

Stork365

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

“Twoje dane Microsoft 365, Twój storage.” Odzyskaj skrzynkę pocztową, plik lub tożsamość, bez uzależnienia od jednego dostawcy (vendor lock-in).

Usługa	Stork365: Backup & odtwarzanie Microsoft 365
Główny obszar	Backup uwzględniający specyfikę obciążeń Exchange, OneDrive, SharePoint, Teams i Entra ID do storage, który kontrolujesz
Wersja	1.0
Data	Czerwiec 2026
Zakres	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Dostawca	BackupSec

1. Czym jest Stork365?

Stork365 to chmurowa usługa backup dla Microsoft 365. Łączy się z Twoim tenantem za pośrednictwem Microsoft Graph i tworzy backup Exchange Online, OneDrive, SharePoint Online, Microsoft Teams oraz Entra ID, każdego z własną, uwzględniającą specyfikę obciążenia semantyką odtwarzania, a nie jako płaski rzut plików. Zaszzyfrowane kopie są zapisywane w storage, który wybierasz i kontrolujesz (BYOS), a Ty odzyskujesz dokładnie to, czego potrzebujesz (wiadomość, plik, witrynę lub tożsamość) z jednej konsoli. Stork365 stanowi warstwę ochrony Microsoft 365 rodziny BackupSec, obok monitorowania ZeroMON, doradztwa ZeroTAM, testów penetracyjnych ZeroPEN oraz ZeroVault, pamięci zgodnej z S3 dla niezmiennych kopii zapasowych Veeam.

Dlaczego Stork365? Natywna retencja Microsoftu to nie backup. Usunięte elementy wygasają, ransomware szyfruje zsynchronizowane pliki, a tożsamości wyłączonych użytkowników znikają. Stork365 przechowuje niezależną, zaszzyfrowaną kopię w storage, który kontrolujesz, możliwą do odtworzenia element po elemencie, długo po wygaśnięciu własnych koszy Microsoftu.

Rodzina BackupSec

Stork365 działa wspólnie z pozostałymi produktami rodziny BackupSec:

Usługa	Rola
ZeroMON	Monitorowanie backupu & obserwowalność: widoczność w czasie rzeczywistym w całym środowisku Veeam
ZeroTAM	Doradztwo eksperckie, opieka nad klientem & wsparcie w sytuacjach kryzysowych
ZeroPEN	Testy penetracyjne backupu & dowód odtwarzalności: testuje backupy tak, jak zrobiłby to atakujący
Stork365	Backup & odtwarzanie Microsoft 365: Exchange, OneDrive, SharePoint, Teams, Entra ID (niniejszy dokument)
ZeroVault	Pamięć zgodna z S3 dla niezmiennych kopii zapasowych Veeam

Dla kogo?

- Zespoły IT i zespoły ds. poczty odpowiedzialne za ochronę i odtwarzanie danych Microsoft 365
- Dostawcy MSP i usługodawcy zarządzający wielodostępnymi (multi-tenant) środowiskami Microsoft 365
- Zespoły ds. bezpieczeństwa i ryzyka egzekwujące niezależną, zaszzyfrowaną kopię backup
- Organizacje z wymogami dotyczącymi rezydencji lub suwerenności danych (bring your own storage)
- Zespoły objęte obowiązkami GDPR / KVKK / DORA / ISO 27001 w zakresie danych biznesowych

2. Katalog zakresu obciążeń

Każde obciążenie Microsoft 365 jest zabezpieczane z własną semantyką i własną ścieżką odtwarzania:

