rewind

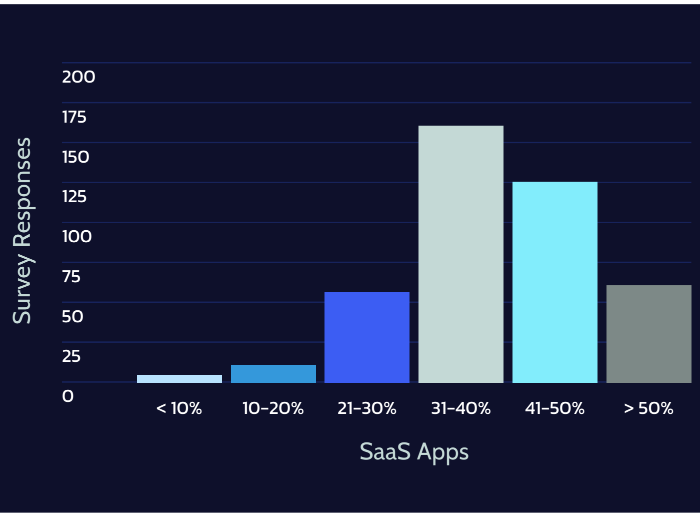
2024 State of SaaS Data and Recovery:

The rise of Backup-as-a-Service

By 2027 IT departments will spend more than $1 trillion[1] on cloud services, a 288% increase[2] from 2020.

As organizations increasingly rely on SaaS applications, IT leaders must know their data backup responsibilities. However, a survey of 400+ IT decision-makers found that many don't know their full responsibilities for backing up their SaaS data, leading to a high-risk gap in most organizations' backup and disaster recovery strategies.

What percentage of your business-critical data is stored in SaaS apps?



This is alarming, given that 84% of survey respondents said at least 30% of their business-critical data lives inside SaaS applications. As more teams outside of IT departments adopt new SaaS applications, organizations will become increasingly vulnerable to data loss if they don't understand how to avoid it.

This report is a critical look at:

- How data loss happens within SaaS applications
- What IT professionals know about their responsibilities in backing up SaaS data
- Strategies for data loss and prevention in the cloud

Data loss is inevitable in the face of *human error*

The threat posed by Shadow IT is even more insidious within the context of human error events, which no amount of preparation can prevent. **84% of survey respondents said human error has caused data loss at their organization**, with 49% saying it happened more than once.

To top off this grim reality, **82% of survey respondents also said third-party applications or integrations have caused data loss in their organization at least once**, with 63% saying it happened more than once.

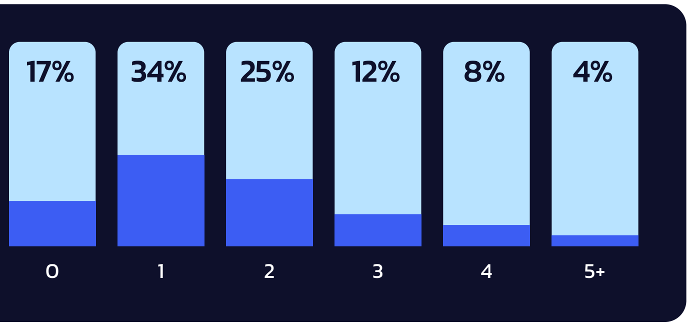
While large-scale cybersecurity events are worth monitoring, the uncomfortable truth is that this isn't how most data loss happens. Human error, either on the IT or SaaS application side, is so common that it's almost inevitable that a company will experience data loss because of it.

This is devastating when you consider how reliant businesses are on their SaaS applications, with almost 60% of respondents saying they're either very or extremely reliant. It's clear that **organizations are vulnerable to data loss**—and mitigating that loss is a large undertaking.

Key findings

- 56% of IT professionals aren't aware of their data backup responsibilities.
- 79% believe that SaaS applications include backup and recovery capabilities by default, but this isn't true.
- Shadow IT is obscuring the shared responsibility of SaaS data protection.
- 83% said human error has caused data loss in their organization.
- 82% said third-party applications or integrations have caused data loss in their organization.
- 84% said at least 30% of their business-critical data live inside SaaS applications.

