rewind

Audit-ready disaster recovery in monday.com

Strengthening productivity, compliance, and security with Rewind

A guide for IT leaders, CISOs, and SaaS resilience strategists

Table of Contents

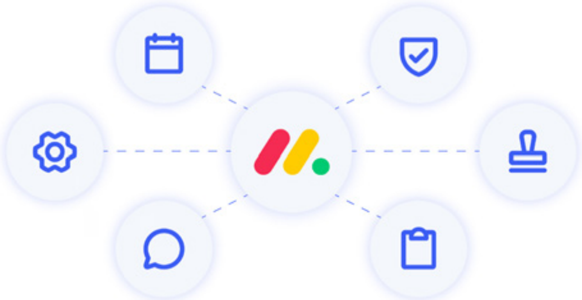
monday.com is more than a productivity tool

Maybe this sounds familiar: Your team starts using monday.com to organize projects, tasks, and workflows. But unlike the 71 other SaaS apps the organization tested that year (an average of 6 per month, according to Zylo[1]), monday.com delivers consistent value. Adoption spreads and before IT leaders know it, monday.com is mission-critical. Project timelines, stakeholder approvals, SOPs, even compliance processes—all of which we'll just call "data"—run through monday.com. It's the operational brain of your business.

Or maybe the route to monday.com-as-mission-critical was more direct. Perhaps your organization was trying to contain *SaaS sprawl* and get all teams working with one Work OS.

monday.com is mission-critical

It doesn't matter how it came to be. Whether gradually or all at once, monday.com isn't just useful, it's essential for your business. If the data your organization holds in monday.com was ever lost, altered, or corrupted, the cost isn't just productivity. It's lost time and revenue, broken workflows, missed SLAs, and potential compliance violations.



You need a backup plan

According to IBM's *2024 Cost of a Data Breach Report*[2], the global average cost of a data breach rose to $4.88 million, up 10% since 2023 ($4.45 million) and more than 25% from 2020 ($3.86 million).

While not every data loss is a breach—indeed, a breach isn't even the most common cause of data loss in SaaS platforms, but we'll get to that—any disruption has a ripple effect that impacts business continuity.

An organization needs a business continuity and disaster recovery plan, and it's critical for that to include a backup plan for monday.com to keep your data secure, resilient, and audit-ready.

So let's talk about that.

If your teams use monday.com for cross-functional projects, treat it like a Tier 1 system in your DR planning.

How Rewind can help

Rewind automatically backs up your monday.com data—boards, items, updates, files, automations, and more—so you can restore what you need, when you need it. That means business continuity doesn't depend on manual exports or wishful thinking.

[1] "111 Unmissable SaaS Statistics for 2025" Zylo.

[2] "Cost of a Data Breach Report 2024" IBM.

