HYCU®

HYCU for Azure:
High-Resilience Recovery by Design

Solution Brief

Table of Contents

The Challenge with Protecting Azure Environments Today

Native features are not complete data protection

Azure snapshots, replication, and built-in retention improve durability, but they do not fully protect against deletion, corruption, or misconfiguration. A single misstep in IAM, keys, or policies can affect multiple subscriptions and regions at once, and it is difficult to prove that everything is truly recoverable.

Too many consoles, too little time

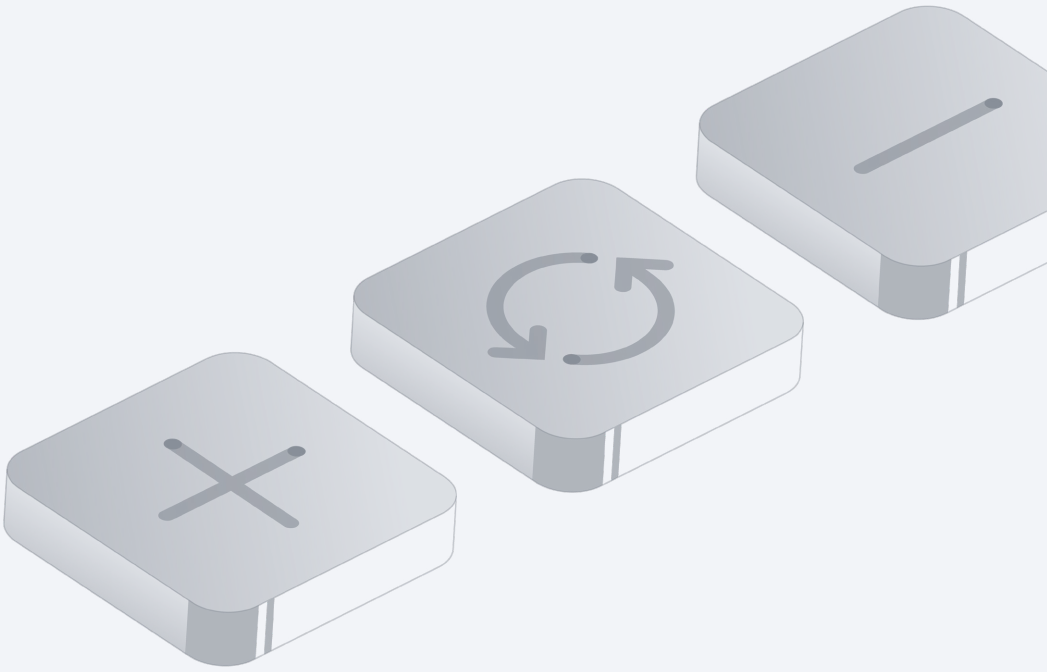
Azure infrastructure, SQL, Files, Blob, Entra ID, Microsoft 365, Dynamics 365, and more are often protected with separate tools and interfaces. When backup management is split across consoles and scripts, configuration gaps slip through, risks go unnoticed, and teams spend more time coordinating systems than protecting workloads.

Policy drift and account sprawl

Every Azure subscription, region, and workload type introduces its own backup policies, vaults, and schedules. Keeping them aligned without a central control plane is tedious and error-prone. Over time, policies drift, coverage becomes inconsistent, and it becomes harder to demonstrate compliance.

Proving recovery is hard before an incident

Many teams know backups are running, but they cannot easily confirm that restores will work across Azure workloads, subscriptions, and regions until something breaks. Recovery testing is often manual, inconsistent, and disruptive, leaving gaps in readiness and making it harder to meet RPO, RTO, and audit expectations.



