

Zero365

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

“Vos données Microsoft 365, votre stockage.” — Restaurez une boîte aux lettres, un fichier ou une identité, sans dépendance vis-à-vis d'un fournisseur.

Service	Zero365 — Backup & restauration Microsoft 365
Objet	Backup adapté à chaque charge de travail d'Exchange, OneDrive, SharePoint, Teams et Entra ID vers un stockage que vous contrôlez
Version	1.0
Date	Juin 2026
Couverture	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Fournisseur	BackupSec

1. Qu'est-ce que Zero365 ?

Zero365 est un service de backup cloud pour Microsoft 365. Il se connecte à votre tenant via Microsoft Graph et sauvegarde Exchange Online, OneDrive, SharePoint Online, Microsoft Teams et Entra ID — chacun avec sa propre sémantique de restauration adaptée à la charge de travail, et non un simple vidage de fichiers. Les copies chiffrées sont écrites vers un stockage que vous choisissez et contrôlez (BYOS), et vous restaurez exactement ce dont vous avez besoin — un message, un fichier, un site ou une identité — depuis une console unique. Zero365 constitue la couche de protection Microsoft 365 de la famille BackupSec, aux côtés de la supervision ZeroMON, du conseil ZeroTAM, des tests d'intrusion ZeroPEN et du stockage immuable ZeroVault.

Pourquoi Zero365 ? La rétention native de Microsoft n'est pas un backup. Les éléments supprimés finissent par expirer, les ransomware chiffrent les fichiers synchronisés et les identités désactivées disparaissent. Zero365 conserve une copie indépendante et chiffrée dans un stockage que vous contrôlez — restaurable élément par élément, bien après l'expiration des corbeilles de Microsoft.

La famille BackupSec

Zero365 fonctionne de concert avec le reste de la famille BackupSec :

Service	Rôle
ZeroMON	Supervision & observabilité des backups — visibilité en temps réel sur l'ensemble de votre parc Veeam
ZeroTAM	Conseil d'expert, gestion de compte & gestion de crise
ZeroPEN	Test d'intrusion des backups & preuve de restauration — teste les backups comme le ferait un attaquant
Zero365	Backup & restauration Microsoft 365 — Exchange, OneDrive, SharePoint, Teams, Entra ID (ce document)
ZeroVault	Stockage cloud immuable pour Veeam — une dernière copie qui ne peut être ni supprimée ni chiffrée

À qui s'adresse-t-il ?

- Les équipes IT et messagerie responsables de la protection et de la restauration des données Microsoft 365
- Les MSP et prestataires de services gérant des environnements Microsoft 365 multi-tenant
- Les équipes sécurité et risques imposant une copie de backup indépendante et chiffrée
- Les organisations ayant des exigences de résidence ou de souveraineté des données (bring your own storage)
- Les équipes soumises à des obligations GDPR / KVKK / DORA / ISO 27001 pour les données métier

2. Catalogue de couverture des charges de travail

Chaque charge de travail Microsoft 365 est sauvegardée avec sa propre sémantique et son propre chemin de restauration :

Charge de travail	Ce qui est protégé	Restauration
Exchange Online	Courrier, calendrier, contacts et tâches pour les boîtes aux lettres principales et partagées — fidélité MIME complète avec synchronisation delta.	Restauration au niveau de l'élément ou de la boîte aux lettres vers la boîte d'origine ou une autre boîte ; export EML/ZIP ; prévisualisation avant validation ; non destructif par défaut.
OneDrive	Hiérarchie du drive, fichiers, dossiers, historique des versions et permissions / ACL.	Restauration à un instant précis et récupération des ACL ; mode <i>restore-only-if-hash-differs</i> pour une restauration chirurgicale face au ransomware.
SharePoint Online	Bibliothèques de documents et contenu structuré basé sur des listes, y compris les valeurs de colonnes personnalisées.	Restauration préservant les métadonnées vers le site d'origine ou un autre site ; récupération différentielle basée sur le hash.
Microsoft Teams	Canaux standard, privés et partagés, ainsi que les conversations 1:1 et de groupe.	Restauré sous forme de lots d'export structurés (JSON avec manifestes) ; pas de réinjection en direct dans les canaux — une limite de l'API Graph que nous indiquons en toute transparence.
Entra ID	Utilisateurs, groupes, applications et principaux de service avec appartenance et propriété.	Trois approches : récupération par soft-delete (30 days), recréation complète de l'objet ou réapplication des propriétés via PATCH ; l'appartenance aux groupes se fait uniquement par ajout.

3. Déploiement & stockage

Connexion	Microsoft Graph avec authentification moderne et un enregistrement d'application — aucune API héritée.
Déploiement	Plateforme SaaS conteneurisée avec console web ; aucune infrastructure de backup à exploiter vous-même.
Stockage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV ou système de fichiers local.
Chiffrement	Charge utile chiffrée écrite via Kopia ; les clés de chiffrement restent sous votre contrôle.
Planification	Backups planifiés et automatisés avec synchronisation incrémentale privilégiant les deltas.
Périmètre cloud	Microsoft 365 commercial global et Entra ID. GCC, GCC High, DoD et 21Vianet ne font pas partie du périmètre de lancement.

Vos données, votre stockage. Les backups sont écrits vers des comptes de stockage que vous possédez — jamais un dépôt verrouillé par un fournisseur. Comme les clés de chiffrement restent chez vous, une copie de vos données Microsoft 365 n'a jamais à quitter votre juridiction.

4. Fonctionnalités clés

- Bring your own storage — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Sémantique de restauration adaptée à chaque service
- Synchronisation incrémentale privilégiant les deltas
- Restauration au niveau de l'élément et en masse
- Prévisualisation avant chaque restauration
- Récupération différentielle par hash face au ransomware (OneDrive & SharePoint)
- Restaurations non destructives par défaut
- RBAC, SSO (SAML / OIDC) et MFA
- Journalisation d'audit et export SIEM
- Séparation des tâches et accès de restauration juste-à-temps

5. Ce que vous obtenez

- 1 Un tenant Microsoft 365 connecté avec des backups planifiés et adaptés à chaque charge de travail
- 2 Des copies de backup chiffrées dans un stockage que vous possédez et contrôlez (BYOS)
- 3 Un explorateur de restauration pour parcourir, rechercher, prévisualiser et restaurer par charge de travail
- 4 Une récupération différentielle tenant compte du ransomware pour OneDrive et SharePoint
- 5 Une récupération d'identité à trois approches pour les objets Entra ID
- 6 Contrôle d'accès, journalisation d'audit et export SIEM pour la gouvernance

6. Sécurité & conformité

Cadre	Comment Zero365 vous aide
GDPR	Une copie indépendante et chiffrée avec un droit clair de restauration ; les données restent dans un stockage que vous contrôlez.
KVKK	Résidence des données grâce au bring-your-own-storage, avec journalisation des accès et séparation des rôles.
DORA	Résilience TIC — backups indépendants et restaurables des données Microsoft 365 critiques.
ISO 27001	Contrôle d'accès, chiffrement et journalisation d'audit alignés sur les contrôles de l'Annex A.
SOC 2	Contrôles de sécurité, de disponibilité et de confidentialité couvrant le backup et la restauration.

7. Étape suivante

Démarrez un essai de Zero365. Connectez votre tenant, choisissez votre stockage et regardez votre premier backup s'exécuter. Zero365 protège ce que la rétention native de Microsoft ne protège pas.
www.backupsec.com · info@backupsec.com · BackupSec