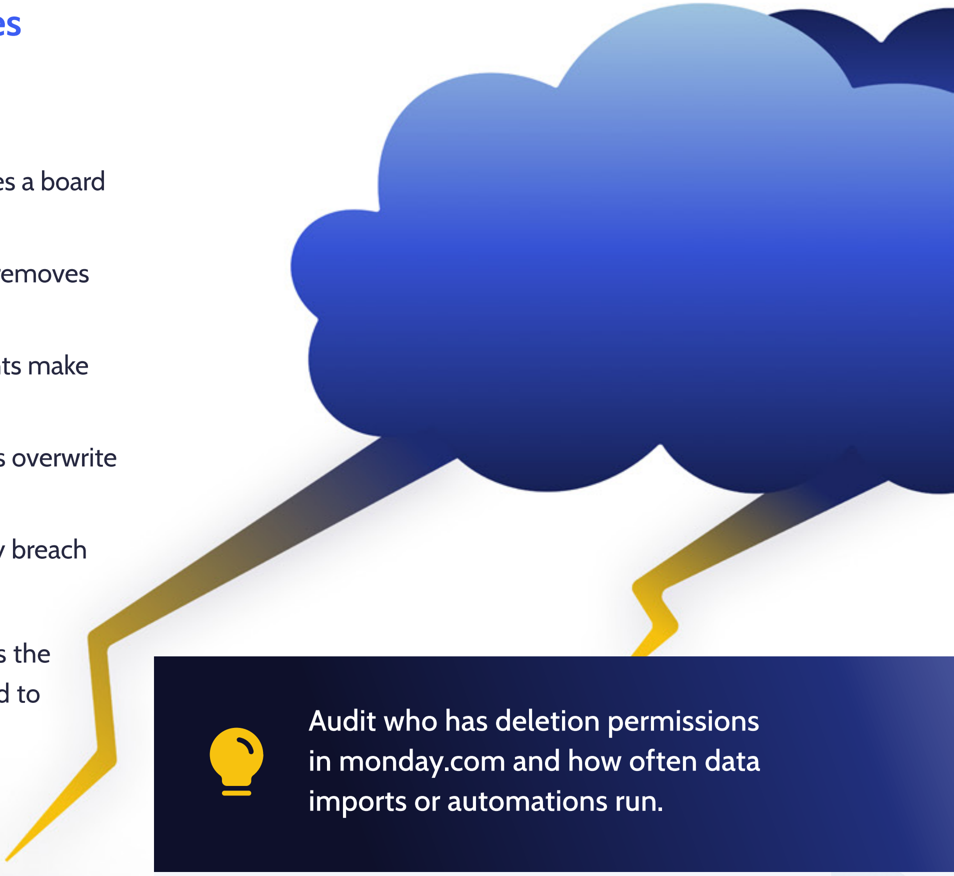
Data threats outside and within your organization

Data loss in SaaS isn't a *what if*, it's a *when*. When we think of data loss, the first thing that comes to mind might be a cyber attack, like ransomware for example. As IT and security leaders know, cyber attacks are real and organizations must take steps to mitigate risks, but attacks are far from the only threat to an organization's critical data. In fact, the threat is often much closer to home.

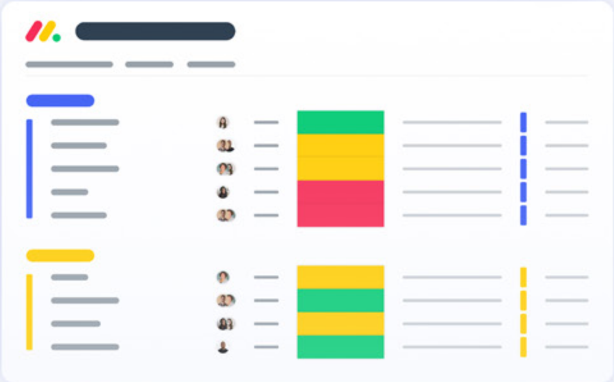
Here are the most common causes to visualize in your disaster recovery planning:

- **Accidental deletion:** A user mistakenly deletes a board or project.
- **Malicious deletion:** A disgruntled employee removes critical data.
- **Agentic AI actions:** Integrations using AI agents make unintended, large-scale changes.
- **Bad data import:** CSV uploads or integrations overwrite or misalign data.
- **Cyber attack:** Account takeover or third-party breach leads to data tampering or loss.

These threats are often user-driven. In SaaS, it's the user's responsibility to defend against them and to have a disaster recovery plan in place.



Audit who has deletion permissions in monday.com and how often data imports or automations run.



How Rewind can help

In addition to role-based access control (RBAC), Rewind offers a full version history for your monday.com environment, not just activity logs. That means you can recover from a bad import, undo rogue changes, or reverse deletions in minutes.

The Shared Responsibility Model and monday.com

In SaaS, the vendor protects the infrastructure. You, the customer, are responsible for protecting your own data. That's the essence of the Shared Responsibility Model[3], and it applies to monday.com, too.

Undo ≠ backup

Relying solely on native features can leave you exposed to both user error and audit failure.

