

Zero365

Microsoft 365 백업 & 복원 — Exchange, OneDrive, SharePoint, Teams & Entra ID

“당신의 Microsoft 365 데이터, 당신의 스토리지.” — 벤더 종속 없이 메일박스, 파일 또는 ID를 복구하십시오.

서비스	Zero365 — Microsoft 365 백업 & 복원
중점 영역	직접 제어하는 스토리지로 Exchange, OneDrive, SharePoint, Teams 및 Entra ID를 워크로드 인식 방식으로 백업
버전	1.0
날짜	2026년 6월
적용 범위	GDPR · KVKK · DORA · ISO 27001 · SOC 2
제공자	BackupSec

1. Zero365란?

Zero365는 Microsoft 365를 위한 클라우드 백업 서비스입니다. Microsoft Graph를 통해 테넌트에 연결하여 Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Entra ID를 백업하며 — 각각 단순한 파일 덤프가 아닌 고유의 워크로드 인식 복원 방식을 갖습니다. 암호화된 사본은 직접 선택하고 제어하는 스토리지(BYOS)에 기록되며, 단일 콘솔에서 메시지, 파일, 사이트 또는 ID 등 필요한 것을 정확히 복구할 수 있습니다. Zero365는 BackupSec 제품군의 Microsoft 365 보호 계층으로, ZeroMON 모니터링, ZeroTAM 자문, ZeroPEN 침투 테스트, ZeroVault 불변 스토리지와 함께합니다.

왜 Zero365인가? Microsoft의 기본 보존은 백업이 아닙니다. 삭제된 항목은 시간이 지나 사라지고, 랜섬웨어는 동기화된 파일을 암호화하며, 오프보딩된 ID는 사라집니다. Zero365는 직접 제어하는 스토리지에 독립적이고 암호화된 사본을 보관하여 — Microsoft 자체 휴지통이 만료된 후에도 오랫동안 항목 단위로 복구할 수 있습니다.

BackupSec 제품군

Zero365는 나머지 BackupSec 제품군과 함께 작동합니다:

서비스	역할
ZeroMON	백업 모니터링 & 옹저버빌리티 — Veeam 환경 전반의 실시간 가시성
ZeroTAM	전문가 자문, 어카운트 관리 & 위기 대응 지원
ZeroPEN	백업 침투 테스트 & 복구 증명 — 공격자의 방식으로 백업을 테스트
Zero365	Microsoft 365 백업 & 복원 — Exchange, OneDrive, SharePoint, Teams, Entra ID (본 문서)
ZeroVault	Veeam을 위한 불변 클라우드 스토리지 — 삭제하거나 암호화할 수 없는 마지막 사본

누구를 위한 제품인가?

- Microsoft 365 데이터 보호 및 복구를 담당하는 IT 및 메시징 팀
- 멀티테넌트 Microsoft 365 환경을 관리하는 MSP 및 서비스 제공업체
- 독립적이고 암호화된 백업 사본을 강제하는 보안 및 리스크 팀
- 데이터 레지던시 또는 주권 요구사항이 있는 조직(자체 스토리지 사용)
- 비즈니스 데이터에 대한 GDPR / KVKK / DORA / ISO 27001 의무가 있는 팀

2. 워크로드 적용 범위 카탈로그

모든 Microsoft 365 워크로드는 고유의 방식과 고유의 복원 경로로 백업됩니다:

