

Zero365

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

“Ihre Microsoft 365-Daten, Ihr Storage.” — Stellen Sie ein Postfach, eine Datei oder eine Identität wieder her, ohne Vendor-Lock-in.

Service	Zero365 — Microsoft 365 Backup & Restore
Fokus	Workload-bewusstes Backup von Exchange, OneDrive, SharePoint, Teams und Entra ID in Storage, den Sie kontrollieren
Version	1.0
Datum	Juni 2026
Abdeckung	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Anbieter	BackupSec

1. Was ist Zero365?

Zero365 ist ein Cloud-Backup-Dienst für Microsoft 365. Er verbindet sich über Microsoft Graph mit Ihrem Tenant und sichert Exchange Online, OneDrive, SharePoint Online, Microsoft Teams und Entra ID — jeweils mit eigener, Workload-bewusster Wiederherstellungslogik, nicht als flacher Datei-Dump. Verschlüsselte Kopien werden in einen Storage geschrieben, den Sie wählen und kontrollieren (BYOS), und Sie stellen genau das wieder her, was Sie brauchen — eine Nachricht, eine Datei, eine Site oder eine Identität — aus einer einzigen Konsole. Zero365 ist die Schutzebene für Microsoft 365 innerhalb der BackupSec-Familie, neben dem Monitoring ZeroMON, der Beratung ZeroTAM, dem Penetrationstesting ZeroPEN und dem unveränderlichen Storage ZeroVault.

Warum Zero365? Die native Aufbewahrung von Microsoft ist kein Backup. Gelöschte Elemente verfallen, Ransomware verschlüsselt synchronisierte Dateien und ausgeschiedene Identitäten verschwinden. Zero365 bewahrt eine unabhängige, verschlüsselte Kopie in einem Storage auf, den Sie kontrollieren — Element für Element wiederherstellbar, lange nachdem die Papierkörbe von Microsoft abgelaufen sind.

Die BackupSec-Familie

Zero365 arbeitet Hand in Hand mit dem Rest der BackupSec-Familie:

Service	Rolle
ZeroMON	Backup-Monitoring & Observability — Echtzeit-Transparenz über Ihre gesamte Veeam-Landschaft
ZeroTAM	Expertenberatung, Account-Management & Krisenunterstützung
ZeroPEN	Backup-Penetrationstesting & Wiederherstellungsnachweis — testet Backups so, wie es ein Angreifer tun würde
Zero365	Microsoft 365 Backup & Restore — Exchange, OneDrive, SharePoint, Teams, Entra ID (dieses Dokument)
ZeroVault	Unveränderlicher Cloud-Storage für Veeam — eine letzte Kopie, die nicht gelöscht oder verschlüsselt werden kann

Für wen ist es gedacht?

- IT- und Messaging-Teams, die für die Sicherung und Wiederherstellung von Daten in Microsoft 365 verantwortlich sind
- MSPs und Service-Provider, die mandantenfähige Microsoft 365-Umgebungen verwalten
- Security- und Risk-Teams, die eine unabhängige, verschlüsselte Backup-Kopie durchsetzen
- Organisationen mit Anforderungen an Datenresidenz oder Datensouveränität (Bring Your Own Storage)
- Teams mit GDPR- / KVKK- / DORA- / ISO 27001-Verpflichtungen für Geschäftsdaten

2. Katalog der Workload-Abdeckung

Jeder Microsoft 365-Workload wird mit eigener Semantik und eigenem Wiederherstellungspfad gesichert:

Workload	Was geschützt wird	Wiederherstellung
Exchange Online	E-Mail, Kalender, Kontakte und Aufgaben für primäre und freigegebene Postfächer — volle MIME-Treue mit Delta-Sync.	Wiederherstellung auf Element- oder Postfachebene in das ursprüngliche oder ein alternatives Postfach; EML/ZIP-Export; Vorschau vor der Übernahme; standardmäßig nicht-destruktiv.
OneDrive	Laufwerkshierarchie, Dateien, Ordner, Versionsverlauf und Berechtigungen / ACLs.	Point-in-Time-Wiederherstellung und ACL-Wiederherstellung; <i>restore-only-if-hash-differs</i> -Modus für gezielte Ransomware-Wiederherstellung.
SharePoint Online	Dokumentbibliotheken und listenbasierte strukturierte Inhalte, einschließlich benutzerdefinierter Spaltenwerte.	Metadaten-erhaltende Wiederherstellung in die ursprüngliche oder eine alternative Site; hash-basierte differentielle Wiederherstellung.
Microsoft Teams	Standard-, private und freigegebene Kanäle sowie 1:1- und Gruppen-Chats.	Wiederhergestellt als strukturierte Export-Bundles (JSON mit Manifesten); kein Live-Channel-Replay — eine Einschränkung der Graph API, die wir offen benennen.
Entra ID	Benutzer, Gruppen, Anwendungen und Service Principals mit Mitgliedschaften und Besitzverhältnissen.	Drei Wege: Soft-Delete-Wiederherstellung (30 days), vollständige Neuerstellung des Objekts oder Eigenschafts-Replay per PATCH; Gruppenmitgliedschaft nur additiv.

