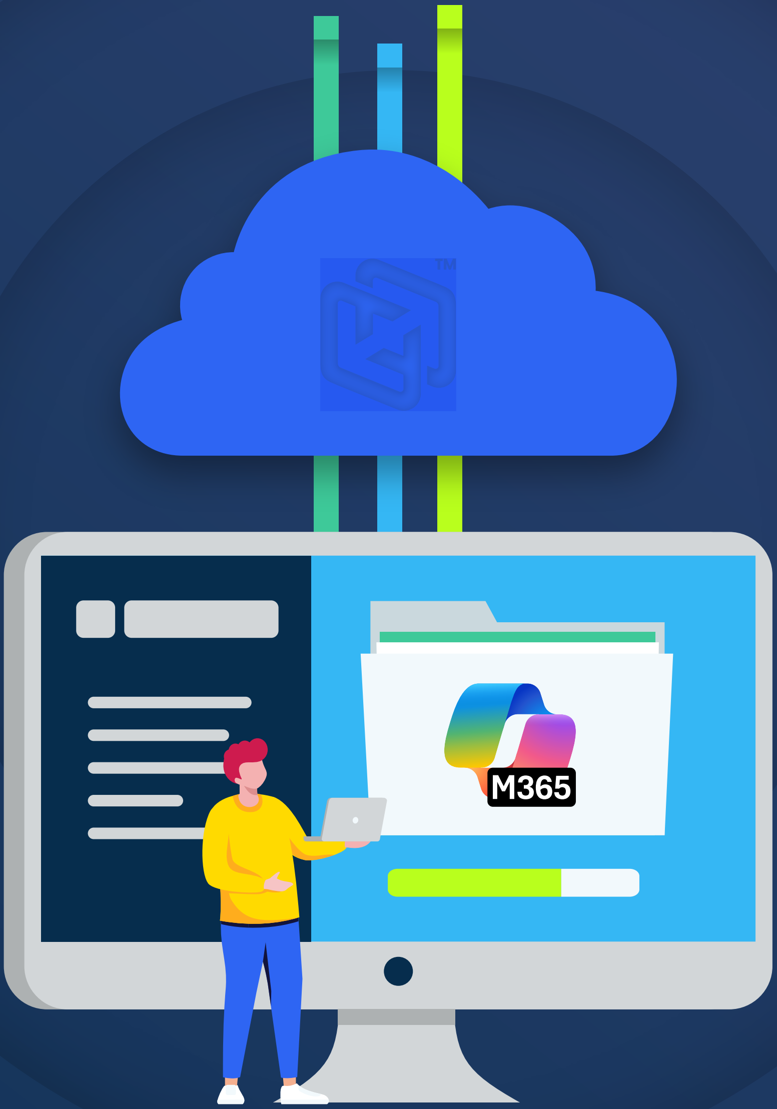


CrashPlan™

A Comprehensive Guide to Microsoft 365 Backup Solutions

CrashPlan™

A Comprehensive Guide to Microsoft 365 Backup Solutions

Outlook emails, SharePoint folders, OneDrive assets, and your entire workflow need reliable data protection.

Microsoft 365 (M365) has transformed the way businesses operate, boasting over 345 million paid subscribers and 321 million active users worldwide. Its cloud-based ecosystem—Outlook, OneDrive, SharePoint, and Teams—has become indispensable. However, 60% of organizations reported security incidents in 2024, so ensuring your critical Microsoft 365 data is truly safe is critical.

Most organizations assume Microsoft has their data covered. But what a lot don't know is that Microsoft follows a shared responsibility model. They protect the infrastructure and ensure platform availability, but protecting your data is your responsibility. Without a dedicated backup solution, businesses risk accidental deletions, ransomware attacks, insider threats, and even potential compliance violations.

This guide explains why backing up Microsoft 365 is essential, how to choose the best solution for your business, and the risks of not having one.

