HYCU® Microsoft Entra ID

HYCU for
Microsoft Entra ID
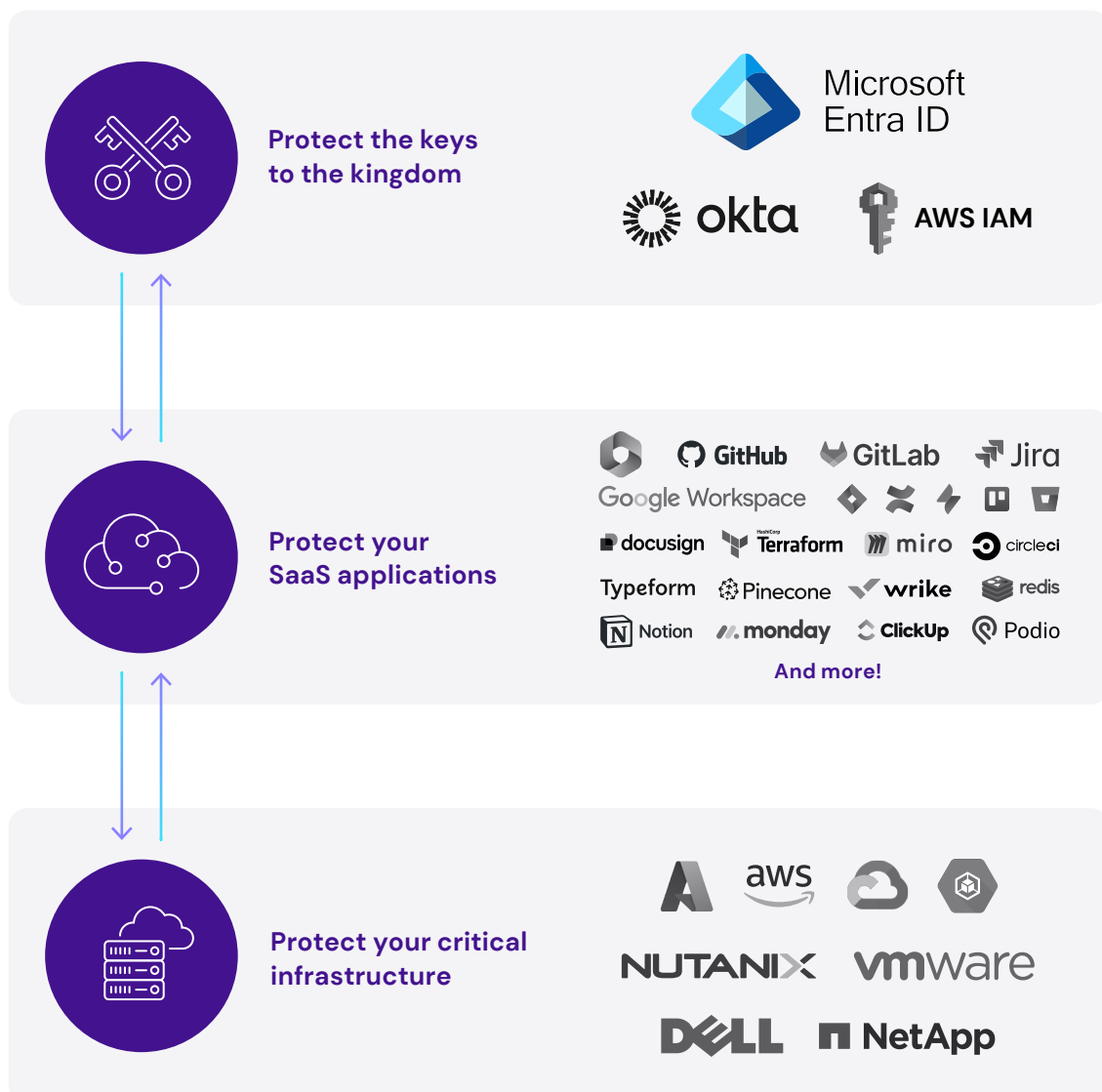(formerly Azure AD)

HYCU R–Cloud™
Data protection for Microsoft Entra ID and your entire data estate

HYCU is the world's leader in SaaS data protection, with 80+ integrations spanning SaaS applications and critical infrastructure, both cloud native and on–premises. HYCU protects your entire data estate, starting with the keys to your kingdom: Identity & Access Management.

