

An eBook for Jira Admins



The Ultimate Guide to: Jira Data Protection

Learn the **why** you need to **protect**
your Jira data



revyz.io

Contents

Revyz is on a mission to help Jira administrators manage their Jira data. It's the first cloud-native data management solution for Atlassian. And, it's backed by Atlassian Ventures and Druva.

	Page
1 Introduction	3
2 Cloud Challenges	4
The Shared Responsibility Model	
You and your Cloud provider	
Atlassian Administrator responsibilities	
Atlassian Data Protection Gaps	
Jira - Single Source of Truth	
3 Jira Backup Protection	8
Data Backup and Retention	
Data Recovery	
Accidental Deletions	
Bulk Changes	
Configuration Changes	
Data Security	
The Insider Threat	
Account Takeover	
Change Management and Compliance Reporting	
eDiscovery	
4 Jira Backup Use Cases	14
Enterprise Technology and eDiscovery	
SOC2 Compliance	
JSM Asset Database Protection	
5 Case Study	18
6 The benefits of using Revyz Data Manager for Jira	21
7 Summary	23
References	

Introduction

Data has become an important asset that can be used to gain a competitive advantage in today's digital economy. Companies that understand the value of data and can effectively collect, manage, and analyze it are more likely to succeed and thrive in the modern business landscape. And they pay top dollar to hire experts that can achieve that. Equally, customers trust that their valuable information is protected beyond a doubt.

Additionally, cloud computing has become increasingly popular in recent years due to its operational, security, and cost benefits. Software-as-a-Service (SaaS) applications are a major part of this landscape change. Now, it's rapidly replacing traditional enterprise and web applications deployed in on-premises data centers.

Post-pandemic, remote work has become the preferred method for many people. And the adoption of product suites that flex for remote work is skyrocketing.

In fact, Atlassian's product suite is the 6th most widely used SaaS application* in businesses globally, behind Office 365, AWS, Google Workspace, Salesforce, and Zoom. Additionally, [Atlassian's cloud revenues have grown by over 50%](#) in FY-Q4 '22 compared to FY-Q4 '21, highlighting the growing adoption of their SaaS offerings. However, despite its popularity, there is still confusion about the built-in data protection capabilities of the Atlassian Product Suite. Particularly for Jira - its most popular application.

Cloud backup should be simple, reliable and useful.

Yet, if you ask your IT department or System Administrator, can they agree that's the current state of play in your business?

*[*Okta's Business At Work report for 2022](#)*

Cloud Challenges



The Shared Responsibility Model

You and Your Cloud Provider

Many business leaders mistakenly assume that cloud adoption eliminates the need for some core IT functions, but the reality is that the customer still has a responsibility to protect and retain their data, even if it's residing with the cloud provider's applications.


Like all cloud providers, Atlassian's product suite, such as Jira and Confluence, follows a shared responsibility model where the cloud provider and the customer have defined responsibilities. For example, the provider is responsible for managing application performance and uptime, and the customer is responsible for data protection and retention.



Atlassian Administrator Responsibilities

Did you know that under the Atlassian shared responsibility model, System Administrators are responsible for the protection and long-term retention of customer data that resides within Atlassian applications? This includes Jira, Confluence, and Jira Service Management. .

01 Policy & Compliance	<ul style="list-style-type: none"> • Assess the suitability of Atlassian Cloud-based platforms based on the information Atlassian provides • Protect your endpoints through good security practices
02 Users	<ul style="list-style-type: none"> • Who accesses the Atlassian platform and what access they have to your data is your responsibility
03 Information	<ul style="list-style-type: none"> • Create backups of your data
04 Marketplace Apps	<ul style="list-style-type: none"> • Assess the suitability of any Marketplace Apps you want to use • Notify Atlassian of any malicious behavior identified in a Marketplace App



