

Stork365

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

“Microsoft 365 verileriniz, sizin storage'ınız.” Bir posta kutusunu, bir dosyayı veya bir kimliği, tedarikçiye bağımlı kalmadan kurtarın.

Hizmet	Stork365: Microsoft 365 Backup & Restore
Odak	Exchange, OneDrive, SharePoint, Teams ve Entra ID'nin, kontrolünüzdeki storage'a workload-aware backup'ı
Sürüm	1.0
Tarih	Haziran 2026
Kapsam	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Sağlayıcı	BackupSec

1. Stork365 nedir?

Stork365, 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 workload-aware restore semantiğiyle backup'lar. Şifrelenmiş kopyalar, seçtiğiniz ve kontrol ettiğiniz storage'a (BYOS) yazılır ve tam olarak ihtiyacınız olanı (bir mesajı, bir dosyayı, bir siteyi veya bir kimliği) tek bir konsoldan kurtarırsınız. Stork365, BackupSec ailesinin Microsoft 365 koruma katmanıdır; ZeroMON izleme, ZeroTAM danışmanlık, ZeroPEN pentest ve immutable Veeam backup'ları için S3 uyumlu storage olan ZeroVault ile birlikte yer alır.

Neden Stork365? Microsoft'un yerleşik retention özelliği bir backup değildir. Silinen öğeler zaman aşımına uğrar, ransomware senkronize edilmiş dosyaları şifreler ve işten ayrılan kullanıcıların kimlikleri kaybolur. Stork365, kontrolünüzdeki storage'da bağımsız, şifreli bir kopya tutar, Microsoft'un kendi geri dönüşüm kutuları dolduktan çok sonra bile öge bazında kurtarılabilir.

BackupSec ailesi

Stork365, BackupSec ailesinin geri kalanıyla birlikte çalışır:

Hizmet	Roİ
ZeroMON	Backup izleme & observability: Veeam ortamınız genelinde gerçek zamanlı görünürlük
ZeroTAM	Uzman danışmanlık, hesap yönetimi & kriz desteği
ZeroPEN	Backup pentesti & kurtarma kanıtı: backup'ları bir saldırganın yapacağı gibi test eder
Stork365	Microsoft 365 backup & restore: Exchange, OneDrive, SharePoint, Teams, Entra ID (bu belge)
ZeroVault	Immutable Veeam backup'ları için S3 uyumlu storage

Kimler için?

- Microsoft 365 veri koruması ve kurtarmasından sorumlu IT ve mesajlaşma ekipleri
- 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 storage'ınızı getirin)
- İş verileri için GDPR / KVKK / DORA / ISO 27001 yükümlülükleri olan ekipler

2. Workload Kapsamı Kataloğu

Her Microsoft 365 workload'ı, kendi semantiği ve kendi restore yoluyla backup'lanır:

Workload	Neler korunuyor	Restore
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 restore; EML/ZIP dışı aktarımı; işlem öncesi önizleme; varsayılan olarak veri kaybına yol açmayan (non-destructive).
OneDrive	Sürücü hiyerarşisi, dosyalar, klasörler, sürüm geçmişi ve izinler / ACL'ler.	Point-in-time restore ve ACL kurtarma; cerrahi hassasiyette ransomware kurtarması için <i>restore-only-if-hash-differs</i> modu.
SharePoint Online	Belge kitaplıkları ve özel sütun değerleri dahil, liste tabanlı yapılandırılmış içerik.	Orijinal veya alternatif bir siteye meta verileri koruyan restore; hash tabanlı diferansiyel kurtarma.
Microsoft Teams	Standart, özel ve paylaşımlı kanallar ile 1:1 ve grup sohbetleri.	Yapılandırılmış dışı aktarım paketleri olarak restore edilir (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 & Storage

Bağlantı	Modern kimlik doğrulama ve bir uygulama kaydı (app registration) ile Microsoft Graph; legacy API yok.
Kurulum	Web konsoluna sahip, container tabanlı SaaS platformu; kendinizin işleteceği bir backup altyapısı yok.
Storage (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 incremental 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 storage'iniz. Backup'lar, sahip olduğunuz storage 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 storage'inizi getirin: S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Hizmet başına workload-aware restore semantiği
- Delta öncelikli incremental senkronizasyon
- Item-level ve toplu restore
- Her restore'dan önce önizleme
- Ransomware hash-diferansiyel kurtarma (OneDrive & SharePoint)
- Varsayılan olarak veri kaybına yol açmayan (non-destructive) restore'lar
- RBAC, SSO (SAML / OIDC) ve MFA
- Audit loglama ve SIEM dışı aktarımı
- Görevler ayrılığı ve just-in-time restore erişimi

5. Neler Elde Edersiniz

- 1 Zamanlanmış, workload-aware backup'lara sahip bağılı bir Microsoft 365 tenant'ı
- 2 Sahip olduğunuz ve kontrol ettiğiniz storage'da şifreli backup kopyaları (BYOS)
- 3 Workload'a göre gözetme, arama, önizleme ve kurtarma için bir restore gezgini
- 4 OneDrive ve SharePoint için ransomware farkındalıklı diferansiyel kurtarma
- 5 Entra ID nesneleri için üç yollu kimlik kurtarma
- 6 Governance için erişim kontrolü, audit loglama ve SIEM dışı aktarımı

6. Güvenlik & Uyumluluk

Çerçeve	Stork365 nasıl yardımcı olur
GDPR	Net bir restore hakkına sahip, bağımsız ve şifreli bir kopya; veriler kontrolünüzdeki storage'da kalır.
KVKK	Kendi storage'inızı getirme yoluyla veri konumlandırma; erişim loglama 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 audit loglama.
SOC 2	Backup ve restore genelinde güvenlik, erişilebilirlik ve gizlilik kontrolleri.

7. Sonraki Adım

Bir Stork365 denemesi başlatın. Tenant'inızı bağlayın, storage'inızı seçin ve ilk backup'ınızın çalışmasını izleyin. Stork365, Microsoft'un yerleşik retention özelliğinin korumadıklarını korur.
www.backupsec.com · info@backupsec.com · BackupSec