Growing trends causing companies to rethink their backup strategies

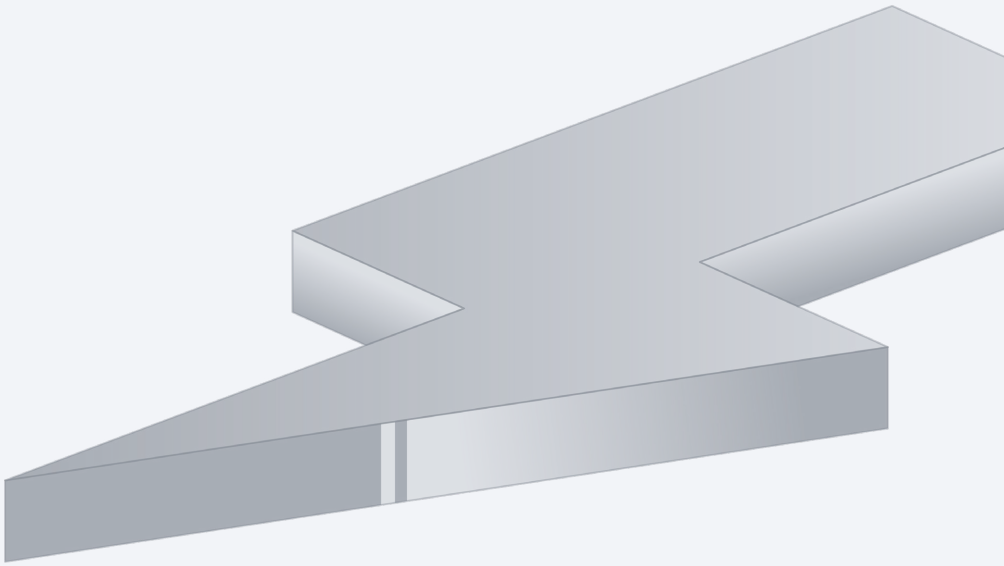
Cloud-conscious and identity-driven attacks
Threat actors now target cloud identities, control planes and backup configurations, not just individual servers. If an attacker can change policies, delete backups or rotate keys in Azure and connected services, a contained incident can quickly become a full-scale outage.

Vendor and service misconfigurations
Even trusted ISVs and cloud services can introduce errors. Accidental changes to Entra ID, backup policies, or SaaS configurations can leave critical data unprotected or difficult to rebuild, forcing organizations to reassess how quickly they could restore core services when something outside their direct control goes wrong.

Supply chain and shared-service compromises
Attackers increasingly focus on shared services and platforms instead of individual tenants. One exploit in a shared service or platform could expose multiple tenants at once, underscoring the need for independently governed, immutable backups residing in your own environment.

Tighter compliance and recovery expectation
Regulations and frameworks such as DORA and NIS-2 are raising the bar on backup, immutability and verified recoverability. Auditors now expect demonstrable offsite or logically isolated copies, clear retention policies and evidence that recovery has been tested and works.

SaaS and data sprawl beyond the Microsoft ecosystem
Azure is only one part of the attack surface. Critical data also lives in GitHub, Salesforce, Box, Atlassian Cloud and dozens of other SaaS platforms. Each has its own characteristics, and all are susceptible to data loss, attack or misconfiguration without a unified protection strategy.



HYCU for Azure Workloads and Microsoft Ecosystem

Five Outcomes Unlocked with HYCU

1. **Greater control over where backup data lives**
Store backups in Azure Blob Storage, another public cloud, or an S3-compatible target you control. This gives you greater flexibility over data location, governance, and storage strategy while helping you avoid vendor-managed backup lock-in.

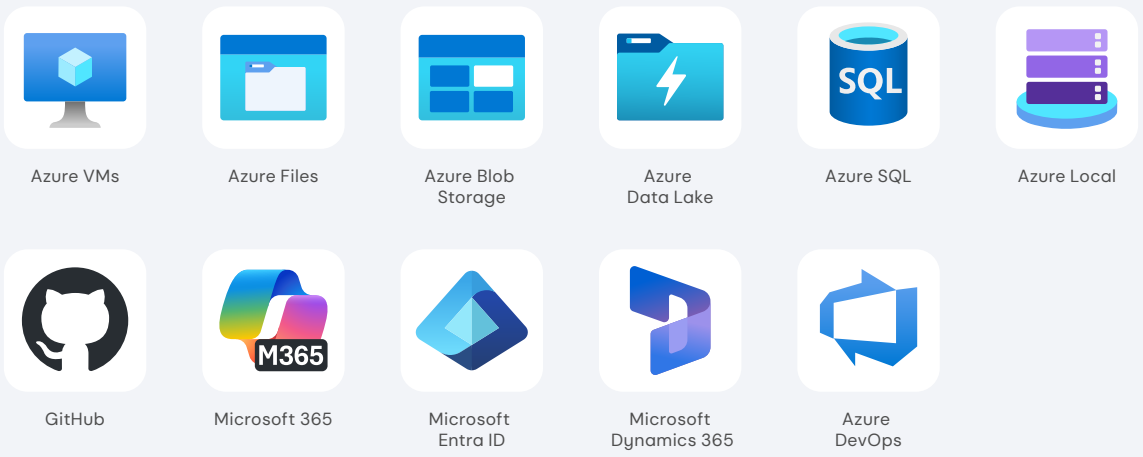
2. **Simplified operations across Azure and beyond**
One SaaS console discovers and protects Azure VMs, SQL, Files, Blob, Entra ID, Microsoft 365, Dynamics 365, and more. This reduces tool sprawl, minimizes scripts, and helps enforce consistent protection across subscriptions and regions.

