

Zero365

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

“Microsoft 365 verileriniz, sizin depolamanız.” — Bir posta kutusunu, bir dosyayı veya bir kimliği, tedarikçiye bağımlı kalmadan kurtarın.

Hizmet	Zero365 — Microsoft 365 Backup & Geri Yükleme
Odak	Exchange, OneDrive, SharePoint, Teams ve Entra ID'nin, kontrolünüzdeki depolamaya iş yükü farkındalıklı backup'ı
Sürüm	1.0
Tarih	Haziran 2026
Kapsam	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Sağlayıcı	BackupSec

1. Zero365 nedir?

Zero365, Microsoft 365 için bir bulut backup hizmetidir. Microsoft Graph üzerinden tenant'ınıza bağlanır ve Exchange Online, OneDrive, SharePoint Online, Microsoft Teams ve Entra ID'yi — her birini, düz bir dosya dökümü olarak değil, kendi iş yükü farkındalıklı geri yükleme semantiğiyle backup'lar. Şifrelenmiş kopyalar, seçtiğiniz ve kontrol ettiğiniz depolamaya (BYOS) yazılır ve tam olarak ihtiyacınız olanı — bir mesajı, bir dosyayı, bir siteyi veya bir kimliği — tek bir konsoldan kurtarırsınız. Zero365, BackupSec ailesinin Microsoft 365 koruma katmanıdır; ZeroMON izleme, ZeroTAM danışmanlık, ZeroPEN penetrasyon testi ve ZeroVault değişmez depolama ile birlikte yer alır.

Neden Zero365? Microsoft'un yerleşik saklama özelliği bir backup değildir. Silinen öğeler zaman aşımına uğrar, ransomware senkronize edilmiş dosyaları şifreler ve işten ayrılan kullanıcıların kimlikleri kaybolur. Zero365, kontrolünüzdeki depolamada bağımsız, şifreli bir kopya tutar — Microsoft'un kendi geri dönüşüm kutuları dolduktan çok sonra bile öge bazında kurtarılabilir.

BackupSec ailesi

Zero365, BackupSec ailesinin geri kalanıyla birlikte çalışır:

Hizmet	Roİ
ZeroMON	Backup izleme & gözlemlenebilirlik — Veeam ortamınız genelinde gerçek zamanlı görünürlük
ZeroTAM	Uzman danışmanlık, hesap yönetimi & kriz desteği
ZeroPEN	Backup penetrasyon testi & kurtarma kanıtı — backup'ları bir saldırganın yapacağı gibi test eder
Zero365	Microsoft 365 backup & geri yükleme — Exchange, OneDrive, SharePoint, Teams, Entra ID (bu belge)
ZeroVault	Veeam için değişmez bulut depolama — silinemeyen veya şifrelenemeyen bir son kopya

Kimler için?

- Microsoft 365 veri koruması ve kurtarmasından sorumlu IT ve mesajlaşma ekipleri
- Çok kiracılı (multi-tenant) Microsoft 365 ortamlarını yöneten MSP'ler ve hizmet sağlayıcılar
- Bağımsız, şifreli bir backup kopyasını zorunlu kılan güvenlik ve risk ekipleri
- Veri konumlandırma veya egemenlik gereksinimleri olan kuruluşlar (kendi depolamanızı getirin)
- İş verileri için GDPR / KVKK / DORA / ISO 27001 yükümlülükleri olan ekipler

2. İş Yüğü Kapsamı Kataloğu

Her Microsoft 365 iş yüğü, kendi semantiği ve kendi geri yükleme yoluyla backup'lanır:

İş Yüğü	Neler korunuyor	Geri Yükleme
Exchange Online	Birincil ve paylaşımlı posta kutuları için posta, takvim, kişiler ve görevler — delta senkronizasyon ile tam MIME doğruluğu.	Orijinal veya alternatif bir posta kutusuna öge ya da posta kutusu düzeyinde geri yükleme; EML/ZIP dışa aktarımı; işlem öncesi önizleme; varsayılan olarak veri kaybına yol açmayan (non-destructive).
OneDrive	Sürücü hiyerarşisi, dosyalar, klasörler, sürüm geçmişi ve izinler / ACL'ler.	Belirli bir zamana geri yükleme ve ACL kurtarma; cerrahi hassasiyette ransomware kurtarması için <i>yalnızca-hash-farklıysa-geri-yükle</i> modu.
SharePoint Online	Belge kitaplıkları ve özel sütun değerleri dahil, liste tabanlı yapılandırılmış içerik.	Orijinal veya alternatif bir siteye meta verileri koruyan geri yükleme; hash tabanlı diferansiyel kurtarma.
Microsoft Teams	Standart, özel ve paylaşımlı kanallar ile 1:1 ve grup sohbetleri.	Yapılandırılmış dışa aktarım paketleri olarak geri yüklenir (manifest içeren JSON); canlı kanal yeniden oynatma yoktur — dürüstçe belirttiğimiz bir Graph API sınırı.
Entra ID	Üyelik ve sahiplik bilgileriyle birlikte kullanıcılar, gruplar, uygulamalar ve service principal'lar.	Üç yol: soft-delete kurtarma (30 gün), nesnenin tam olarak yeniden oluşturulması veya PATCH ile özellik yeniden uygulama; grup üyeliği yalnızca ekleme (add-only).