How many times has human error caused data loss in your organization?



More than half of IT professionals *aren't aware* of their data backup responsibilities

SaaS solutions remove the burden of maintaining software infrastructure—but that doesn't mean SaaS companies are responsible for data loss. These organizations are clear about this in their terms of service: their clients are responsible for the management and security of their own data—including user access, permissions, and backup—not them.

GitHub Terms of Service

O. Limitation of Liability

"You understand and agree that we will not be liable to you or any third party for any loss of profits, use, goodwill, or data"

https://docs.github.com/en/site-policy/github-terms/github-terms-of-service

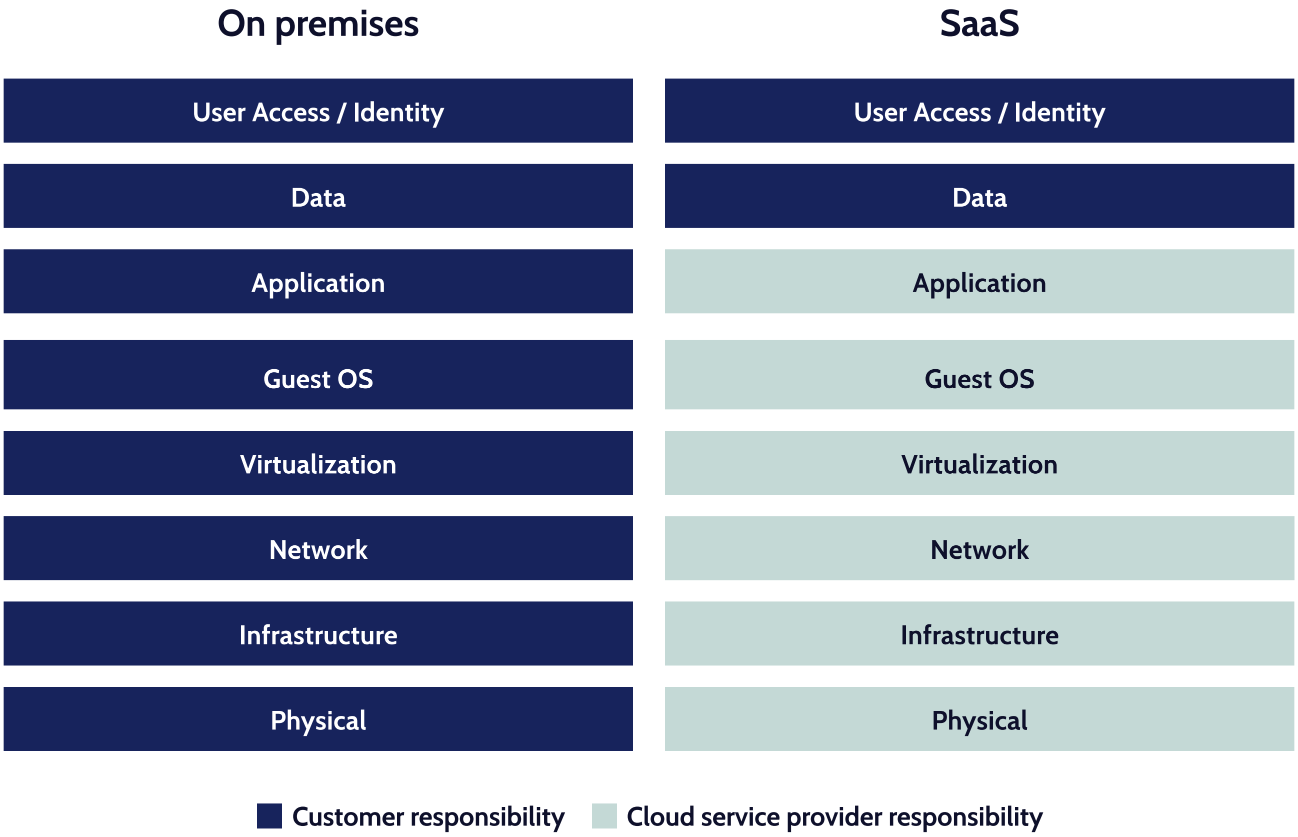
Yet **56% of survey respondents don't understand their responsibility**. When we asked whose responsibility it is to back up cloud applications, only 44% of respondents stated correctly that it's theirs.

