# Data Protection for Azure and the Microsoft Estate

SOLUTION BRIEF

# Table of Contents

3 The Challenge with Protecting Azure Environments Today

4 Complete Data Protection for Microsoft Azure and your Microsoft Ecosystem

Five Outcomes Unlocked with HYCU

5 HYCU R-Cloud Capabilities

Protect Azure Native Cloud Services

Protect SaaS Applications onto Azure Blob Storage

Protect Hybrid-Cloud Workloads Using Azure

6 Protecting Native Azure Services (IaaS and DBaaS) using DDVE hosted on Azure

7 How it Works – Storing SaaS Backups with DDVE Hosted on Azure

8 How it Works – Hybrid-Cloud Data Protection and Mobility with Azure

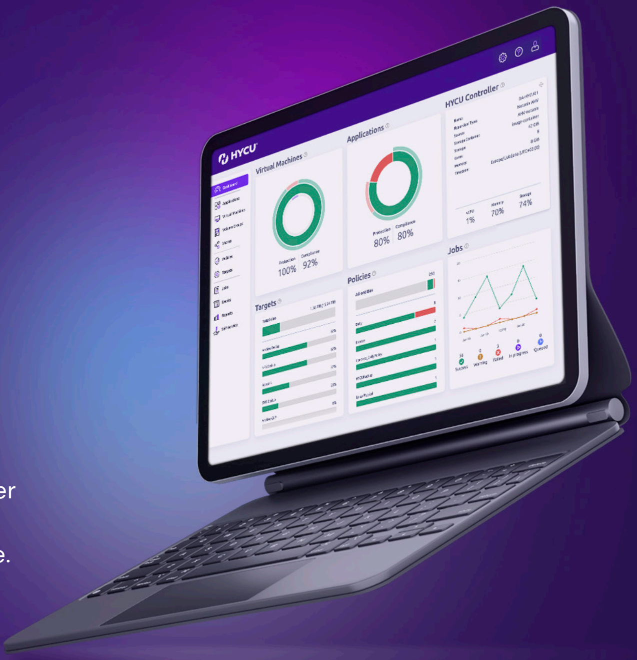
## The Challenge with Protecting Azure Environments Today

- **You Don't Really Own Your Data.** Most third-party backup tools store your data in their own proprietary format, under their control. That means less visibility, exfiltration exposure with no control, more hoops to jump through during audits, and little leverage when it's time to renegotiate your contract. If you ever want to leave, you find yourself always boxed in.
- **Too Many Consoles, Too Little Time.** Azure infrastructure, Microsoft 365, Entra ID, SQL. The list keeps growing. When backup management is split across multiple interfaces, errors slip through, risks go unnoticed, and teams spend more time coordinating systems than protecting them.
- **Policy Drift and Account Sprawl.** Every Azure subscription brings its own backup policies, vaults, and configurations. Keeping them consistent is tedious and time-consuming without a centralized dashboard. It pulls your team away from higher-value work and increases risk of non-compliance.
- **Rising storage costs with no warning.** Without efficient deduplication or smart storage management, backup costs can spike fast. Bills grow month over month with little transparency. Budgeting becomes harder, and explaining the numbers to finance gets even harder.

## Growing trends causing companies to rethink their backup strategies

- **Vendor-side misconfigurations.** As more workloads run in Azure, threat actors are shifting their focus. Compromising cloud-based services is faster, quieter, and harder to detect.
- **Cloud-conscious attacks.** Even trusted ISVs can make mistakes. In some cases, customers have lost access to critical data after accidental deletions or configuration errors. If someone changed your Entra ID setup today, how quickly could you rebuild it?
- **Supply chain compromises.** Attackers are targeting vendors instead of individual customers. One exploit in a shared service or platform could expose multiple tenants at once.
- **Tighter compliance on backups.** Directives like DORA, NIS-2 have elevated backup and recovery requirements for ICTs, mandating offsite backups and continuous testing.
- **SaaS sprawl beyond Microsoft 365.** Azure isn't the only surface to protect. From GitHub and Salesforce to Box and Atlassian Cloud, your data lives in dozens of places—and each is vulnerable to loss, attack, or misconfiguration.

# HYCU R-Cloud™
# Complete Data Protection for Microsoft Azure and your Microsoft Ecosystem



### What is HYCU R-Cloud™?

An enterprise platform that helps you protect, recover, and move data—across cloud, SaaS, and hybrid environments. From backup and disaster recovery to ransomware recovery and cyber resilience, it's everything you need in one place. No complexity. No lock-in. Just visibility and control over your entire data estate.

