

1010 0010
0011 1000
1001 1001
0011 1100
1010 0010
0011 1000
1001 1001
0011 1100

 eBOOK

Seven Reasons to Back Up Microsoft 365 Data

Introduction

Businesses have increasingly turned to cloud services. Cloud services can make things more convenient for businesses by shifting maintenance to the vendor. Plus, moving more critical systems to software-as-a-service (SaaS) can reduce costs compared to purchasing on-premises hardware.

One of the biggest players in this space is Microsoft®. More and more businesses are using the cloud-based Microsoft 365™ (formerly Office 365®). Microsoft 365 encompasses a full suite of tools, giving you a bundle for email, data storage, and productivity tools, to name just a few. However, when it comes to the retention and recoverability of Office 365 data, it may be helpful to consider a supplemental solution to help.

As an MSP, you're a trusted advisor for your clients. They look to you to keep them productive and make sound strategic IT decisions for their business. As a result, it's important you take extra steps to protect their data. You don't want to be in the unenviable position of explaining that data is unrecoverable.

With that in mind, supplementing your customers' Microsoft 365 instances with additional backup and data protection is essential. This eBook covers seven reasons why this is critical. Knowing these reasons can show you where gaps may exist in Microsoft 365, and help you craft your sales presentations, so you can persuade prospects to sign up for the service.

With that in mind, why should you back up Microsoft 365 data? Why isn't Microsoft 365 enough on its own?

1. Accidental deletion

It happens. A user sits down and accidentally deletes a folder with critical documents in it. It could occur for any number of reasons—the person doesn't realize the contents within a folder or they may have nested their folders. Perhaps on Microsoft 365 email, they decide to delete old emails not realizing one day they'll need critical information from months or even years ago.

In addition, in the Business Standard edition, the recycle bin deletes once every 14 days by default, although the administrator can set it to 30 days. If someone deletes information and it isn't caught quickly, they may be unable to retrieve the information. Having a supplemental backup in place can help you prevent these issues and save your customers from huge problems down the line.

2. Retention gaps

Microsoft retains email data as long as the user is active. But let's face it—many people won't want to continue paying for a subscription after an employee leaves or is let go. This could lead to the company losing important information or intellectual property stored within email.

Of course, you can always share mailboxes before an employee leaves. However, this can get complicated as it relies on communication that an employee is leaving and is prone to error. Why take a chance? SolarWinds® Backup retains Microsoft 365 Exchange data for up to seven years, so you don't have to worry about missing data when an employee walks out the door.

3. Insider threats

We all want to assume people have the best of intentions. And most employees are on the level. However, sometimes, even some good employees can turn bad. For instance, someone may get mad at their employer for a bad review and decide to delete critical data in retaliation. If they do it and quietly wait out the 14- or 30-day retention period (assuming the company uses the Business Standard edition), that data will be gone for good. Sabotage may be rare, but it's a risk you should account for. With a secondary backup in place on behalf of your clients, you can help prevent this risk from becoming a reality.

4. External threats

Of course, malicious insiders aren't the only threat—outsider threats are common as well. In particular, weak passwords could lead to real challenges; for example, your end users may reuse passwords across accounts. If they use a username and password combo that has been breached before, then criminals may be able to find a match and break into an employee's Microsoft 365 account and steal or delete data. Another possibility involves spreading keylogging malware on someone's computer, then figuring out which keystrokes were usernames and passwords. Either way, passwords can be a weak link that lets people break into Microsoft 365 accounts.

Cloud-based apps like Microsoft 365 are high-value targets for cybercriminals. Finding ways to take over user accounts or victimize users can be a lucrative goal for cybercriminals. Whether phishing attacks aimed to push malware or account takeovers via stolen or hacked customer credentials, cybercriminals increasingly target users of cloud services. For that reason, having a strong backup is crucial for protecting their data.

5. Legal and compliance reasons

As you're probably aware, many compliance regulations set rules around the amount of time you have to retain data. For example, companies in the healthcare industry in the United States (US) must keep medical data for six years at a minimum.

6. Customer experience

Part of your job involves providing an excellent experience for your customers. They come to you to fix all things IT—you want to make sure you can provide that near one-stop shop for them as much as you can. By having your own backup, you have greater control over data in the event of a data loss incident.

Beyond that, you can offer customers greater peace of mind. Data loss can be catastrophic for businesses whether it's loss of customer information, financial data, or important intellectual property. By running your own backup, you're offering customers a greater assurance you'll stand as their business partner, ready to prevent data loss and its fallout.

7. Cost savings

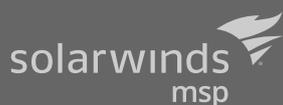
There are plenty of reasons why someone may want to go beyond the Business Standard edition of Microsoft 365, including gaining more features and applications. However, many businesses may want to keep costs low and stick with the Business Standard edition. With SolarWinds Backup, you can offer your customers the benefit of additional data protection and long-term retention for Microsoft 365 data, if budget is a concern.

SolarWinds Backup and your business

Most of this guide has been about the benefits of adding backup for Microsoft 365 to your customers. However, SolarWinds Backup is built to be convenient, fast, and effective for you as an MSP as well.

For starters, you can back up Microsoft 365 Exchange® email, contacts, and calendars as well as Microsoft 365 OneDrive® and SharePoint® data from the same web-based dashboard you use to back up servers, workstations, and critical business documents. This helps you deliver better service, improve efficiency, and greatly simplify the backup and data protection process. Beyond that, SolarWinds Backup gives you the power to select which Microsoft 365 accounts and mailboxes to protect, giving you granular control.

Learn more about SolarWinds Backup can help by visiting solarwindmsp.com/products/backup today.



Learn more today at
solarwindmsp.com

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses.

© 2020 SolarWinds MSP Canada ULC and SolarWinds MSP UK Ltd. All rights reserved.

The SolarWinds and SolarWinds MSP trademarks are the exclusive property of SolarWinds MSP Canada ULC, SolarWinds MSP UK Ltd. or its affiliates. All other trademarks mentioned herein are the trademarks of their respective companies.

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information.