. AI-enabled phishing campaigns, deep-fake impersonations, and automated vulnerability exploitation pose new challenges for IT security teams.

These threats can specifically target cloud platforms and SaaS tools, exploiting gaps in authentication or user access controls.

Nearly six out of 10 (58%) organizations experienced data loss in SaaS applications according to Forrester[6]. It's not just outside forces that organizations need to defend against. When it comes to threats to your SaaS data, the call is coming from inside the house as well.

Accidental deletion[7] remains one of the most common causes of data loss. Even a well-intentioned team makes mistakes, and in SaaS platforms, a single click can wipe out critical records. A CSV file with one value out of place can compromise data at scale. An AI tool, implemented with the best of intentions, can make far-reaching changes in seconds, amplifying small mistakes and turning them into major data events.

Again, data loss is a *when*, not an *if*. And whatever the cause, recovery can be impossible without a reliable backup partner and solid data protection strategy.

Human error is inevitable and cyber threats are mounting; a backup solution with version history and quick recovery capabilities minimizes the impact of data loss.

5 Hans, Joel. "Protecting SaaS data in an AI-powered world." Rewind, Aug. 30, 2024.

6 Trzcinski, Arielle. "Key Recommendations For Optimizing Self-Triage Tools To Help Consumers Today And Beyond COVID-19." Forrester, Jun. 5, 2020.

7 Hans, Joel. "Reminder: People are the No. 1 threat to your SaaS data security." Rewind, Sept. 5, 2024.

Doing nothing comes at a cost

Ignoring the risks associated with SaaS data can be a costly mistake. The financial toll of data breaches, downtime, and ransom payments is only part of the equation.

Think beyond immediate recovery costs. Data resilience is an investment in your brand's longevity and customer trust.

According to IBM[8], the average cost of a data breach reached $4.88 million in 2024—a 10% increase over the previous year.

For smaller companies, a cyberattack can be catastrophic. Even for larger enterprises who are better prepared for and positioned to survive a cyberattack, the impacts can be far-reaching and long-lasting. The broader impacts (lost opportunities, investor/shareholder scrutiny, lost consumer trust) are harder to measure but no less real as a result.

The direct and immediate cost of a cyberattack (containment, downtime, recovery) can be quantified; downtime from data loss costs businesses an average of $9,000 per minute according to Atlassian[9]. That's more than $500,000 per hour. It's not just lost revenue that contributes to that heady number. There's a high human resource cost too as work is interrupted and teams pull together to contain the damage.

Beyond short-term monetary impacts, the reputational damage and loss of customer trust carry longer-lasting consequences. These costs are no less significant even if they are harder to quantify in purely monetary terms. Data loss erodes customer trust, can incur regulatory penalties, and jeopardizes invaluable compliance certifications like ISO 27001, HIPAA, DORA, SOC 2/3.

For industries like finance and healthcare, operational disruptions can have severe—perhaps even life-or-death—implications.

The better prepared an organization is for a data event, the fewer $9,000 minutes (and >$500,000 hours) it will spend recovering from said data loss. In addition, the better (and faster) an organization's recovery strategy, the more credible, dependable, and trustworthy that organization appears.

8 "Cost of a Data Breach Report 2024." IBM.

9 "Calculating the cost of downtime." Atlassian.

Understanding the Shared Responsibility Model for SaaS data security

The Shared Responsibility Model defines where a SaaS platform's responsibility for stored data ends and where the user's responsibility begins—both of which occur much sooner than you may think.

Nearly half (49%) of organizations blamed confusion around the Shared Responsibility Model for SaaS data loss in an Oracle / ESG survey[10].

Many organizations mistakenly believe that the data stored in SaaS platforms can be recovered in case of loss. While every SaaS platform has backups and contingency plans for issues impacting their business, their Terms of Service explicitly disavow any responsibility for backing up or restoring data at an account level.

This means that while SaaS platforms ensure uptime, infrastructure security, and disaster recovery for their own systems, data recovery for user and account level data is left to the customer. If data is lost—whether due to an accident, cyberattack, or software failure—the responsibility for retrieving that data falls on the user, not the SaaS provider.

In other words, unless a data event occurs at the level of the SaaS platform itself, the SaaS platform can't help recover lost data. This is the Shared Responsibility Model, and businesses that misunderstand it leave themselves vulnerable to data loss events.