Your Microsoft 365 environment holds essential business data like emails, files, and collaborative projects. Without proper backups, accidental deletions, cybersecurity threats, or outages could cause permanent loss of critical information. Microsoft 365 data backups ensure your business keeps running smoothly, protecting productivity and reputation.

Microsoft 365's native data protection vs. third-party backup solutions

Microsoft 365 offers native data protection, of course. However, it is key to understand the differences between built-in protection and third-party backup solutions when it comes to ensuring comprehensive data security.

What Microsoft 365 offers in terms of data protection (& where they fall short)

Microsoft provides several built-in features for data protection, like retention policies, version history, and recycle bins, but these are not a substitute for a dedicated backup solution. Instead, they function as short-term retention mechanisms that can help with limited data recovery and are typically only useful in certain situations.

Retention policies

Microsoft 365 retention policies allow organizations to configure rules that preserve or delete data based on compliance needs. However, data is permanently deleted once the retention window has passed and it cannot be recovered.

Recycle bin and versioning

Deleted files in OneDrive and SharePoint go to the Recycle Bin where they can be restored **within 93 days** before being permanently removed. Versioning allows users to restore previous iterations of documents, but it has limitations on the number of versions stored. Many times, recovering these files also requires an IT admin or SharePoint admin, leading to increased tickets for the IT team and increased downtime for the employee.

Litigation hold and compliance features

For organizations needing compliance-driven data retention, Microsoft offers litigation hold and in-place hold to preserve emails and files indefinitely. However, these features are designed for extended data retention and do not include creating a separate, backed-up copy.

Why native Microsoft 365 protection is NOT a backup solution

Here’s why relying solely on Microsoft’s default protections is not recommended as a true backup solution:

Limited retention periods

Deleted emails and files are only recoverable for a short window. Once that period ends, the files disappear permanently.

Accidental deletion

Human error accounts for 52% of the root causes of data security breaches. A simple mistaken deletion can lead to permanent loss if not caught in time.

Cybersecurity threats

Ransomware attacks on cloud platforms have surged, with incidents increasing by 195% in the past two years. Microsoft does not offer immutable backups, meaning cybercriminals can encrypt or delete files permanently.

Compliance risks

Many industries require long-term data retention for regulatory compliance. Default Microsoft 365 policies often fail to meet these mandates.

Data overwritten & accidental deletions

If a file is mistakenly overwritten or deleted, version history may not be able to restore it.

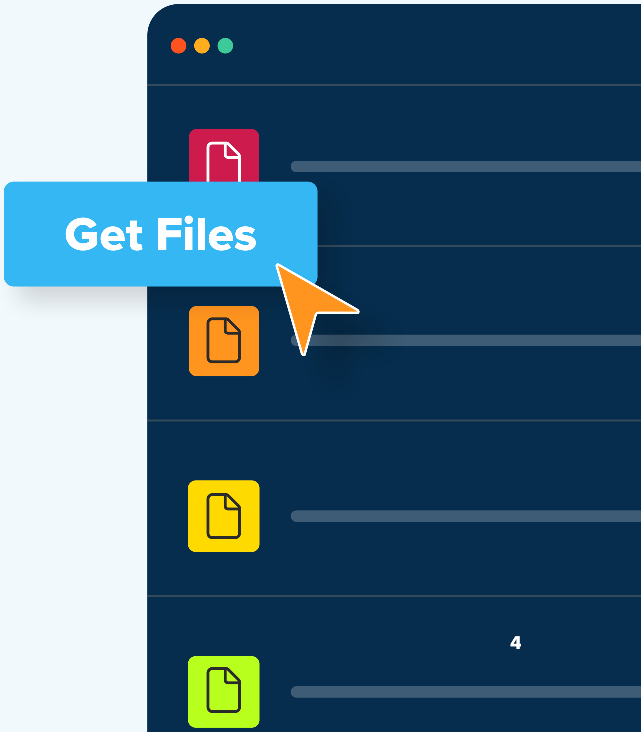
Slow and limited restores

Microsoft’s recovery process is complex, slow, and lacks granularity, making it difficult to restore specific items quickly.