Atlassian Data Protection Gaps

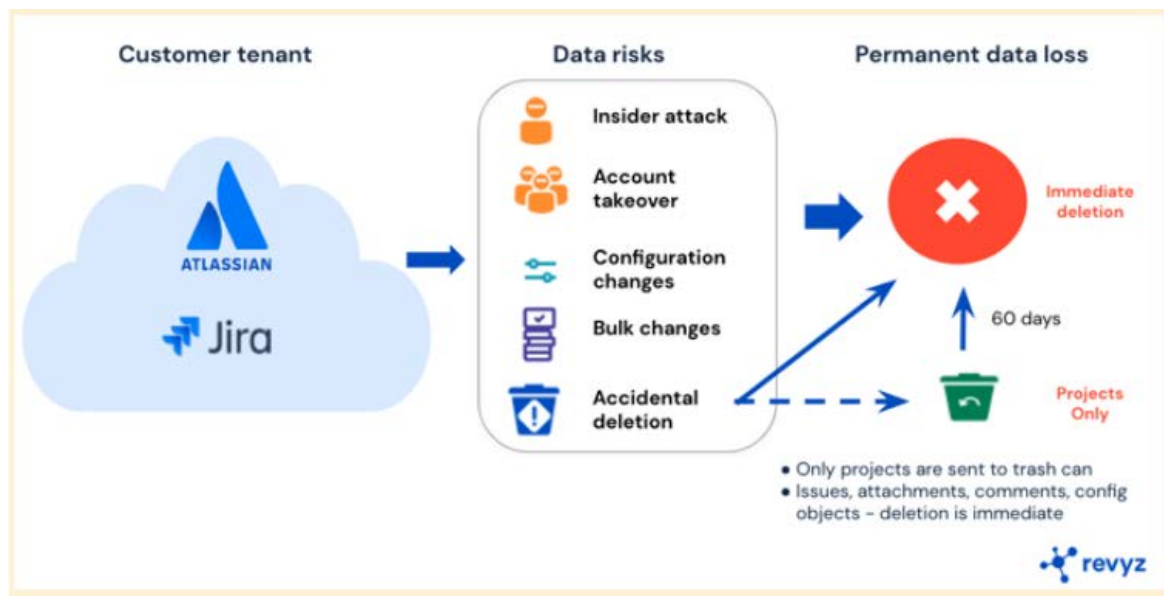
Did you also know that Atlassian’s service-level agreements (SLAs) are actually designed to protect them, not you?

In fact, they only apply to data scenarios that Atlassian loses involving their own infrastructure-related issues. Not the data you lose because of your own accidents.

What’s more? The recovery capabilities are limited - expiring within 60 days. So, to avoid data loss, regular backups are recommended. It’s even part of Atlassian’s Security Practices and their Shared Responsibility Model.

Now, Jira does have some native data protection tools, but they require administrators and users to have knowledge of the policies for each application. Relying solely on these tools puts your organization’s data and projects at risk for all sorts of mishaps including:

- **Accidental deletions.**
- **Bulk changes that need to be reverted back.**
- **Configuration changes that could be disastrous.**
- **Malicious data loss caused by employees or even hackers.**
- **Regulatory and compliance-related data retention.**



Jira - Single Source of Truth

Silos are so old school, aren't they? Critical information should in fact be centralized in the Atlassian product suite including Jira and Confluence. Creating a Single Source of Truth (SSoT).

SSoT = less confusion and friction + more productivity and efficiency.

But, what if you lost that centralized SSoT via threat or accident? Could your business continuity plan work effectively for days whilst you wait for most cloud backup solutions to restore you to a point in time? And, that's only on the basis you have a backup and the data hasn't been lost forever. Wouldn't it just be great if there was a solution that could provide a backup in minutes?

“Revyz Data Manager for Jira is a game-changer for Sys Admins. It backs up the data every day, and data is recoverable in minutes. Now there's a tool where you can 'set it and forget it'. And when you want to recover something, simply search for a specific ticket instead of a full point-in-time restore. It's absolutely revolutionary.”

- Carlos Almeida, Vice President of Engineering, SPK and Associates.

Jira Backup Protection



Data Backup and Retention

IT administrators should have adequate backup strategies for your critical data. They should be able to tell you the schedules, and retention periods of your backups with confidence. But what about Jira backups? Suddenly, that confidence fades, doesn't it?