워크로드	보호 대상	복원
Exchange Online	기본 및 공유 메일박스의 메일, 캘린더, 연락처 및 작업 — 델타 동기화와 함께 완전한 MIME 충실도.	원본 또는 대체 메일박스로의 항목 단위 또는 메일박스 단위 복원; EML/ZIP 내보내기; 커밋 전 미리보기; 기본적으로 비파괴적.
OneDrive	드라이브 계층 구조, 파일, 폴더, 버전 기록 및 권한 / ACL.	특정 시점 복원 및 ACL 복구; 정밀한 랜섬웨어 복구를 위한 <i>해시가 다를 때만 복원</i> 모드.
SharePoint Online	사용자 지정 열 값을 포함한 문서 라이브러리 및 목록 기반 구조화 콘텐츠.	원본 또는 대체 사이트로의 메타데이터 보존 복원; 해시 기반 차등 복구.
Microsoft Teams	표준, 비공개 및 공유 채널과 1:1 및 그룹 채팅.	구조화된 내보내기 번들(매니페스트가 포함된 JSON)로 복원; 라이브 채널 재생은 불가 — 저희가 솔직히 밝히는 Graph API의 제약입니다.
Entra ID	멤버십 및 소유권을 포함한 사용자, 그룹, 애플리케이션 및 서비스 주체.	세 가지 경로: 소프트 삭제 복구(30 days), 전체 개체 재생성, 또는 PATCH를 통한 속성 재적용; 그룹 멤버십은 추가 전용.

3. 배포 & 스토리지

연결	최신 인증 및 앱 등록을 사용하는 Microsoft Graph — 레거시 API 없음.
배포	웹 콘솔을 갖춘 컨테이너화된 SaaS 플랫폼; 직접 운영할 백업 인프라 없음.
스토리지 (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV 또는 로컬 파일 시스템.
암호화	Kopia를 통해 기록되는 암호화된 페이로드; 암호화 키는 사용자의 제어 하에 유지됩니다.
스케줄링	델타 우선 증분 동기화를 통한 자동 예약 백업.
클라우드 범위	글로벌 커머셜 Microsoft 365 및 Entra ID. GCC, GCC High, DoD 및 21Vianet은 출시 범위에 포함되지 않습니다.

당신의 데이터, 당신의 스토리지. 백업은 사용자가 소유한 스토리지 계정에 기록되며 — 벤더에 종속된 리포지토리는 결코 사용되지 않습니다. 암호화 키가 사용자에게 유지되므로, Microsoft 365 데이터의 사본은 관할 구역을 벗어날 필요가 없습니다.

4. 주요 기능

- 자체 스토리지 사용 — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- 서비스별 워크로드 인식 복원 방식
- 델타 우선 증분 동기화
- 항목 단위 및 일괄 복원
- 모든 복원 전 미리보기
- 랜섬웨어 해시 차등 복구 (OneDrive & SharePoint)
- 기본적으로 비파괴적 복원
- RBAC, SSO (SAML / OIDC) 및 MFA
- 감사 로깅 및 SIEM 내보내기
- 직무 분리 및 적시(just-in-time) 복원 접근

5. 제공 항목

- 1 예약된 워크로드 인식 백업이 연결된 Microsoft 365 테넌트
- 2 소유하고 제어하는 스토리지의 암호화된 백업 사본(BYOS)
- 3 워크로드별로 탐색, 검색, 미리보기 및 복구할 수 있는 복원 탐색기
- 4 OneDrive 및 SharePoint를 위한 랜섬웨어 인식 차등 복구
- 5 Entra ID 개체를 위한 3경로 ID 복구
- 6 거버넌스를 위한 접근 제어, 감사 로깅 및 SIEM 내보내기

6. 보안 & 컴플라이언스

프레임워크	Zero365가 지원하는 방식
GDPR	명확한 복원 권한을 갖춘 독립적이고 암호화된 사본; 데이터는 직접 제어하는 스토리지에 유지됩니다.
KVKK	자체 스토리지 사용을 통한 데이터 레지던시, 접근 로깅 및 역할 분리 포함.
DORA	ICT 복원력 — 복구 가능하고 독립적인 중요 Microsoft 365 데이터 백업.
ISO 27001	Annex A 통제에 부합하는 접근 제어, 암호화 및 감사 로깅.
SOC 2	백업 및 복원 전반의 보안, 가용성 및 기밀성 통제.

7. 다음 단계

Zero365 체험을 시작하십시오. 테넌트를 연결하고 스토리지를 선택한 후 첫 백업이 실행되는 것을 확인하십시오. Zero365는 Microsoft의 기본 보존이 보호하지 못하는 것을 보호합니다.
www.backupsec.com · info@backupsec.com · BackupSec