While monday.com does offer some safety nets, such as the *trash bin* and limited undo and document/file versioning, these are a first line of defense. They are not intended to take the place of a reliable and secure backup and recovery strategy, because they:

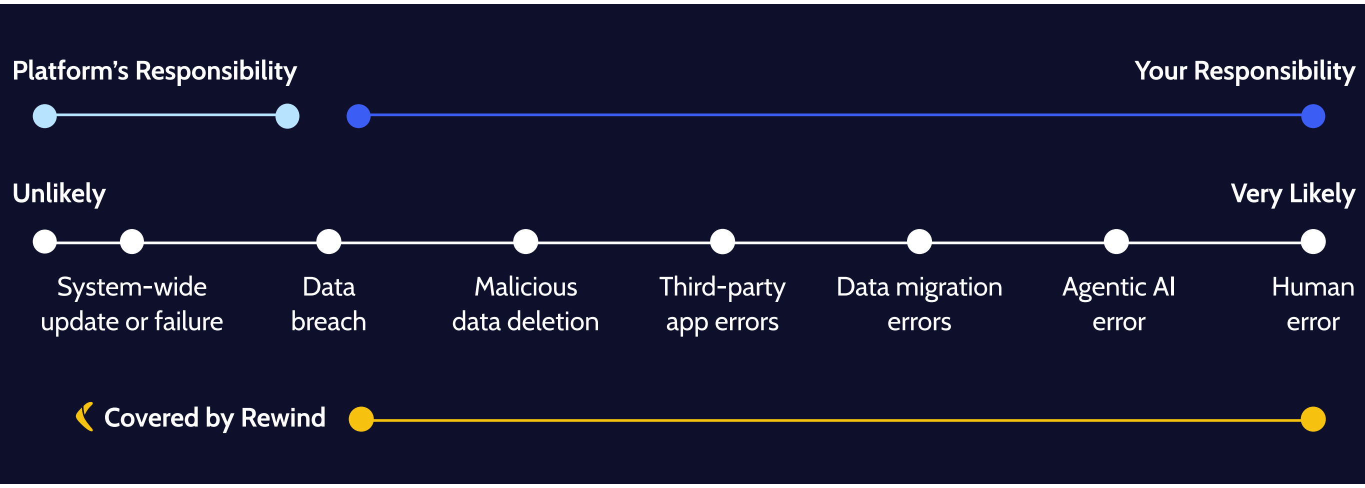
- Don't capture full boards or account-wide settings
- Have limited data retention periods
- Can't granularly restore data at the account or workspace level
- Won't save your account-level data in the event of loss

The point is clear: if you store critical data in monday.com, you need a backup plan. Don't wait until after your data is permanently deleted due to an accident or something more malicious.

Review the monday.com documentation on data recovery to understand what's recoverable—and what isn't—by default.

How Rewind can help

Using Rewind fulfills the organizational obligation to secure user data, in accordance with the Shared Responsibility Model. Rewind captures and backs up data automatically, outside the monday.com platform, and lets you restore data in context.



[3] "The Shared Responsibility Model and SaaS, explained" Rewind.

The 3-2-1 rule for SaaS backup

The 3-2-1 rule has long been the standard for data protection:

- Keep **3** copies of your data
- In **2** locations in the cloud
- **1** of which is not the SaaS provider

The rule predates SaaS, but the central idea is no less relevant today, when most data is not stored on-prem but rather in the cloud. The 3-2-1 rule for SaaS backup[4] updates the long-standing rule to align with this reality:

Keep 3 copies of your data

Store them on 2 different media

Ensure 1 is offsite and immutable

In practical terms, that means:

- One copy of your data lives in the platform (monday.com)
- One copy of your data is backed up automatically
- One copy of your data is off-platform, secure, and immutable

Considering the Shared Responsibility Model for SaaS data, not having an independent backup solution means having a single point of failure.

