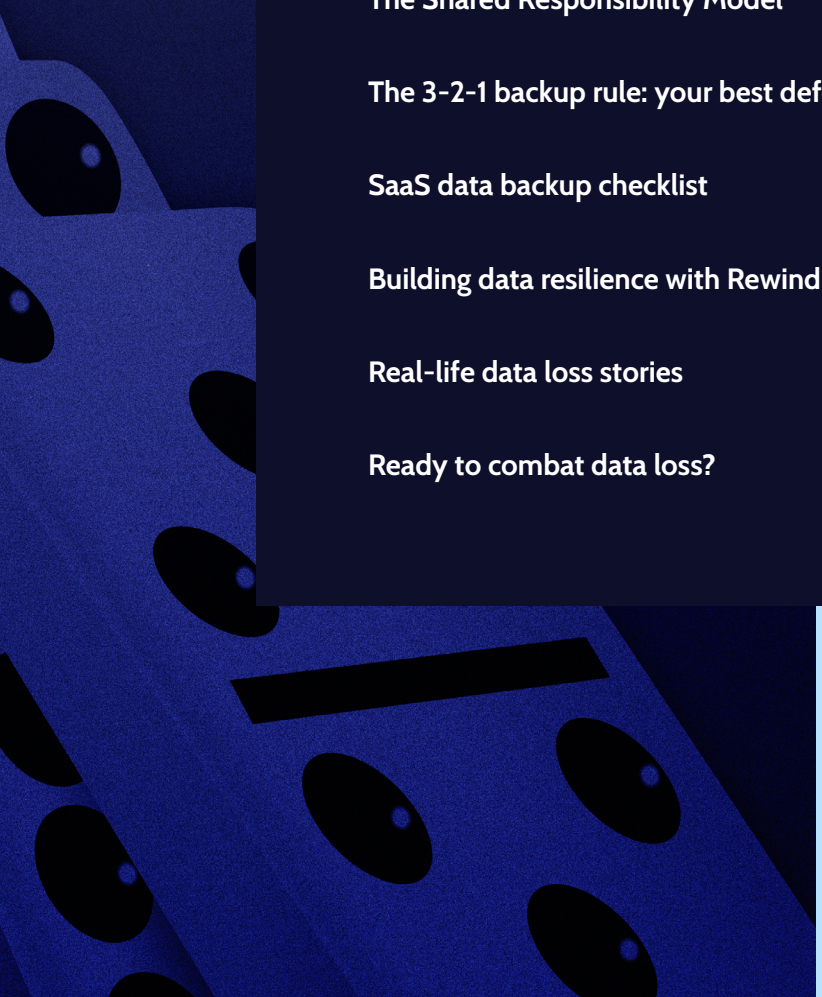
rewind

The data loss *domino effect*

How to avoid a silent chain reaction that will topple your software development lifecycle

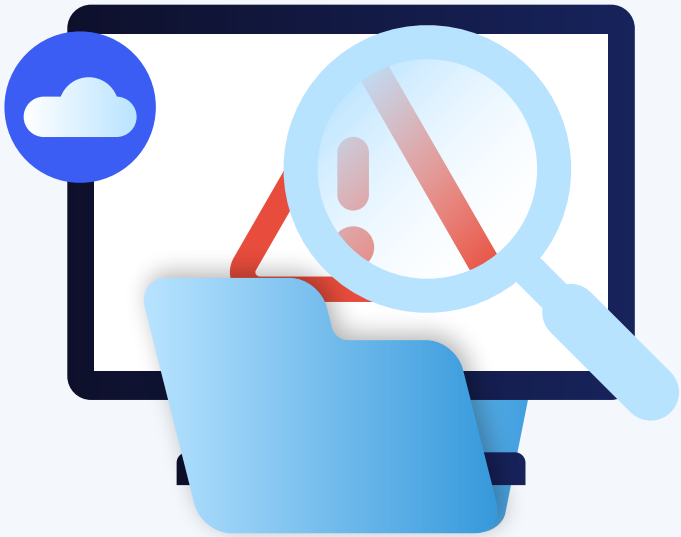
rewind

Table of Contents



The hidden dangers in your SaaS stack

Data continuity is business continuity and data resilience is business resilience. By the same token, data loss is a business loss that can be measured in lost time, lost money, and lost momentum.



The software development lifecycle moves at lightning speed. DevOps teams depend on SaaS platforms like Atlassian, GitHub, and Azure DevOps to maintain productivity, foster collaboration, and deliver projects on time. But while organizational SaaS adoption has surged, resilience hasn't kept pace.