3. Kurulum & Depolama

Bağlantı	Modern kimlik doğrulama ve bir uygulama kaydı (app registration) ile Microsoft Graph — legacy API yok.
Kurulum	Web konsoluna sahip, konteynerleştirilmiş SaaS platformu; kendinizin işleteceği bir backup altyapısı yok.
Depolama (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV veya yerel dosya sistemi.
Şifreleme	Kopia aracılığıyla yazılan şifreli veri; şifreleme anahtarları sizin kontrolünüzde kalır.
Zamanlama	Delta öncelikli artımlı senkronizasyon ile otomatik zamanlanmış backup'lar.
Bulut kapsamı	Global ticari Microsoft 365 ve Entra ID. GCC, GCC High, DoD ve 21Vianet lansman kapsamında değildir.

Verileriniz, sizin depolamanız. Backup'lar, sahip olduğunuz depolama hesaplarına yazılır — asla tedarikçiye kilitli bir repository'ye değil. Şifreleme anahtarları sizde kaldığı için, Microsoft 365 verilerinizin bir kopyası hiçbir zaman yargı bölgenizin dışına çıkmak zorunda kalmaz.

4. Temel Özellikler

- Kendi depolamanızı getirin — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Hizmet başına iş yükü farkındalıklı geri yükleme semantiği
- Delta öncelikli artımlı senkronizasyon
- Öge düzeyinde ve toplu geri yükleme
- Her geri yüklemeden önce önizleme
- Ransomware hash-diferansiyel kurtarma (OneDrive & SharePoint)
- Varsayılan olarak veri kaybına yol açmayan (non-destructive) geri yüklemeler
- RBAC, SSO (SAML / OIDC) ve MFA
- Denetim günlükleme ve SIEM dışı aktarımı
- Görevler ayrılığı ve tam zamanında (just-in-time) geri yükleme erişimi

5. Neler Elde Edersiniz

- 1 Zamanlanmış, iş yükü farkındalıklı backup'lara sahip bağlı bir Microsoft 365 tenant'ı
- 2 Sahip olduğunuz ve kontrol ettiğiniz depolamada şifreli backup kopyaları (BYOS)
- 3 İş yüküne göre gözetme, arama, önizleme ve kurtarma için bir geri yükleme gezgini
- 4 OneDrive ve SharePoint için ransomware farkındalıklı diferansiyel kurtarma
- 5 Entra ID nesneleri için üç yollu kimlik kurtarma
- 6 Yönetişim için erişim kontrolü, denetim günlükleme ve SIEM dışı aktarımı

6. Güvenlik & Uyumluluk

Çerçeve	Zero365 nasıl yardımcı olur
GDPR	Net bir geri yükleme hakkına sahip, bağımsız ve şifreli bir kopya; veriler kontrolünüzdeki depolamada kalır.
KVKK	Kendi depolamanızı getirme yoluyla veri konumlandırma; erişim günlükleme ve rol ayrımı ile birlikte.
DORA	ICT dayanıklılığı — kritik Microsoft 365 verilerinin kurtarılabilir, bağımsız backup'ları.
ISO 27001	Annex A kontrolleriyle uyumlu erişim kontrolü, şifreleme ve denetim günlükleme.
SOC 2	Backup ve geri yükleme genelinde güvenlik, erişilebilirlik ve gizlilik kontrolleri.

7. Sonraki Adım

Bir Zero365 denemesi başlatın. Tenant'ınızı bağlayın, depolamanızı seçin ve ilk backup'ınızın çalışmasını izleyin. Zero365, Microsoft'un yerleşik saklama özelliğinin korumadıklarını korur.
www.backupsec.com · info@backupsec.com · BackupSec