## Five Outcomes Unlocked with HYCU

1 **One View with 100% Control**
No more jumping between consoles or chasing policies and vaults across Azure accounts. HYCU gives you a single place to manage backups across all your Azure subscriptions and services. Set policies once, eliminate drift, and stay compliant with less effort.

2 **One Platform for Every Microsoft Workload**
HYCU protects the full Microsoft stack: Azure infrastructure, Microsoft 365, Entra ID, hypervisors, and Git repositories. No more stitching together tools for every account, vault, or workload. One interface. One experience. Total coverage.

3 **Cross-Cloud Protection and Mobility**
Not only can you protect Azure alongside AWS and Google Cloud, but you can also keep cross-cloud backups for supply chain resilience and move these workloads without limitations. HYCU gives you complete mobility.

4 **Keep Control of Your Backups Without Compromise**
With HYCU, you stay in control. Backups live in your Azure Blob storage or in any public cloud you choose. You get the simplicity of a managed service without giving up governance, residency, or access.

5 **Lower backup costs across the board**
Reduce storage costs with built-in deduplication. Cut waste with automated policy enforcement across all accounts. And shrink backup administration from days to minutes. HYCU keeps your environment protected and efficient.

## Protect your entire Microsoft Estate with HYCU R-Cloud™

- ✓ Azure Instances
- ✓ Azure Blob Storage
- ✓ Azure SQL
- ✓ Azure Local
- ✓ Azure Government
- ✓ Microsoft Hyper-V
- ✓ Microsoft Entra ID
- ✓ SharePoint Online
- ✓ Exchange Online
- ✓ OneDrive for Business
- ✓ Teams
- ✓ GitHub

# HYCU R-Cloud™ Capabilities

**Fully Managed Protection.** HYCU auto-discovers Azure workloads and applies policies through tags without the need for scripts or manual setup. Most environments are operational within minutes.

**Customer-Owned Storage.** Store backups in your own Azure Blob storage—across any tier—or choose other public clouds and S3-compatible targets. You keep full control of your backup data.

**Immutable Backups.** Ensure backups cannot be altered or deleted—even by internal users—helping protect against ransomware and accidental changes.

## Protect Azure Native Cloud Services

- **Granular Recovery.** Recover specific files, folders, or user data across Azure infrastructure, Microsoft 365, and Entra ID. No need to roll back an entire system to get back what you need.
- **Cross-Regional Recovery.** Quickly restore workloads in a different Azure region to maintain operations during an outage or regional disruption.
- **Cross-Cloud Backups.** Keep an offsite copy of your Azure backups in AWS, Google Cloud, or other public cloud environments. This adds another layer of resilience against supply chain risk and meets evolving compliance needs.
- **Support for Dev-Test Workflows.** Use instant-clone and live-mount features to accelerate development and testing. No need to wait for full restores or create duplicate environments from scratch.
- **Application Aware Backups.** Deliver agentless, application-consistent backups for self-managed Microsoft SQL Server on Azure VMs. Enable seamless discovery of SQL instances, transactionally consistent snapshots, and granular point-in-time recovery.
- **Protect Data Lakes and Azure Blob Storage.** Whether you're managing analytics pipelines, app-generated logs, or unstructured datasets, HYCU protects Blob containers with storage-efficient snapshots and granular recovery—all without scripting or extra infrastructure.

## Protect SaaS Applications onto Azure Blob Storage

- **Unified SaaS Backup to Azure Blob.** Protect Microsoft 365 and over 80 applications directly into your Azure Blob Storage. Meet backup, offsite retention, and resilience testing requirements using one platform and one storage target.

## Protect Hybrid-Cloud Workloads Using Azure

- **Low-Cost Long-Term Retention.** Protect on-prem environments like Azure Local, Hyper-V, VMware, and Nutanix with agentless, incremental-forever backups stored in Azure regions. No egress charges for restores.
- **Built-In Disaster Recovery.** Use Azure as a disaster recovery target without adding infrastructure or complexity. Recovery workflows are pre-integrated and cost-efficient.
- **Seamless Lift-and-Shift.** Move workloads from on-prem or other cloud platforms to Azure without re-architecting. HYCU ensures application-consistent transfers, so services stay intact and ready.

