



# High-Resilience, Low-TCO Protection for Azure

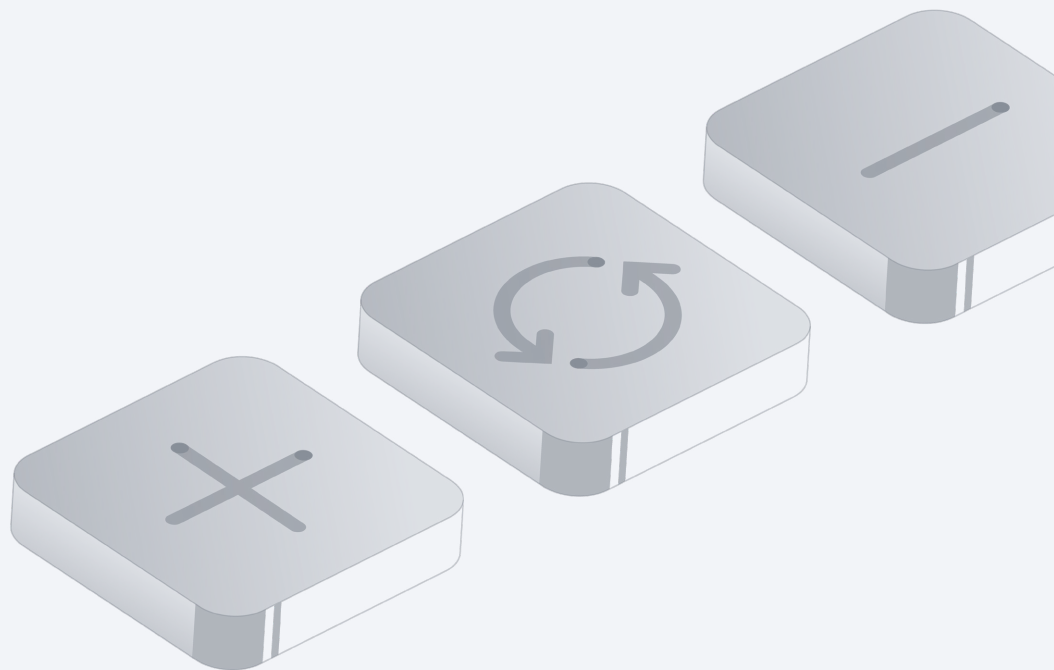


## Table of Contents

- 3 The challenge with protecting Azure Environments today**
- 4 Growing trends causing companies to rethink their backup strategies**
- 5 HYCU + Dell PowerProtect DDVE for Azure Workloads and Microsoft Ecosystem**  
Five Outcomes Unlocked with HYCU
- 6 HYCU + Dell PowerProtect DDVE Capabilities**  
Protect Azure Native Cloud Services  
Protect SaaS Workloads onto Customer-Owned DDVE  
Protect Hybrid-Cloud Workloads Using Azure
- 8 How it Works – Protecting Native Azure Services using Dell DDVE hosted on Azure**
- 9 How it Works – Protecting SaaS Workloads Using Dell DDVE Hosted on Azure**
- 10 How it Works – Hybrid-Cloud Data Protection & Mobility with Azure**

