



Microsoft  
Entra ID

# HYCU für Microsoft Entra ID

(ehemals Azure AD)



BRIEF DER LÖSUNG

# HYCU R-Cloud™

## Datensicherung für Microsoft Entra ID und Ihren gesamten Datenbestand

HYCU ist der weltweit führende Anbieter von SaaS-Datenschutz mit mehr als 80 Integrationen für SaaS-Anwendungen und kritische Infrastrukturen, sowohl in der Cloud als auch vor Ort. HYCU schützt Ihren gesamten Datenbestand, angefangen bei den Schlüsseln zu Ihrem Königreich: Identitäts- und Zugriffsmanagement.



Schützen Sie die  
Schlüssel zum  
Königreich



Microsoft  
Entra ID



okta



AWS IAM



Schützen Sie Ihre  
SaaS- Anwendungen



GitHub

GitLab

Jira

Google Workspace

Slack

Zoom

Dropbox

DocuSign

Terraform

Miro

CircleCI

Typeform

Pinecone

Wrike

Redis

Notion

Monday

ClickUp

Podio

And more!



Schützen Sie Ihre  
kritische Infrastruktur



aws



NUTANIX

vmware

DELL

NetApp



# Ein einfacher Fehler in Microsoft Entra ID kann Ihr Unternehmen zum Stillstand bringen

Die Microsoft Entra ID ist der Schlüssel zu wichtigen Anwendungen und Diensten. Fehlkonfigurationen, Löschungen oder Cyberangriffe können zu erheblichen Unterbrechungen, Sicherheitslücken und schwerwiegenden finanziellen Schäden führen. Und ohne ein zuverlässiges Backup kann die Wiederherstellung von Entra ID-Daten und -Konfigurationen langsam und teuer sein.

Denken Sie, dass Microsoft für die Wiederherstellung von Entra-ID-Konfigurationen verantwortlich ist? Denken Sie noch einmal nach.

Microsoft verfolgt das Modell der geteilten Verantwortung. Das bedeutet, dass Sie für die Wiederherstellung Ihrer Daten im Falle eines menschlichen Fehlers oder einer Insider-Bedrohung verantwortlich sind.

[Hier erfahren Sie mehr](#)

## Lösung: HYCU für Microsoft Entra ID

HYCU für Microsoft Entra ID ist eine speziell entwickelte Sicherungs- und Wiederherstellungslösung für Entra ID. Mit HYCU können Sie Backups automatisieren, IAM-Konfigurationen schnell wiederherstellen und sicherstellen, dass kritische Daten im Falle von menschlichem Versagen oder Cyberangriffen jederzeit wiederherstellbar sind.



**Vermeiden Sie Umsatzeinbußen.** Stellen Sie Objekte und Konfigurationen schnell wieder her, um Ihr Unternehmen vor massiven finanziellen Verlusten aufgrund von Ransomware-Forderungen und längeren Ausfallzeiten zu bewahren.



**Schützen Sie Ihr Unternehmen vor Betriebsunterbrechungen.** Stellen Sie Entra ID-Daten schnell wieder her, um den Zugang zu wichtigen Anwendungen und Diensten wiederherzustellen und Betriebsunterbrechungen nach einem Vorfall drastisch zu minimieren.



**Blieben Sie vor Risiken Dritter geschützt.** Schützen Sie Ihr Unternehmen mit zuverlässigen Backups vor unvorhergesehenen technischen Ausfällen oder Fehlern, die von Anbietern, einschließlich Microsoft, verursacht werden.



**Verbringen Sie eine Minute pro Woche mit Backups.** Automatisieren Sie Ihre Backups, um Tausende von Stunden manueller Backup- und Wiederherstellungsaufgaben zu vermeiden, und bleiben Sie mit Berichten, Benachrichtigungen und 24/7-Protokollierung auf dem Laufenden.



**Verbessern Sie Ihre Sicherheits- und Compliance-Position.** Schaffen Sie eine solide Sicherheits- und Compliance-Struktur, indem Sie Ihre geschäftskritischen IAM-Daten sichern und die Kontrolle darüber behalten.

# Schützen Sie die Schlüssel zu Ihrem IT-Reich mit HYCU



## Ein-Klick-Wiederherstellung für Entra ID

Stellen Sie Ihren gesamten Entra ID-Tenant oder nur ein einzelnes Element oder eine Konfiguration wieder her – HYCU bietet Ihnen vollständige Flexibilität und Kontrolle darüber, was genau Sie wiederherstellen möchten.



## Schützen Sie Entra ID und Okta gemeinsam

Vermeiden Sie Datensilos und Punktlösungen, schützen und stellen Sie Entra ID, Okta Workforce Identity Cloud (WIC), Okta Customer Identity Cloud (ehemals AuthO) und AWS Identity and Access Management (IAM) wieder her. Behalten Sie alle wichtigen IAM-Konfigurationen unter Ihrer Kontrolle.



## Backups auf Autopilot mit vollständiger Flexibilität

Hochflexible Backup-Richtlinien, die rund um die Uhr laufen und Ihnen Sicherheit und Gewissheit bei der Sicherung bieten.