Why? Because Jira's native data protection capabilities provide organizations with limited control over data backup and retention policies. Your Jira data can be manually backed-up as a database XML file. But, managing the backup file is essentially your headache.

It's no secret that Jira backups may be "smoke and mirrors" to your IT administrators. Atlassian's Jira simply doesn't meet the standards that virtually all security professionals recommend for data backup and retention:

The 3-2-1 rule:

Three independent copies of your critical enterprise data on two different platforms/media, and in at least one remote location.

Data Recovery

Here's the thing. Accidents happen. Computers crash. Hard drives fail. Files get deleted.

And when that happens, you need to be able to recover that data. Fast. Otherwise, you risk losing all of that valuable information forever.

That's why data recovery is essential. It's a safety net. It allows you to restore lost or damaged Jira data and continue your operations with minimal disruptions. A cloud-native backup solution like Revyz Data Manager for Jira is the answer for protecting your Jira data.

Accidental Deletions

Management is always pushing timelines, aren't they?

That's just one of the reasons as a System Administrator it's important to keep your site tidy and effective. So, automated cleanup scripts are a common practice. But, they can sometimes delete critical attachments or comments along with redundant data. For instance, a well-intentioned project admin may delete redundant Jira Issues but unintentionally erase essential attachments and comments.

Accidental deletions of important data by Jira users or admins are bound to happen. And the worst part? Sometimes, they don't even realize it until months later...when it's too late.

Did you know that there are no audit logs when Jira issues get deleted?

Months can go by before someone discovers the missing data, and by then, it's most likely lost forever. Without a third-party Jira backup solution, like Revyz Data Manager for Jira, your data is at risk.

Bulk Changes

Jira's bulk change feature is fantastic isn't it?

Allowing end users and admins to make changes or edit multiple issues at once. Oh, the joy of saving time and avoiding repetitive tasks. However... humans can make mistakes, leading to incorrect selections and a tedious effort to revert changes.

To avoid these issues, an incremental backup solution with granular point-in-time restores can be a game changer. With this capability, you can:

- **Easily undo bulk changes.**
- **Save valuable time and energy.**
- **Work confidently and efficiently in Jira.**

Configuration Changes

Sharing configuration objects across multiple projects is the best practice in Jira. We all know that.

However, making changes to shared configuration objects can cause problems for project administrators. So, whilst sharing configuration objects is a great way to declutter your Jira site, a reliable backup solution is also the best practice for mitigating potential issues.

A comprehensive third-party Jira backup solution like Revyz Data Manager for Jira includes regular point-in-time backups and a clear data retention policy. That means your project administrators can quickly revert to a previous configuration if necessary, without risking data loss.

Data Security



The Insider Threat

Project management is fast-paced. And balancing cyber-security isn't just important - it's critical.

Malicious insiders can pose a threat to your Jira environment. And, according to the Verizon 2019 Data Breach Investigations Report, insiders are responsible for almost one-third of all security incidents and around one-fifth of all data breaches. These rogue employees have the ability to delete, alter, hide, or even steal critical data, causing irreparable damage to your organization.

Without a Jira backup solution, the loss of important data can be immediate and no one would know who did it. Investing in a comprehensive Jira backup solution can offer peace of mind to project managers and administrators, knowing that their data is well-protected and secure from insider threats. With such a solution, you can:

- **Continuously capture data, including deleted Jira issues, and associated attachments, comments, and configuration objects like workflows and screens.**
- **Isolate a copy of historic data outside the Jira environment, providing additional protection.**
- **Conduct data investigations and forensic analysis with built-in search and analytics capabilities, enabling you to quickly identify any security incidents and take necessary action.**

Account Takeover Recovery and RaaS

One particularly concerning trend is the exponential increase in account takeovers. These are ransomware attacks that can wreak havoc on a business by destroying critical data.

What's even more alarming is the emergence of Ransomware as a Service (RaaS).

RaaS makes it disturbingly easy for just about anyone to launch a ransomware attack against an organization.