3. **Cross-cloud resilience without lock-in**
Portable backup architecture and policy-driven orchestration support backup and recovery across regions and clouds, helping organizations improve resilience and maintain flexibility as environments evolve.

4. **Assured business continuity**
Automated recovery verification, orchestrated recovery workflows, and granular restore options help teams prove recoverability before an incident and restore critical Azure workloads with confidence.

5. **Stronger compliance and governance**
Centralized policies, flexible retention, and customer-controlled storage help organizations strengthen governance, support compliance, and simplify audit preparation across Azure and Microsoft workloads.

Protect your entire Azure and Microsoft Ecosystem with HYCU



HYCU for Azure: Key Capabilities

Agentless, SaaS-based protection

HYCU connects to Azure through native APIs and IAM to automatically discover workloads and apply policy-based protection across subscriptions and regions. No agents, plugins, or media servers are required.

Customer-controlled backup storage

Backup data can be stored in Azure Blob Storage, other public clouds, or S3-compatible targets you choose, giving you greater control over data location, retention, and governance.

Automated, verified recovery

Policy-driven recovery testing and orchestrated restore workflows help validate recoverability before an incident and support fast, confident restores when needed.

Unified coverage for Azure and Microsoft services

Protect Azure VMs, SQL, Blob, Files, Data Lake Storage, Azure DevOps, Azure Local, Microsoft Hyper-V, Entra ID, Microsoft 365, Dynamics 365 from the same console.

Policy-driven resilience at scale

Centralized policies, tags, and templates help reduce configuration drift, standardize protection, and improve compliance readiness across Azure subscriptions and regions.

HYCU for Azure: Key Capabilities

Protect Native Azure Cloud Services

Azure VMs & Managed Disks – Agentless, application-aware backups with fast VM and disk-level recovery and granular file restores.

Azure SQL – Database- and point-in-time recovery for Azure SQL Database and Managed Instance, orchestrated across subscriptions and regions.

Azure Files – Share-, directory-, and file-level recovery with ACL preservation and efficient snapshot orchestration.

Azure Blob & Data Lake Storage – Policy-based protection for object and analytics data with granular recovery and centralized management.

Protect SaaS Workloads

Microsoft 365, Dynamics 365 & Entra ID – Protect mailboxes, Teams, SharePoint, OneDrive, Dynamics 365 data, and directory objects from the same HYCU control plane used for Azure workloads.

DevOps & Collaboration SaaS – Protect Azure DevOps, GitHub, GitLab, Jira, Confluence, and dozens of other SaaS apps with a consistent policy model and centralized recovery workflows.

Unified SaaS Protection – Use HYCU as a single SaaS control plane to protect 95+ SaaS applications alongside Azure services.

Protect Hybrid-Cloud Workloads

On-premises and hybrid workloads – Extend consistent protection and recovery across Azure, on-premises, and multi-cloud environments from one console.

File & NAS workloads – Protect NetApp ONTAP, Dell PowerScale, and Nutanix Files with the same policies used for Azure Files and Blob.

Azure-based DR for on-prem workloads – Use Azure as a disaster recovery target for on-prem workloads, with HYCU orchestrating failover and failback through policy-driven backup and recovery workflows.

Protecting Native Azure Services

Supported Azure Workloads

- Azure Instances
- Azure Blob Storage
- Azure SQL
- Azure Files
- Azure Data Lake

