

Zero365

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

“Dina Microsoft 365-data, din lagring.” — Återställ en brevlåda, en fil eller en identitet, utan inläsning till leverantören.

Tjänst	Zero365 — Microsoft 365 Backup & återställning
Fokus	Arbetslastmedveten backup av Exchange, OneDrive, SharePoint, Teams och Entra ID till lagring du kontrollerar
Version	1.0
Datum	Juni 2026
Täckning	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Leverantör	BackupSec

1. Vad är Zero365?

Zero365 är en molnbaserad backup-tjänst för Microsoft 365. Den ansluter till din tenant via Microsoft Graph och tar backup av Exchange Online, OneDrive, SharePoint Online, Microsoft Teams och Entra ID — var och en med sin egen arbetslastmedvetna återställningssemantik, inte en platt fildump. Krypterade kopior skrivs till lagring du väljer och kontrollerar (BYOS), och du återställer exakt det du behöver — ett meddelande, en fil, en webbplats eller en identitet — från en enda konsol. Zero365 är Microsoft 365-skyddslagret i BackupSec-familjen, tillsammans med ZeroMON-övervakning, ZeroTAM-rådgivning, ZeroPEN penetrationstestning och ZeroVault oföränderlig lagring.

Varför Zero365? Microsofts inbyggda lagring är inte en backup. Raderade objekt gallras ut, ransomware krypterar synkroniserade filer och avregistrerade identiteter försvinner. Zero365 behåller en oberoende, krypterad kopia i lagring du kontrollerar — återställningsbar objekt för objekt, långt efter att Microsofts egna papperskorgar har löpt ut.

BackupSec-familjen

Zero365 fungerar tillsammans med resten av BackupSec-familjen:

Tjänst	Roll
ZeroMON	Backup-övervakning & observerbarhet — realtidssynlighet över hela ditt Veeam-bestånd
ZeroTAM	Expertrådgivning, kontohantering & krisstöd
ZeroPEN	Backup-penetrationstestning & återställningsbevis — testar backuper på samma sätt som en angripare skulle göra
Zero365	Microsoft 365 backup & återställning — Exchange, OneDrive, SharePoint, Teams, Entra ID (detta dokument)
ZeroVault	Oföränderlig molnlagring för Veeam — en sista kopia som inte kan raderas eller krypteras

Vem är den till för?

- IT- och meddelandeteam som ansvarar för dataskydd och återställning av Microsoft 365
- MSP:er och tjänsteleverantörer som hanterar multi-tenant-miljöer för Microsoft 365
- Säkerhets- och riskteam som upprätthåller en oberoende, krypterad backup-kopia
- Organisationer med krav på datalokalisering eller suveränitet (ta med din egen lagring)
- Team med skyldigheter enligt GDPR / KVKK / DORA / ISO 27001 för verksamhetsdata

2. Katalog över arbetslasttäckning

Varje Microsoft 365-arbetslast tas backup av med sin egen semantik och sin egen återställningsväg:

Arbetslast	Vad som skyddas	Återställning
Exchange Online	E-post, kalender, kontakter och uppgifter för primära och delade brevlådor — full MIME-återgivning med deltasynkronisering.	Återställning på objekt- eller brevlådenivå till den ursprungliga eller en alternativ brevlåda; EML/ZIP-export; förhandsgranskning innan bekräftelse; icke-destruktiv som standard.
OneDrive	Enhetshierarki, filer, mappar, versionshistorik och behörigheter / ACL:er.	Tidsspecifik återställning och ACL-återställning; <i>restore-only-if-hash-differs</i> -läge för kirurgisk ransomware-återställning.
SharePoint Online	Dokumentbibliotek och listbaserat strukturerat innehåll, inklusive anpassade kolumnvärden.	Metadatabevarande återställning till den ursprungliga eller en alternativ webbplats; hash-baserad differentiell återställning.
Microsoft Teams	Standardkanaler, privata och delade kanaler samt 1:1- och gruppchattar.	Återställs som strukturerade exportpaket (JSON med manifest); ingen live-uppspelning av kanaler — en begränsning i Graph API som vi anger ärligt.
Entra ID	Användare, grupper, applikationer och tjänsteprinciper med medlemskap och ägarskap.	Tre vägar: återställning från soft-delete (30 dagar), fullständig återskapning av objekt eller egenskapsuppspelning via PATCH; gruppmedlemskap endast tillägg.

3. Driftsättning & lagring

Anslutning	Microsoft Graph med modern autentisering och en appregistrering — inga äldre API:er.
Driftsättning	Containeriserad SaaS-plattform med webbkonsol; ingen backup-infrastruktur att driva själv.
Lagring (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV eller lokalt filsystem.
Kryptering	Krypterad nyttolast skriven via Kopia; krypteringsnycklar förblir under din kontroll.
Schemaläggning	Automatiserade schemalagda backuper med delta-först inkrementell synkronisering.
Molnomfattning	Global kommersiell Microsoft 365 och Entra ID. GCC, GCC High, DoD och 21Vianet ingår inte i lanseringsomfattningen.

Dina data, din lagring. Backuper skrivs till lagringskonton du äger — aldrig ett leverantörslåst repository. Eftersom krypteringsnycklarna stannar hos dig behöver en kopia av dina Microsoft 365-data aldrig lämna din jurisdiktion.

4. Viktiga funktioner

- Ta med din egen lagring — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Arbetslastmedveten återställningssemantik per tjänst
- Delta-först inkrementell synkronisering
- Återställning på objektnivå och i bulk
- Förhandsgranskning före varje återställning
- Hash-differentiell ransomware-återställning (OneDrive & SharePoint)
- Icke-destruktiva återställningar som standard
- RBAC, SSO (SAML / OIDC) och MFA
- Revisionsloggning och SIEM-export
- Ansvarsfördelning och just-in-time-åtkomst för återställning

5. Vad du får

- 1 En ansluten Microsoft 365-tenant med schemalagda, arbetslastmedvetna backuper
- 2 Krypterade backup-kopior i lagring du äger och kontrollerar (BYOS)
- 3 En återställningsutforskare för att bläddra, söka, förhandsgranska och återställa per arbetslast
- 4 Ransomware-medveten differentiell återställning för OneDrive och SharePoint
- 5 Identitetsåterställning i tre vägar för Entra ID-objekt
- 6 Åtkomstkontroll, revisionsloggning och SIEM-export för styrning

6. Säkerhet & efterlevnad

Ramverk	Hur Zero365 hjälper
GDPR	En oberoende, krypterad kopia med en tydlig rätt att återställa; data stannar i lagring du kontrollerar.
KVKK	Datalokalisering genom bring-your-own-storage, med åtkomstloggning och rollseparation.
DORA	IKT-motståndskraft — återställningsbara, oberoende backuper av kritiska Microsoft 365-data.
ISO 27001	Åtkomstkontroll, kryptering och revisionsloggning i linje med kontrollerna i Annex A.
SOC 2	Kontroller för säkerhet, tillgänglighet och konfidentialitet över backup och återställning.

7. Nästa steg

Starta en Zero365-testperiod. Anslut din tenant, välj din lagring och se din första backup köras. Zero365 skyddar det som Microsofts inbyggda lagring inte gör.
www.backupsec.com · info@backupsec.com · BackupSec