THE DOMINO EFFECT

Data loss in SaaS platforms is not an "if" proposition but a "when," and a single data loss event doesn't stop at the deleted file or corrupted database. The impacts can cascade across the organization as processes break, teams scramble, and timelines extend. According to IBM's Cost of a Data Breach Report[1], the global average cost of a breach reached a record $4.88 million in 2024, marking a 10% increase from the previous year. When data is lost in a critical SaaS system, the DevOps pipeline freezes, deadlines slip, and customer trust erodes.

There is a blind spot in the DevOps lifecycle. Too many organizations mistakenly assume their SaaS platforms back up user data and can bring back data in case of loss. Rewind's 2024 State of SaaS Data and Recovery report[2] found that 79% of IT professionals labored under this belief.

Audit your SaaS platforms' Terms and Conditions to clarify exactly where your provider's responsibility for your data ends and your organization's begins.

The truth is, responsibility for safeguarding critical data in SaaS platforms ultimately lies with the user. Once data is lost—whether to an accident, a rogue process, ransomware or a data breach—it's already too late. Without a full resilience plan that includes a bulletproof SaaS data backup and recovery strategy, lost data is just that.

Read on as we explore how data loss in SaaS platforms starts a domino effect and more importantly, how to stop that chain reaction from happening in your organization.

External threats

A cyber attack might be the first thing that comes to mind when thinking about data loss. It makes sense; in fact, the US lost a record $16.6 billion to cybercrime in 2024[3]. And DevOps environments are certainly a target.

Continuous integration/continuous deployment (CI/CD) pipelines can give entry into many—even most—critical systems in a business: secrets and keys, cloud configurations, and deployment processes. An attack that penetrates DevOps can have massive and far-reaching implications.

Obsidian's 2025 SaaS Security Threat Report found that 85% of SaaS breaches began with compromised identities[4]. It emphasizes the escalating threats from adversary-in-the-middle (AiTM) attacks and misconfigured integrations. These attacks are becoming common, bypassing traditional multi-factor authentication (MFA) in 84% of incidents due to weak implementation or exceptions.

The dominoes begin to topple with just one seemingly small misstep. Each link in the chain is interconnected: one compromised account or deleted repository cascades into widespread operational, financial, and reputational damage. Understanding these scenarios is critical to building proactive resilience.

Implement strict role-base access control (RBAC), and audit/monitor all third-party integrations to limit risk exposure.

Threats from within

While building defenses against attacks is a critical component of any data resilience strategy, it's far from the whole story.

Human error, insider threats, and attempts at efficiency gone awry are often the first dominoes in the chain.

Consider these real-world scenarios:

These are just a few examples of how a single event can easily set off a chain reaction as data loss dominos fall and business continuity is impacted.

Think about all the ways critical SaaS data could be lost and build your disaster recovery plan with those contingencies in mind.

If
A project manager unintentionally deletes a crucial Jira story...

Then
Developers lose critical information, their current sprint, and are left scrambling for context. Projects vanish, momentum is lost, deadlines shift, and launches stall.

If
An engineer who is departing the company maliciously deletes an important GitHub repo...

Then
The CI/CD pipeline is disrupted, hotfixes mount, and your support team becomes overwhelmed by customer bug reports. The longer it takes to fix, the more customers begin to lose trust in your company. They may even take their business elsewhere, impacting your revenue. Your reputation is damaged, often irreparably.

If
An AI agent, data import, or cleanup script contains an easily overlooked but no less critical mistake...

Then
The mistake propagates rapidly, critical data is corrupted, and dependencies break. Valuable time is lost trying to untangle the knot.

The real cost of data loss

$4.88 million USD.

That's the average cost of a single data breach event according to IBM's 2024 Cost of a Data Breach report[5]. 75% of the increase in average breach costs in the 2024 study was due to the cost of lost business and post-breach response activities. The lesson: investing in post-breach response preparedness can help dramatically lower breach costs.

Data loss doesn't just kill momentum. It's a critical business risk. Every minute that organizational data is unavailable has a real cost associated, counted in lost time, lost revenue, and lost opportunity.

In 2023, the average cost of downtime to a large organization was estimated at $5,600 per minute[6]. More recently, the estimate has grown to $9,000 per minute[7].

Quick math

$9,000 / min x 60 = $540,000 / hr.
$540,000 hr x 24hr = $12,960,000 / day

There are many variables at play that make the real cost of data loss equation as unique as the organization running it. But fundamentally, data loss means downtime and downtime can cost (a lot of) money.