The single best defense against these types of attacks is a reliable data backup. A Jira backup solution will protect your critical Jira data and ensure that you're ready to recover quickly if the worst happens.

“With a cloud-native backup solution like Revyz Data Manager for Jira, Sys Admins can complete selective restores of deleted items – whether by accident or on purpose. With no downtime and without a lot of effort. Revyz is changing the way our industry works.”

- Michael Roberts, Vice President, SPK and Associates.

Change Management & Compliance Reporting

When it comes to compliance audits like SOC2, PCI, ISO27001, or FDA, missing or lost change management records can be disastrous for a business.

To ensure a smooth audit process, companies export Jira issues related to changes made during the audit period. The solution to maintaining crucial change management records is to invest in a backup solution that provides regular point-in-time backups and a clear data retention policy. Yes, you guessed correctly....Revyz Data Manager for Jira does exactly that.

eDiscovery

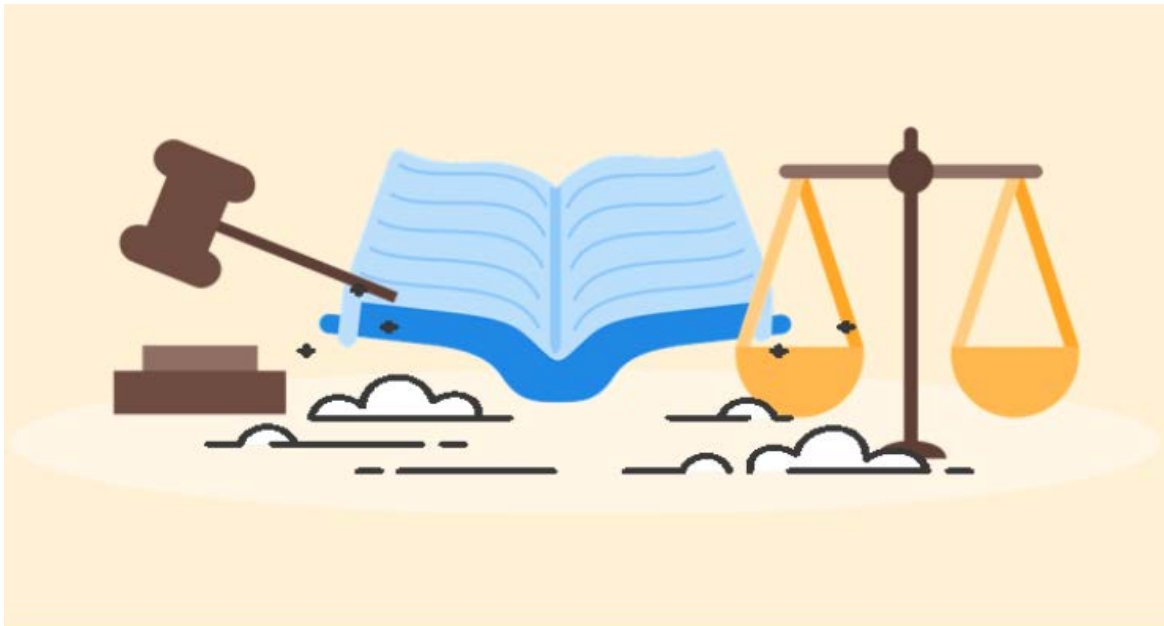
In legal disputes, you'll need to meet eDiscovery and legal hold obligations to avoid penalties and liability, won't you?

These include eDiscovery requiring all relevant end-user data across the organization to be quickly accessible and protected from deletion or alteration, to avoid potential penalties and/or liability.

Now, Jira lacks specific capabilities for data preservation and compliance, making compliance a risky and difficult process. And, gaps in data retention, such as deleting or departing employees, also create challenges. But, these challenges can be overcome with a solution like Revyz Data Manager for Jira that can fully address data preservation and compliance.

Jira Backup Use Cases

So, now we're all aligned on the current cloud backup challenges, let's show you the versatility of Revyz Data Manager for Jira with some real-world customer success stories across three industries.