HOW IT WORKS

# Protecting Native Azure Services (IaaS and DBaaS) using DDVE hosted on Azure

## Supported Azure Workloads

Azure Instances

Azure Blob Storage

Azure SQL

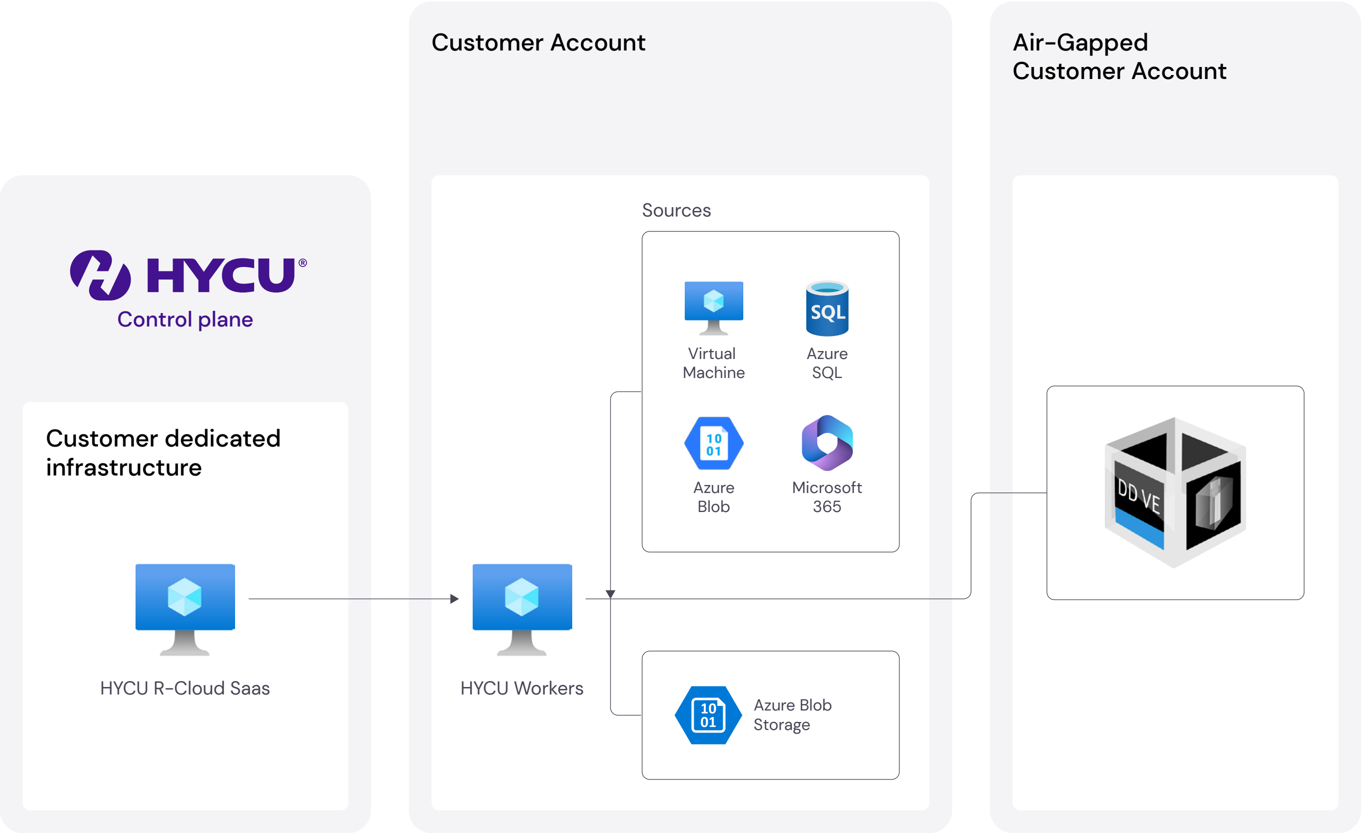
## Use Cases

- ✓ Backup and Recovery
- ✓ Granular Recovery
- ✓ Cross-Regional and Cross-Account Recovery
- ✓ Long-Term Retention
- ✓ Cross-Cloud Backups
- ✓ Cross-Cloud Mobility

## HYCU R-Cloud™: How It Works

HYCU R-Cloud, leverages native Azure APIs and snapshots and dynamically scales up and down based on needs. Customers connect HYCU to their Azure environments and store backups solely in their Azure Blob (or other S3-compatible storage) to meet data governance and residency. HYCU is available in the marketplace and integrated into Azure Billing. Additionally, HYCU is integrated into Azure access management policies.

Below is an architectural diagram of HYCU R-Cloud™ protecting native services running on Azure.



HOW IT WORKS

# Protecting SaaS using DDVE hosted on Azure

HYCU stores SaaS Backups onto customer-owned Azure Blob Storage across any tier of their choice. All SaaS applications are connected to HYCU via API.