Protect the keys to the kingdom

Microsoft Entra ID

okta   AWS IAM

Protect your SaaS applications

GitHub   GitLab   Jira
Google Workspace
docusign   Terraform   miro   circleci
Typeform   Pinecone   wrike   redis
Notion   monday   ClickUp   Podio

And more!

Protect your critical infrastructure

aws

NUTANIX   vmware

DELL   NetApp

A simple mistake in Microsoft Entra ID can bring your business to a standstill

Microsoft Entra ID holds the keys to critical applications and services. Misconfigurations, deletions, or cyberattacks can cause major disruptions, security vulnerabilities, and severe financial damage. And without a reliable backup, restoring Entra ID data and configurations can be slow and expensive.

Think Microsoft is responsible for recovering Entra ID configurations? **Think again.**

Microsoft follows the Shared Responsibility Model. Which means you are responsible for recovering your data in case of human error or an insider threat.

[Learn more here]

Solution: HYCU for Microsoft Entra ID

HYCU for Microsoft Entra ID is a purpose-built backup and recovery solution for Entra ID. With HYCU, you can automate backups, quickly restore IAM configurations, and ensure critical data is always recoverable in the event of human error or cyberattacks.

Avoid loss of revenue. Restore objects and configurations swiftly to save your organization from massive financial loss due to ransomware demands and prolonged downtimes.

Protect your organization from operational disruptions. Quickly restore Entra ID data to restore access to critical applications and services, drastically minimizing operational disruptions after an incident.

Stay protected from third-party risks. Keep your organization safe from unforeseen technical failures or errors caused by vendors, including Microsoft, with reliable backups in place.

Spend one minute a week on backups. Automate your backups to avoid thousands of hours of manual backup and recovery tasks, and stay on track with reporting, notifications, and 24/7 logging.

Improve your security and compliance posture. Establish a robust security and compliance posture by backing up and staying in control of your mission-critical IAM data.

Protect the keys to your IT kingdom with HYCU

One-click restore for Entra ID
Restore your entire Entra ID tenant or just a single item or configuration – HYCU gives you complete flexibility and control over exactly what you want to restore.

Protect Entra ID and Okta together
Avoid data siloes and point solutions, protect and restore Entra ID, Okta Workforce Identity Cloud (WIC), Okta Customer Identity Cloud (formerly Auth0), and AWS Identity and Access Management (IAM). Keep all critical IAM configurations stored in your control.

Backups on autopilot with complete flexibility
Highly flexible set-and-forget backup policies that run 24/7, providing you with backup assurance and peace of mind.

Security-first approach
All backups are stored in your own storage. Keeping backups in your control is critical for third party risk management, compliance, and data governance.

Data residency & governance
Ability to ensure your data is processed and kept in your desired regions. HYCU gives you complete control over where to run your backups and recovery operations from.