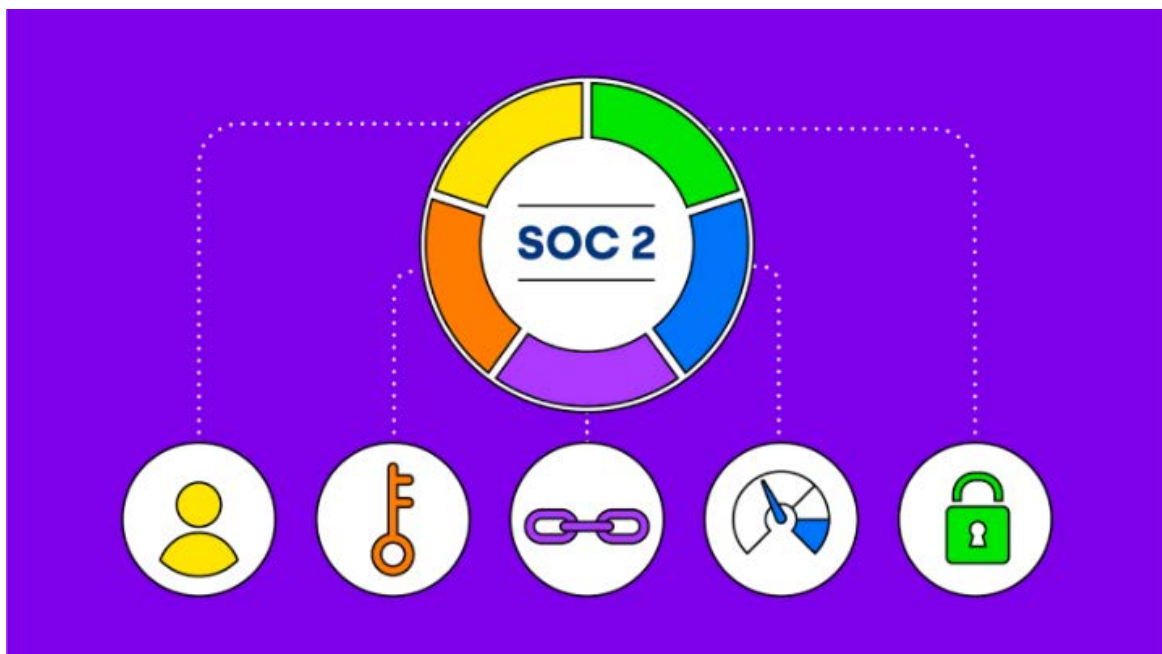
Enterprise Technology and eDiscovery

Our client, a leading supplier of enterprise technology solutions, was expanding rapidly into multiple markets worldwide. They were utilizing Salesforce and Atlassian Jira in their order management and fulfillment processes. Initially, they used the on-premises Data Center version of Jira, where they backed up data every 24 hours (using an on-premises database backup solution from Commvault). However, the IT team was repeatedly tasked by the legal team to retrieve deleted Jira objects for ongoing disputes and lawsuits.

This time-consuming task required multiple IT engineers to spin up a separate instance of Jira, search for deleted objects, and repeat the process across different backup snapshots. Tedious to say the least. Expertise is drowned in non-expert tasks to embellish. This challenge became more acute when they migrated their Atlassian applications to the cloud in 2021.

To streamline the process and reduce costs, the IT team deployed the Revyz Data Manager for Jira solution for Jira Cloud. This eliminated the need for manual XML-based backups and saved man-hours for backups, storage, and additional hardware for data restoration. It also significantly reduced the time required to search for the needed information, from days or weeks down to minutes. And, their expertise got back to those business growth tasks.

Financial Services: SOC2 Compliance



A leading Financial Services company implemented a change management process as part of its SOC2 compliance to mitigate system instability problems. Their change management processes revolve around Jira and Jira boards.

All changes were reviewed by the security and compliance team on a daily basis. Additionally, the company's infrastructure was managed as code, and changes passed through a standard code review process for approval. Only emergency changes can bypass this process, subject to retrospective review.