## Supported SaaS Workloads

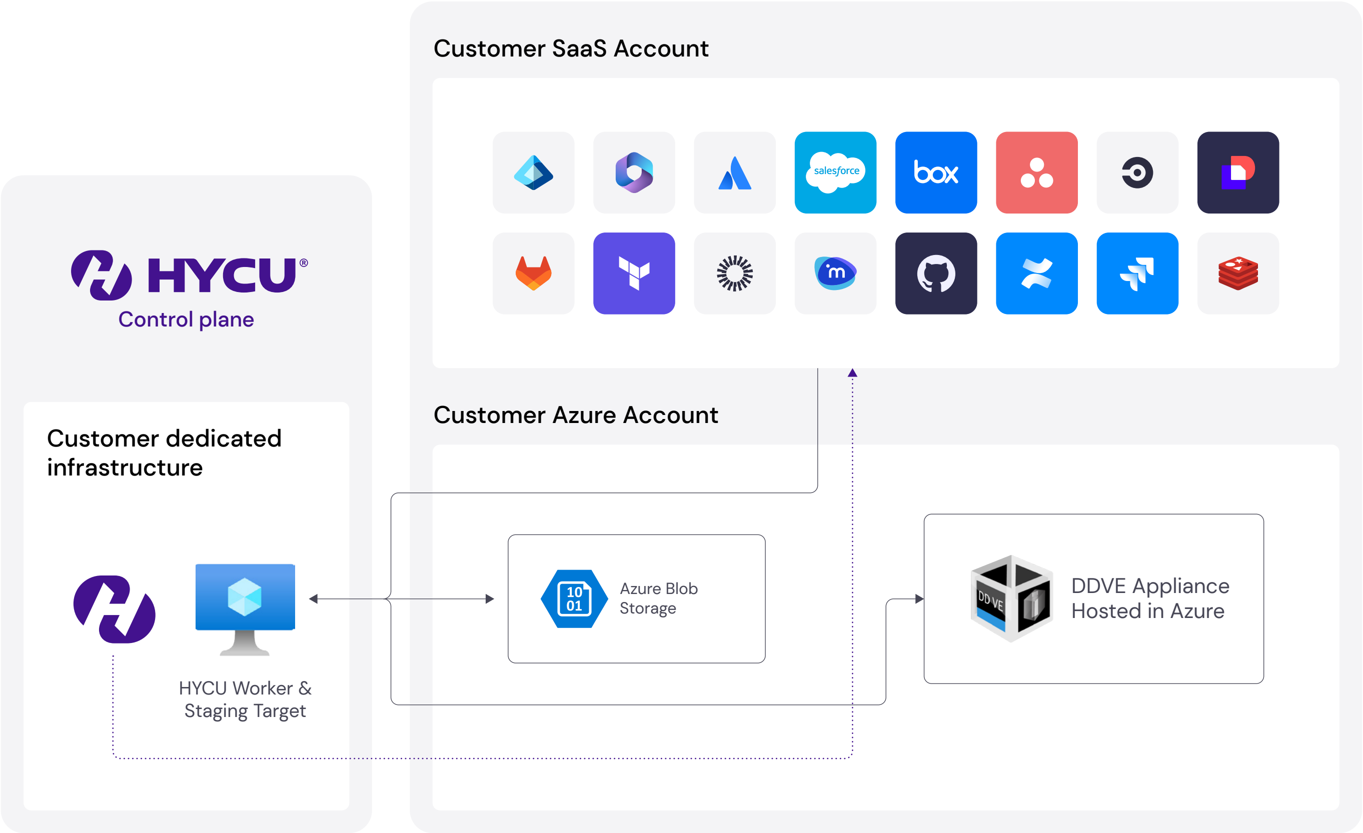
- Microsoft 365
- Microsoft Entra ID
- GitHub
- Box
- iManage
- Salesforce
- Jira
- Confluence
- Gitlab
- Miro
- Trello
- Asana
- Docusign
- Notion
- And many more!

## SaaS Use Cases

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

## How it Works – Storing SaaS Backups with DDVE Hosted on Azure

HYCU stores SaaS Backups onto customer-owned Azure Blob Storage across any tier of their choice. All SaaS applications are connected to HYCU via API and available for immediate connection in the HYCU Marketplace.



