DELL Technologies

APEX

TOP REASONS

Top reasons to choose APEX Backup Services to protect Microsoft 365

APEX Backup Services for SaaS Apps provides a comprehensive, secure and scalable cloud-based solution that cost-effectively protects data for Microsoft 365, along with other cloud workloads such as other SaaS applications, endpoints, and hybrid workloads, all from a single point of control. With APEX Backup Services for SaaS Apps, you can rest assured that critical data protection gaps are addressed and your data is recoverable from key data risks like human errors, internal threats, and ransomware. The solution also helps your organization be compliant with regulation for data privacy, retention, and residency as well as legal hold and eDiscovery. Our goal is to help your organization protect end-user productivity and ensure business continuity.

1 | Data loss and corruption

Microsoft leaves backup and restore responsibilities in the hands of their customers, and data loss is always a risk.Your data is prone to human error such as accidental file deletion and overwrites by employees and their collaborators and potentially deletion of an entire SharePoint site. Data can also be corrupted by OneDrive synchronization and third-party apps.

APEX Backup Services enables you to quickly recovery after deletion, overwrites, and data corruption

- Ongoing automatic backups of data
- Flexible and granular recovery with unlimited “time travel”
- Easy-to-use self-service restore or IT-led recovery
- Many restore options, including mailbox, individual file or bulk recovery, “in-place,” “as a copy” or “point in time” recovery, as well as recovery outside Microsoft 365

2 | Ransomware protection

Microsoft 365 natively only allows recovery from versions at an individual file level. In the worst case scenario, if the attack started outside the Microsoft retention window, there is no recourse or means to return to clean data. Only a third-party solution can quickly recover your system to clean data and meet your business continuity SLAs.

APEX Backup Services quickly recovers your data and returns users to full productivity

- Data retention enables full and quick recovery to pre-attack “point in time” data
- Recover in minutes through single-click bulk-recovery and meet your SLAs
- Flexible recovery options, including “in place” or “as a copy,” or “outside” Microsoft 365 using bulk, flexible, and granular options as needed
- Data isolation through an immutable and independent copy, stored in a different environment from Microsoft 365, to comply with disaster recovery requirement

3 | Insider threats

Microsoft cannot identify malicious Microsoft 365 user actions and when an employee leaves the company their Microsoft 365 account is suspended. IT cannot easily access the data to assess and undo potential damage and archiving the departing employee accounts does not retain previously deleted data. Therefore, you need a third-party data protection solution that allows you to restore data from a point in time.

APEX Backup Services helps you detect, assess, and quickly recover from data loss

- Employee investigations of prior activities adds insights
- Data off-boarding to departing employee's manager
- Audit logs monitor user activity over a selected period of time

4 | Data retention and compliance

Data retention is a key component in many organizations' data governance policies. Microsoft Business editions have a data retention policy limited to 30-93 days, depending on your licensing tier and use case. Data retention differs for Microsoft Exchange, SharePoint, OneDrive and Teams.

- Exchange: Data is purged from the recycle bin at 28 days and cannot be restored to a point in time.
- SharePoint Online: Document library or lists are purged from the recycle bin at 93 days.
- OneDrive for Business: Data is purged from the recycle bin at 93 days. It is also possible for data to be overwritten and the original data cannot be recovered.
- Teams: Message and file data, channels and Teams data are recoverable for 30 days after deletion. However, the process is tedious and manual.

Additionally, Microsoft 365 only offers 90 days maximum audit history, which may be insufficient. And not to mention that Microsoft 365 data is retained in the same primary environment, thus not providing sufficient data isolation to comply with disaster recovery requirements. Such data retention gaps expose your organization and puts you at risk of non-compliance with government and organization policies.

APEX Backup Services enables compliance with data retention to meet your organization's data governance requirements

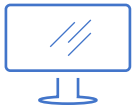
- Employee investigations of prior activities adds insights
- Data off-boarding to departing employee's manager
- Audit logs monitor user activity over a selected period of time

5 | Legal hold and eDiscovery

Microsoft Business editions do not offer legal hold capabilities while common Microsoft Enterprise plans do offer limited legal hold capabilities for Microsoft 365 data only. Legal hold capabilities, if included in Microsoft 365, do not integrate with eDiscovery third-party tools. Data retention gaps may also impede full compliance, such as departing employees or intentional deletion. Therefore, only a third-party data protection solution can support end-to-end legal hold and eDiscovery requirements across enterprise data workloads, with no disruption to employees.

APEX Backup Services provides support for legal hold and eDiscovery requests, not only for Microsoft 365, but across supported SaaS applications and endpoint devices

- Centralized and automated data collection, with no disruption to employees
- Bulk custodian holds, faster export and support for multiple file formats
- Data retention capabilities allow unlimited "time travel" and data collection from departing employees or despite intentional deletions
- Integrated with third-party eDiscovery tools and offers speedy download time



Learn more about APEX Backup Services

Contact a Dell Technologies Expert

DELL Technologies

APEX