The company recognized the critical importance of change management data for maintaining SOC2 compliance and ensuring audit requirements. So, to eliminate the risk of accidental or malicious deletions, they implemented Revyz Data Manager for Jira's automated backup and restore solution. This assured both the company and SOC2 auditors during the SOC2 re-attestation process.

Financial Services: JSM Asset Database Protection



A leading Financial Services company uses the Assets functionality extensively as part of their service management processes. As part of their Asset database, they imported critical IT and non-IT assets. These that provide additional context for a given services management request from internal and external customers.

But, while there are plenty of benefits of JSM Assets, its value is contingent on accurate and available data 24/7. JSM Assets are only helpful if it contains high-quality, accurate, and well-maintained information. When configuration items (CI) data in JSM Assets is lost or corrupted, the risk of business disruption increases. Additionally, the ability to diagnose outages, manage assets, and maintain compliance are severely weakened. In fact, having inaccurate or incomplete CI data in JSM Assets can cause bigger problems if businesses aren't careful.

Furthermore, having a JSM Assets database that contains "dirty" data can create confusion, waste effort, and lose time when a major incident occurs. Also, more issues arise as CI data can be lost or corrupted for weeks before anyone notices. Over that period of time, business decisions and changes to the various business assets compound the problem. Especially if teams responsible for the data cannot examine historical information to trace changes. Or, identify how and when their data loss or corruption occurred.

The company recognized the critical importance of protecting its database. They took action to eliminate the risk of accidental deletions, malicious deletions and stale data. They implemented Revyz Data Manager for Jira. The automated backup and restore solution helped eliminate business impact.

Case Study



Travel Leader Automates Backup And Recovery For Efficiency

Our client, a leading active travel company, takes people on unforgettable biking, walking, and hiking trips around the world. They also have a distributed workforce operating out of multiple locations. Their IT team managed customer support, data storage, telecommunications, and application support. Seeking to accelerate cloud projects, the company moved all its Atlassian applications to the cloud, including critical software like Jira, used for tracking tasks and guest preferences.

The move accelerated its cloud projects and improved collaboration between the company's dispersed workforce. However, reliance on Jira's backup and restore functionality to recover data made Backroads vulnerable to data loss.

Additionally, backing up Jira data using the built-in capabilities offered by Jira was extremely time-consuming and error-prone. Then, an administrator accidentally deleted critical customer data, including attachments and information.

Without secure backups in place, the company knew it risked irreparable data loss due to accidental deletion and also platform disruption, and security threats. The IT team tried to automate backups using private APIs but failed due to the large dataset size.

After searching for a solution, they found the Revyz Data Manager for Jira app in the Atlassian Marketplace, which they installed with a few clicks.

Revyz Data Manager for Jira offers an automatic daily backup solution with a Jira native console for Jira Administrators to manage backups and restore operations. Additionally, Revyz is built on AWS, so it provides secure off-site backup, with all the necessary controls needed to further secure data. This included encrypting the data at rest with the tenant and object-specific encryption keys. Backups cut ties with the original data, protecting against corruption if a security breach occurs. So, the Jira Admins could confidently recover data back to a granular manner from the offsite and secure Revyz cloud. And it took just a few clicks to install the simple, reliable and useful software.

The result was 100% protection of all data in the Jira Software cloud, which is secure 24/7 and recoverable in minutes - not days.

“With Revyz Data Manager for Jira we were able to instantaneously recover Jira issues and attachments deleted accidentally. The Revyz solution had our backs!”

- Oscar Hernandez, Sr Systems Administrator.

Revyz's security posture and enterprise-class capabilities such as audit logs, backup, and restore job details, provided the travel company with peace of mind against further accidental data loss.

With Revyz, the travel team's Jira Administrators can now recover lost or deleted data almost instantaneously. The solution removes the tedious process of manual backups and restores, which used to take days.

“We will likely experience a security incident, and how we recover is going to be a testament to our character and the controls we now have in place. Revyz is a key part of that recovery plan.”