## Sicherheit hat Vorrang

Alle Backups werden in Ihrem eigenen Speicher gespeichert. Dass Sie die Kontrolle über die Backups behalten, ist entscheidend für das Risikomanagement für Dritte, die Einhaltung von Vorschriften und die Datenverwaltung.



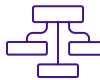
## Datenresidenz und Governance

Mit HYCU behalten Sie volle Kontrolle über die Verarbeitung und Speicherung Ihrer Daten in den gewünschten Regionen, einschließlich Backups und Wiederherstellungen.



## Ransomware-sichere Offsite-Backups

Unveränderliche Backups, auf die Sie sich verlassen können und die sicherstellen, dass Sie immer über eine sichere Datensicherung verfügen, die nicht manipuliert werden kann. im Falle eines Angriffs. Speichern Sie Ihre Kopien in einem S3-Bucket, auf das nur Sie über Amazon S3, Azure Blob, Google Cloud Storage oder andere S3-kompatible Ziele zugreifen können.



## Visualisieren Sie Ihren Datenbestand

Visualisieren Sie alle Quellen in Ihrem Datenbestand mit Entra ID und legen Sie alle genutzten Anwendungen nach Abteilungen offen, um Lücken im Datenschutz und Verstöße gegen die Vorschriften zu erkennen.



## Arbeiten Sie mit einer von Gartner anerkannten Plattform mit einem NPS von 91

HYCU ist bei den Marktführern beliebt und genießt deren Vertrauen – von Gartner anerkannt als Visionär mit einem Net Promoter Score (NPS) von 91, dem höchsten in der Datenschutzbranche.

## HYCU für Microsoft Entra ID: Wie es funktioniert



# HYCU für Microsoft Entra ID

## Recovery Optionen und Abdeckung

Im Folgenden finden Sie eine Aufschlüsselung Ihrer Wiederherstellungsoptionen mit HYCU, von Wiederherstellungen auf Mieterebene bis hin zu Wiederherstellungen auf Objektebene und den damit verbundenen Objekten.

<b>Mieter</b>	<ul style="list-style-type: none"> <li>• Benutzer-Mieter-Einstellungen</li> <li>• Einstellungen für Gruppenmieter</li> </ul>	
<b>Benutzer</b>	<ul style="list-style-type: none"> <li>• Gruppen</li> <li>• Rollen</li> <li>• Anwendungen</li> <li>• Lizenzen</li> <li>• Azure-Rollenzuweisungen</li> <li>• Konto-Status</li> </ul>	<ul style="list-style-type: none"> <li>• Benutzertyp</li> <li>• Bescheinigungen</li> <li>• Benutzer-Eigenschaften</li> <li>• Benutzerdefinierte Sicherheitsattribute</li> </ul>
<b>Gruppen</b>	<ul style="list-style-type: none"> <li>• Mitglieder</li> <li>• Eigentümer</li> <li>• Rollen &amp; Verwaltung</li> <li>• Verwaltungseinheiten</li> <li>• Mitgliedschaft in der Gruppe</li> </ul>	<ul style="list-style-type: none"> <li>• Anwendungen</li> <li>• Lizenzen</li> <li>• Azure-Rollenzuweisungen</li> </ul>
<b>Roles &amp; Administrators</b>	<ul style="list-style-type: none"> <li>• Eingebaut</li> <li>• Benutzerdefiniert</li> <li>• Förderfähige Zuweisungen</li> <li>• Aktive Zuweisungen</li> </ul>	<ul style="list-style-type: none"> <li>• Rolleneinstellungen</li> <li>• Beschreibungen</li> </ul>
<b>Benutzerdefinierte Sicherheitsattribute</b>	<ul style="list-style-type: none"> <li>• Attributsatz</li> <li>• Aktive Attribute</li> <li>• Deaktivierte Attribute</li> </ul>	<ul style="list-style-type: none"> <li>• Rollen &amp; Administratoren</li> </ul>
<b>Politik der bedingten Zugangskontrolle</b>	<ul style="list-style-type: none"> <li>• Politiken</li> <li>• Benannte Standorte</li> </ul>	<ul style="list-style-type: none"> <li>• Auth Stärke</li> </ul>
<b>Benutzerdefinierter Bereich</b>	<ul style="list-style-type: none"> <li>• Einschließlich benutzerdefinierter Domainnamen</li> </ul>	
<b>Verwaltungseinheiten</b>	<ul style="list-style-type: none"> <li>• Eigenschaften</li> <li>• Benutzer</li> <li>• Gruppen</li> </ul>	<ul style="list-style-type: none"> <li>• Geräte</li> <li>• Rollen &amp; Administratoren</li> </ul>
<b>App-Registrierungen</b>	<ul style="list-style-type: none"> <li>• Branding &amp; Eigenschaften</li> <li>• Bescheinigungen</li> <li>• Token-Konfiguration</li> <li>• API-Berechtigungen</li> <li>• Eine API freigeben</li> </ul>	<ul style="list-style-type: none"> <li>• App-Rollen</li> <li>• Rollen &amp; Verwaltung</li> </ul>
<b>Unternehmensanwendungen</b>	<ul style="list-style-type: none"> <li>• Einzelanmeldung</li> <li>• Branding &amp; Eigenschaften</li> <li>• Bescheinigungen</li> <li>• Token-Konfiguration</li> <li>• API-Berechtigungen</li> </ul>	<ul style="list-style-type: none"> <li>• Eine API freigeben</li> <li>• App-Rollen</li> <li>• Rollen &amp; Verwaltung</li> </ul>

