Barracuda Cloud-to-Cloud Backup

Easy-to-use, cloud-first backup for your Microsoft 365 data

Microsoft recommends you use third-party backup for your Microsoft 365 data. A good backup with quick recovery is critical after a ransomware attack or accidental deletion. Restoring sites, entire folders, or mailboxes can be a tedious, manual process — and if the data you need is mission-critical, that means costly downtime you can't afford.

Barracuda Cloud-to-Cloud Backup is an easy-to-use cloud-first solution that provides comprehensive, cost-effective, scalable backup and recovery for your Microsoft 365 data, including including Teams, Exchange Online, SharePoint, OneDrive and OneNote.

Easy to use

A newly redesigned, globally accessible user interface makes it fast and easy to find and recover data. Very fast search and filter options make restoring data back to your organization as easy as possible. And you can go from sign-up to running your first backup in five minutes. Complete visibility and reporting of source backup status, health monitoring, and storage statistics make it easy to understand backup status, while the audit log and email alerts keep you informed about the details of every action.

Flexible, comprehensive Microsoft 365 support

Barracuda Cloud-to-Cloud Backup gives you the flexibility to restore Teams, Exchange, SharePoint, OneDrive, and OneNote data either fully or with highly granular detail. Full SharePoint support means you can backup and restore everything in SharePoint, including different site templates, custom lists, permissions, and metadata.

Cloud-first backup

Cloud-to-Cloud Backup is a SaaS solution. There's no software or hardware for you to manage. Because your Microsoft 365 data is already in the cloud, retaining your encrypted backup files in the network means better performance and instant scalability. With three external copies of your backup files for redundancy and security, backing up to the cloud just makes sense. And you can sign up and start running your first backup in just five minutes.

DATA PROTECTION

Features

Ease of use

- Flexible full or granular restore of Teams, Exchange, SharePoint, OneDrive, and OneNote
- Easy to deploy, manage, and use
  - All-inclusive, per-user licensing
  - Sign up to running first backup in five minutes
- Customizable backup selection using Azure AD groups, M365 Groups, or Distribution Lists
- Intuitive UI
- Fast and easy to find and recover data
- Point-in-time recovery
- Scheduled or on-demand backup
- Multi-factor authentication
- Five levels of role-based access control — you decide who can back up, restore, or view data
- Barracuda Cloud storage is SSAE Type II certified
- Support for files encrypted using Azure Information Protection (AIP)
- Multi-tenant support
- Available in Japanese, French, Italian, German, Spanish, and English localized versions

Flexible recovery

- Protect Teams, Exchange Online, SharePoint Online and OneDrive for Business
- Unlimited storage and retention — retain all your data for as long as you need
- Flexible Recovery
  - Restore any data to original location, alternate location, or export as needed
  - Restore email to another user
  - Retain data for inactive users (ex-employees)
  - File-revision recovery — recover specific file revisions as needed
  - Delayed cloud purging for ransomware protection
- Full SharePoint support
  - Back-up and restore everything in SharePoint, from all different site templates, permissions, custom lists, and metadata.
  - Restore SharePoint libraries, lists, and documents to other SharePoint sites
- Back-up and restore Archive & Recoverable items in Exchange
- Granular reporting
  - Detailed reporting for backups and restores
  - Audit-log reporting for all actions across your account
  - Configurable email notification — monitor your account through customizable email reports

Cloud native

- Full Software-as-a-Service solution — no hardware, software, or patches to manage
- Instant scalability
- 13 regional storage locations available worldwide to meet data storage and residency requirements
- Independent SOC2 audited and certified annually
- User data is encrypted in transit (TLS) and at rest using industry standard AES 256* encryption
- Retain multiple external copies of backed up data