

Zero365

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

“I tuoi dati Microsoft 365, il tuo storage.” — Ripristina una casella di posta, un file o un’identità, senza vendor lock-in.

Servizio	Zero365 — Backup & Ripristino di Microsoft 365
Ambito	Backup workload-aware di Exchange, OneDrive, SharePoint, Teams ed Entra ID su storage che controlli tu
Versione	1.0
Data	Giugno 2026
Copertura	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Fornitore	BackupSec

1. Che cos'è Zero365?

Zero365 è un servizio di backup cloud per Microsoft 365. Si connette al tuo tenant tramite Microsoft Graph ed esegue il backup di Exchange Online, OneDrive, SharePoint Online, Microsoft Teams ed Entra ID — ciascuno con la propria semantica di ripristino workload-aware, non un dump piatto di file. Le copie cifrate vengono scritte su uno storage che scegli e controlli tu (BYOS), e ripristini esattamente ciò che ti serve — un messaggio, un file, un sito o un'identità — da un'unica console. Zero365 è il livello di protezione Microsoft 365 della famiglia BackupSec, accanto al monitoraggio ZeroMON, alla consulenza ZeroTAM, al penetration testing ZeroPEN e allo storage immutabile ZeroVault.

Perché Zero365? La retention nativa di Microsoft non è un backup. Gli elementi eliminati scadono, il ransomware cifra i file sincronizzati e le identità disattivate scompaiono. Zero365 conserva una copia indipendente e cifrata su uno storage che controlli tu — ripristinabile elemento per elemento, molto dopo la scadenza dei cestini di Microsoft.

La famiglia BackupSec

Zero365 opera al fianco del resto della famiglia BackupSec:

Servizio	Ruolo
ZeroMON	Monitoraggio & osservabilità del backup — visibilità in tempo reale su tutto il tuo parco Veeam
ZeroTAM	Consulenza esperta, account management & supporto nelle crisi
ZeroPEN	Penetration testing del backup & prova di ripristino — testa i backup come farebbe un attaccante
Zero365	Backup & ripristino di Microsoft 365 — Exchange, OneDrive, SharePoint, Teams, Entra ID (questo documento)
ZeroVault	Cloud storage immutabile per Veeam — una copia finale che non può essere eliminata né cifrata

A chi è rivolto?

- Team IT e messaging responsabili della protezione e del ripristino dei dati Microsoft 365
- MSP e service provider che gestiscono ambienti Microsoft 365 multi-tenant
- Team di sicurezza e rischio che impongono una copia di backup indipendente e cifrata
- Organizzazioni con requisiti di residenza o sovranità dei dati (bring your own storage)
- Team con obblighi GDPR / KVKK / DORA / ISO 27001 per i dati aziendali

2. Catalogo della Copertura dei Workload

Ogni workload di Microsoft 365 viene sottoposto a backup con la propria semantica e il proprio percorso di ripristino:

Workload	Cosa viene protetto	Ripristino
Exchange Online	Posta, calendario, contatti e attività per le caselle primarie e condivise — piena fedeltà MIME con sincronizzazione delta.	Ripristino a livello di elemento o di casella verso la casella originale o alternativa; export EML/ZIP; anteprima prima del commit; non distruttivo per impostazione predefinita.
OneDrive	Gerarchia dei drive, file, cartelle, cronologia delle versioni e permessi / ACL.	Ripristino point-in-time e recupero delle ACL; modalità <i>restore-only-if-hash-differs</i> per un ripristino chirurgico dal ransomware.
SharePoint Online	Raccolte documenti e contenuti strutturati basati su liste, inclusi i valori delle colonne personalizzate.	Ripristino con conservazione dei metadati verso il sito originale o alternativo; recupero differenziale basato su hash.
Microsoft Teams	Canali standard, privati e condivisi più chat 1:1 e di gruppo.	Ripristinati come pacchetti di export strutturati (JSON con manifest); nessuna riproduzione live dei canali — un limite dell'API Graph che dichiariamo con onestà.
Entra ID	Utenti, gruppi, applicazioni e service principal con appartenenze e ownership.	Tre percorsi: recupero soft-delete (30 days), ricreazione completa dell'oggetto o replay delle proprietà tramite PATCH; appartenenza ai gruppi in sola aggiunta.

3. Deployment & Storage

Connessione	Microsoft Graph con autenticazione moderna e una app registration — nessuna API legacy.
Deployment	Piattaforma SaaS containerizzata con console web; nessuna infrastruttura di backup da gestire in proprio.
Storage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV o filesystem locale.
Cifratura	Payload cifrato scritto tramite Kopia; le chiavi di cifratura restano sotto il tuo controllo.
Pianificazione	Backup pianificati automatici con sincronizzazione incrementale delta-first.
Ambito cloud	Microsoft 365 ed Entra ID commerciale globale. GCC, GCC High, DoD e 21Vianet non rientrano nell'ambito di lancio.

I tuoi dati, il tuo storage. I backup vengono scritti su account di storage di tua proprietà — mai un repository con vendor lock-in. Poiché le chiavi di cifratura restano con te, una copia dei tuoi dati Microsoft 365 non deve mai lasciare la tua giurisdizione.

4. Funzionalità Principali

- Bring your own storage — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Semantica di ripristino workload-aware per ciascun servizio
- Sincronizzazione incrementale delta-first
- Ripristino a livello di elemento e in blocco
- Anteprima prima di ogni ripristino
- Recupero differenziale basato su hash dal ransomware (OneDrive & SharePoint)
- Ripristini non distruttivi per impostazione predefinita
- RBAC, SSO (SAML / OIDC) e MFA
- Audit logging ed export SIEM
- Separazione dei compiti e accesso al ripristino just-in-time

5. Cosa Ottieni

- 1 Un tenant Microsoft 365 connesso con backup pianificati e workload-aware
- 2 Copie di backup cifrate su uno storage di tua proprietà e controllo (BYOS)
- 3 Un restore explorer per navigare, cercare, visualizzare in anteprima e ripristinare per workload
- 4 Recupero differenziale consapevole del ransomware per OneDrive e SharePoint
- 5 Recupero delle identità a tre percorsi per gli oggetti Entra ID
- 6 Controllo degli accessi, audit logging ed export SIEM per la governance

6. Sicurezza & Conformità

Framework	Come aiuta Zero365
GDPR	Una copia indipendente e cifrata con un chiaro diritto al ripristino; i dati restano su uno storage che controlli tu.
KVKK	Residenza dei dati grazie al bring-your-own-storage, con logging degli accessi e separazione dei ruoli.
DORA	Resilienza ICT — backup indipendenti e ripristinabili dei dati Microsoft 365 critici.
ISO 27001	Controllo degli accessi, cifratura e audit logging allineati ai controlli dell'Annex A.
SOC 2	Controlli di sicurezza, disponibilità e riservatezza in tutto il backup e il ripristino.

7. Prossimo Passo

Avvia una prova di Zero365. Connetti il tuo tenant, scegli il tuo storage e osserva l'esecuzione del tuo primo backup. Zero365 protegge ciò che la retention nativa di Microsoft non protegge.

www.backupsec.com · info@backupsec.com · BackupSec