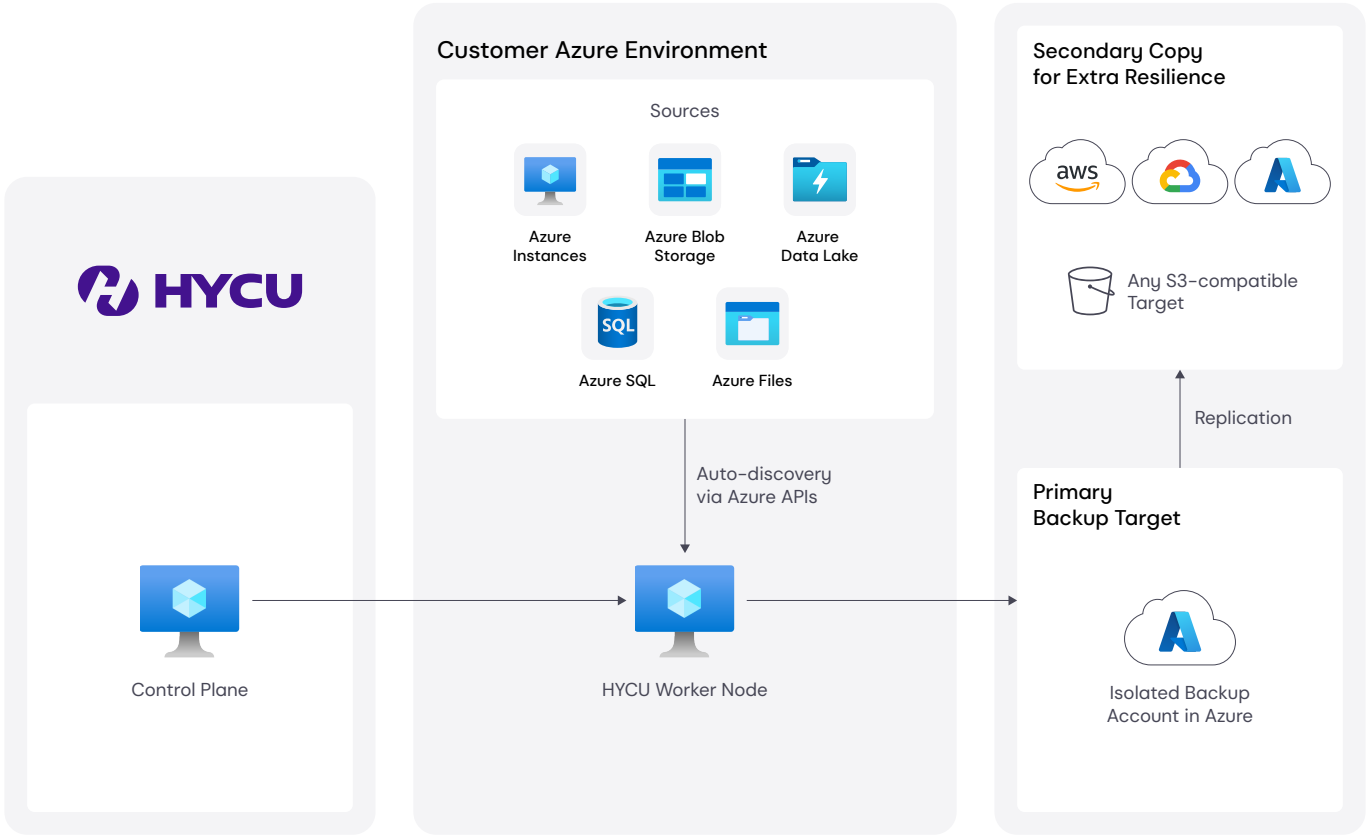
Supported Use Cases

- Backup and Recovery
- Granular Recovery
- Cross-Regional and Cross-Subscription Recovery
- Long-Term Retention
- Cross-Cloud Protection
- Cross-Cloud Mobility

How It Works

HYCU R-Cloud acts as a SaaS control plane. It connects to your Azure tenants through native APIs and Azure AD or Entra permissions, automatically discovering VMs, disks, SQL databases, Azure Files, Blob Storage, and Data Lake services. Policies are applied using tags, resource groups, and templates to help ensure consistent protection across subscriptions and regions.

When a backup runs, HYCU uses Azure-native protection workflows and stores backup data in Azure Blob Storage or other storage of your choice. For added resilience, backup data can also be replicated to another storage target, helping support recovery across regions or clouds.



