

Zero365

Microsoft 365 备份 & 恢复 — Exchange、OneDrive、SharePoint、Teams & Entra ID

“您的 *Microsoft 365* 数据，您的存储。” — 恢复一个邮箱、一个文件或一个身份，无需担心供应商锁定。

服务	Zero365 — Microsoft 365 备份 & 恢复
聚焦	面向 Exchange、OneDrive、SharePoint、Teams 和 Entra ID 的工作负载感知备份，写入由您掌控的存储
版本	1.0
日期	2026年6月
覆盖范围	GDPR · KVKK · DORA · ISO 27001 · SOC 2
提供方	BackupSec

1. 什么是 Zero365？

Zero365 是面向 Microsoft 365 的云备份服务。它通过 Microsoft Graph 连接到您的租户，并备份 Exchange Online、OneDrive、SharePoint Online、Microsoft Teams 和 Entra ID — 每一项都具有各自的工作负载感知恢复语义，而非简单的平面文件转储。加密副本会写入由您选择并掌控的存储 (BYOS)，您可以精准恢复所需内容 — 一条消息、一个文件、一个站点或一个身份 — 全部在单一控制台中完成。Zero365 是 BackupSec 家族的 Microsoft 365 保护层，与 ZeroMON 监控、ZeroTAM 咨询、ZeroPEN 渗透测试和 ZeroVault 不可变存储并肩协作。

为什么选择 Zero365？ Microsoft 的原生保留并不等于备份。已删除的项目会过期清除，勒索软件会加密已同步的文件，离职员工的身份也会消失。Zero365 会在由您掌控的存储中保留一份独立的加密副本 — 可逐项恢复，即使在 Microsoft 自身的回收站早已过期很久之后依然有效。

BackupSec 家族

Zero365 与 BackupSec 家族的其余成员协同工作：

服务	角色
ZeroMON	备份监控 & 可观测性 — 全面实时洞察您的 Veeam 环境
ZeroTAM	专家咨询、客户管理 & 危机支持
ZeroPEN	备份渗透测试 & 恢复验证 — 以攻击者的方式测试备份
Zero365	Microsoft 365 备份 & 恢复 — Exchange、OneDrive、SharePoint、Teams、Entra ID（本文档）
ZeroVault	面向 Veeam 的不可变云存储 — 一份无法被删除或加密的最后副本

适用于谁？

- 负责 Microsoft 365 数据保护与恢复的 IT 和消息处理团队
- 管理多租户 Microsoft 365 环境的 MSP 和服务提供商
- 强制实施独立加密备份副本的安全与风险团队
- 具有数据驻留或数据主权要求的组织（自带存储）
- 对业务数据负有 GDPR / KVKK / DORA / ISO 27001 合规义务的团队

2. 工作负载覆盖目录

每一种 Microsoft 365 工作负载都以各自的语义和各自的恢复路径进行备份：

工作负载	受保护内容	恢复
Exchange Online	主邮箱和共享邮箱的邮件、日历、联系人和任务 — 完整保真的 MIME，并支持增量同步。	可将项目级或邮箱级内容恢复到原始邮箱或备用邮箱；支持 EML/ZIP 导出；提交前预览；默认非破坏性。
OneDrive	驱动器层次结构、文件、文件夹、版本历史以及权限 / ACL。	时间点恢复和 ACL 恢复；仅在哈希不同时恢复模式，用于精准的勒索软件恢复。
SharePoint Online	文档库和基于列表的结构化内容，包括自定义列的值。	保留元数据地恢复到原始站点或备用站点；基于哈希的差异恢复。
Microsoft Teams	标准频道、私密频道和共享频道，以及 1:1 和群组聊天。	以结构化导出包（带清单的 JSON）形式恢复；不支持实时频道重放 — 这是 Graph API 的限制，我们如实说明。
Entra ID	用户、组、应用程序和服务主体，包含成员关系和所有权。	三种途径：软删除恢复（30 天）、完整对象重建，或通过 PATCH 进行属性重放；组成员关系仅支持新增。

3. 部署 & 存储

连接	采用新式身份验证和应用注册的 Microsoft Graph — 不使用旧版 API。
部署	带有 Web 控制台的容器化 SaaS 平台；无需自行运行备份基础设施。
存储 (BYOS)	AWS S3、Cloudflare R2、Azure Blob、Google Cloud Storage、SFTP、WebDAV 或本地文件系统。
加密	通过 Kopia 写入加密载荷；加密密钥始终由您掌控。
调度	自动化的计划备份，采用增量优先的增量同步。
云范围	全球商业版 Microsoft 365 和 Entra ID。GCC、GCC High、DoD 和 21Vianet 不在首发范围内。

您的数据，您的存储。 备份会写入由您拥有的存储账户 — 绝非受供应商锁定的存储库。由于加密密钥始终由您保管，您的 Microsoft 365 数据副本无需离开您所在的司法管辖区。

4. 核心功能

- 自带存储 — S3、R2、Azure Blob、GCS、SFTP、WebDAV
- 针对每项服务的工作负载感知恢复语义
- 增量优先的增量同步
- 项目级和批量恢复
- 每次恢复前预览
- 勒索软件哈希差异恢复 (OneDrive & SharePoint)
- 默认非破坏性恢复
- RBAC、SSO (SAML / OIDC) 和 MFA
- 审计日志记录和 SIEM 导出
- 职责分离和即时恢复访问

5. 您将获得

- 1 一个已连接的 Microsoft 365 租户，具备计划的、工作负载感知的备份
- 2 存放在由您拥有并掌控的存储 (BYOS) 中的加密备份副本
- 3 一个恢复浏览器，可按工作负载浏览、搜索、预览和恢复
- 4 针对 OneDrive 和 SharePoint 的勒索软件感知差异恢复
- 5 针对 Entra ID 对象的三途径身份恢复
- 6 用于治理的访问控制、审计日志记录和 SIEM 导出

6. 安全 & 合规

框架	Zero365 如何提供帮助
GDPR	一份独立的加密副本，具有明确的恢复权利；数据保留在由您掌控的存储中。
KVKK	通过自带存储实现数据驻留，并配备访问日志记录和角色分离。
DORA	ICT 韧性 — 对关键 Microsoft 365 数据进行可恢复的独立备份。
ISO 27001	与 Annex A 控制项相符的访问控制、加密和审计日志记录。
SOC 2	贯穿备份与恢复的安全性、可用性和保密性控制。

7. 下一步

开始 Zero365 试用。 连接您的租户、选择您的存储，然后见证您的第一次备份运行。Zero365 保护 Microsoft 原生保留所无法保护的内容。

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