While your data may be *saved* in the cloud, it isn't saved in a format that can be easily restored. Recovering your data is worse than looking for a needle in a haystack—it's like looking for a needle in a *field* of haystacks.

79%

of respondents believe that SaaS applications include backup and recovery capabilities by default —**but this isn't true.**

In reality, the shared responsibility between IT departments and SaaS applications looks more like this:



On premises	SaaS
■ User Access / Identity	■ User Access / Identity
■ Data	■ Data
■ Application	□ Application
■ Guest OS	□ Guest OS
■ Virtualization	□ Virtualization
■ Network	□ Network
■ Infrastructure	□ Infrastructure
■ Physical	□ Physical

■ Customer responsibility □ Cloud service provider responsibility

Shadow IT obscures *shared responsibility* even further

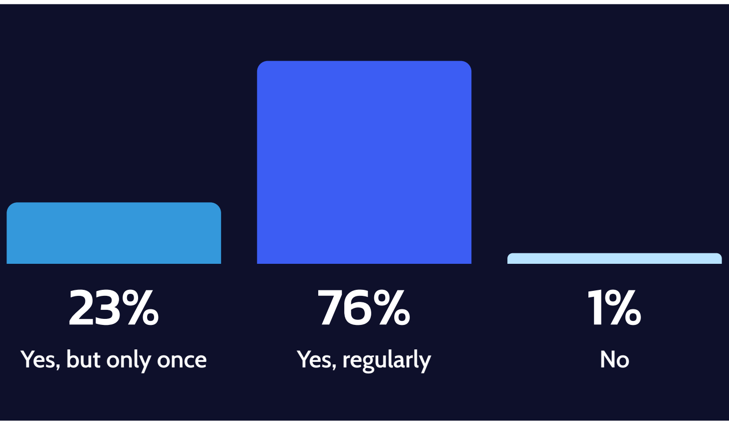
As an organization grows, so does its use of SaaS applications. In 2023, a report from Zylo[3] counted an average of **422 SaaS apps per company with 2,500–5,000 employees.**

Every department has unique software needs. The problem is that they're not relying on IT to procure and manage that software. Instead, Finance, Marketing, Product Development, and other teams are allocating budgets to acquire their own SaaS applications and managing them internally.

The result is Shadow IT, a decentralized IT infrastructure created when software is deployed by departments other than IT. This means that non-technical staff are often expected to manage user access, sharing permissions, and data security.

So, **76% of survey respondents reported reading their terms of service multiple times**. This likely only applies to the apps they procure and manage themselves. In reality, shadow IT is obscuring shared responsibility even further by leaving it in the hands of people who don't know how to manage data security effectively. This leaves their data and tools open to considerable risk that, in most cases, goes unnoticed until critical data is lost.

Have you reviewed the terms and conditions of your cloud apps?



