Choosing the right backup solution for your clients' Microsoft 365 data

SaaS applications like Microsoft 365 are a critical part of modern business, but data stored in them isn't as safe as many believe. MSPs that lead with robust SaaS backup solutions can fill the data protection gaps and create a new recurring revenue stream. In fact, major MSPs are already cashing in on this opportunity, with over 60% currently offering SaaS backup services to clients. It's your turn now!

How data loss can happen in Microsoft 365

Before we dive into how data is lost in Microsoft 365, it's important to understand why relying solely on Microsoft or its built-in protections can be risky for your clients.

Many organizations, and even some MSPs, mistakenly assume that Microsoft automatically protects their data. Although Microsoft does offer a highly secure and reliable infrastructure, that's only part of the picture.

Like most SaaS providers, Microsoft operates on the "shared responsibility model." While Microsoft is responsible for application uptime and availability, data loss or downtime due to human mistakes, programmatic errors, insider activities or cyberattacks are the customer's responsibility. In short, cloud data protection is a shared responsibility between the CSP and the customer.

There are countless ways your clients can lose their Microsoft 365 data.

- **Accidental deletion** is the most common cause of Microsoft 365 data loss. Employees can delete a file or a folder, assuming it's no longer needed, only to realize their mistake later. In other scenarios, users can click the wrong buttons without realizing it (especially for mobile devices).
- Any **misconfiguration in the migration process** can lead to data loss. Manual migration of Microsoft 365 data from one account to another is error-prone due to its complex and time-consuming nature, leading to data being left behind or overwritten.
- **Bad integrations** of third-party apps with Microsoft 365 can lead to data deletion, overwriting or loss. Sometimes, it could be the user's fault, and other times, the app itself could be faulty. The data lost, as a result, will be gone forever, unless there's a backup.
- Microsoft 365 data is highly susceptible to **malware (particularly ransomware) attacks.** Microsoft's built-in protection against malware doesn't guarantee detection of every infection.
- Disgruntled employees can **intentionally delete important files** as an act of vengeance, making data recovery and restoration difficult. For whatever reason customer data gets deleted, Microsoft has no way of knowing whether it was intentional or accidental. What's scarier is that if a hacker made the request, Microsoft would interpret the action as coming from a customer. As a result, there will be no scope to hold extra copies for data restoration afterward.
- **A cloud-to-cloud backup solution** is the need of the hour for dependable protection against data loss risks like user errors, cyberthreats, natural disasters and sync errors.

What to avoid when implementing backup for Microsoft 365

As an MSP, selecting a Microsoft 365 backup solution is critical to effectively protecting clients that rely on the cloud productivity tool. Unfortunately, with misleading assumptions and multiple backup options available today, it's easy to fall into common traps that compromise data protection, customer trust and profit margins. Below, we outline key pitfalls to avoid to ensure your backup strategy is both resilient and profitable.

WHAT TO AVOID	DESCRIPTION
Relying solely on Microsoft retention policies ☐	Retention policies are designed for short-term recovery and compliance scenarios, not long-term business continuity. For instance, the default retention period for deleted OneDrive files is 93 days, after which they are permanently deleted.
Storing backups inside Microsoft's ecosystem ☐	Storing backup data within the same platform can put your clients at risk. If Microsoft experiences a service outage or account-level compromise (e.g., tenant-wide ransomware or admin credential theft), your backups could be lost or compromised.
Assuming all apps are covered ☐	Many backup solutions only protect major apps like Exchange, OneDrive and SharePoint, often neglecting other critical apps like Teams and Tasks. Without complete coverage across Microsoft 365, data recovery may be incomplete or complex.
Overlooking automation and scalability ☐	MSPs service multiple clients and operate at scale. Without automation for deployment, policy enforcement and reporting, the chances of human error and the administrative burden will increase significantly.
Hidden fees that kill margins ☐	Some backup vendors offer low starting prices but later add extra charges for common operational tasks like restores, API usage or extra storage. These hidden fees can impact profitability and complicate client billing.

Choosing the right Microsoft 365 backup solution: Key considerations

Not every backup solution will be ideal for you and your clients. Let's look at the factors to consider when selecting a Microsoft 365 backup solution.

FACTORS TO CONSIDER	DESCRIPTION
Air gap ☐	**Does the solution store backups outside of Microsoft 365/Azure?** The standard method of data backup — the 3-2-1 rule — applies to any data, including SaaS applications. For on-premises backups, at least one copy should be stored in a remote location so that it can be restored in case of a cloud outage.
Data sovereignty ☐	**Does the solution offer you a choice of data centers in different regions?** Numerous data regulations, like the GDPR, require storing customer data in in-country data centers. This ensures sensitive data isn't easily abused by cybercriminals. Your clients can easily access their Microsoft 365 data in the event of a data disaster and recover it quickly when needed.
All applications ☐	**Does the solution back up Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams?** Due to data sprawl, your clients' data gets distributed across multiple Microsoft apps. All data stored in those Microsoft applications are critical. An ideal backup should be able to offer protection for all these apps.