Ransomware-proof, offsite backups
Immutable backups that you can rely on, ensuring that you always have a secure data backup that can't be tampered with in case of an attack. Store your copies in an S3 Bucket only accessible to you with Amazon S3, Azure Blob, Google Cloud Storage or other S3-compatible targets.
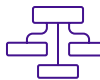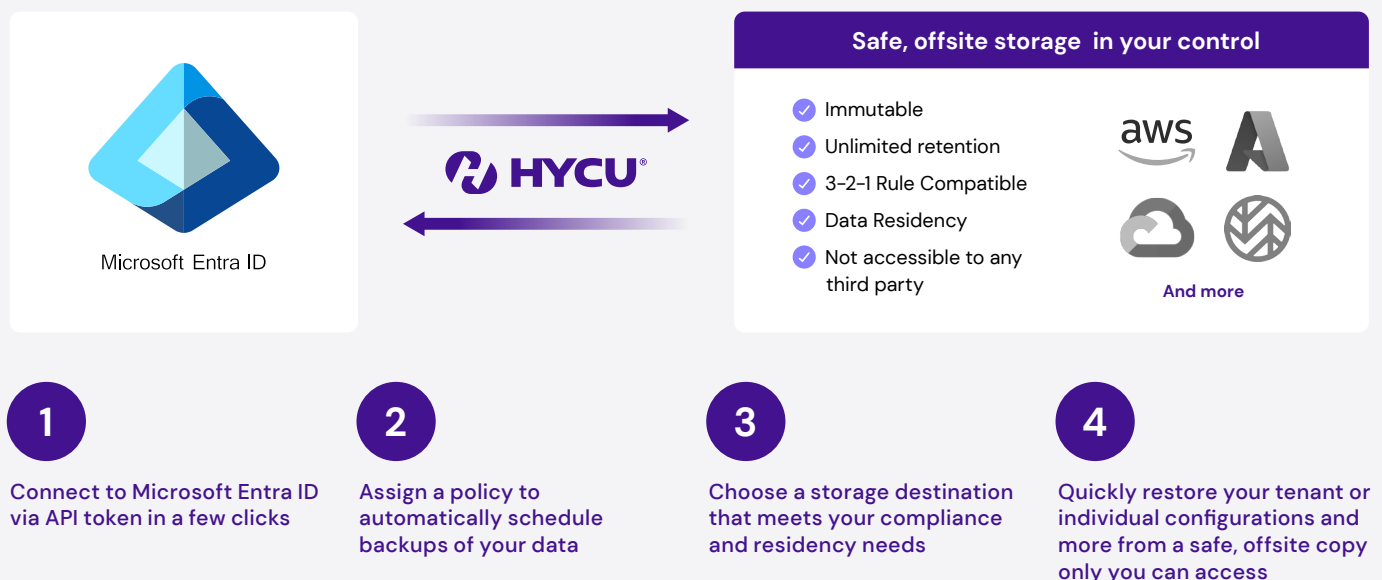
Visualize your data estate
Visualize all sources in your data estate using Entra ID and expose all applications in use, by department, to identify gaps in data protection and non-compliance.

Work with a Gartner recognized platform with an NPS of 91
HYCU is loved and trusted by the leaders in the market – recognized by Gartner as a Visionary with a Net Promoter Score (NPS) of 91, the highest in the data protection industry.

HYCU for Microsoft Entra ID: How it works

Microsoft Entra ID

Safe, offsite storage in your control
- ✓ Immutable
- ✓ Unlimited retention
- ✓ 3-2-1 Rule Compatible
- ✓ Data Residency
- ✓ Not accessible to any third party

And more

1 Connect to Microsoft Entra ID via API token in a few clicks

2 Assign a policy to automatically schedule backups of your data

3 Choose a storage destination that meets your compliance and residency needs

4 Quickly restore your tenant or individual configurations and more from a safe, offsite copy only you can access

HYCU for Microsoft Entra ID
Recovery options and coverage

The following is a breakdown of your recovery options with HYCU, from tenant-level restores to item-level restores and their associated objects.

Tenant	• User Tenant Settings • Group Tenant Settings	
Users	• Groups • Roles • Applications • Licenses • Azure Role Assignments • Account Status	• User Type • Certificates • User Properties • Custom Security Attributes • Federated Users
Groups	• Members • Owners • Roles & Admin • Admin Units • Group Membership	• Applications • Licenses • Azure Role Assignments
Roles & Administrators	• Built-in • Custom • Eligible Assignments • Active Assignments	• Role Settings • Descriptions
Custom Security Attributes	• Attribute Set • Active Attributes • Deactivated Attributes	• Roles & Admins
Conditional Access Control Policy	• Policies • Named Locations	• Auth Strengths
Custom Domain	• Includes custom domain names	
Administrative Units	• Properties • Users • Groups	• Devices • Roles & Admins
App Registrations	• Branding & properties • Certificates • Token Config • API Permissions • Expose an API	• App Roles • Roles & Admin
Enterprise Applications	• Single Sign-On • Branding & Properties • Certificates • Token Config • API Permissions	• Expose an API • App Roles • Roles & Admin

Make Microsoft Entra ID come to life with R-Graph

Your SaaS applications are your responsibility when it comes to data protection, recovery, and compliance. In today's era of cyber-attacks and third-party risk, it's critical to understand your risk profile and act immediately.