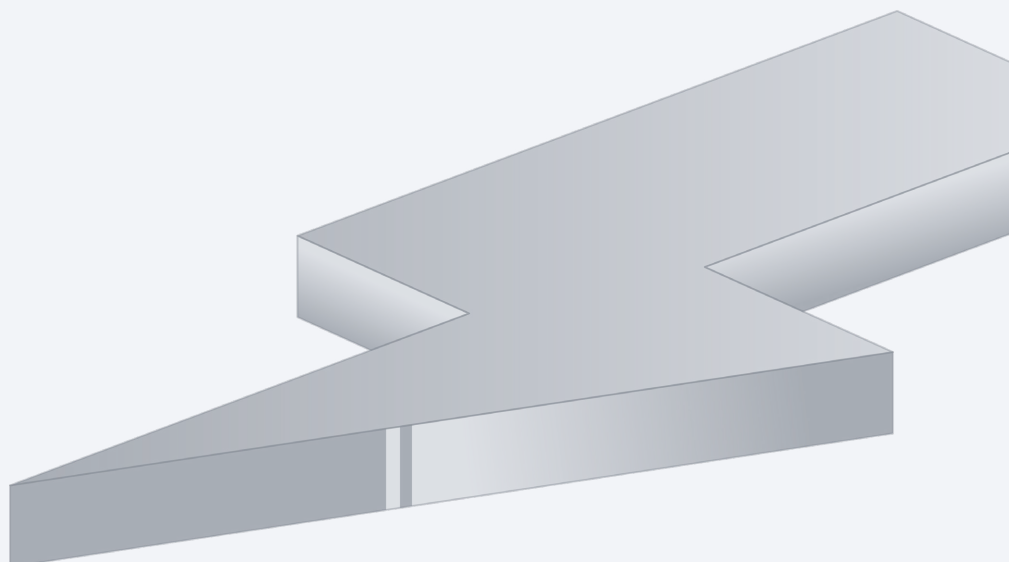
## The Challenge with Protecting Azure Environments Today

- **Native features aren't full data protection**  
Azure snapshots, replication and built-in retention keep data durable, but they don't fully protect you from deletion, corruption or misconfiguration. A single misstep in IAM, keys, or policies can impact multiple subscriptions and regions at once, and it's hard to prove that everything is actually 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 gets harder to demonstrate compliance.
- **Rising protection costs with little transparency**  
As data grows, so do backup copies, egress, rehydration and inter-region transfer charges. Without efficient global deduplication or clear cost controls, bills climb month over month and it becomes difficult to predict spend or explain it to finance.



## 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-side 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 hard 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 expectations**  
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 Sprawl and the Expanding Risk Surface**  
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.

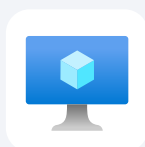


# HYCU + Dell PowerProtect DDVE for Azure Workloads and Microsoft Ecosystem

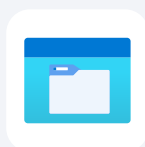
## Five Outcomes Unlocked with HYCU + Dell DDVE

- 1 Lower data protection TCO**  
Dell DDVE's industry-leading global deduplication (up to 40:1 depending on the workload) and compression reduce backup storage and egress costs, while HYCU's incremental-forever jobs and policy automation shorten backup windows and cut operational overhead.
- 2 Simplified operations across Azure and beyond**  
One SaaS console discovers and protects Azure VMs, SQL, Blob, Files, Azure Local, Microsoft 365, Dynamics 365, Entra ID, and 95+ SaaS apps, reducing tool sprawl, eliminating scripts, and enforcing consistent policies across subscriptions and regions.
- 3 Cross-cloud resilience without lock-in**  
Region-aware policies and portable backup formats enable cross-region and cross-cloud backup and recovery across Azure, AWS, and GCP. This gives you resilience against regional or vendor disruption without sacrificing cost efficiency or sovereignty.
- 4 Assured business continuity**  
Automated policy-driven recovery tests, immutable backups, and orchestrated DR ensure that critical Azure workloads can be recovered quickly across regions and clouds, with confidence, not guesswork.
- 5 Stronger compliance and governance**  
Customer-owned DDVE with Retention Lock, encryption, and audit trails delivers immutable, independently governed backups that support retention, residency, and audit requirements in regulated industries.

## Protect your entire Azure and Microsoft Ecosystem with HYCU



Azure VMs



Azure Files



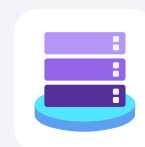
Azure Blob Storage



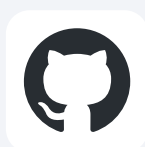
Azure Data Lake



Azure SQL



Azure Local



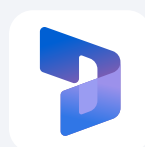
GitHub



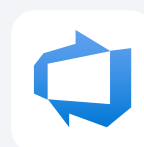
Microsoft 365



Microsoft Entra ID



Microsoft Dynamics 365



Azure DevOps

# HYCU + Dell PowerProtect DDVE Capabilities



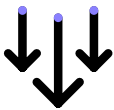
## Agentless, SaaS-based protection

HYCU connects to Azure via native APIs and IAM, auto-discovers workloads, and applies tag- and template-based policies. No agents, plugins, or media servers are required. Most environments are protected in minutes.



