HYCU

# The Ultimate Guide to Protecting and Securing Jira Service Management

ATLASSIAN CLOUD

# Jira Service Management is the lifeblood of ITSM

The success of your operations and customer satisfaction hinges on the reliability of your ITSM (IT Service Management) tools like Jira Service Management.

Jira Service Management is where all critical business data—like incidents, service requests, and IT assets—lives. It keeps your IT services running smoothly, supports your team's communication, and helps deliver outstanding customer service. Keeping this data intact means your business can run without a hitch.

## 5 reasons you need to protect Jira Service Management

01

### Bad actors & malicious deletions

Underestimating the threat of targeted data deletions by malicious parties can be a grave mistake. Organizations of all sizes are at risk, making it critical to have defenses in place.

02

### Ransomware attacks

As ransomware attacks escalate globally, possessing a secured backup of your data is a last line of defense. It's an effective strategy to preclude potential crises and maintain operational integrity.

03

### Accidental Deletions

Data or configuration deletions—whether accidental or intentional—can occur unexpectedly. With Atlassian Cloud, the onus is on you to recover. Quick and flexible recovery processes protect your service efficiency and provide a safety net, offering invaluable peace of mind.

04

### Corruptions, Bugs, and Misconfigurations

Data corruption and software bugs can disrupt service management. A robust backup system ensures that you can swiftly revert to a clean state, minimizing downtime and maintaining continuity.

05

### Compliance, regulation, and mandates

For industries governed by strict standards or subject to regulations like NIS2 or DORA, adhering to backup and recovery protocols is not optional. It's a must to avoid severe penalties, ensuring data security and resilience.

# Backup and recovery is your responsibility, even in Atlassian Cloud

Congratulations. You've made the right choice to migrate to Atlassian Cloud. The cloud offers new capabilities and interoperability and saves you time and resources on patching and management. The cloud frees you from managing and updating Atlassian applications hosted on a server or data center. Atlassian takes care of system-level security, high availability, and disaster recovery. In the event of a global outage, it's Atlassian's responsibility to recover all systems and meet its uptime SLAs.

But what about your data? Atlassian Cloud follows a shared responsibility model, which means that while they handle system-level activities, you are responsible for your security, protection, and recovery. If you lose your data, for example, a critical project or asset information...it's your responsibility to recover.

**Here is what you are directly responsible for:**

- Creating backups of Jira Service Management. Atlassian explicitly states that you are responsible for creating backups of your data.
- Recovering lost data. If someone accidentally deletes an IT asset or a service request, you must recover it, not Atlassian.
- Storing backups under your control. If you have data retention requirements due to compliance or litigation holds, you must store the data offsite yourself. Atlassian will delete its system-level snapshots after a short, designated period.

See for yourself and access
Atlassian's Shared Responsibility Model by

**clicking here**

# To build or buy a backup? That is the question

The assets and configurations in Jira Service Management are critical, and backups and recovery must be simple, fast, and reliable to ensure your IT and customer experiences run smoothly.

## Challenges of relying on best-effort support for recovery

Submitting a support ticket and expecting Atlassian to help recover your data every single time is not a strategy.

- **Atlassian is not responsible for your data.** Atlassian is not legally responsible for recovering your data. Of course, they will try and help, but they have clearly stated in their shared responsibility model that you are responsible.

- **Lengthy recovery SLAs.** There are no contractual SLAs to restore your Jira Service Management data. If critical assets, configurations, or even projects are deleted, recovery times of your JSM instance are unpredictable.

- **Instance recovery only.** If Atlassian can help you, they will restore your instance into a sandbox. This means that every single time data is deleted in your organization you will have to submit a ticket, wait, and then parse through your entire JSM instance to find the deleted config, asset, or issue, and restore relevant data manually.

## Challenges of scripting your own backups

Building your own backup using the Atlassian API introduces similar challenges of data loss and lengthy recovery times. In the scenario that you script backups, you will encounter the following challenges:

- **Lengthy recovery times.** Recovering your data requires a manual process to parse, find, restore, and relink deleted items or pieces of information. This means even if the most critical of items is deleted, it will require time and patience your business may not have.
- **Incomplete.** Standard API method of capturing data using scripting does not export information about your assets.
- **Error prone.** Scripts require constant attention and are notorious for corruptions if not constantly reviewed. Trying to restore critical data from a script is not a reliable solution for mid-sized and large organizations.
- **Time-consuming.** Building and managing scripts across all of your Atlassian apps and enterprise SaaS requires expensive time and resources your organization does not have.

# HYCU: Automated backups and rapid restore of your critical IT Assets and Configurations

## HYCU R-Cloud Platform: Total Coverage of Atlassian Cloud

HYCU, an Atlassian Ventures company, offers the broadest support of Atlassian Cloud and SaaS applications in the R-Cloud Platform. HYCU brings a fully managed backup and restore service that offloads all backup activities and always puts your data in your control.