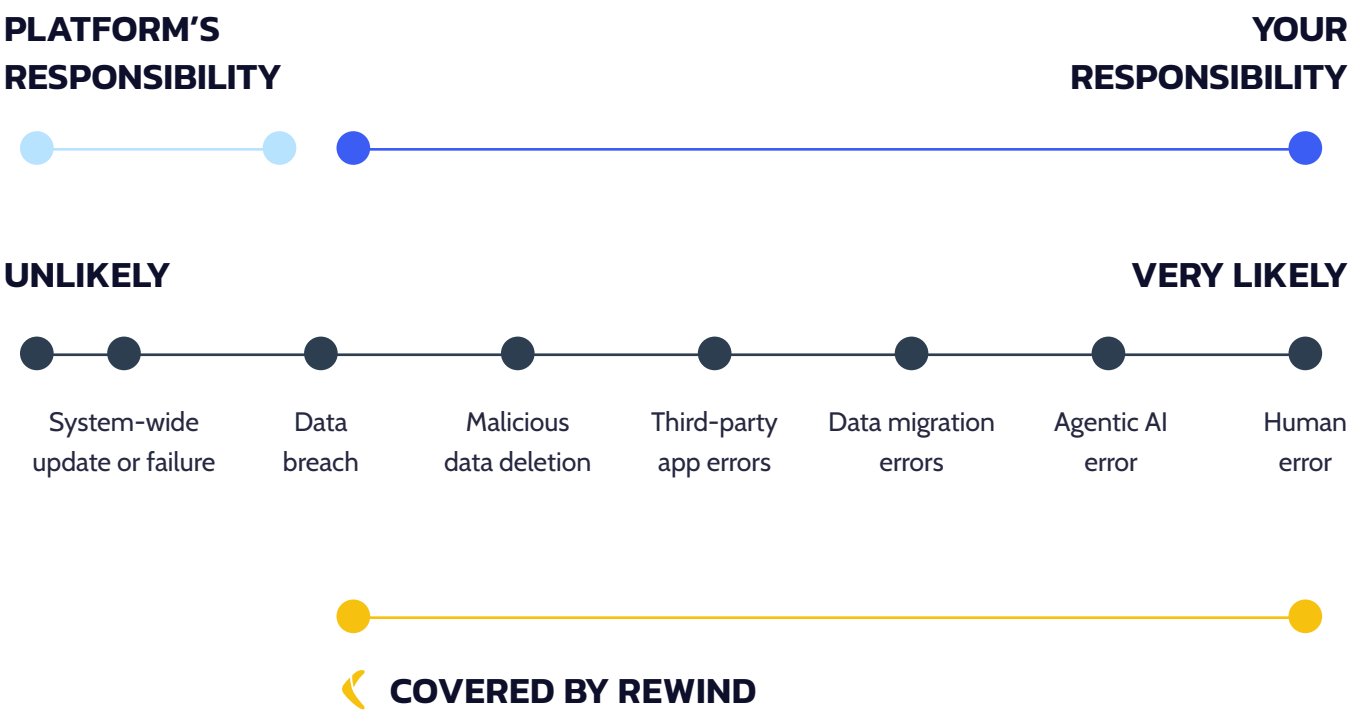
Without a third-party backup solution, businesses face serious risks:

- **Accidental deletion:** human error remains a leading cause of data loss.
- **Malicious insider threats:** employees with access can delete or manipulate critical data.
- **Ransomware and cyberattacks:** attackers can encrypt or destroy cloud-based data.
- **SaaS downtime or API failures:** unforeseen outages can leave businesses unable to access essential information.

To mitigate these risks, organizations should implement a dedicated backup strategy, independent of their SaaS provider. This ensures business continuity and compliance with data protection regulations.

10 "Demystifying the Cloud Shared Responsibility Security Model." Oracle and KPMG Cloud Threat Report, Oracle.

This chart visually demonstrates wherea SaaS platform's responsibility for stored data ends and where the user's responsibility begins.



Review your SaaS provider's Terms of Service. Look for "limitation of liability," "responsibility for content," "data," or "backups" to understand where the SaaS platform's responsibility for your data begins and ends.

How the 3-2-1 backup rule applies to SaaS data

3 **Three** copies of your data stored in...

2 **Two** locations in the cloud...

1 **One** of which that is not your SaaS provider.

The 3-2-1 backup rule has been around since the days of the tape drive. It states:

> Keep *three* copies of your data on *two* different media, with *one* copy stored offsite.

Before we collectively migrated to the cloud, this meant internal and external backups. However, in a SaaS environment, 'offsite' means storing backups in an independent cloud platform, separate from the SaaS provider. So the 3-2-1 rule for backups has been updated accordingly.

> Keep *three* copies of your data in *two* different locations in the cloud, *one* of which is not your SaaS provider.