## Customer-owned, immutable DDVE storage

Backups are written to Dell DDVE deployed in your Azure subscription, or in other clouds—with optional Retention Lock for immutability and customer-managed keys for full control.



## Global deduplication and compression

Dell DDVE delivers up to 40:1 data reduction (workload-dependent), shrinking backup windows and dramatically lowering Azure storage and egress costs, especially at enterprise scale.



## Automated, verified recovery

Policy-driven DR tests and health checks validate that backups are recoverable. HYCU orchestrates point-in-time and granular restores across Azure services, without manual runbooks.



## 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.

# HYCU + Dell PowerProtect DDVE 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 efficient, deduplicated copies on DDVE and granular recovery.

## Protect SaaS Workloads onto Customer-Owned DDVE

**Microsoft 365, Dynamics 365 & Entra ID** – Protect mailboxes, Teams, SharePoint, OneDrive, Dynamics 365 data, and directory objects onto your DDVE, not a vendor-controlled tenant.

**DevOps & Collaboration SaaS** – Protect Azure DevOps, GitHub, GitLab, Jira, Confluence and dozens of other SaaS apps with one policy model, and store backups on DDVE in Azure or other clouds.

**Unified SaaS to Dell DDVE** – Use HYCU as a single SaaS control plane to back up 95+ SaaS apps into your own DDVE instance over secure, API-driven connections.

## Protect Hybrid-Cloud Workloads Using Dell DDVE on Azure

**On-prem hypervisors** – Agentless protection for VMware, Nutanix, Microsoft Hyper-V, and Azure Local, with backup copies stored on DDVE in Azure regions.

**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 DDVE in Azure as a DR target for on-prem workloads, with HYCU orchestrating low-cost failover to Azure and failback to on-prem using deduplicated backups stored on DDVE.