Protecting SaaS Workloads

Supported SaaS workloads

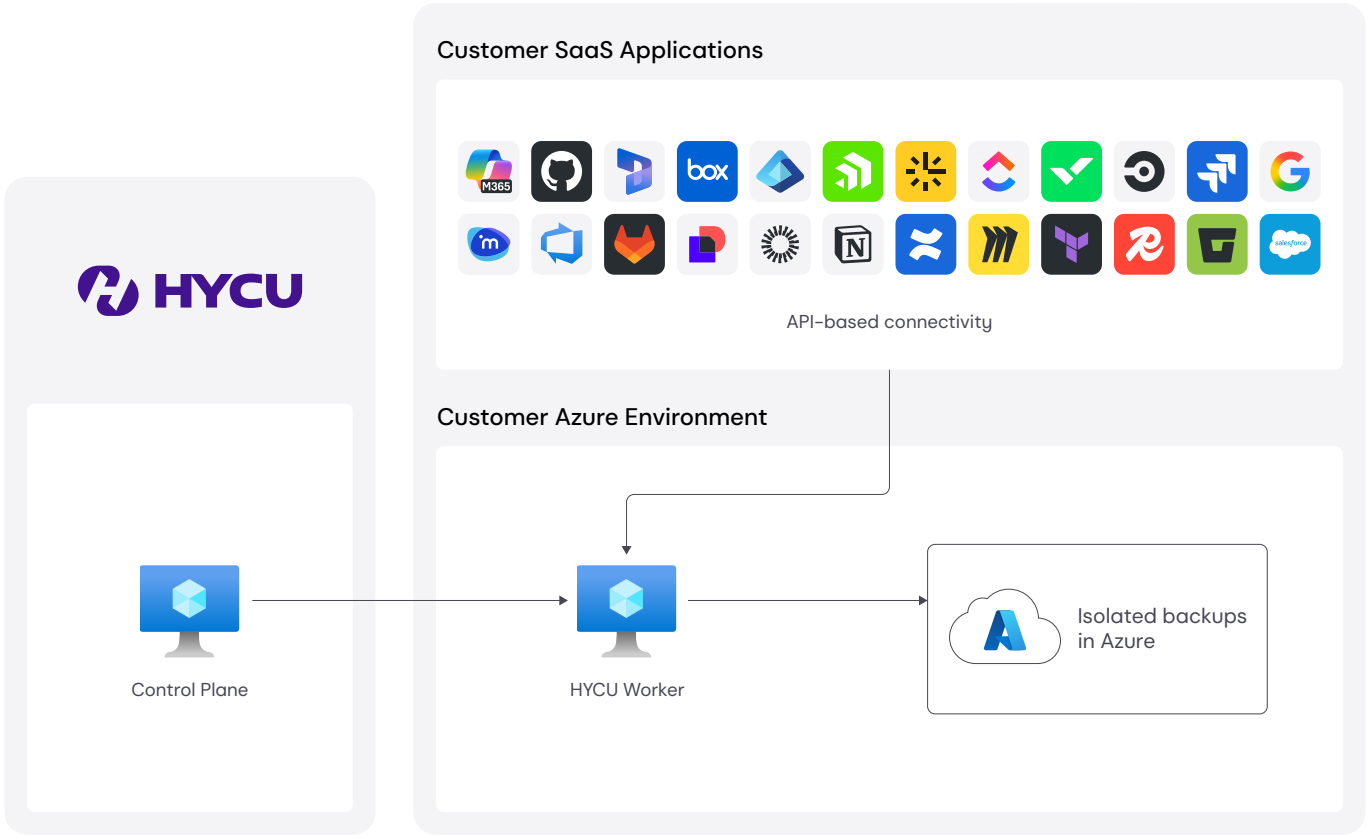
Microsoft 365
Entra ID
GitHub
Box
iManage
Salesforce
Jira
Dynamics 365
GitLab
Miro
Trello
Asana
Docusign
Azure DevOps
And many more!

SaaS & Object Use Cases

- Backup and Recovery
- Granular Recovery
- Cross-Instance Recovery
- Long-Term Retention
- Offline Recovery

How It Works

HYCU connects to SaaS platforms such as Microsoft 365, Dynamics 365, Entra ID, Azure DevOps, GitHub, Salesforce, Jira, and Confluence through native APIs. It discovers tenants, sites, repositories, and objects, then applies policy templates to automate backup frequency, retention, and protection settings. Backup data is stored in Azure Blob Storage or other storage of your choice, helping you maintain control and flexibility over where backup data resides.