INDIRECT COSTS OF DATA LOSS

The cost of the damage to an organization's reputation and trust following a data loss event are harder to quantify, but no less real as a result—especially if that data is unrecoverable.

Organizations are judged on their response to a data event. Ensure your disaster recovery strategy includes a bullet-proof SaaS data backup and recovery strategy.

Consider this the baseline: 65% of customers lose faith in a brand following a breach resulting in data loss[8].

Brand equity is hard to calculate in terms of dollars and cents. You might even say that brand is priceless. Accordingly, there is no calculation to reliably measure the monetary impact of damage to a brand following a data loss event. But it is clear that lost trust is lost brand equity, and lost brand equity has a material impact on the bottom line.

In instances where the data isn't immediately (or at least relatively quickly) recoverable, such as the major 2024 CrowdStrike-Microsoft outage and the two-week Atlassian outage in 2022, just the bad press alone can be enough to deter prospective customers.

Customer churn also spikes to as much as 7%[9]. For a business generating $100 million annually, that translates to a $7 million revenue loss. To say nothing of the costs to rebuild churned pipeline or the time and money that go into customer win-back programs. And if that data isn't recoverable, your business risks permanent financial and reputational damage.

The point is, if time is money (which it is) and if lost data means lost time (which it does) then it holds true that lost data = lost revenue.

The Shared Responsibility Model

It's easy to assume that SaaS platforms protect users against data loss. They don't.

In reality, SaaS platforms operate under the Shared Responsibility Model[10]. Under this model, the SaaS service provider is responsible for data continuity and uptime at the platform level, but account-level (and item-level) data remains the user's responsibility.

In other words, if it's **your data**, it's **your responsibility** to protect it.

YOUR DATA, YOUR RESPONSIBILITY

Some providers offer limited native data recovery options—basic version history for documents, an undo button, and/or a trash bin for example. These are useful features, but they do not meet enterprise-level data recovery needs.

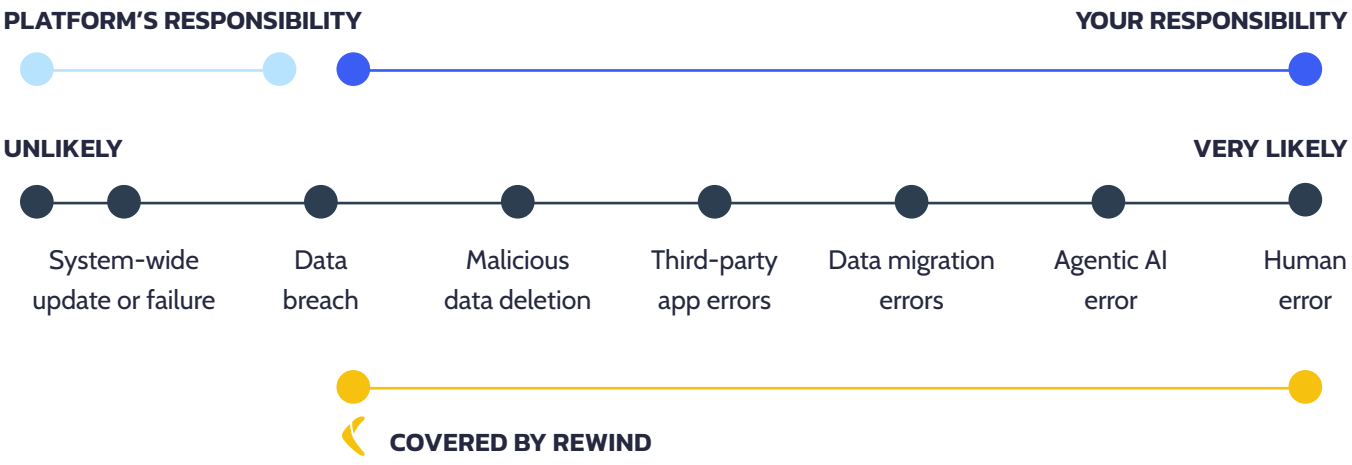
Some SaaS platforms offer the option to restore from a native backup, but recovery is typically limited to a full-instance restore and lacks the granularity to restore what was lost without overwriting other data.

Clearly document and communicate your organization's specific data backup and recovery processes and responsibilities internally to avoid assumptions.

According to Gartner, in 99% of cloud security failures through 2025, the fault will lie squarely with the customer, not the platform[11].

Without a data backup plan, recovering from accidental data deletions, malicious attacks, or other data loss events becomes costly and complex. Enterprises must proactively manage backup solutions to secure their data before it's too late.