# Protecting Native Azure Services

## Supported Azure Workloads



Azure  
Instances



Azure  
Blob Storage



Azure  
SQL



Azure  
Files



Azure  
Data Lake

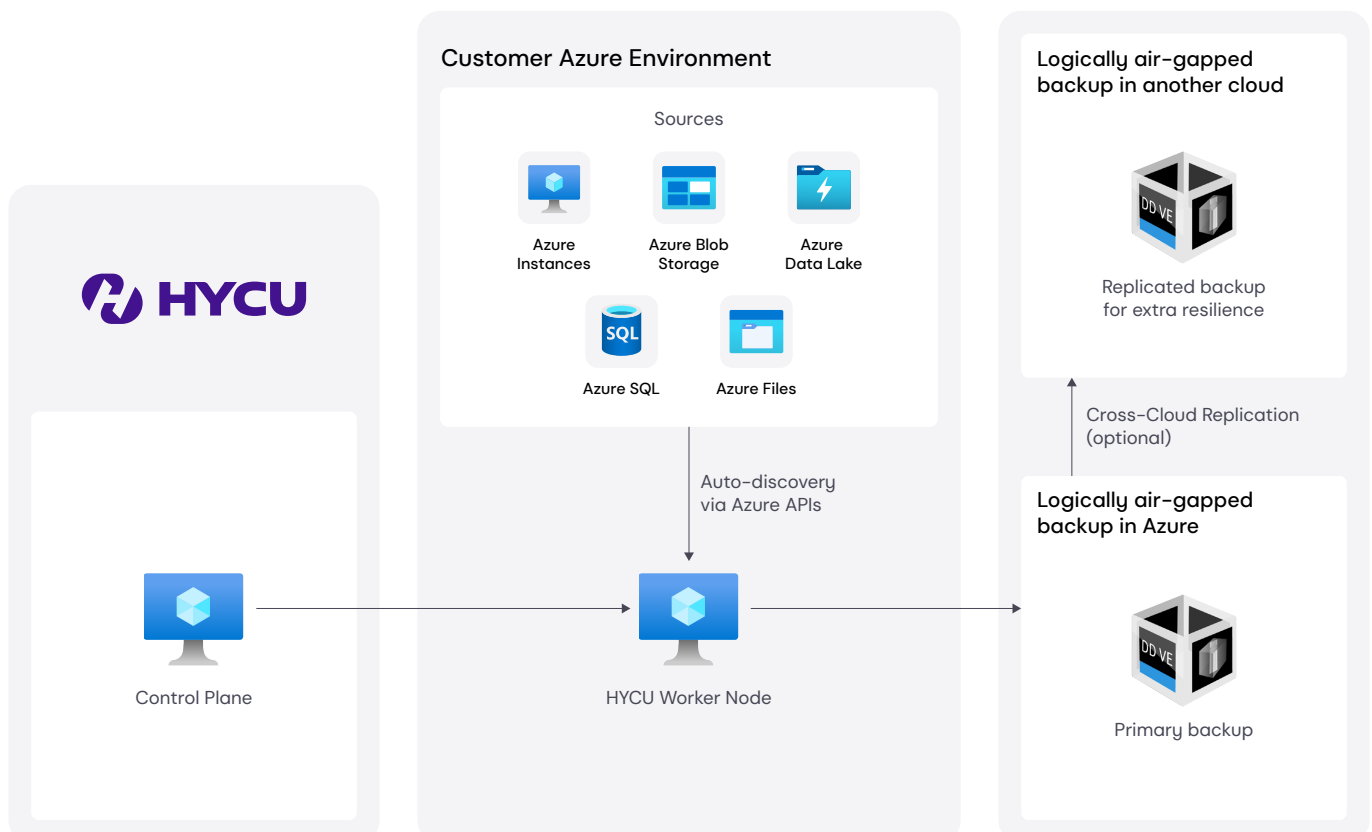
## Supported Use Cases

- ✓ 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 via native APIs and Azure AD/Entra permissions, automatically discovering VMs, disks, SQL databases, Files, Blob storage and other services. Policies are applied using tags, resource groups and templates to ensure consistent protection across subscriptions and regions.

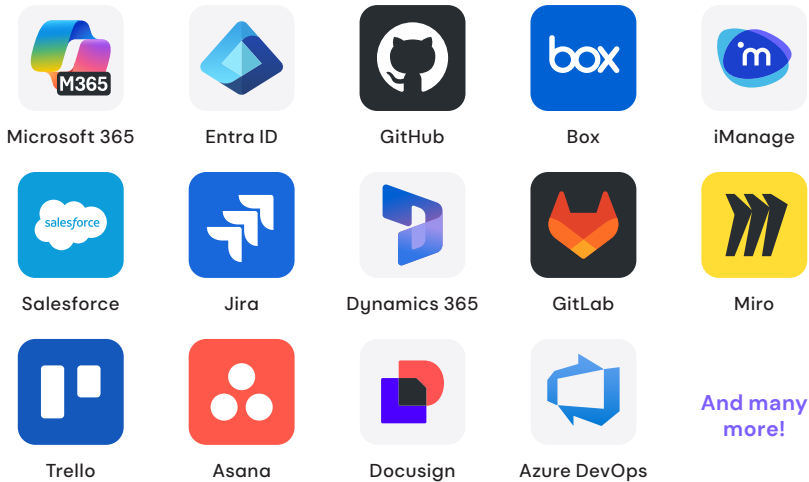
When a backup runs, HYCU orchestrates Azure-native snapshots and streams deduplicated data to your Dell DDVE instance in your Azure subscription or in other cloud environments such as AWS or Google Cloud. DDVE applies global deduplication and compression, immutability (Retention Lock) and encryption, and can replicate to another region or cloud as needed.