FACTORS TO CONSIDER	DESCRIPTION
Retention policies ☐	**Does the solution offer multiple retention policies to match your clients' needs and budgets?** Your clients may require seven-year or even 20-year retention of backups. Look for a solution that offers flexible retention to meet your clients' legal, regulatory and business needs.
Scalability ☐	**Does the solution easily scale without additional complexity?** You may have multiple clients, each with thousands of users. This scale makes data monitoring and management increasingly complex. In addition, a complicated user interface can lead to inefficiencies, which can significantly drive up costs for your business.
Credentials isolation ☐	**Does the solution offer a separate set of credentials for backups versus primary data? Or can your Microsoft 365 and Azure admins access Microsoft 365 and backups with the same credentials?** As part of the air gap principle, it is crucial to control and isolate data access, including credentials.
Operational integrations ☐	**Does the solution integrate natively with tools like PSA, RMM, billing, IT documentation, dark web monitoring and other out-of-the-box solutions?** Operational integrations manage the workload, allowing technicians to focus on other business-critical tasks. This ultimately ensures productivity and helps your clients grow their businesses.
Predictable pricing and TCO ☐	**Does the solution have a simple and predictable pricing model, or are there any hidden costs, like storage fees or egress, to be aware of?** A simple and predictable pricing model without hidden costs is ideal for planning and forecasting MSP margins.
Credentials isolation ☐	**Does the solution offer a separate set of credentials for backups versus primary data? Or can your Microsoft 365 and Azure admins access Microsoft 365 and backups with the same credentials?** As part of the air gap principle, it is crucial to control and isolate data access, including credentials.
Established technology ☐	**Is the solution established and proven for years across multiple customers, or is it in a beta/ public review?** A reliable solution ensures client satisfaction, and most importantly, it allows your clients to quickly and intuitively restore the lost data to their environment.

How to offer BaaS

Selling SaaS backup isn't just about ticking a compliance box — it's about peace of mind, risk reduction and building trust.

Here's how to launch or improve your Backup-as-a-Service (BaaS) model:

PRO TIP	DESCRIPTION
Offer bundled services ☐	Bundle it with Microsoft 365 management for baked-in protection or even into a broader support package that includes endpoint protection, device management, phishing protection, dark web monitoring and security awareness training.
Educate clients ☐	Lead with education, not fear — show real data loss scenarios. Your clients may not be aware of or underestimate the threats lurking in the SaaS world; therefore, it's important to highlight the consequences of not backing up SaaS data using real-world data breach stories or anonymized case studies.

PRO TIP	DESCRIPTION
Sell the value ☐	It's easier to sell the value by showcasing what's included and the reasons why in agreements. Integrate the backup offering directly into your service agreements or managed service packages. Explain to them the risks of not backing up data and how implementing a reliable backup solution aligns with their business needs.
Leverage compliance and cyber insurance incentives ☐	Industry regulations are constantly evolving, and cyber insurance policies are more difficult to obtain. Today, businesses need strong data protection to meet stringent regulations or qualify for cyber insurance. Use this as a key reason for positioning SaaS backup as a business necessity.
Position it as insurance like cyber insurance, but with guaranteed recovery ☐	Your clients want more than just protection — they want assurance that their critical data is safe and that they can keep operating in the event of a crisis. While cyber insurance helps mitigate the financial impact of an incident, a reliable backup solution ensures your clients can actually recover from it with minimal to no data loss or downtime.

Datto SaaS Protection: Reliable protection for your client's Microsoft 365 data

Built exclusively for MSPs, Datto SaaS Protection for Microsoft 365 ticks all the boxes cited above. It ensures that your clients' Microsoft 365 data is safe and secure. The solution scans Microsoft 365 for cyberthreats and protects it with 3x daily backups and flexible, fast recovery.

Datto SaaS Protection helps MSPs go beyond basic protection. It empowers you to:

- **Comprehensively protect your clients** from data loss, ransomware, accidental deletions, misconfigurations and insider threats.
- **Drive recurring revenue** through a scalable, low-overhead backup service that strengthens your MSP portfolio and boosts margins.
- **Stand out in a crowded market** by offering integrated, high-value solutions built specifically for MSPs that combine security, backup and business continuity.

With Datto SaaS Protection, you can deliver true BaaS: hands-free for clients and high-margin for you.

Want to see firsthand how Datto SaaS Protection can help you confidently protect your clients' Microsoft 365 data?

Schedule a demo today!

datto
A Kaseya COMPANY

Corporate Headquarters
Kaseya Miami
701 Brickell Avenue
Suite 400
Miami, FL 33131

partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

DATTO CONFIDENTIAL – Use and disclosure strictly limited as per the Kaseya Master Agreement

All information accurate to the best of Datto's knowledge at the time prepared; Datto reserves the right to correct errors/discrepancies.

Copyright © 2025 Datto, Inc.

All rights reserved.
Effective July 2025.