Jira Service Management
Jira Software
Confluence
Bitbucket
Jira Product Discovery
Jira Work Management
Trello

Over 60 integrations in the HYCU Marketplace

Uses Cases for

# Jira Service Management

### 1-click restore of JSM assets, configurations, and issues

Restore individual JSM assets, links, configurations, or specific items directly to production – no scripts, no parsing necessary. Simply identify the item and restore immediately.

### 1-Click Backup Automation

Automatically assign backup policies across all your Atlassian applications. These policies will run 24/7 and you'll spend five minutes a week on backups. No scripts, no babysitting.

### Ransomware-proof backups

Store your data in immutable, offsite storage under your control. This will give you a safe, recoverable copy in case a ransomware attack strikes.

### Meet data security, sovereignty and retention requirements.

All data is kept in your storage account, not HYCU's – giving you the flexibility to store backups and copies for a few days or several years – it's your choice.

### Extend protection across all of your apps

Avoid stacking backup tools. Protect Atlassian applications, Microsoft 365, Google Workspace, Okta, Entra ID and many more Enterprise IT services with one platform – HYCU R-Cloud.

# Rapid, granular restore.

## From projects and issues to assets and configurations

Did someone delete a project, configuration, or issue? No problem. Since your backup policies are always running, you only need to click on a restore point and select the restore you want. This same experience applies to all Atlassian applications protected by HYCU.

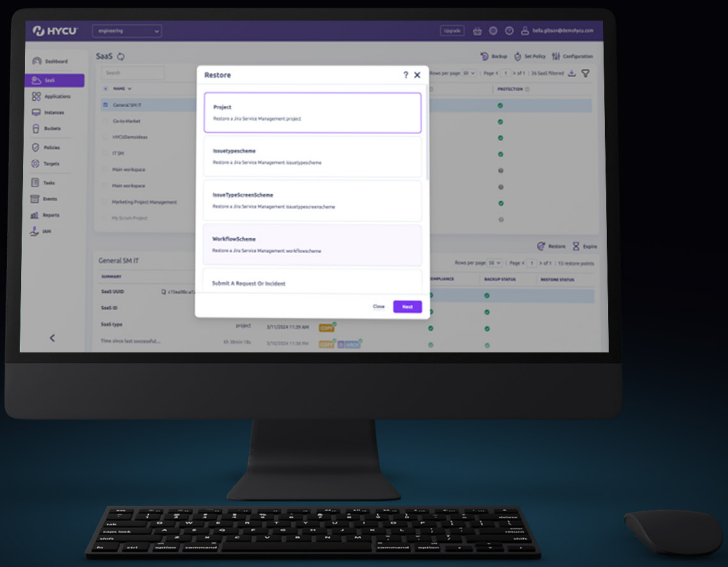
### Restore Jira Service Objects, Assets,and Configurations

- ✓ Project
- ✓ IssueTypeScheme
- ✓ IssueTypeScreen Scheme
- ✓ Workflow Scheme
- ✓ Submit a Request or Incident
- ✓ Custom Issue
- ✓ Task
- ✓ Ask a Question
- ✓ Attachment
- ✓ Sub-task
- ✓ Asset-workspace

And don't worry, your fields and links are preserved.

## Real Scenario

Oops! Someone has accidentally deleted a critical asset. Without HYCU, you would have to recover the entire instance and spend a significant amount of time to restore. With HCYU, simply search and select the asset  and click restore. That's it.



Restore

Project
Restore a Jira Service Management project

Issuetypescheme
Restore a Jira Service Management issuetypescheme

IssueTypeScreenScheme
Restore a Jira Service Management issuetypescreenscheme

WorkflowScheme
Restore a Jira Service Management workflowscheme

Submit A Request Or Incident

# Automated ‘set and forget’ policies.

## Spend less than 5 mins a week on backups

With one click, HYCU will automatically discover your Atlassian instances to assign a backup policy. You can choose the backup frequency (ex. daily), retention times (ex. 5 years), and the storage target of your data. Once a policy is assigned, it will run 24/7, and you’ll always have notifications and logging available anytime. You can even integrate HYCU notifications with your ITSM tool.