# Protecting SaaS Workloads

## Supported SaaS workloads



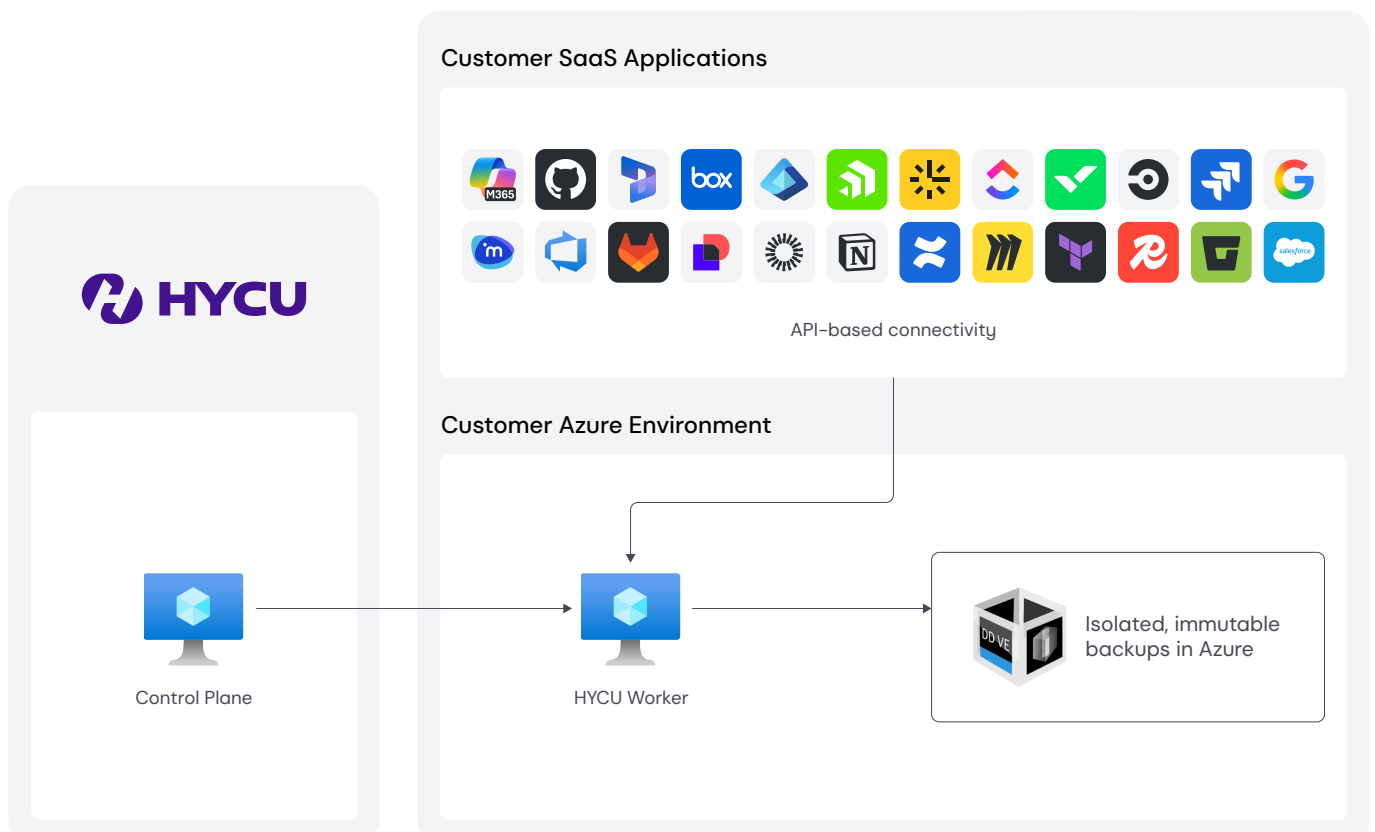
## SaaS & Object Use Cases

- ✓ 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, Azure DevOps, Entra ID, GitHub, Salesforce, Jira, Confluence, and others via APIs. It discovers tenants, sites, repositories, and objects, then applies policy templates that control backup frequency, retention, and residency.

Backups are streamed through HYCU workers to customer-owned DDVE in Azure (or other clouds). Data is deduplicated globally, encrypted, and stored immutably according to your retention policies.