Backing up the SaaS data you rely on to the same SaaS platform you're trying to protect is akin to backing up your hard drive to your hard drive. Or keeping your spare car keys in the glove box.

Cloud-native businesses must adopt this rule for SaaS applications.

Even in the rare cases where SaaS providers offer their own native backup solutions, businesses should seek third-party tools that ensure independent, automated backups that cannot be compromised by the same threats affecting the primary system.

Why the 3-2-1 rule matters for SaaS:

- **Protection against ransomware:** attackers often target cloud data, and a separate backup ensures rapid recovery.
- **Defense against accidental deletion:** with multiple copies, businesses can recover files lost due to human error.
- **Compliance and audit readiness:** regulations such as GDPR, SOC 2, HIPAA, ISO 27001, etc. require organizations to implement proper data retention policies.
- **Business continuity:** if a SaaS provider experiences an outage, an independent backup ensures that critical data is safe and minimizes interruptions.

SaaS backups should also include version history, which allows organizations to restore data from specific points in time. Ideally, a backup solution should also offer granular restoration; recovering a deleted file/folder/board/bucket/project shouldn't require a system-wide roll back.

To protect your SaaS data, look for a reliable, external backup solution that offers daily and on-demand backups, 365+ day retention, advanced and granular data restoration across multiple SaaS platforms and services.

Mitigate risk with a smart SaaS backup strategy

Businesses that rely on SaaS applications and cloud services must back up the data they store within those SaaS applications. The Shared Responsibility Model states that SaaS platforms are not responsible for data loss at the user or account level.

Organizations must take a proactive approach to data protection by implementing structured backup policies tailored to their operational needs.

As IT and security leaders build out backup strategies for their organizations, here are some key points to consider and some pitfalls to avoid.

The best time to build out your organization's SaaS data backup strategy is *before you need it*!

DO:

- **Automate backups:** automating the backup process eliminates reliance on manual interventions, lowering the risk of human error and ensuring data consistency.
- **Store backups securely:** ensure that backups are encrypted and stored in a separate cloud platform that cannot be compromised if the primary SaaS provider is attacked.
- **Define retention policies:** businesses should align backup retention policies with compliance requirements. For example, financial records may need to be retained for 7+ years.
- **Test data recovery regularly:** a backup is only as good as its restore process. Organizations should schedule routine recovery drills and run tabletop tests[11] to confirm that they can restore critical data quickly in the event of an incident.
- **Ensure Role-Based Access Controls (RBAC):** limit access to backups so that only authorized personnel can retrieve or modify backup data.

DON'T:

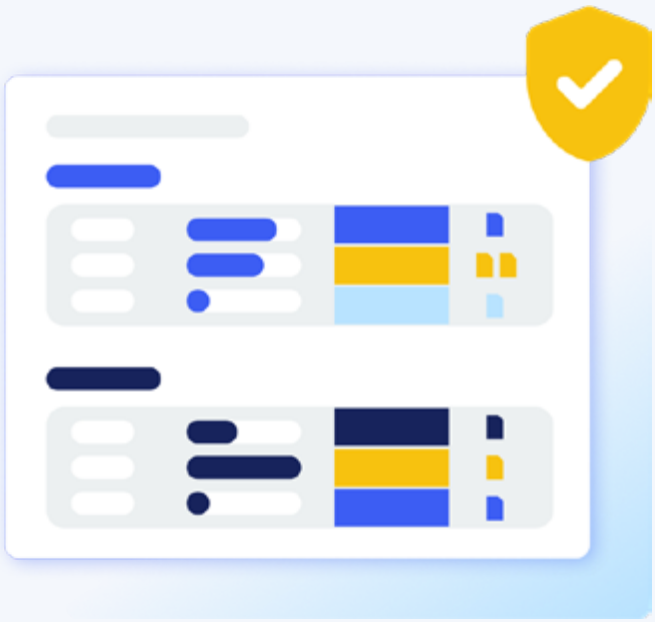
- **Wait until it's too late:** the best time to implement a SaaS backup solution is before it's needed.
- **Rely solely on SaaS vendor snapshots:** many SaaS vendors offer limited snapshots that do not meet business continuity needs.
- **Back up only some of your SaaS applications:** backup solutions should cover all mission-critical SaaS applications, not just a select few.
- **Ignore backup health:** look for a SaaS backup solution that offers real-time monitoring and that notifies of any backup failures or issues immediately.
- **Overlook compliance requirements:** ensure your SaaS backup solution supports your organization's compliance (e.g. SOC 2/3, HIPAA, DORA, ISO 27001) requirements for security, data retention, data residency, etc.