3. Bereitstellung & Storage

Verbindung	Microsoft Graph mit moderner Authentifizierung und einer App-Registrierung — keine Legacy-APIs.
Bereitstellung	Containerisierte SaaS-Plattform mit Web-Konsole; keine eigene Backup-Infrastruktur zu betreiben.
Storage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV oder lokales Dateisystem.
Verschlüsselung	Verschlüsselte Payload, geschrieben über Kopia; die Verschlüsselungsschlüssel bleiben unter Ihrer Kontrolle.
Zeitplanung	Automatisierte geplante Backups mit Delta-First-Inkrementell-Sync.
Cloud-Geltungsbereich	Globales kommerzielles Microsoft 365 und Entra ID. GCC, GCC High, DoD und 21Vianet sind nicht im Launch-Umfang enthalten.

Ihre Daten, Ihr Storage. Backups werden in Storage-Accounts geschrieben, die Ihnen gehören — niemals in ein herstellergebundenes Repository. Da die Verschlüsselungsschlüssel bei Ihnen bleiben, muss eine Kopie Ihrer Microsoft 365-Daten Ihre Jurisdiktion niemals verlassen.

4. Wichtige Funktionen

- Bring Your Own Storage — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Workload-bewusste Wiederherstellungssemantik pro Dienst
- Delta-First-Inkrementell-Sync
- Wiederherstellung auf Elementebene und Massenwiederherstellung
- Vorschau vor jeder Wiederherstellung
- Hash-differentielle Ransomware-Wiederherstellung (OneDrive & SharePoint)
- Standardmäßig nicht-destruktive Wiederherstellungen
- RBAC, SSO (SAML / OIDC) und MFA
- Audit-Logging und SIEM-Export
- Funktionstrennung und Just-in-Time-Wiederherstellungszugriff

5. Was Sie erhalten

- 1 Ein verbundener Microsoft 365-Tenant mit geplanten, Workload-bewussten Backups
- 2 Verschlüsselte Backup-Kopien in Storage, den Sie besitzen und kontrollieren (BYOS)
- 3 Ein Restore-Explorer zum Durchsuchen, Suchen, Vorschauen und Wiederherstellen nach Workload
- 4 Ransomware-bewusste differentielle Wiederherstellung für OneDrive und SharePoint
- 5 Identitätswiederherstellung über drei Wege für Entra ID-Objekte
- 6 Zugriffskontrolle, Audit-Logging und SIEM-Export für Governance

6. Security & Compliance

Framework	Wie Zero365 hilft
GDPR	Eine unabhängige, verschlüsselte Kopie mit klarem Wiederherstellungsrecht; die Daten bleiben in einem Storage, den Sie kontrollieren.
KVKK	Datenresidenz durch Bring-Your-Own-Storage, mit Zugriffsprotokollierung und Rollentrennung.
DORA	IKT-Resilienz — wiederherstellbare, unabhängige Backups kritischer Microsoft 365-Daten.
ISO 27001	Zugriffskontrolle, Verschlüsselung und Audit-Logging, ausgerichtet an den Annex A-Kontrollen.
SOC 2	Kontrollen für Sicherheit, Verfügbarkeit und Vertraulichkeit über Backup und Restore hinweg.

7. Nächster Schritt

Starten Sie eine Zero365-Testversion. Verbinden Sie Ihren Tenant, wählen Sie Ihren Storage und beobachten Sie, wie Ihr erstes Backup läuft. Zero365 schützt, was die native Aufbewahrung von Microsoft nicht abdeckt.

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