# 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)

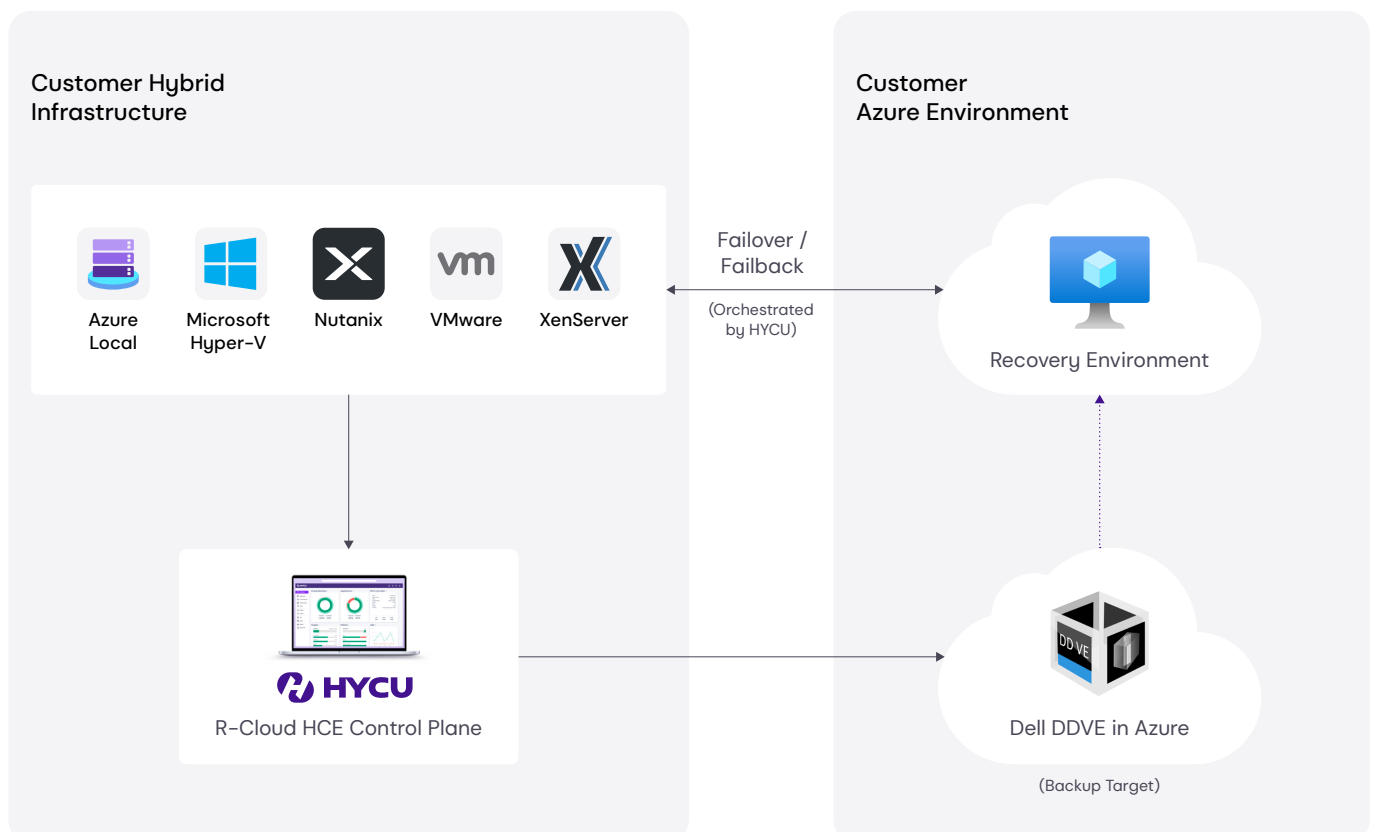
## Supported Hybrid-Cloud Use Cases

- ✓ 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 (VMware, Nutanix, Microsoft Hyper-V, Azure Local) and NAS or file services (NetApp, Dell PowerScale, Nutanix Files). Backups are sent incrementally forever to Dell PowerProtect DDVE in your Azure account, with optional replication to another cloud, region, or Dell PowerProtect Data Domain target for added resiliency and retention flexibility.

In a DR scenario, HYCU orchestrates automated failover to Azure and failback to on-premises infrastructure by using deduplicated backups for fast, bandwidth-efficient recovery.





# Protect Your Entire Microsoft Estate



[Schedule a Demo](#)

**High-Resilience, Low-TCO Protection**  
for Azure