HOW IT WORKS

# Cost-Effective Backup and Disaster Recovery for Hybrid-Cloud Workloads

## Supported Hybrid Cloud Workloads

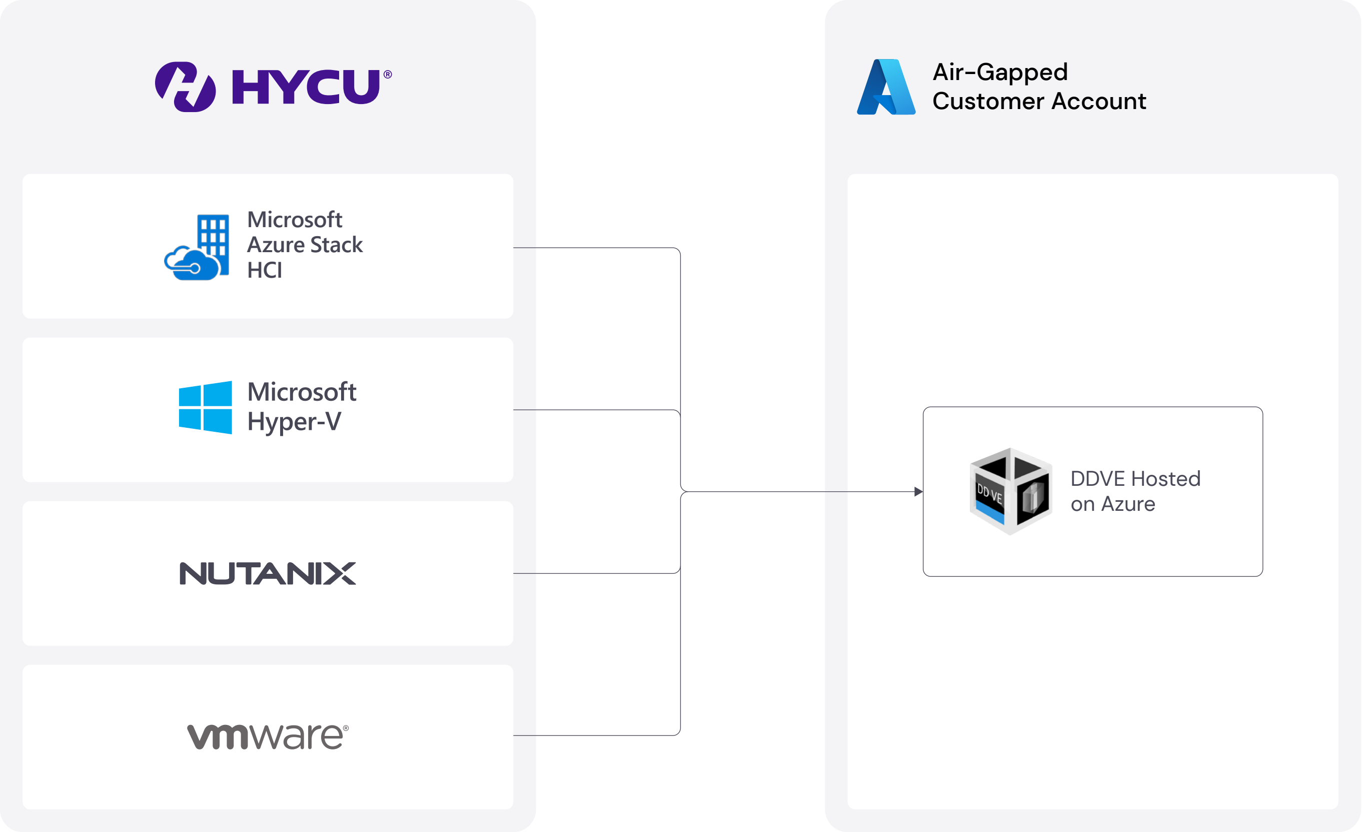
- Microsoft Hyper-V
- VMware
- NetApp ONTAP
- Azure Local
- Nutanix
- Nutanix Cloud Clusters on Azure (NC2)
- Nutanix Files
- Dell PowerScale (Isilon)

## Supported Use Cases with Azure

- ✓ Backup and Recovery
- ✓ Disaster Recovery
- ✓ Long-Term Retention
- ✓ Lift and Shift
- ✓ Cross-Hypervisor migration
- ✓ Malware Detection
- ✓ Anomaly Detection

## How it Works – Hybrid-Cloud Data Protection and Mobility with Azure

Customers protect hybrid workloads (virtual and file share) using a native, agentless approach. Backups can be stored incrementally forever in regional Azure Blob Storage for no egress. For disaster recovery, customers can spin workloads up and down to Azure for built-in, low-cost failovers.



# Protect Your Entire Microsoft Estate with HYCU and Dell

Schedule a Demo