# Erwecken Sie Microsoft Entra ID mit R-Graph zum Leben

Ihre SaaS-Anwendungen liegen in Ihrer Verantwortung, wenn es um Datenschutz, Wiederherstellung und Compliance geht. In der heutigen Zeit der Cyberangriffe und Risiken durch Dritte ist es entscheidend, Ihr Risikoprofil zu kennen und sofort zu handeln.

## Wie es funktioniert

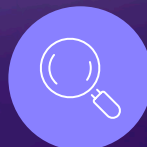
HYCU R-Graph™ ist ein integrierter Dienst, der Entra ID und/oder Okta nutzt, um Ihren SaaS-Bestand sofort zu visualisieren. Verbinden Sie sich einfach mit Entra ID über ein API-Token und in wenigen Sekunden visualisiert HYCU alle Anwendungen. Wenn Sie diese Anwendungen schützen, können Sie mit R-Graph alle geschützten Anwendungen auf Konformität und Schutzstatus überwachen.



Visualisieren  
Sie Ihren  
Datenbestand



Organisieren Sie  
Ihr technisches  
Paket nach  
Abteilungen

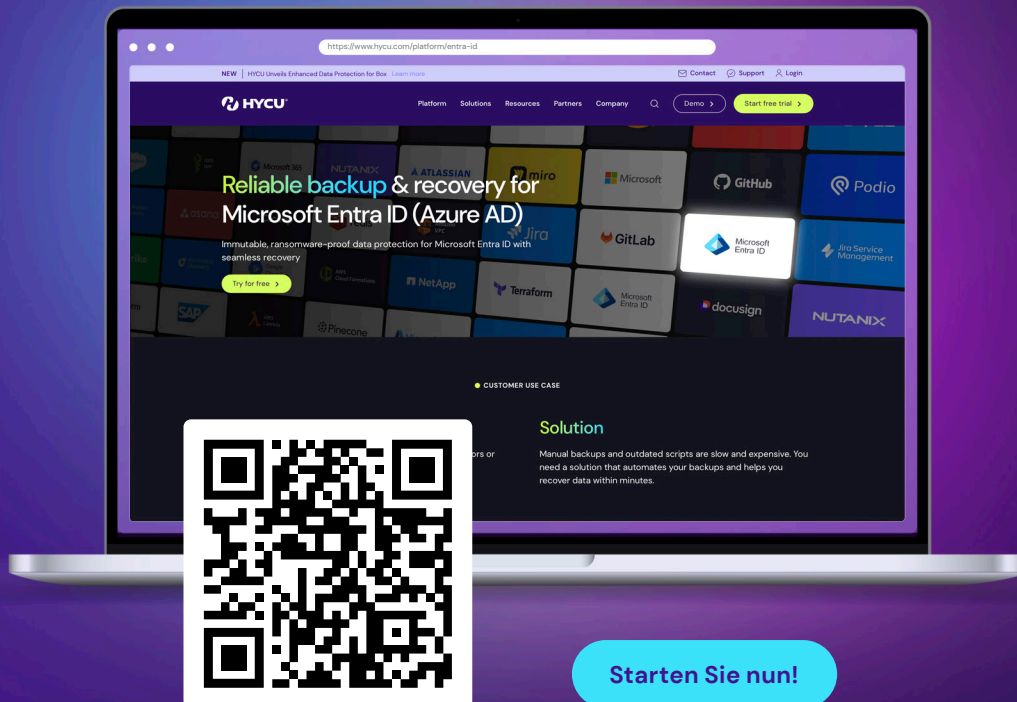


Anwendungen  
ohne Schutz  
freilegen



Planung der IKT  
für DORA und NIS2  
Einhaltung der  
Vorschriften

# Sicherer Ransomware Schutz für Entra ID



https://www.hycu.com/platform/entra-id

NEW | HYCU Unlocks Enhanced Data Protection for Box | Learn more

HYCU

Platform Solutions Resources Partners Company

Reliable backup & recovery for  
Microsoft Entra ID (Azure AD)

Immutable, ransomware-proof data protection for Microsoft Entra ID with  
seamless recovery

Try for free >

Microsoft, GitHub, Podio, Jira, GitLab, NetApp, Terraform, Microsoft Entra ID, docusign, NUTANIX

CUSTOMER USE CASE

Solution

Manual backups and outdated scripts are slow and expensive. You need a solution that automates your backups and helps you recover data within minutes.

Starten Sie nun!