Making data security, privacy, and safety a priority can set an organization apart in a world where others fall short. Being vocal about the ways you are proactively mitigating data loss risks creates a competitive advantage.



The 3-2-1 backup rule: your best defense

The 3-2-1 backup rule is the industry standard, recommended by information security professionals and government agencies like the Cybersecurity and Infrastructure Security Agency (CISA) in the USA[12]. The 3-2-1 rule for SaaS data recommends having:

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

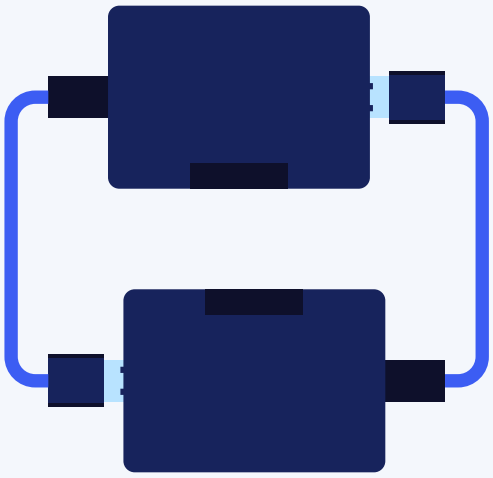
2 **Two** different places in the cloud...

1 **One** of which is not your SaaS provider copy off-platform and immutable.

Following the 3-2-1 backup rule ensures true organizational data resilience.

Having three copies of your data builds necessary redundancy. Storing your data in two different locations creates an "air gap" and ensures that you always have access to your data. Keeping one copy off-platform and immutable means that changes impacting the SaaS platform won't impact the security and safety of your data.

Engage a trusted data protection partner and make regular data recovery testing part of your disaster recovery (DR) strategy.



Solely backing up your SaaS platform data with the SaaS platform's capabilities is like backing up your hard drive to your hard drive.

Business continuity requires having a bulletproof data backup and recovery plan as part of a larger disaster recovery strategy. Partnering with a third-party backup provider offers a reliable safety net, ensuring fast recovery and minimal disruption in the event of data loss—regardless of how the loss occurs.

Rewind's automated, secure SaaS backup and recovery solution is in line with the 3-2-1 rule for SaaS backup across Jira, Confluence, GitHub, Azure DevOps, and other business-critical SaaS platforms.

SaaS data backup checklist

Many SaaS platforms let you download and save a copy of your data. Having a copy of your data is important, but in a data loss situation, a backup is of no use without a clearly defined plan to bring that data back. You need a plan that doesn't compromise on business continuity.

Regularly revisit your backup strategy as your SaaS ecosystem evolves, to ensure it continues to meet your organization's needs and can scale with your business.

As you build and test your DevOps data disaster recovery plan, ensure your backup and recovery strategy meets these basic criteria:

- ◯ **Are all critical platforms covered?**
  Your strategy must account for data in any mission-critical SaaS apps your organization relies on.
- ◯ **Is it automated?**
  Backups must run on a regular schedule without human intervention or any other single point of failure.
- ◯ **Is it granular?**
  Do you have the flexibility to restore individual files, boards, repos, projects, etc. at various time intervals?
- ◯ **Is it monitored?**
  If there's an error with your data or backup, how will you be alerted? What actions will an error trigger?
- ◯ **Is it immutable?**
  If today's data overwrites yesterday's, you may have a backup, but you don't have a reliable, working backup strategy.
- ◯ **Is it secure?**
  Is your backup data encrypted, and protected with role-based access controls (RBAC)?
- ◯ **Is it documented?**
  If your backup and recovery strategy isn't clearly defined, it doesn't exist.
- ◯ **Is it auditable?**
  Do you have access to an immutable audit log that will pass ISO, SOC, GDPR, HIPAA, etc. scrutiny?
- ◯ **Is it off-platform?**
  If your SaaS platform goes down, ensure you can still access critical data off-site in order for your business to function properly.
- ◯ **Is it a secret? Is it safe?**
  Would Gandalf approve? Remember that even the very wise cannot see all ends.

Building data resilience with Rewind

Rewind serves as your trusted silent protector, working hard behind the scenes every day to ensure your SaaS data remains resilient, recoverable, and compliant. Our backup platform is designed specifically for DevOps and other business-critical SaaS tools, offering:

Run regular training on your SaaS backup processes. Appoint data protection champions to promote privacy, educate teams, and encourage secure data practices.