How it works

HYCU R-Graph™ is a built-in service that uses Entra ID and/or Okta to instantly visualize your SaaS estate. Simply connect with Entra ID using an API token and in a few seconds, HYCU will visualize all applications. Once you start protecting these applications, R-Graph will help you monitor all protected apps for compliance and protection status.
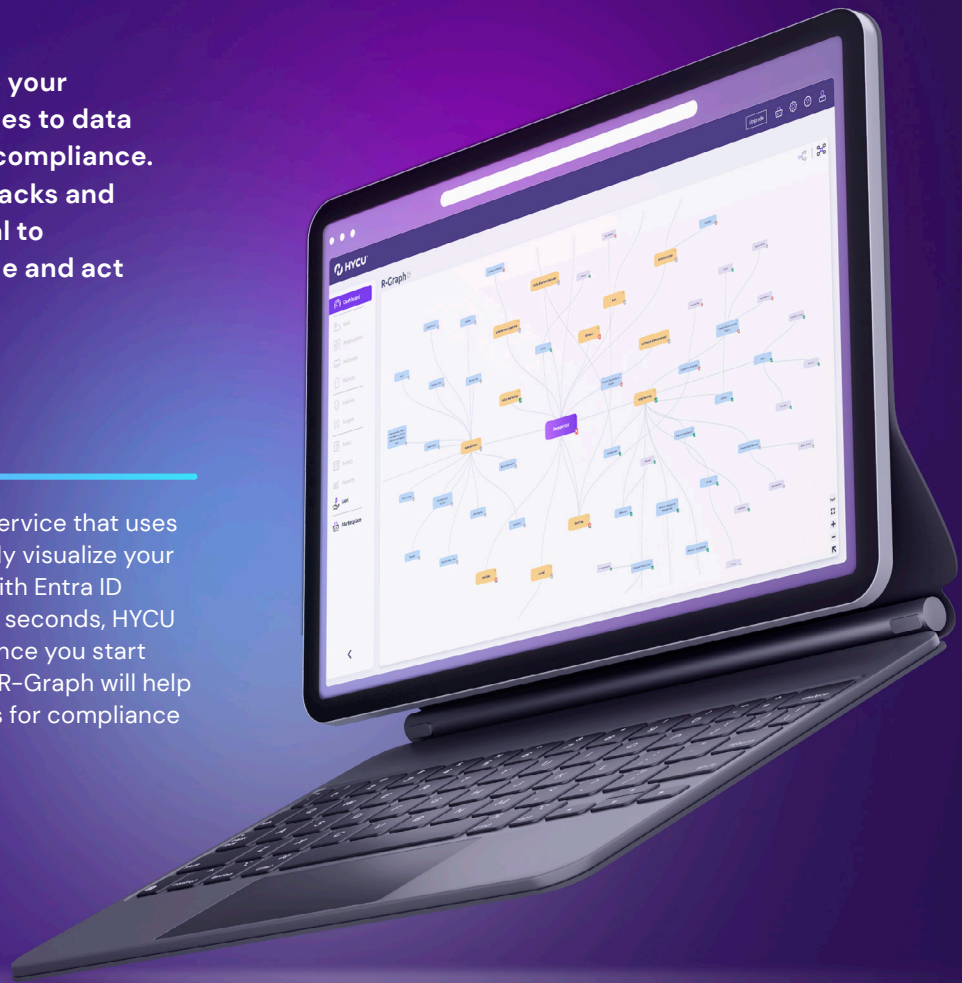
Visualize your data estate

Organize your tech stack by department
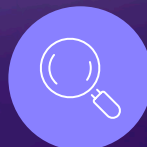
Expose applications without protection

Map out ICTs for DORA and NIS2 Compliance

Ransomware-proof data protection for Entra ID

Get Started