HYCU R-Cloud™

Data protection across your entire AWS infrastructure

SOLUTION BRIEF

HYCU R-Cloud™ Data Protection as a Service for AWS

HYCU is the industry-leader in multi-cloud and SaaS data protection. Purpose-built for AWS, HYCU R-Cloud™ offers enterprise-class data protection for your applications and infrastructure running in AWS.

Protect your entire AWS infrastructure with HYCU R-Cloud™

Your applications are made of dozens of decoupled services – all holding critical data and configurations that keep your application secure, available, and accessible. HYCU protects many services beyond compute and databases – extending protection and recovery across security, network, and access management.

Protect your entire AWS infrastructure with HYCU R-Cloud™

- Amazon EC2
- Amazon S3
- Amazon S3 Express Zone One
- Amazon RDS
- Amazon Aurora
- Amazon DynamoDB
- AWS Lambda
- AWS CloudFormation
- Amazon VPC
- AWS IAM
- AWS WAF
- AWS Parameter Store
- AWS Key Management Service (KMS)
- Amazon Route 53

Protect cloud-hosted applications used to build, test, and secure your AWS infrastructure.

From code to prod, HYCU protects critical SaaS applications in your data and DevOps pipelines.

Microsoft Entra ID | okta | GitHub | GitLab | Bitbucket | Confluence
Terraform | circleci | Jira Product Discovery | monday | Jira Service Management

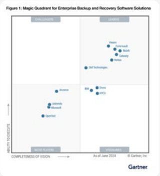
And many more applications!

Our Strengths

AWS Cloud Backup 2022-23 DCIG TOP 5 Large Enterprise

DCIG

DCIG TOP 5 AWS Cloud Backup Solutions Report



Gartner

Recognized as a Visionary in the Gartner Magic Quadrant for Enterprise Backup and Recovery

LEADER GIGAOM SONAR REPORT CLOUD-NATIVE DATA PROTECTION 2024

GIGAOM

Leader in the GigaOM Cloud Native Data Protection Report

Leader SUMMER 2024

Leading in SaaS Backup, File Recovery, DRaaS, Server Backup, and Database Backup

HYCU R-Cloud™

AWS Data Protection: Zero Burden, Complete Ownership

Protect Your Entire Data Estate

Many AWS applications rely on third-party tools like GitHub, Terraform, Jira, and CircleCI. HYCU R-Cloud protects over 80 cloud services and SaaS applications from a single view—all secured in your Amazon S3 storage buckets.

Back Up Your Identity, IP, and Data

HYCU delivers holistic data protection for your AWS accounts starting with your identity through IAM, expanding to your Intellectual property with your applications and git and finally your infrastructure and data, the lifeblood of digital businesses.

Multi-Cloud and Hybrid Cloud Protection

HYCU delivers comprehensive data protection across multiple cloud providers and critical on-premises infrastructure such as VMware and Nutanix.

Script-Free Backup and Recovery

HYCU delivers 1-click simplicity, tight integration with AWS services, and built-in compliance for your AWS workloads. Rest assured with ‘set and forget’ backups automating all activities, reducing costs, and ensuring you can always restore rapidly.

Operational Recovery and Item-Level Restore

Avoid costly, time-consuming bulk recoveries by restoring precisely what you need. Quickly recover individual files from EC2 instances, files from Amazon S3 buckets, roles from AWS IAM, subnets from Amazon VPC, and more. **See page 8 for recovery options**.

Cross-Regional Recovery

Rapidly clone and recover instances across regions in one click. Consolidate your backup and disaster recovery operations into one unified view.

Ransomware and Supply Chain Protection

Maintain complete control and access to your backups by following the 3-2-1 rule with logically separated copies in Amazon S3 or another public cloud. Pair it with Object lock to retain immutable backup copies. **See page 6 to learn how HYCU gives you full control of your AWS data.**

Why backup AWS Data?

Downtime and data loss are unacceptable, leading to revenue loss, broken user experiences, and constant fixes that burden your teams. Backups are the only way to ensure rapid recovery of your AWS applications, including your configurations. While AWS provides a secure and highly available infrastructure, your organization remains responsible for recovering data when mistakes occur or vulnerabilities are exploited.

Common Threats to Your AWS Application

- **Human Error:** Unintended deletions or misconfigurations can erase data or disrupt services.
- **Data Corruption:** Bugs, hardware failures, or faulty updates can corrupt data, making recovery difficult without backups.
- **Insider Threats:** Authorized personnel may accidentally or intentionally delete data or alter configurations.
- **Cyberattacks:** Attackers commonly exploit cloud security misconfigurations to compromise your application.