### Choose how often you want to backup.

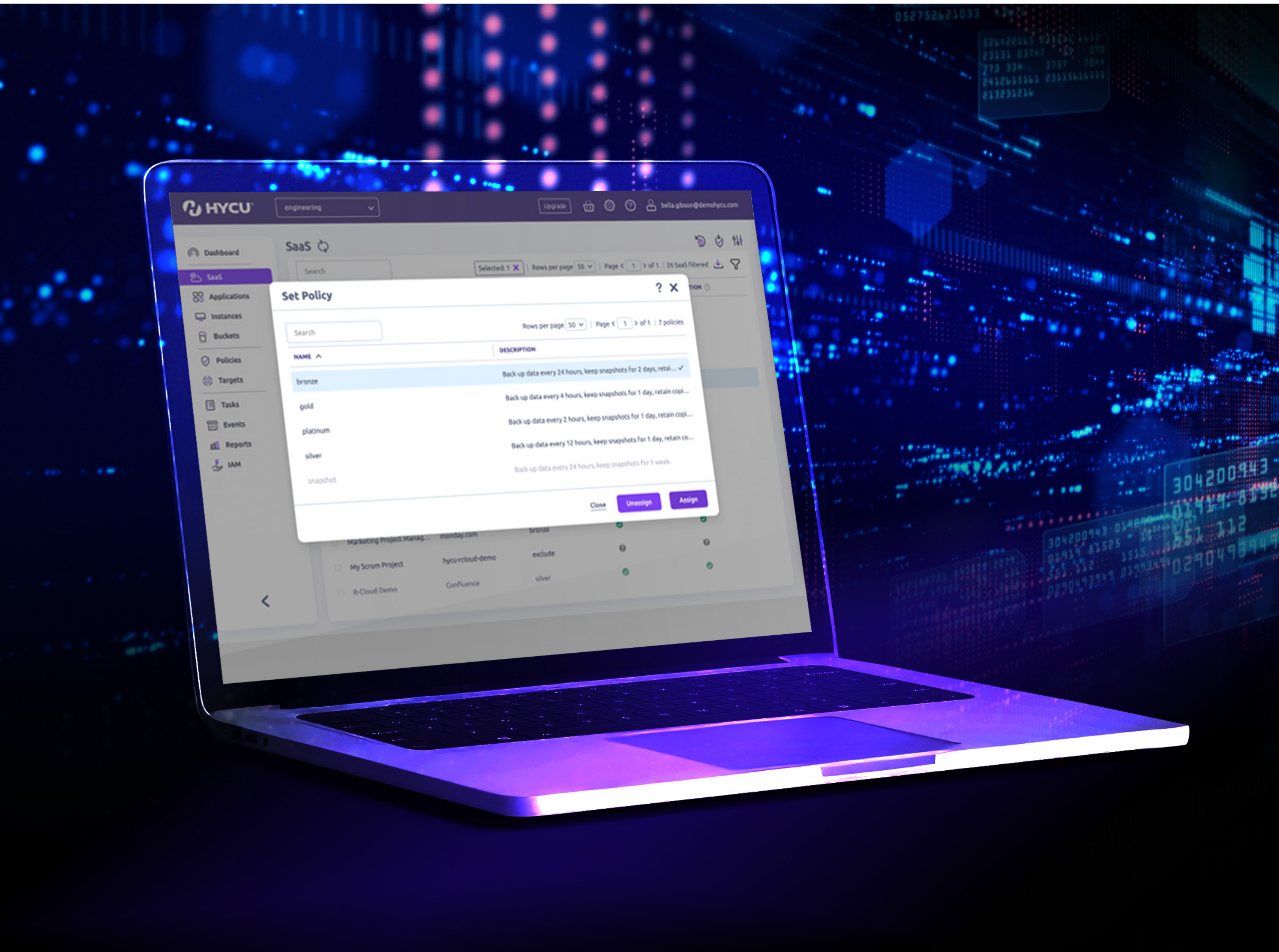
Some projects can be more critical than others. With HYCU, you can assign backup policies and customize the backup frequency by the hour.

### Choose your retention period.

Choose how long you want to store your backup copies – from days to years – the choice is yours.

### Set and Forget Policies

Once your backup policies are assigned, they will automatically work until you decide to cancel or change the backup policy. Removing the need for scripting, gives you peace of mind and guaranteed recovery assurance.



Set Policy

Search

Rows per page 50 | Page 1 of 1 | 7 policies

| NAME | DESCRIPTION |
|---|---|
| bronze | Back up data every 24 hours, keep snapshots for 2 days, retai... ✓ |
| gold | Back up data every 4 hours, keep snapshots for 1 day, retain copi... |
| platinum | Back up data every 2 hours, keep snapshots for 1 day, retain copi... |
| silver | Back up data every 12 hours, keep snapshots for 1 day, retain co... |
| snapshot | Back up data every 24 hours, keep snapshots for 1 week. |

| | | |
|---|---|---|
| Marketing Project Manag... | monday.com | bronze |
| My Scrum Project | hycu-rcloud-demo | exclude |
| R-Cloud Demo | Confluence | silver |

# Security First: Data in your control

## Automatically store backups in your company storage.

Storing backups in someone else's controlled account introduces risk and new vulnerabilities. Keeping backup copies in your storage buckets is safer and gives you an uncompromised copy of your data that you can always count on for recovery.