Obciążenie	Co jest chronione	Odtwarzanie
Exchange Online	Poczta, kalendarz, kontakty i zadania dla podstawowych i współdzielonych skrzynek pocztowych; pełna wierność MIME z synchronizacją delta.	Odtwarzanie na poziomie elementu lub skrzynki do oryginalnej lub alternatywnej skrzynki; eksport EML/ZIP; podgląd przed zatwierdzeniem; domyślnie niedestrukcyjne.
OneDrive	Hierarchia dysku, pliki, foldery, historia wersji oraz uprawnienia / ACL.	Odtwarzanie do punktu w czasie i przywracanie ACL; tryb <i>restore-only-if-hash-differs</i> do precyzyjnego odtwarzania po ataku ransomware.
SharePoint Online	Biblioteki dokumentów i strukturalna zawartość oparta na listach, w tym wartości kolumn niestandardowych.	Odtwarzanie z zachowaniem metadanych do oryginalnej lub alternatywnej witryny; różnicowe odtwarzanie oparte na hashach.
Microsoft Teams	Kanały standardowe, prywatne i współdzielone oraz czaty 1:1 i grupowe.	Odtwarzane jako strukturalne pakiety eksportu (JSON z manifestami); brak odtwarzania kanałów na żywo (ograniczenie Graph API, o którym mówimy ucziwie).
Entra ID	Użytkownicy, grupy, aplikacje i jednostki usługi (service principals) wraz z członkostwem i własnością.	Trzy ścieżki: odzyskiwanie z soft-delete (30 dni), pełne odtworzenie obiektu lub odtworzenie właściwości przez PATCH; członkostwo w grupach wyłącznie w trybie dodawania.

3. Wdrożenie & storage

Połączenie	Microsoft Graph z nowoczesnym uwierzytelnianiem i rejestracją aplikacji; bez starszych API.
Wdrożenie	Skonteneryzowana platforma SaaS z konsolą webową; brak infrastruktury backup do samodzielnego utrzymywania.
Storage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV lub lokalny system plików.
Szyfrowanie	Zaszyfrowany ładunek zapisywany przez Kopię; klucze szyfrowania pozostają pod Twoją kontrolą.
Harmonogramowanie	Zautomatyzowane backupy według harmonogramu z przyrostową synchronizacją delta-first.
Zakres chmury	Globalny komercyjny Microsoft 365 i Entra ID. GCC, GCC High, DoD oraz 21Vianet nie są objęte zakresem premiery.

Twoje dane, Twój storage. Backupy są zapisywane na kontach storage, które należą do Ciebie, nigdy w repozytorium uzależnionym od dostawcy. Ponieważ klucze szyfrowania pozostają u Ciebie, kopia Twoich danych Microsoft 365 nigdy nie musi opuszczać Twojej jurysdykcji.

4. Kluczowe funkcje

- Bring your own storage: S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Semantyka odtwarzania uwzględniająca specyfikę obciążenia dla każdej usługi
- Przyrostowa synchronizacja delta-first
- Odtwarzanie na poziomie elementu i zbiorcze
- Podgląd przed każdym odtwarzaniem
- Odtwarzanie różnicowe oparte na hashach po ataku ransomware (OneDrive & SharePoint)
- Domyślnie niedestrukcyjne odtwarzanie
- RBAC, SSO (SAML / OIDC) i MFA
- Rejestrowanie audytu i eksport do SIEM
- Rozdział obowiązków i dostęp do odtwarzania w modelu just-in-time

5. Co otrzymujesz

- 1 Podłączony tenant Microsoft 365 z zaplanowanymi backupami uwzględniającymi specyfikę obciążeń
- 2 Zaszyfrowane kopie backup w storage, który posiadasz i kontrolujesz (BYOS)
- 3 Eksplorator odtwarzania do przeglądania, wyszukiwania, podglądu i odzyskiwania według obciążeń
- 4 Różnicowe odtwarzanie z uwzględnieniem ransomware dla OneDrive i SharePoint
- 5 Trójścieżkowe odtwarzanie tożsamości dla obiektów Entra ID
- 6 Kontrola dostępu, rejestrowanie audytu i eksport do SIEM na potrzeby governance

6. Bezpieczeństwo & zgodność

Framework	Jak pomaga Stork365
GDPR	Niezależna, zaszyfrowana kopia z jasnym prawem do odtwarzania; dane pozostają w storage, który kontrolujesz.
KVKK	Rezydencja danych dzięki bring-your-own-storage, z rejestrowaniem dostępu i rozdziałem ról.
DORA	Odporność ICT: odtwarzalne, niezależne backupy krytycznych danych Microsoft 365.
ISO 27001	Kontrola dostępu, szyfrowanie i rejestrowanie audytu zgodne z zabezpieczeniami Annex A.
SOC 2	Mechanizmy kontroli bezpieczeństwa, dostępności i poufności w całym procesie backupu i odtwarzania.

7. Następny krok

Rozpocznij okres próbny Stork365. Podłącz swój tenant, wybierz storage i obserwuj, jak wykonuje się pierwszy backup. Stork365 chroni to, czego nie chroni natywna retencja Microsoftu.

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