Enhancing Microsoft 365 data protection with a third-party backup solution

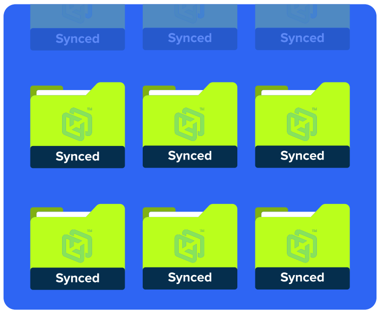
A dedicated third-party backup solution provides comprehensive data protection by offering:

- ✓ Automated, scheduled backups to eliminate manual retention concerns.
- ✓ Granular search to recover specific emails, files, or chat messages within minutes.
- ✓ Immutable storage to ensure ransomware cannot modify or delete backups.
- ✓ Long-term retention to meet compliance needs beyond Microsoft’s limited retention policies.
- ✓ Quick disaster recovery to reduce downtime with instant restores.
- ✓ Data archiving options to reduce storage space within your Microsoft 365 environment and save money



What features should you look for in an Microsoft 365 backup?

Choosing the right backup solution is critical to ensuring your M365 data remains protected and easily recoverable. Here are the essential features to look for:



Comprehensive data protection across Microsoft 365 services

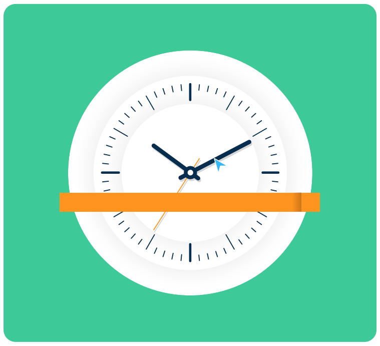
A backup solution should provide complete coverage for all Microsoft 365 applications:

- Outlook backup, including emails, attachments, calendars, and contacts.
- OneDrive and SharePoint backup, including files, folders, libraries, and metadata.
- Teams backup includes at least files shared in conversations, meeting recordings.

Security and administration

With cyber threats ever-evolving, your backup must be resilient against attacks with:

- Encryption (in-transit and at-rest) to ensure your data is always protected.
- Ransomware protection and immutable backups to prevent unauthorized modifications or deletions.
- Role-based access control (RBAC) grants controlled access based on user roles.



Retention and restore capabilities

A powerful backup should allow for flexible restore options, including:

- → Granular and point-in-time restore to recover exactly what you need when you need it.
- → Retention policies for long-term compliance to ensure data storage meets legal and industry regulations.
- → Versioning and file recovery options to restore previous versions of documents in case of accidental changes or data corruption.

Backup automation and monitoring

To minimize manual intervention, your backup solution should offer:

- → Scheduled and continuous backups to ensure real-time or frequent data protection.
- → Monitoring, alerts, and reporting to keep you informed about backup statuses and potential failures.

Data sovereignty and compliance adherence

Many industries and regions have strict data residency requirements:

- → Ensure your backup solution complies with HIPAA, GDPR, FINRA, and other regulatory standards.
- → Choose a provider with geographically distributed data centers to meet local compliance needs.

How does Microsoft 365 backup support different teams?

Creative files, code, reports, and every team member rely on something.
A solid Microsoft 365 backup plan protects it all and keeps work on track.

IT Teams

Streamline user transitions

Quickly move or restore user data when employees join, leave, or change roles within the organization.

Reduce support tickets

Empower users to recover their files and reduce the load on the help desk team. Support legal hold requirements with dedicated legal hold policies.

Stay audit-ready

Keep detailed logs and file histories that help meet compliance and audit requirements.

Prevent internal data loss

Ensure business data stays safe even when users delete files intentionally or by mistake.

Legal and Compliance Teams

Protect legal files and emails

Back up signed agreements, compliance documents, and legal communications stored across SharePoint, OneDrive, and Exchange Online.