- Steven Huang, Head of IT.

Revyz's security posture and enterprise-class capabilities such as audit logs, backup, and restore job details, provided the travel company with peace of mind against further accidental data loss.

Results:

- Improved productivity through automation and fast data recovery.
- Extended cloud-native data protection, governance, and recovery for Jira.
- 20% reduction in labor costs through task automation.
- 15% operational savings by eliminating XML backup maintenance costs.
- 100% of Jira Software data is secure 24/7 and recoverable in minutes.
- Exponentially faster and granular data recovery for all Jira Software data.
- Complete confidence in data recovery in the event of accidental or malicious deletion or a bulk data change event.
- Recovery of configuration objects, saving time for Jira Administrators.

The benefits of using Revyz Data Manager for Jira

The Revyz Data Manager for Jira helps Administrators with their Jira data management needs.

- **Manage** | Cloud to Cloud data Cloning | *Example use case: Sandbox to production*
- **Protect** | Backup & Restore | *All Jira project types (JSW, JSM etc.. including JSM Assets)*
- **Analyze** | Jira site analytics for the Administrator
- **Optimize** | Jira site optimization | *Example use case: Cleanup of Jira site, easily delete unwanted configuration*

It's the first cloud-native backup solution for Atlassian. And, it's backed by Atlassian Ventures and Druva.

Backup, Recover, Restore, Retain

- Automated and secure Jira data backups and restores.
- Instantaneous recovery of Jira data.
- Regular point-in-time backups and unlimited retention.
- Bulk and granular point-in-time restores.

Operational Efficiency and Compliance

- Elimination of manual labor costs associated with traditional backup methods.
- Reduced time to fulfill eDiscovery requests, with data searchable within minutes.
- Quick recovery and self-serve options to meet SLAs and operational-level agreements (OLAs).
- 100% of Jira Software data is secure 24/7 and recoverable in minutes.
- Recovery of configuration objects, saving time for Jira administrators.
- Automatic daily backups with a Jira native console for IT to manage backups and restore operations.

Security

- Complete confidence in data recovery in the event of accidental or malicious deletion or a bulk data change event.
- Isolated backups on the AWS platform, keeping backups fully separate from the Atlassian environment.
- Confidently recover data back in a granular manner from the off-site and secure Revyz cloud.
- Continuously capture data, including deleted Jira issues, and associated attachments, comments, and configuration objects like workflows and screens.
- Isolate a copy of historical data outside the Jira environment, providing additional protection.
- Restore data sets back to the manager or even outside the Microsoft 365 environment, providing greater control over your data.
- Conduct data investigations and forensic analysis with built-in search and analytics capabilities, enabling you to quickly identify any security incidents and take necessary action.

Summary

Traditional Jira backup capabilities are limited. And, in most cases, they're inadequate to meet the data protection, data recovery, data security, change management and compliance requirements of today's businesses. A comprehensive third-party Jira solution is the only way to ensure that your Jira data is properly protected, quickly recoverable, and compliant with various industry and legal requirements.

Implementing a data protection strategy for the Atlassian Jira cloud has become a necessity and equally complex. With limited native options from Atlassian, you will have to either build some custom scripts and manage data on your own to address your data protection needs or leverage 3rd party SaaS applications such as Revyz to offload data protection from your core IT team.

Revyz is the first Jira native data protection application in the Atlassian Marketplace.

Revyz Data Manager for Jira can store data securely and remotely, making it available for various recovery scenarios without having you roll back the entire site. It's simple, reliable and useful.

[Try Revyz for free](#)

Or contact us to learn more at:

info@revyz.io

References

Atlassian Security Practices

<https://www.atlassian.com/trust/security/security-practices#backups>

“We do not use these backups to revert customer-initiated destructive changes, such as fields overwritten using scripts, or deleted issues, projects, or sites. To avoid data loss, we recommend making regular backups.”

Cloud Security Shared Responsibilities

<https://www.atlassian.com/whitepapers/cloud-security-shared-responsibilities>

“Your role - Create backups of your data”