## Ransomware Recovery

You can recover your JSM data from a ransomware-proof immutable copy stored offsite. This air-gapped copy is safe from supply chain or direct ransomware attacks.

## Data Sovereignty and Governance

You can store your data in a storage bucket that meets your security and data residency requirements.

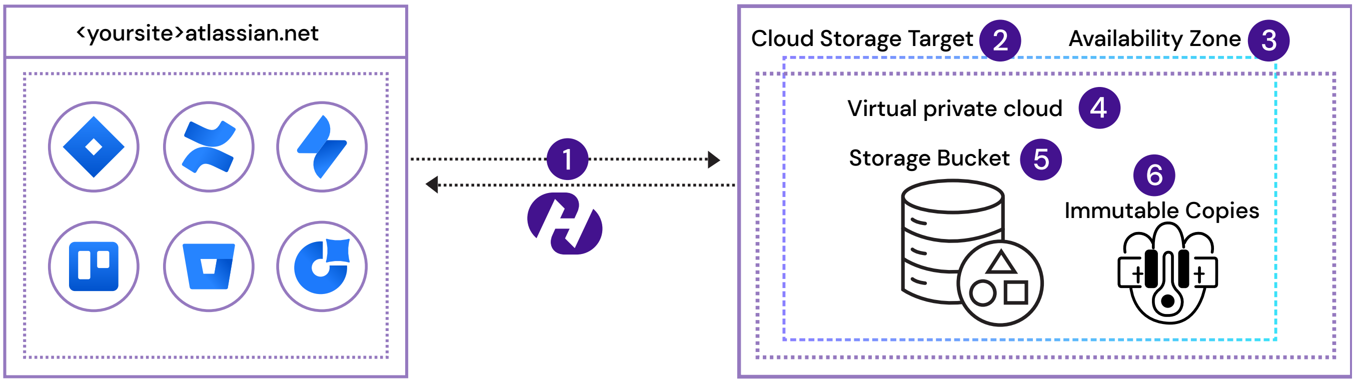
## Encryption at rest, in flight

HYCU encrypts all data and automatically stores backups in your storage of choice.

## Storage Agnostic

You can store your backups in Amazon S3, Google Cloud Storage, Azure Blob, or S3-Compatible Storage like Wasabi.

## HYCU Architecture: Keeping your data in your control



1. Data is encrypted at rest and in flight.
2. Data is stored in the customer's account. HYCU does not store customer backups.
3. Customer controls where the data resides.
4. Customer controls networking and access of storage account.
5. Data is stored on Amazon S3 or another S3-compatible storage.
6. Enable immutable backups in case of attack.

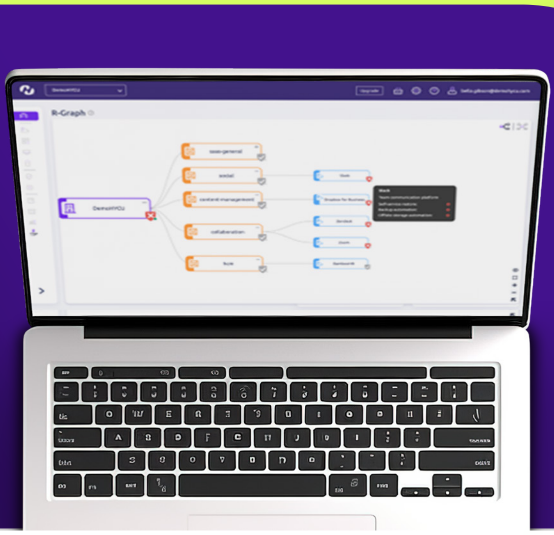
# Discover and protect your entire data estate

## Protect ITSM, Enterprise IT, and your IT infrastructure using one platform.

Gone are the days of managing and protecting all your applications from your data center. Today, all organizations have a data center presence, cloud-native applications, and hundreds of SaaS and cloud services that make up their new data estate. This introduces severe security and data availability challenges. The HYCU R-Cloud Platform™ is built to help you discover, protect, and recover your critical apps no matter where they are.

# Visualize your data estate in a few clicks.

Using Okta or Entra ID, HYCU visualizes your entire data estate and helps you identify unprotected SaaS applications across your entire organization – by department. Quickly discover, identify, and protect your critical apps with HYCU.



## HYCU Marketplace:

# Protect SaaS, Cloud, and On-Premises

The R-Cloud Platform™ is built to protect all your apps and scale with your needs. Each integration is purpose-built and gives you deep integration into your critical apps. Unlocking granular, item-level restore for all your SaaS apps that require data protection and rapid recovery.

Get started

HYCU

27-43 Wormwood Street Suite #650, Boston MA 02210, USA

| Phone: +1 617 681 9100 | E-mail: Info@hycu.com |