Protecting Hybrid-Cloud Workloads

Supported Hybrid-Cloud Workloads

- Microsoft Hyper-V
- Nutanix
- VMware
- Nutanix Cloud Clusters on Azure (NC2)
- NetApp ONTAP
- Nutanix Files
- Azure Local
- Dell Power-Scale (Isilon)

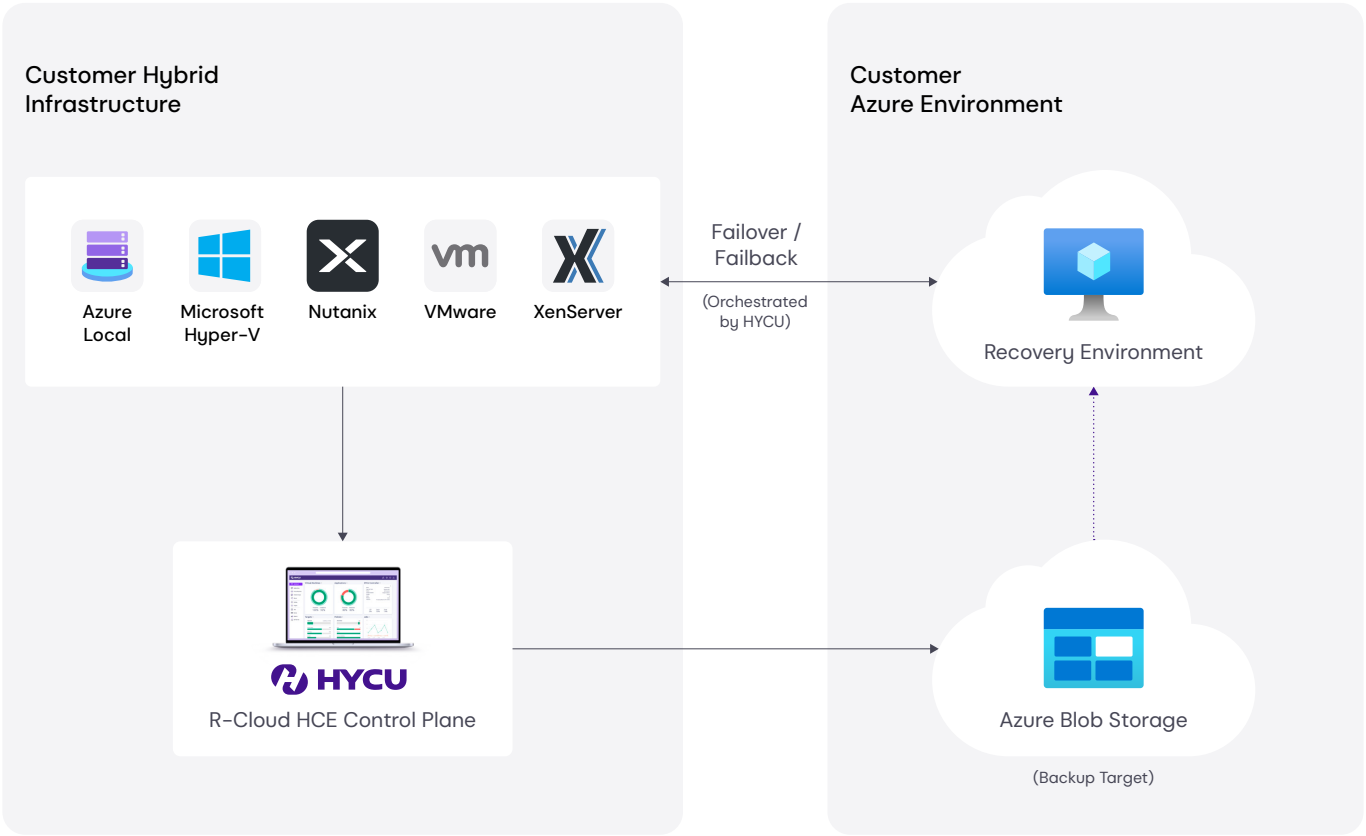
Supported Hybrid-Cloud Use Cases

- Backup and Recovery
- Disaster Recovery
- Long-Term Retention
- Lift and Shift
- Cross-hypervisor migration
- Ransomware Resilience

How It Works

HYCU uses an agentless approach to protect on-premises hypervisors such as Microsoft Hyper-V, Azure Local, VMware, and Nutanix, as well as NAS and file services including NetApp, Dell PowerScale, and Nutanix Files. From a single SaaS control plane, HYCU helps apply consistent protection and recovery policies across hybrid environments without adding operational complexity.

In a disaster recovery scenario, HYCU orchestrates failover and failback workflows to support recovery to Azure or back to on-premises infrastructure. This helps organizations simplify hybrid-cloud recovery and extend consistent protection across environments from one platform.



HYCU®

Protect Your Entire Microsoft Estate

Schedule a Demo

HYCU for Azure:
High-Resilience Recovery by Design