

HYCU R-Cloud™ for Azure DevOps

Resilience for the whole delivery system: Repos, Boards, Pipelines, Test Plans, Artifacts, and the project and organization settings that hold them together



THE SHARED RESPONSIBILITY MODEL

Microsoft protects the platform. You protect the data.

Microsoft replicates your data within a region and to a second region, and keeps point-in-time database backups for 28 days. Those exist for business continuity and recovery from outage or disaster. Microsoft's own documentation states plainly that it does not support restoring assets that customers accidentally delete. Backing up your own data is your responsibility.

NATIVE RECOVERY IS BOUNDED

The recycle bins are real and useful, but they are bounded differently in each place, and all of them live inside the tenant that had the incident.

What native recovery does	Structural gaps HYCU closes
Deleted projects Soft-deleted and recoverable for 28 days, then permanently removed.	→ No point-in-time restore. There is no customer-facing point-in-time restore of a project or organization. Support cannot roll you back to last Tuesday.
Deleted Git repositories 30 days in the recycle bin.	→ Nothing for history rewrites. A force push destroys branch history without deleting the repository. There is nothing to click restore on.
Work item Recycle Bin Holds deleted items until someone restores or purges them.	→ No API coverage. Items destroyed permanently through the API or a script never reach the bin, and the bin is not a point-in-time copy of a board.
Test Plans and packages 14-day window for deleted test plans and suites; 30 days for Azure Artifacts packages.	→ Shortest windows on audit evidence. The data an assessor asks about later gets the least native protection.
Pipeline run retention 30-day default, configurable, with leases up to 730 days.	→ Everything shares one blast radius. Every native copy lives inside the same tenant, under the same credentials as the incident.
Storage Microsoft-managed replication in Microsoft-owned storage only.	→ No independent copy. No storage you own, no immutability you control, no long-term retention you set.

AN INDEPENDENT COPY IS CRITICAL

Every delivery organization faces these five failures, and none of them are covered by recycle bins or a developer's clone.



Bad automation

A script with broad permissions bulk-deletes work items.



History rewrite

A force push destroys branch history everyone assumed was safe because it is Git.



Cleanup cascade

An admin deletes a project and the deletion reaches further than expected.



Compromised token

A personal access token corrupts or removes everything it can reach.



The audit request

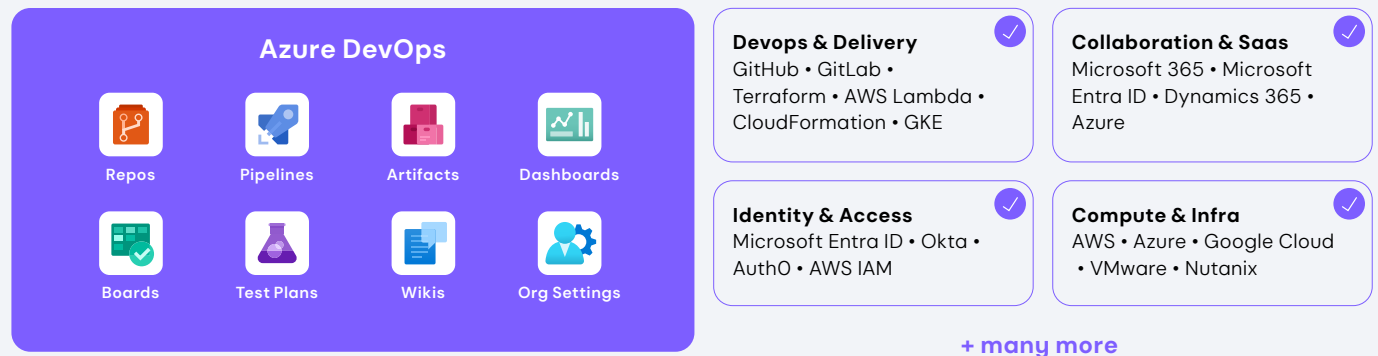
An assessor asks about a release from eighteen months ago.

HYCU R-Cloud for Azure DevOps

Full Delivery System Coverage	Resilience for the whole delivery system: Repos, Boards, Pipelines, Test Plans, Artifacts, and the project and organization settings that hold them together.
Granular Recovery	Restore a repository, work item, pipeline, wiki, or team in place, without disturbing anything still running.
Your Storage, Immutable	Backups land in storage you own, in your account and region, locked immutable if you choose. Nothing that compromises Azure DevOps can reach them.
Evidence That Survives	Retained work items and test plans produce the record an assessor asks for, on retention and residency you set.
One Console, Whole Estate	Azure DevOps joins Microsoft 365, Entra ID, Azure, and GitHub under one policy engine.
Your Backup, Your SLA	30-minute, hourly, daily, or any custom backup frequency. Retain for as long as you need, and restore in minutes.

R-CLOUD COVERAGE MAP

End-to-end resilience for the delivery system, spanning **100+ workloads** through a single policy engine.



Key Capabilities

Nothing is left to reconstruct from memory

- Repos, Boards, Pipelines, Test Plans, and Artifacts are protected as one system, along with the wikis, dashboards, process configuration, teams, and service hooks that make them usable.
- The objects that exist only in the service are the ones a clone cannot give you back. Those are the ones we hold.

One failure stays one failure

- Put back the repository with its branches and policies, the deleted work items with their fields, comments, and attachments, the wiki, the team, or the whole project, in place.
- Nobody stands down a delivery organization to retrieve one object, and the teams not affected never know it happened.

The copy outlives the incident

- Backups land in storage you own, in the account and region you choose, on Amazon S3, Azure Blob, Google Cloud Storage, Wasabi, Dell Data Domain, or any S3-compatible target.
- Locked immutable with object lock or WORM, so a compromised token or a mistaken admin action cannot reach the copy you need.

Protection runs without anyone watching it

- Incremental backups on the schedule you set, policy-driven, with no export scripts to maintain and no one to remember to run them.
- Retention measured in years you decide, not the days a recycle bin allows, so the window is never the reason something is gone.

The record is still there when someone asks for it

- Retained work items and test plans produce the release evidence an assessor asks about eighteen months later, including the test plans, suites, and results that are hardest to rebuild.
- Where the data sits and how long it is kept are your decisions, not a platform default you inherit.

One console for the whole Microsoft estate

- Azure DevOps runs under the same policies, the same console, and the same role-based controls as Microsoft 365, Entra ID, Azure, and GitHub.
- Because GitHub and Azure DevOps protection are both generally available, a migration in progress stops gating the protection decision.

Keep the Delivery System Recoverable

[Get Started](#)