- **Multi-platform coverage**
  Rewind offers a single, access-controlled interface to manage backup and restoration across the board for your organization's tech stack, making it a one-stop shop for all your backup needs.
- **Automated backup**
  Zero-touch backups that reduce the manual burden on IT teams. Cloud Sync to AWS, Azure, and Google Cloud Platform for further redundancy, and as required by some compliance standards.
- **Granular recovery**
  Roll back to a point in time or find just the lost or corrupted data and bring it back into production while preserving your state, structure, dependencies, etc.
- **Active monitoring**
  Receive event notifications (e.g. new user added, backup and restore start/stop/fail, critical security event) and create flows to trigger ITSM actions (e.g. PagerDuty, Opsgenie, Jira Service Management).
- **365-day retention**
  A full year of backup data to fall back on with options to bring your own storage (BYOS).
- **Secure by design**
  AES-256 encryption in transit and at rest, with configurable data residency and the option to bring your own key (BYOK). Independently certified to SOC 2, ISO/IEC 27001:2022, and other data security standards.
- **Documented**
  Rewind's SaaS data backup and recovery platform makes it easy to document your disaster recovery plan with clear RTO/RPO (recovery time/point objectives).
- **Compliance audit-ready**
  Export audit logs that prove your SaaS data backup and recovery strategy for ISO, SOC, GDPR, HIPAA, and other compliance laws and frameworks.
- **Secret, safe, and trustworthy**
  100% white wizard certified, with over 25,000 customers worldwide. Never abandoning reason for madness.

Real-life data loss stories

Global Rail Group had no backup infrastructure for their Atlassian tools—putting years of engineering knowledge stored in Confluence and Jira at risk of permanent loss. With no cloud redundancy and no backup strategy, any data corruption or accidental deletion could have erased critical intellectual property. They implemented Rewind to enable automated backups, secure EU-based data residency and granular recovery, protecting their core systems from catastrophic data loss.

> "We had an issue where someone got access to our web host passwords and was sending us DDoS attacks. You can try your best with multi-factor authentication, but at the end of the day, when you work in the cloud, your biggest threat is other people."

FLORIAN POLTERAUER, HEAD OF BUSINESS SUPPORT, GLOBAL RAIL GROUP

Costain, a global engineering and construction firm headquartered in the UK, struggled with a time-consuming and fragile manual backup process for their Jira and Confluence data. These three-times-weekly ZIP backups required constant oversight and relied on a single person's knowledge—putting project continuity at risk.

> "You have no access to any backups Atlassian makes—and even if you did, using them would completely wipe your current Jira data and roll everything back to the last disaster recovery point. [However] Rewind has probably given me 10 hours a week back, including after hours, because I no longer have to run manual backups after everyone's done for the day."

MICHAEL WHEATSTONE, FORMER JIRA ORGANISATION ADMINISTRATOR, COSTAIN

Rewind proactively safeguards your critical SaaS data, empowering your teams to focus on innovation, secure in the knowledge that their data remains safe and always accessible.

TRUSTED BY OVER 25,000 ORGANIZATIONS

COSTAIN · Bullish · LUTRON · Dr. Martens AirWair · Abbott

Don’t wait for the *first domino to fall*

The question isn’t if a data loss event will occur, but when. Every moment without a secure SaaS backup strategy increases your organization’s exposure to operational disruption, financial loss, and reputational damage.

From sprint to shipped, ensure your DevOps data remains secure, resilient, and ready for whatever challenges come next.

TAKE CONTROL TODAY AND COMBAT THE DATA LOSS DOMINO EFFECT:

- Review your current SaaS backup strategy.
- Assess vulnerabilities and gaps.
- Implement a reliable backup solution.
- Test your backup and recovery strategy before you need it.

Book your demo today

Sources cited

1 Cost of a Data Breach 2024 - IBM

2 2024 State of SaaS Data and Recovery - Rewind

3 FBI: Cybercrime Losses Surpassed $16.6 Billion in 2024 - Securityweek

4 2025 SaaS Security Threat Report - Obsidian

5 Cost of a Data Breach 2024 - IBM

6 Average Cost of Downtime per Industry - Pingdom

7 The True Cost Of Downtime (And How To Avoid It) - Forbes

8 What causes the most damage, losing data or trust? - Cyber Magazine

9 Breaches rank in top 3 negative impacts on brand reputation: Above CEO Scandal - Delinia

10 The Shared Responsibility Model and SaaS explained - Rewind

11 Is the Cloud Secure? - Gartner

12 Data Backup Options - CSIA