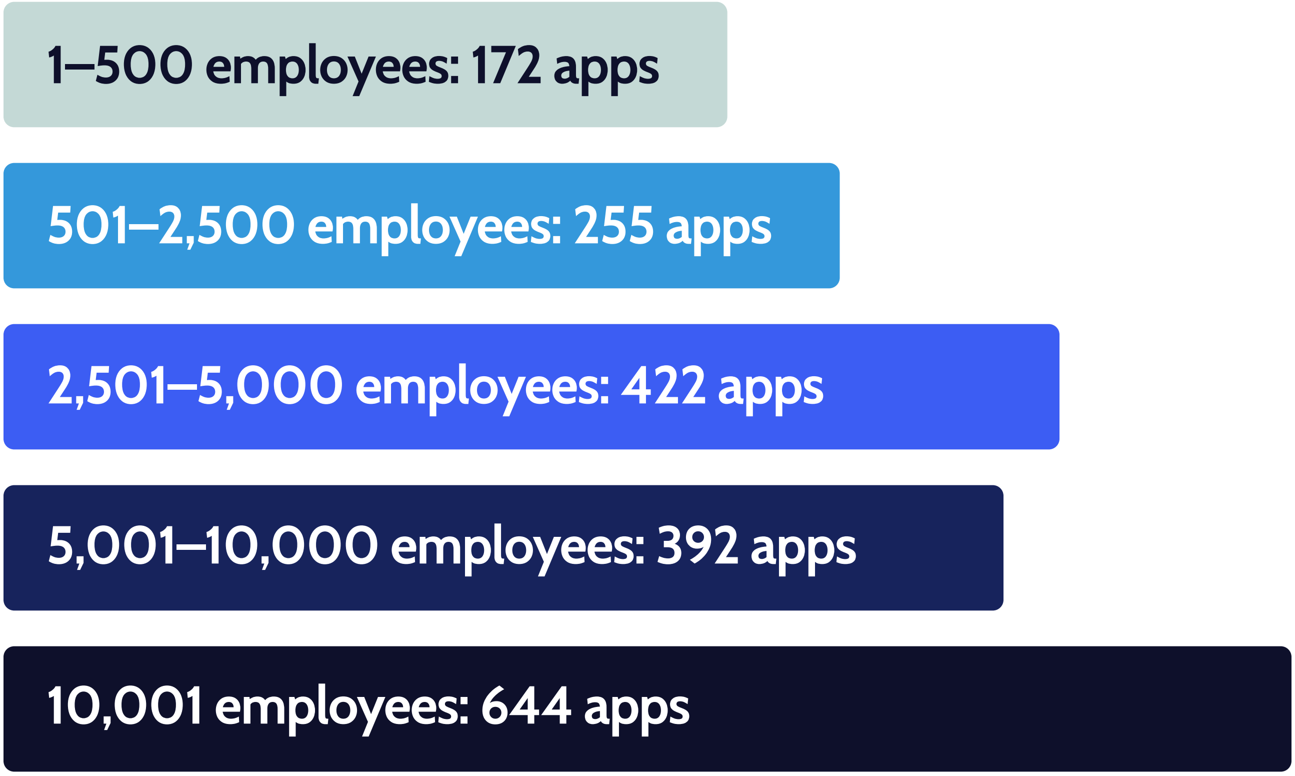
How IT professionals *back up and recover* data loss

While **most survey respondents (85%) have backup or recovery capabilities for their SaaS applications beyond what their vendors provide,** methods for doing so are often limited and time-consuming.

While **17% of survey respondents mistakenly rely on their vendor for data backup, most survey respondents (35%) use an in-house tool for their backup**. A surprising number of respondents (29%) still rely on manual processes that are time-intensive and prone to human error—which, as was previously covered, is the primary cause of data loss in the first place.

In-house backup scripts must be monitored against frequently changing connections with SaaS vendor APIs. We mentioned earlier that the average large company uses 422 apps.[4]

Here's a further breakdown by company size:



While some in-house solutions and backup scripts can remove the manual work of exporting data, they still add a maintenance layer that becomes problematic as an organization's application usage scales. With in-house solutions, IT departments must update their DIY tool every time a SaaS application revises its API or platform—which can be often. Multiply those instances by 644 apps if you're an enterprise company, and the resources needed become untenable.

Backup-as-a-Service (BaaS) makes *data protection scaleable*

Backup-as-a-Service (BaaS) addresses the scalability problem using a subscription-based approach to data backups. BaaS is a fully managed and automated backup and recovery solution that runs continuously, maintaining a constant and reliable backup of your SaaS applications in one place.

BaaS integrates directly with your SaaS applications, capturing and transmitting data over a secure network to the cloud server. Instead of being saved to a local server, data is written directly to the cloud, stored and retained until needed. Then, if you lose data, you can recover what you need from your backup, whether it's disaster recovery of your entire system or a single item, project, or image, in a few clicks.