That's why compliance frameworks, laws, and regulations as well as cyber insurance providers increasingly expect organizations to follow 3-2-1 or equivalent strategies.

Add monday.com to your enterprise backup policy checklist. It's easy to overlook, but your data is just as easy to lose.

How Rewind can help

Rewind gives you the second and third copies, automatically backed up and securely stored offsite. No scripts, no exports, no user intervention. Just always-on comprehensive data protection you can trust.

[4] "Understanding the 3-2-1 rule for cloud backups" Rewind.

Building a disaster recovery plan for monday.com

If monday.com plays a key role in your operational tech stack, it deserves its own disaster recovery (DR) plan. The best DR plans are scenario-based, tested regularly, and able to answer one simple question: How fast can we get back to normal following a data loss incident?

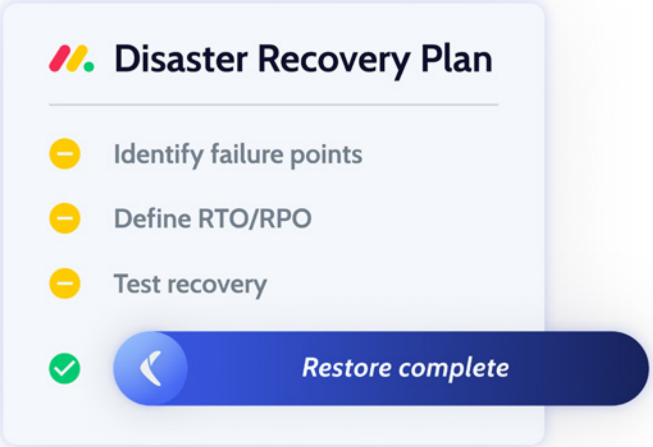
Start by identifying key failure points:

- What happens if an automation overwrites an important board?
- How would you recover if a user deleted a project pipeline?
- Could you roll back an AI automation or other bulk change gone wrong?
- Would you be able to get your data back if it was held for ransom?

Then, define your Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs):

- **RTO:** What's the maximum amount of time for restoring and regaining access to data after an unplanned disruption?
- **RPO:** What's the maximum amount of data you can afford to lose?

Finally, simulate recovery scenarios in disaster recovery tabletop and other preparedness exercises. Because a DR plan that hasn't been battle-tested is not battle-ready.



Disaster Recovery Plan

⊖ Identify failure points

⊖ Define RTO/RPO

⊖ Test recovery

✓ Restore complete

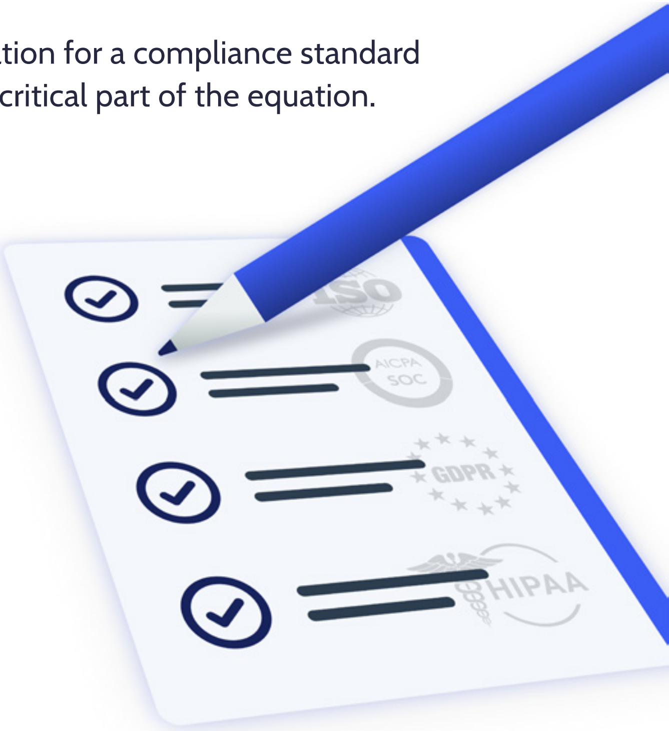
Treat monday.com boards like any other cloud application by including them in quarterly DR tabletop drills. This builds team confidence and shows stakeholders you're serious about data security.