Maintain chain of custody

Restore exact file and email versions to prove proper handling during audits, disputes, or investigations. Support legal hold requirements with dedicated legal hold policies.

Access records faster

Quickly retrieve critical compliance documents and communications during audits, inquiries, or legal reviews.

Preserve legal histories

Recover earlier drafts of contracts, filings, and emails to support defense strategies or timeline reconstructions.

Human Resources (HR)

Protect employee records

Protect onboarding files, payroll details, performance reviews, benefits information, and other sensitive employee data.

Meet privacy requirements

Back up contracts, consent forms, and personal documents to stay compliant with GDPR, HIPAA, and employment regulations.

Simplify employees transitions

Quickly restore employee files during hiring, promotions, exits, or internal moves.

Support reviews and audits

Retrieve past records, disciplinary files, and policy documents easily when handling investigations or compliance checks.

Keep smooth operations

Ensure uninterrupted access to essential files that support payroll, onboarding, benefits updates, and daily HR activities.

Finance Teams

Backup financial data

Protect budgets, revenue reports, and forecasts across M365 to avoid disruptions during planning cycles.

Track clean audit trails

Keep reliable version histories of financial records to trace discrepancies quickly during audits or reviews.

Store tax and compliance files safely

Back up tax filings, regulatory reports, and SEC submissions to stay ready for compliance audits.

Support smooth financial closes

Keep monthly closes, quarterly filings, and year-end reporting on track with uninterrupted access to critical files.

Retain transaction and payment records

Back up invoices, purchase orders, and expense reports that are needed for reconciliations and audits.

Keep approval workflows intact

Save approvals, reconciliations, and financial review files that support SOX requirements and internal controls.

Sales Teams

Back-up proposals and deal files

Protect critical sales documents like contracts, quotes, and customer proposals from accidental loss or data issues.

Recover lost sales materials

Quickly restore lost, deleted, or overwritten sales decks, proposals, and pricing documents without disrupting negotiations.

Retain customer and account histories

Store customer conversations, deal notes, and account plans safely to maintain continuity when sales reps move or exit.

Retrive older proposals easily

Retrieve past quotes, proposals, and agreements quickly to accelerate upsell, renewal, and re-engagement opportunities.

Speed up sales cycles

Ensure teams always have the latest sales collateral ready during critical deal stages, client meetings, or final negotiations.

Reduce downtime during CRM transitions

Back up customer records and sales activities to avoid data gaps when switching CRM systems or restructuring teams.

How to choose the right Microsoft 365 backup strategy

Not all backups are created equal. Choosing the right Microsoft 365 backup strategy is crucial. There are many things to consider before securing your critical business data, like:

Identify business needs and compliance requirements

Every business has unique data protection requirements. Before selecting a backup strategy, you must assess your industry regulations, business continuity needs, and data retention policies. Compliance frameworks such as GDPR, HIPAA, and FINRA require organizations to maintain strict data security measures. Understanding these requirements will help you determine the level of backup protection necessary for your Microsoft 365 environment.

Evaluate recovery point objectives (RPO) and recovery time objectives (RTO)

When considering an MIcrosoft 365 backup solution, two critical factors come into play:

- Recovery point objective (RPO): Defines how much data you can afford to lose. A lower RPO means more frequent backups, minimizing data loss in case of failure.
- Recovery time objective (RTO): Determines how quickly you need to restore operations. A lower RTO ensures faster recovery, reducing downtime and business disruption.

Your business operations should dictate these metrics. A financial institution might require near-instant recovery, whereas a small business might be comfortable with daily backups.