Are You Protecting Your Entire Application or Just a Fraction of It?

Your AWS applications consist of numerous interconnected services. Errors, corruption, or automation failures in any service can disrupt your critical applications. If you're only backing up EC2 instances and databases, you're addressing just a fraction of potential risks.

Questions to evaluate data loss risk in AWS

- ✓ Do we have backups to recover files if our S3 buckets are compromised or data is deleted?
- ✓ Are our network configurations backed up to restore connectivity if misconfigurations lead to data access issues?
- ✓ Can we quickly restore DNS settings if misconfigurations or attacks cause downtime or misdirect traffic?
- ✓ Do we back up IAM policies to recover from accidental changes that could result in data loss?
- ✓ Are WAF configurations backed up to reinstate security measures if rules are altered or deleted?
- ✓ Do we have backups of encryption keys and policies to recover data if keys are lost or compromised?
- ✓ Are our infrastructure templates backed up to recreate resources if they are lost or corrupted?
- ✓ Do we have safe copies of our repositories and access to infrastructure configurations in case they are deleted or there is a cyber threat?

What's different about HYCU

Total Coverage – Unified Protection

- **Comprehensive AWS Service Protection:** Safeguard more AWS services than any other backup provider or native tooling.
- **Comprehensive SaaS Protection:** Safeguard more SaaS applications adjacent to AWS than any other backup provider or native tooling.
- **Infrastructure Security:** Protect critical infrastructure services across networking, firewalls, and identity management (IAM).
- **Multi-account and Multi-Cloud Management:** Protect all your cloud accounts and assets through one service.

Save Time, Cost, and Resources

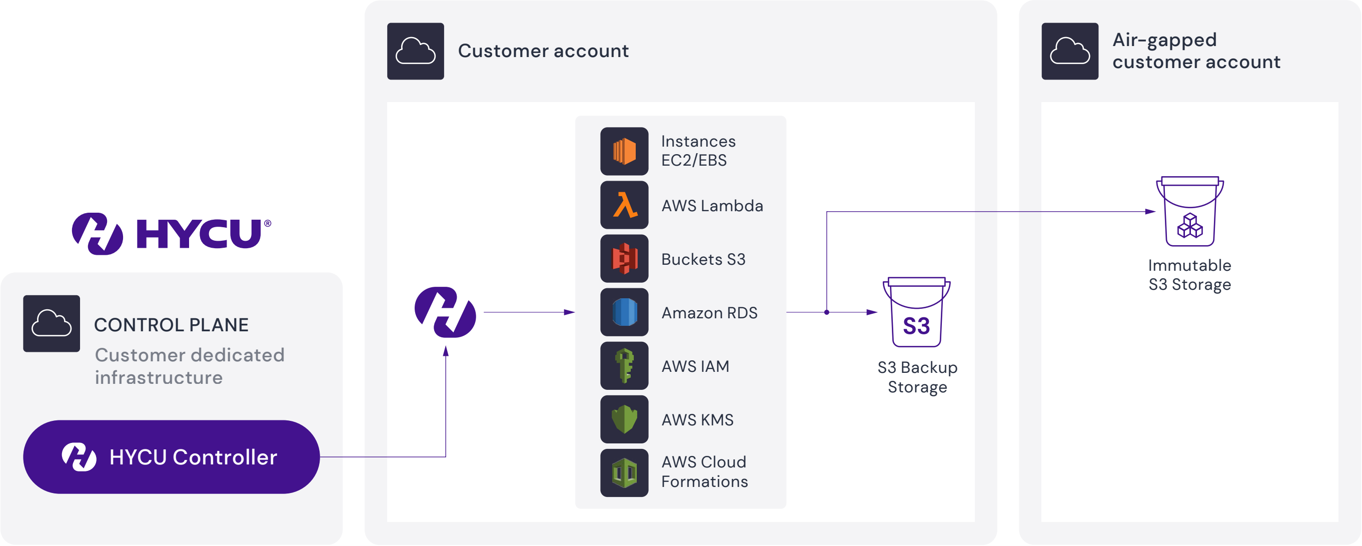
- **One-click Automation:** Simplify operations with one-click backups, migrations, and data recovery.
- **Multi-Region Recovery and Cloning:** Unify backups, disaster recovery, and dev/test activities with recovery and cloning across multiple AWS regions.
- **Excellent Customer Support:** Backed by world-class global support with an industry-high NPS score among 4000+ customers.