11 Hans, Joel. "Tabletop exercises: Role-playing your way to better data protection." Rewind. Aug. 30, 2024

How to choose a SaaS backup solution

Selecting the right SaaS backup provider is critical for your organization's long-term data resilience.

Not all backup solutions are created equal, and businesses should evaluate providers based on security, compliance, automation, and scalability.



KEY FACTORS TO CONSIDER WHEN CHOOSING A BACKUP SOLUTION:

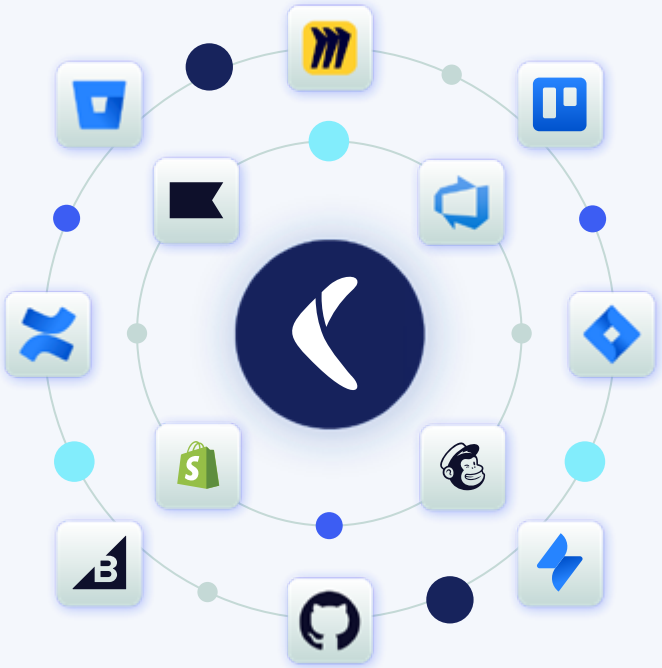
- **Security and compliance:** ensure your backup provider has clear security, compliance, data retention, data residency, and other important policies and meets industry-recognized certifications.
- **Compliance support:** compliance requirements vary greatly by industry. Ensure your backup provider actively supports your organizational compliance requirements for standards like SOC 2/3, ISO 27001, CSA, HIPAA, DORA, GDPR, and so on.
- **Automation and reliability:** a good backup solution should be fully automated and offer real-time alerts for any issues or failures.
- **Multi-SaaS coverage:** the provider should support multiple SaaS applications, as businesses typically have a diverse tech stack (e.g. Jira, Confluence, Bitbucket, Azure DevOps, GitHub, monday.com, Miro, Trello). All the data in all the SaaS applications your business relies on needs to be backed up.
- **Ease of use and scalability:** the backup solution should integrate seamlessly with existing workflows and scale with business growth.

Seek third-party certifications and audit reports to verify a backup provider's security credentials.

How Rewind solves the SaaS backup problem

Rewind is the trusted backup solution for over 25,000 businesses worldwide.

It offers comprehensive backup coverage for the top SaaS platforms. With enterprise-grade security, deep compliance support, and rapid recovery capabilities, Rewind ensures your organization's critical data is always safely backed up and can be quickly restored, whether it's lost to a sophisticated cyberattack or a simple accident.



WHY CHOOSE REWIND?

- **Comprehensive SaaS backup coverage:** protect data across SaaS platforms including Jira, Confluence, GitHub, Bitbucket, Azure DevOps, Miro, Trello, and more.
- **Enterprise-grade security and compliance:** Rewind uses AES-256 encryption and is SOC 2/3, CCPA/CPRA, CSA-STAR certified.
- **Compliance support:** Rewind backups support compliance certifications including SOC 2/3, CPRA, HIPAA, DORA, ISO 27001, and more.
- **Fast, on-demand recovery:** 365 day backup retention and the ability to easily restore data to any recorded point in time, with granular recovery for many platforms down to the individual asset level.
- **Seamless automation:** fully automated backups eliminate manual effort and lower the risk of human error.
- **Dedicated support:** a dedicated team of subject matter and product experts who are always ready to help you integrate Rewind, recover lost data, pass a compliance audit, or anything else you need.

Learn more about Rewind's extensive security practices, compliance certifications, and how Rewind supports your data protection needs at security.rewind.com.

Ready to protect your *critical data?*

Don’t leave your data to chance.

Rewind is an enterprise-grade backup solution that ensures business continuity for over 25,000 organizations worldwide. Protect your critical SaaS data today and gain peace of mind knowing your backups are automated, secure, and available when you need them.

Speak with an expert today to discover how Rewind supports your SaaS data backup needs.

Let’s chat