On-premises vs. Cloud-based backup

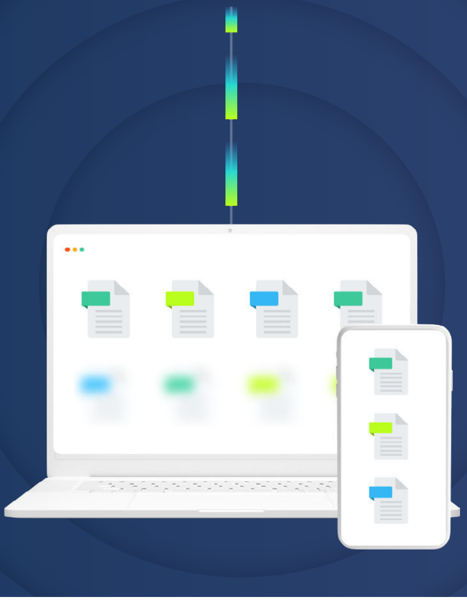
When implementing an MIcrosoft 365 backup strategy, you have two primary choices: on-premises storage or cloud-based backup solutions. Here's how they compare:

Backup Type	Pros	Cons
On-Premises Backup	✓ Full control over data storage ✓ Lower long-term costs ✓ Compliance with local regulations	× Require significant infrastructure investment × Prone to physical disasters × Require specialized employee skillset
Cloud-Based Backup	✓ Scalable and automated ✓ Accessible from anywhere ✓ Reduced maintenance costs	× Ongoing subscription fees × Dependent on provider reliability

Many businesses choose a hybrid approach, combining both strategies for redundancy and failover protection. A hybrid backup approach offers the best of both worlds by storing copies of M365 data both on-premises and in the cloud. This ensures that even if a cloud provider experiences downtime, you still have access to local copies of critical data.

What are the best practices for Microsoft 365 backup?

Microsoft 365 offers some built-in data protection features, but they have retention, recovery, and security limitations. To ensure complete data protection, follow these best practices for implementing a robust backup strategy.



Assess your backup needs

Identify critical business data across Exchange, OneDrive, SharePoint, and Teams. Understand compliance requirements, retention policies, and recovery objectives to determine the level of protection your organization needs.

Implement a clear retention policy

Define retention policies that align with legal and compliance requirements. Avoid relying on Microsoft's default retention settings, which may not cover long-term data storage or accidental deletions.

Ensure granular recovery options

Choose a backup solution that allows you to restore individual files, emails, or entire user accounts without restoring unnecessary data. This method speeds up recovery and minimizes downtime.

Choose a reliable third-party backup solution

Select a backup provider that offers automated, scheduled backups, granular recovery, and data encryption. Ensure the solution aligns with industry standards and provides features like ransomware protection and compliance support.

Automate backup processes

Enable automated, incremental backups to capture changes without manual intervention. This method reduces human errors and ensures up-to-date data is always available for recovery.

Secure your backups with encryption

Protect your backups with end-to-end encryption, both in transit and at rest. This method prevents unauthorized access and ensures data integrity in case of a cyberattack.

Store backups in a separate, secure location

Maintain copies of your data in a separate, immutable storage environment. This protects against insider threats, accidental deletions, and ransomware attacks that target primary storage.

Regularly test backup and recovery processes

Conduct periodic recovery drills to ensure your backup system works as expected. Validate restoration times and data integrity to avoid surprises during an actual data loss event.

Monitor and audit backup activities

Implement logging and monitoring for backup operations. Set up alerts for failed backups, unusual data deletion patterns, or unauthorized access attempts to detect potential threats early.

Train employees on backup best practices

Educate users on data retention, versioning, and recovery procedures. Ensure IT teams understand how to manage backups effectively to prevent accidental data loss or misconfigurations.

CrashPlan™

CrashPlan provides cyber-ready data resilience and governance in a single platform for organizations whose ideas power their revenue. Trusted by entrepreneurs, professionals, and businesses of all sizes worldwide, CrashPlan's comprehensive backup and recovery solutions ensure the safety and compliance of data without disruption, anywhere at any time.

Now available on Microsoft Azure MARKETPLACE

SPRING 2025 Grid Leader ENTERPRISE

Contact us to learn more at crashplan.com/contact-sales

crashplan

crashplan

crashplan

www.crashplan.com