Complete Data Residency & Backup Control

- **Compliance and Governance:** Meet data residency and governance requirements according to geographic mandates.
- **Backup Ownership:** Maintain control of backups in your Amazon S3 buckets or across different AWS accounts with optional immutability.
- **Regulatory Compatibility:** Compatible with NIS2 and DORA requirements for backup policies, offsite copies, and resilience testing.

How it works

Below is an architectural diagram of HYCU R-Cloud™ protecting native services running on AWS. Diagrams are available for virtual applications on-premises using AWS for backup storage and disaster recovery.



1. Subscribe to HYCU directly or via AWS. HYCU leverages dynamic data movers running in your compute and region to meet residency requirements for data processing and storage.

2. Once connected to your AWS environment, HYCU auto-discovers all resources. No scripting or initial setup required.

3. Choose a storage target that meets your protection and/or cost requirements. Additionally, you can enable object-lock for ransomware.

4. Assign backup policies, defining backup frequency and data retention periods for your protected sources.

What your organization does

- ✓ Create an R-Cloud account and connect to your AWS environment
- ✓ Choose a storage target
- ✓ Assign default backup or create your own backup policies in a few clicks
- ✓ Access HYCU and restore data in one click

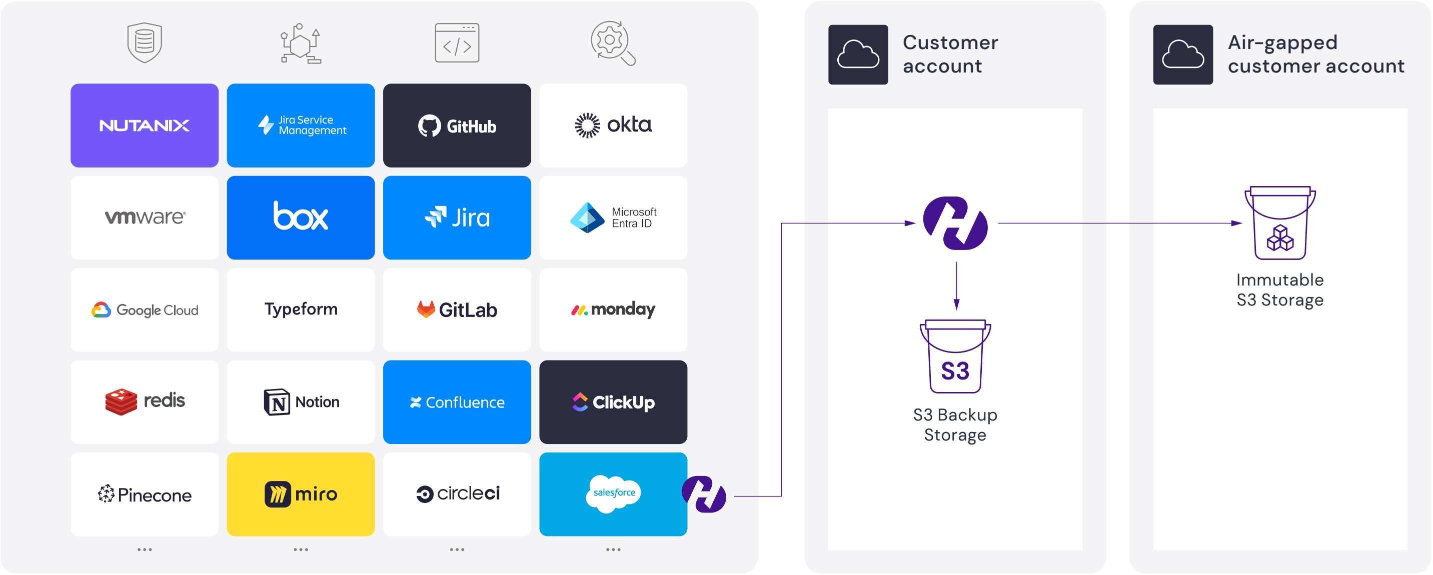
What HYCU does

- ✓ Automate all backup operations
- ✓ Orchestrate storage targets and ensure copies are kept offsite
- ✓ Continuously monitor for protection status
- ✓ Provide notifications and reporting

HYCU R-Cloud is meant to automate all data protection activities and only be used when data recovery is needed.

Protect your entire technology stack on AWS

Leverage your Amazon S3 storage as a central backup repository for 80+ integrations.



