HYCU ATLASSIAN

Data Sheet

HYCU R-Cloud™ for the **Atlassian System of Work**

Platform-grade resilience for Jira, Confluence, Bitbucket, Trello, and the DevOps, SaaS, and identity services connected to them.



THE SHARED RESPONSIBILITY MODEL

Atlassian protects the platform. You protect the data.

Atlassian's RDS snapshots exist for platform-level disaster recovery. They will not roll back customer-initiated destructive changes like deleted projects, overwritten fields, bad scripts, rogue admins, or ransomware. Backing up your own data is your responsibility.

NATIVE TOOLING IS GAPPED

Atlassian's native Backup and Restore went GA in 2026 as a paid add-on for Premium and Enterprise. It covers the basics, enterprises hit its ceiling fast.

What atlassian native backup does		Structural gaps HYCU closes
Apps in scope Jira, JSM, JPD, and Confluence only	→	**Hard size caps.** 300 GB Jira / 32 GB Confluence / 7M attachments; you cannot purchase above these limits.
Schedule and storage Daily or weekly; Atlassian-owned storage only	→	**No Bitbucket, no Trello.** Git repos, Trello, Rovo, and Marketplace app data are outside scope entirely.
Retention 30 days maximum in Atlassian storage	→	**No granular restore.** Cannot restore a single project, space, issue, or page. All or nothing.
Encryption Atlassian-managed keys or BYOK via AWS KMS	→	**No automation coverage.** Jira and Confluence automations are not backed up or restored.
Sandboxes Restore into empty sandbox; sandbox backups supported	→	**No BYOC going forward.** AWS S3 BYOC closed to new customers. No Azure, GCP, Dell, Wasabi, or on-prem.
Automated restore Weekly restore drill (health check)	→	**No unified view.** Per-app and per-site. No cross-org or cross-workload visibility.

A THIRD-PARTY PLATFORM IS CRITICAL

Every enterprise faces these five vectors, and none are covered by single-app native tools.

Accidental deletion
Human error deletes the wrong project, epic, or page.

Malicious insider
Rogue admins or compromised accounts corrupt data at scale.

Supply-chain attack
Compromised Marketplace apps inject bad data or delete records.

Configuration drift
Bad automations or bulk edits corrupt production; no rollback

Compliance and audit
DORA, NIS2, GDPR, SOC 2 need immutable, customer-owned copies.

HYCU ATLASSIAN

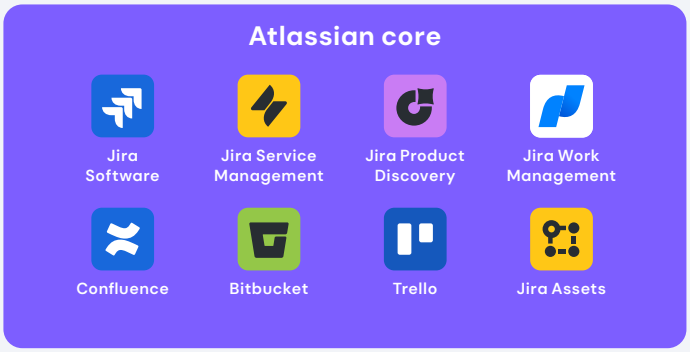
Data Sheet

HYCU R-Cloud for the Atlassian System of Work

Platform-Level Coverage	Jira, JSM, JPD, JWM, Confluence, Bitbucket, Trello, and Assets, protected as one system.
No Hard Ceilings	Protect instances of any size, with long-term retention measured in years, not days.
Granular Recovery	Restore a single issue, page, repo branch, automation, or custom field without touching the rest of the instance.
Compliance Ready	Data residency choice, audit-ready reporting, and recovery evidence for DORA, NIS2, GDPR, HIPAA, and SOC 2.
One Console, Whole Stack	Unified policy engine across Atlassian, DevOps, SaaS, and identity. One pane, one recovery experience.

R-CLOUD COVERAGE MAP

End-to-end resilience for the Atlassian System of Work, spanning **100+ workloads** through a single policy engine.



Devops & Delivery
GitHub • GitLab • Azure DevOps • CircleCI • Terraform • AWS Lambda • CloudFormation • GKE

Collaboration & Saas
Microsoft 365 • Google Workspace • Salesforce • Notion • Miro • Asana • ClickUp • Box

Identity & Access
Microsoft Entra ID • Okta • Auth0 • AWS IAM

Compute & Infra
AWS • Azure • Google Cloud • VMware • Nutanix

+ many more

Key Capabilities

Complete Atlassian protection

- Full coverage of Jira family, Confluence, Bitbucket, Trello, and JSM Assets with schemas, attachments, and history.
- Backup and restore Jira and Confluence automations, not just content.

Granular and cross-instance restore

- Restore a single issue, page, space, project, repo, board, or asset schema, in place or to a different instance.
- Sandbox and production seeding for safe validation before cutover.

Customer-owned, immutable storage

- Bring your own storage on AWS, Azure, Google Cloud, Wasabi, Dell, or S3-compatible targets.
- Immutable, object-locked copies isolated from production admin credentials.

Backup on autopilot

- Policy-driven protection with incremental and change-data-capture, no brittle exports or CSV scripts.
- Scheduled recovery drills and audit-ready recovery evidence.

One console, one recovery experience

- Unified policy engine across 100+ workloads spanning Atlassian, DevOps, SaaS, and identity.
- Role-based access, SSO, and tenant-level reporting across the full estate.

Compliance and governance

- Retention, residency, and chain-of-custody controls aligned to DORA, NIS2, GDPR, HIPAA, and SOC 2.
- Detailed audit logs, legal hold, and exportable, human-readable recovery artifacts.

Full-site recovery for Jira and Confluence

- Restore an entire Jira or Confluence site to a separate destination in a single operation. The destination site contains all spaces, configurations, and cross-space relationships intact.
- Purpose-built for cross-site disaster recovery and environment cloning.

Continuity through disruptions

- Turn your Confluence backups into a browsable copy that opens in any browser, no Atlassian login.
- Reach runbooks and troubleshooting guides anytime, independent of the live service.

Keep the Atlassian System of Work Resilient

Get Started

©2026 HYCU. All rights reserved.