CARBONITE an opentext company | WEBROOT an opentext company

Carbonite® Backup for Microsoft 365

Why it's necessary to back up Microsoft collaboration tools

Microsoft 365 is a powerful suite of business productivity applications. But like any cloud platform, it's not immune to data loss. Microsoft does not bear responsibility for the protection and retention of data. While Microsoft ensures the availability of its infrastructure, it recommends that customers assume responsibility for protecting the data in its suite of cloud applications. Beyond Microsoft's recommendations, organizations using Microsoft 365 often have their own reasons for deploying backup for cloud data.

Regulations, compliance and data preservation

Whether dictated by federal, state or industry authorities, regulatory mandates are pervasive across all sectors of the economy. Data handling practices are under scrutiny as regulators impose stricter standards and higher fines for falling out of compliance.

Since data preservation practices and procedures are subject to regulatory guidelines, organizations have a need to deploy and enforce policies more consistently across their systems. Uniform policies for data retention, recoverability, rectification and deletion are necessary for businesses of all sizes and across all industries. These requirements apply to data whether it's stored on-premises or in a cloud platform like Microsoft 365.

Policy creation and deployment

Control over backup and retention policy has not historically been a problem with on-prem systems. But since more organizations are migrating to the cloud, they've been willing to forego some of the control over backup and retention policy because they lack purpose-built tools for backing up cloud environments. In an ideal scenario, businesses would have the same granular control over backup and retention policies in the cloud as they do for on-prem systems. Carbonite® Backup for Microsoft 365 is designed to do exactly this.

Mitigation of ransomware and other external threats

Microsoft apps are also not immune to ransomware or other malicious external threats. When files become corrupt, they're automatically synced in OneDrive. Modern malware often stays hidden while it propagates across different file systems. The time it takes the business to discover the existence of the malware often exceeds the default retention policy, leaving no safe recovery point to restore from.

Common causes of data loss in Microsoft 365 include:

- Accidental file deletion
- File overwriting
- Inadequate retention policy
- Malicious insiders
- External threats

Security rollback and file history

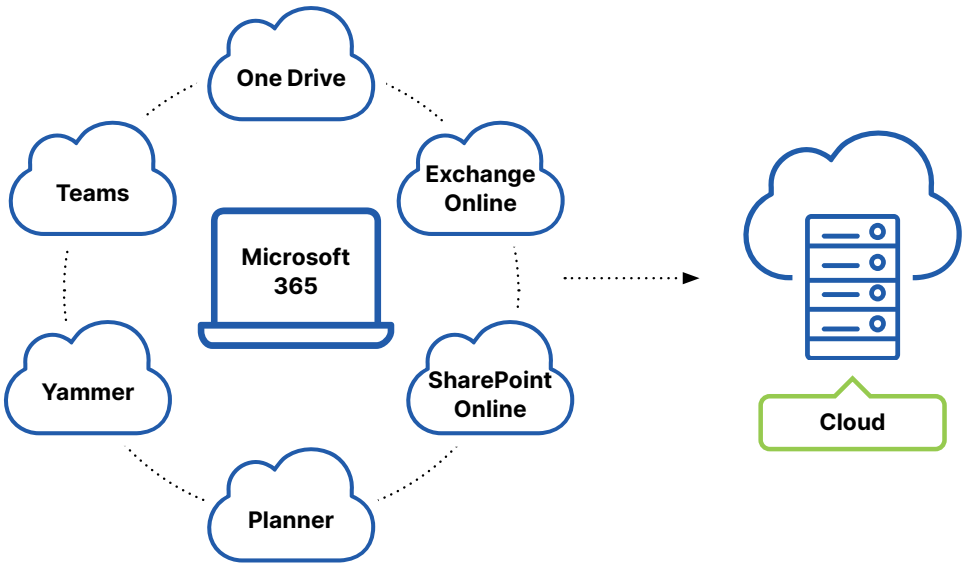
Collaboration tools only work when the appropriate stakeholders for a project or task share access privileges within the application where the work is being performed. In a data loss scenario, restoring security permissions can often be a time-consuming, manual and error-prone process. This is in addition to the time it takes to recover the lost files and folders or site collection. The ability to automatically restore security permissions can save significant time and resources when performing disaster recovery mitigation.

Another challenge when performing disaster recovery is restoring from the most desirable recovery point based on the file history. IT administrators often resort to recovering prior versions from the recycle bin – an improvised approach that doesn't guarantee full recovery. Malicious insiders, in fact, often erase files from the recycle bin for maximum destructive impact. Carbonite® Backup for Microsoft 365 includes file history with customizable retention settings to ensure relevant recovery points are available.

Carbonite® Backup for Microsoft 365

Disaster recovery of cloud data presents many of the same challenges as on-premises scenarios. Since disasters come in different forms, IT administrators will always need a range of options for recovering precisely the data they need to recover. Recovering too much data can be just as problematic as not being able to recover enough data.

Carbonite® Backup for Microsoft 365 gives administrators the tools they need to recover as much or as little data as necessary to mitigate a data loss event. This includes granular recovery of files and folders, full site recovery as well as security privileges and file history.



Carbonite® Backup for Microsoft 365 – Rapid recovery for Microsoft cloud apps

Complete protection:
Protect the entire Microsoft 365 suite – including SharePoint, OneDrive, Email and Teams.

Rapid recovery:
Perform site-level rollback or recover individual items including mailboxes, conversations and files.

Backup and retention:
Run automatic backups up to four times per day.

Central management:
Simplify administrative tasks with legal hold, audit reporting, role-based access and exports.

Data loss prevention:
Protect against data loss threats including human error, hardware failure and ransomware.

Professional support:
Enjoy on-boarding and recovery support from experts, 24×7.

Contact us to learn more – Carbonite US

Phone: 877-542-8637

Email: carb-data_protection_sales@opentext.com

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.