Use Amazon S3 as your backup storage for your entire organization

- Store SaaS backups in Amazon S3
- Leverage AWS as a backup and disaster recovery target for virtual workloads on-premises
- Backups are automatically stored on Amazon S3 buckets
- Customers can add WORM-enabled, object-locked copies
- Leverage any storage class
- Meet data residency requirements
- Keep all stored data in your AWS footprint

Achieve cyber-resilience and protect your organization from third-party risk

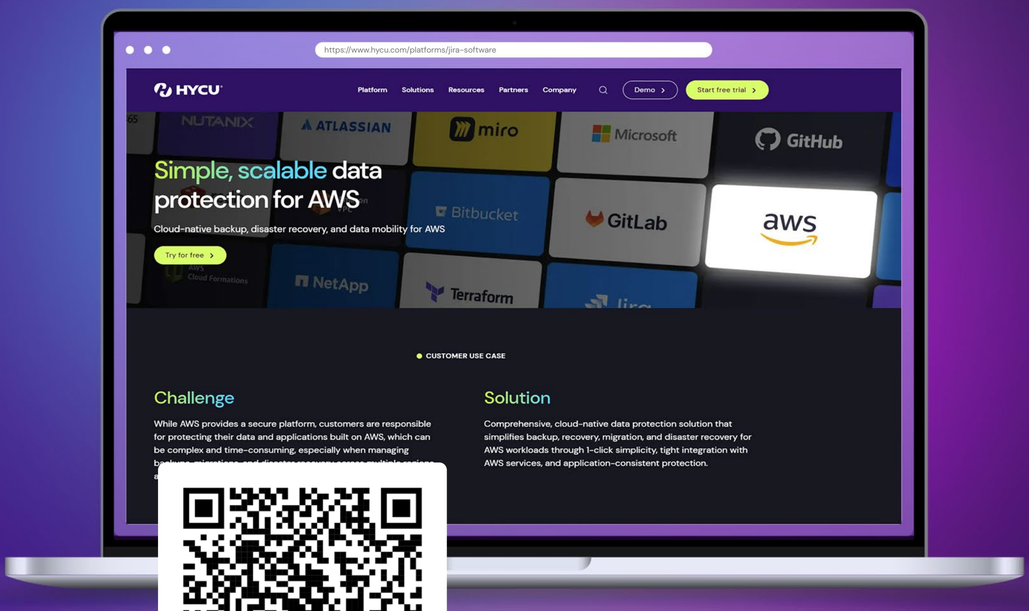
- Safely recover data and configurations of as-a-service applications
- Protect from cyber-attacks and insider threats
- Meet offsite data retention and recovery requirements
- Protect other public cloud workloads in AWS storage
- Comply with DORA, NIS2, HIPAA requirements for backup and recovery using AWS

Recovery and item-level restore options in AWS

AWS Service	Recovery Operations Supported
Amazon EC2	• Restore instance to an original location, clone or move instances. • Instance and files can also be restored to an instance or to a bucket.
Amazon S3	Restore files to the original or new bucket.
Amazon S3 Express Zone One	Restore files to the original or new bucket.
Amazon RDS	Restore a database instance from a snapshot.
Amazon Aurora	Restore a database instance from a snapshot.
Amazon DynamoDB	Restore a table from snapshots.
AWS Lambda	Restore functions.
Amazon VPC	Restore: • VPC • DHCP Option • Elastic IP • Route Table • Internet Gateway • Subnet • Security Group • Network ACL • Elastic Network Interface
AWS IAM	Restore: • Users • Groups • Roles • Policies • IAM Identity Providers
AWS WAF	Restore: • Web ACL • IP Set • Regex Pattern Set • Rule Group • Logging Configuration • Web ACL Rule

AWS Service	Recovery Operations Supported
Amazon KMS	In multi-region keys, restore: • Keys • Aliases • Policies • Tags • Key Rotations
AWS Route 53	Restore: • Hosted zone • CIDR collections • Health check • Traffic policy • Profile • Route 53 Resolver Resources • DNS firewall domain list • DNS firewall rule groups • Route 53 Application Recovery Controller resources • ARC control panel • ARC readiness resources
AWS Parameter Store	Restore all parameters from all regions or restore a single parameter.

Register for a free trial



Simple, scalable data protection for AWS

Cloud-native backup, disaster recovery, and data mobility for AWS

Try for free

CUSTOMER USE CASE

Challenge

While AWS provides a secure platform, customers are responsible for protecting their data and applications built on AWS, which can be complex and time-consuming, especially when managing backups, migrations, and disaster recovery across multiple regions

Solution

Comprehensive, cloud-native data protection solution that simplifies backup, recovery, migration, and disaster recovery for AWS workloads through 1-click simplicity, tight integration with AWS services, and application-consistent protection.

Get Started