

Zero365

Microsoft 365 Backup & Restore — Exchange, OneDrive, SharePoint, Teams & Entra ID

“Uw Microsoft 365-data, uw storage.” — Herstel een mailbox, een bestand of een identiteit, zonder vendor lock-in.

Service	Zero365 — Microsoft 365 Backup & Restore
Focus	Workload-bewuste backup van Exchange, OneDrive, SharePoint, Teams en Entra ID naar storage die u zelf beheert
Versie	1.0
Datum	Juni 2026
Dekking	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Leverancier	BackupSec

1. Wat is Zero365?

Zero365 is een cloud backup-service voor Microsoft 365. Het maakt via Microsoft Graph verbinding met uw tenant en maakt backups van Exchange Online, OneDrive, SharePoint Online, Microsoft Teams en Entra ID — elk met zijn eigen workload-bewuste herstelsemantiek, geen platte bestandsdump. Versleutelde kopieën worden weggeschreven naar storage die u zelf kiest en beheert (BYOS), en u herstelt precies wat u nodig hebt — een bericht, een bestand, een site of een identiteit — vanuit één console. Zero365 vormt de Microsoft 365-beschermingslaag van de BackupSec-familie, naast ZeroMON monitoring, ZeroTAM advies, ZeroPEN penetratietesten en ZeroVault immutable storage.

Waarom Zero365? De native retentie van Microsoft is geen backup. Verwijderde items verlopen, ransomware versleutelt gesynchroniseerde bestanden en identiteiten van vertrokken medewerkers verdwijnen. Zero365 bewaart een onafhankelijke, versleutelde kopie in storage die u zelf beheert — item voor item herstelbaar, lang nadat de eigen prullenbakken van Microsoft zijn verlopen.

De BackupSec-familie

Zero365 werkt samen met de rest van de BackupSec-familie:

Service	Rol
ZeroMON	Backupmonitoring & observability — realtime zichtbaarheid over uw Veeam-omgeving
ZeroTAM	Deskundig advies, accountmanagement & crisisondersteuning
ZeroPEN	Backup-penetratietesten & herstelbewijs — test backups zoals een aanvaller dat zou doen
Zero365	Microsoft 365 backup & restore — Exchange, OneDrive, SharePoint, Teams, Entra ID (dit document)
ZeroVault	Immutable cloud storage voor Veeam — een laatste kopie die niet kan worden verwijderd of versleuteld

Voor wie is het bedoeld?

- IT- en messagingteams die verantwoordelijk zijn voor de gegevensbescherming en het herstel van Microsoft 365
- MSP's en serviceproviders die multi-tenant Microsoft 365-omgevingen beheren
- Security- en risicoteams die een onafhankelijke, versleutelde backupkopie afdwingen
- Organisaties met eisen op het gebied van dataresidentie of soevereiniteit (bring your own storage)
- Teams met GDPR / KVKK / DORA / ISO 27001-verplichtingen voor bedrijfsgegevens

2. Catalogus met workloaddekking

Elke Microsoft 365-workload krijgt een backup met zijn eigen semantiek en zijn eigen herstelpad:

Workload	Wat wordt beschermd	Herstel
Exchange Online	E-mail, agenda, contactpersonen en taken voor primaire en gedeelde mailboxen — volledige MIME-getrouwheid met delta-sync.	Herstel op item- of mailboxniveau naar de originele of een alternatieve mailbox; EML/ZIP-export; preview vóór commit; standaard niet-destructief.
OneDrive	Drive-hiërarchie, bestanden, mappen, versiegeschiedenis en machtigingen / ACL's.	Point-in-time-herstel en ACL-herstel; <i>restore-only-if-hash-differs</i> -modus voor chirurgisch ransomwareherstel.
SharePoint Online	Documentbibliotheken en op lijsten gebaseerde gestructureerde inhoud, inclusief aangepaste kolomwaarden.	Metadata-behoudend herstel naar de originele of een alternatieve site; hash-gebaseerd differentieel herstel.
Microsoft Teams	Standaard-, privé- en gedeelde kanalen plus 1:1- en groepschats.	Hersteld als gestructureerde exportbundels (JSON met manifesten); geen live channel-replay — een beperking van de Graph API die we eerlijk benoemen.
Entra ID	Gebruikers, groepen, applicaties en service principals met lidmaatschap en eigenaarschap.	Drie paden: soft-delete-herstel (30 days), het object volledig opnieuw aanmaken, of property-replay via PATCH; groepslidmaatschap alleen toevoegen.

3. Implementatie & storage

Verbinding	Microsoft Graph met moderne authenticatie en een app-registratie — geen legacy-API's.
Implementatie	Gecontaineriseerd SaaS-platform met een webconsole; geen backup-infrastructuur die u zelf hoeft te draaien.
Storage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV of lokaal bestandssysteem.
Versleuteling	Versleutelde payload weggeschreven via Kopia; versleutelingssleutels blijven onder uw beheer.
Planning	Geautomatiseerde geplande backups met delta-first incrementele sync.
Cloud-scope	Wereldwijde commerciële Microsoft 365 en Entra ID. GCC, GCC High, DoD en 21Vianet vallen niet binnen de launch-scope.

Uw data, uw storage. Backups worden weggeschreven naar storage-accounts die u zelf bezit — nooit een vendor-locked repository. Omdat de versleutelingssleutels bij u blijven, hoeft een kopie van uw Microsoft 365-data uw jurisdictie nooit te verlaten.

4. Belangrijkste functies

- Bring your own storage — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Workload-bewuste herstelsemantiek per service
- Delta-first incrementele sync
- Herstel op itemniveau en bulkherstel
- Preview vóór elk herstel
- Ransomware hash-differentieel herstel (OneDrive & SharePoint)
- Standaard niet-destructieve hersteloperaties
- RBAC, SSO (SAML / OIDC) en MFA
- Auditlogging en SIEM-export
- Functiescheiding en just-in-time hersteltoegang

5. Wat u krijgt

- 1 Een gekoppelde Microsoft 365-tenant met geplande, workload-bewuste backups
- 2 Versleutelde backupkopieën in storage die u zelf bezit en beheert (BYOS)
- 3 Een restore-explorer om per workload te bladeren, zoeken, previewen en herstellen
- 4 Ransomware-bewust differentieel herstel voor OneDrive en SharePoint
- 5 Identiteitherstel via drie paden voor Entra ID-objecten
- 6 Toegangscontrole, auditlogging en SIEM-export voor governance

6. Beveiliging & compliance

Framework	Hoe Zero365 helpt
GDPR	Een onafhankelijke, versleutelde kopie met een duidelijk herstelrecht; data blijft in storage die u zelf beheert.
KVKK	Dataresidentie via bring-your-own-storage, met toegangslogging en rolscheiding.
DORA	ICT-veerkracht — herstelbare, onafhankelijke backups van kritieke Microsoft 365-data.
ISO 27001	Toegangscontrole, versleuteling en auditlogging afgestemd op de controls van Annex A.
SOC 2	Controls voor beveiliging, beschikbaarheid en vertrouwelijkheid over backup en herstel.

7. Volgende stap

Start een Zero365-proefperiode. Koppel uw tenant, kies uw storage en zie uw eerste backup draaien. Zero365 beschermt wat de native retentie van Microsoft niet beschermt.
www.backupsec.com · info@backupsec.com · BackupSec