How Rewind can help

Rewind's restore features are built for real-world testing. Restore a single item, full board, or entire account—on demand. You can test without disruption and know exactly how recovery would play out.

Backup and recovery are a compliance requirement

If your organization is working toward or maintaining attestation for a compliance standard like SOC 2, HIPAA, ISO 27001, or DORA, data resilience is a critical part of the equation.



Regulators and auditors increasingly expect organizations to:

- Demonstrate that business-critical SaaS data is backed up
- Show they can restore data quickly and accurately
- Prove that backup solutions meet stringent security standards

monday.com data can include sensitive information, operational workflows, approval chains, and process logs. If that data can't be restored reliably—or if you can't prove that you can get it back and comply with regulatory requirements—you are not audit-ready.

The good news? You don't have to over-engineer your way to compliance. You just need to show that your data recovery posture is active, verifiable, and independently secured.

Review your last compliance audit report. If data backup and recovery was flagged, you need to take action. If not, you should prepare now to ensure it never is.

How Rewind can help

Rewind supports compliance with secure, immutable, encrypted backups that feature configurable data residency, granular restore capabilities, and full recovery logs, which makes compliance audit documentation fast, easy, and defensible.

What Rewind brings to monday.com

Rewind is built from the ground up with a security-first ethos[5]. As experts in data backups, security isn't just a feature. It's at the core of what we do.

Rewind extends monday.com benefits with purpose-built backup and recovery capabilities that help your team meet security, recovery, and compliance goals without friction.

Enterprise-grade backup solution

- Tailor-made data protection solution available for all monday.com customers
- Fully-integrated, seamless experience
- Minimize downtime by quickly restoring data
- Enhance data resilience

Security and compliance

- Immutable, encrypted backups
- Configurable data residency
- SOC 2 Type II, ISO/IEC 27001:2022 and other attestations
- Support for compliance frameworks like HIPAA, DORA, GDPR, etc.

Zero trust architecture

- SSO (Single Sign-On)
- MFA (Multi-Factor Authentication)
- RBAC (Role-Based Access Control)
- BYOK (Bring Your Own Key) encryption support

Disaster recovery

- Automated daily backups
- Unlimited version history
- Granular restore by item, board, or full account
- Point-in-time recovery

It's not just about protection, it's about proving protection in an audit. Rewind gives IT leaders the confidence to say, "yes, our monday.com data is safe, secure, and restorable" and provides the tools to easily prove it in a compliance audit.

Do you have a backup plan for monday.com? If not, you should. If you have a "solution" but it doesn't check all these boxes, it's time to reassess.

How Rewind can help

Rewind checks every box above—without complex setup or steep learning curves. You'll be live in minutes, protected continuously, and always in control.

[5] "Rewind's Security Portal" Rewind.

Get started with Rewind

monday.com is central to how your teams work, collaborate, and deliver. But that centrality comes with responsibility—because operational excellence, business continuity, and compliance depend on data you can't afford to lose.

Native recovery features in your favorite SaaS platforms have limits. Manual data exports don't solve for data restoration, and hope is not a data loss prevention strategy.

With Rewind, your monday.com data is:

- Backed up automatically
- Protected from internal and external threats
- Instantly recoverable by workspace, board, item, sub-items, or full account
- Audit-ready by design

Your disaster recovery posture shouldn't stop at infrastructure. It should include the SaaS tools powering the heart of your organization.

If your DR plan covers email, storage, and infrastructure, but not monday.com, you've got a gap. Fill it before it's tested.

True cloud data resilience, simplified.

Start your free trial of Rewind for monday.com today.