Many enterprise companies have a full-time IT staff who oversee and maintain manual backups. These resources are often stretched thin and struggle to keep up with an organization's app usage. BaaS reduces their burden and eliminates the need for additional local storage.

Features of a *strong* BaaS provider

For organizations growing or processing massive amounts of data, BaaS is essential as it lowers IT costs and provides reliable protection against data disasters.

The best BaaS solutions are like silent partners. They're always in the background protecting your data when you need them, so you can have peace of mind knowing your data is always safe and secure. Here are some of the features you should look for in a BaaS provider:

☑ **High availability** Excellent uptime, ideally “four nines” or greater. Anything less could potentially impact your business continuity.

☑ **Disaster recovery** The BaaS provider you choose should have a solid disaster recovery plan (DRP) that ensures data and server redundancy. They should also partner with you to help you craft, manage, and enhance your DRP with resources.

☑ **Customizable solutions** Every business is different, and so are its backup needs. Your backup solution should allow you to configure backups in a way that makes the most sense for you and your business model.

☑ **Data security** One of the biggest benefits of working with BaaS providers is having access to the latest data security technology and encryption techniques. Your data must be protected in use, transit, and rest.

☑ **Support options** Your backup solution provider should offer 24/7 support options to ensure you always have someone on your side at any time of the day or night.

☑ **Scalability** Choosing a BaaS provider isn’t always straightforward, and you certainly don’t want to repeat the process if you grow out of them. Be sure your provider can scale up or down with you to ensure a sustainable solution.

☑ **Integrations** Look for BaaS providers integrating with your tech stacks, such as Confluence, Jira, Miro, Shopify, QuickBooks Online, Trello, and GitHub. Managing multiple products in one third-party backup platform allows you to ensure the protection of your full tech stack and the data that drives your business.

Why *protect your data* with Rewind

Businesses today run on technology. From the moment you open your email to the time you finish up work for the day, you're using some type of technological device or software. This means your business-critical data is spread across dozens of different SaaS apps; what would happen if you suddenly lost access to that data? What would it cost to get it back?

It's not your SaaS vendor's responsibility to back up your data; in the event of data loss, they only safeguard their own data. So it's your data, and it's your responsibility. Your data must be backed up and secure. If something happens to your computer, phone, or tablet, you could lose all of the data your business runs off of—and that's not a risk worth taking.

That's why Rewind is such a valuable asset for businesses. Rewind is the leading provider of BaaS apps, helping businesses back up their data on Jira, Confluence, BitBucket, GitHub, Miro, Azure DevOps, Shopify, BigCommerce, and more.

Protect your mission-critical SaaS data now with an on-demand backup and recovery solution. With Rewind, you can:

- Safeguard your IP with automated data backups for top SaaS Apps
- Recover quickly from simple and complex data mistakes
- Work with a platform that is SOC 2, SOC 3, GDPR, CCPA compliant
- Mitigate the risk of data loss and downtime
- Restore data in minutes

Get peace of mind knowing that your data is always safe and secure.

rewind

Proven and *trusted.*

Join the *25,000+ organizations* that have trusted Rewind to protect their cloud data.

Meltwater LUTRON Mail Online ABS

Request a demo to learn more today >

Survey methodology

Report data were sourced from 419 IT decision-makers in November 2023 in partnership with Propeller Insights. Most respondents self-identified as IT directors, IT managers, and security management professionals across several industries. Respondents also worked in DevOps, IT Systems Architecture, and Information Management Systems.

SOURCES

[1] Gartner says cloud will become a business necessity by 2028. Accessed May 5, 2024.

[2] Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021. Accessed May 5, 2024.

[3] 2024 SaaS Management Index. Accessed May 5, 2024.

[4] 2024 SaaS Management Index. Accessed May 5, 2024.

KEY LINKS

- Shadow IT
- GitHub T&C's
- Shared responsibility
- Backup-as-a-Service
- Disaster recovery plan
- Rewind