eBook

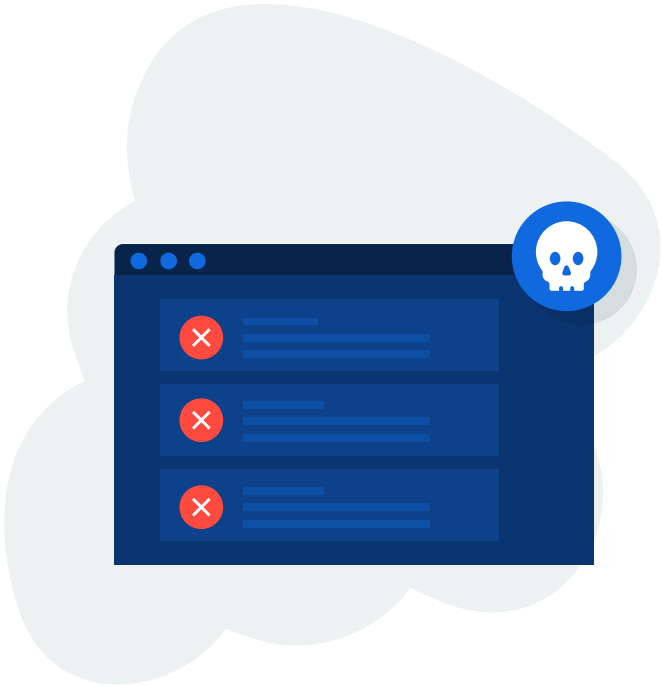
SaaS Protection Buyer's Guide

Introduction

Businesses all over the world are relying on SaaS applications to keep their businesses up and running. With more remote work, SaaS applications have become essential supporting collaboration and ensuring easy access to files and folders from anywhere to keep workforces productive and connected.

Unfortunately, many organisations still believe that these tools are completely secure and make the need for backup obsolete. This simply isn't true. Backup is just as important for data in SaaS apps as it is for data hosted on-premises.

In this eBook, you'll learn some common myths and misconceptions about SaaS, why having SaaS protection is important, and how we can help you select a SaaS protection solution that's right for your business.

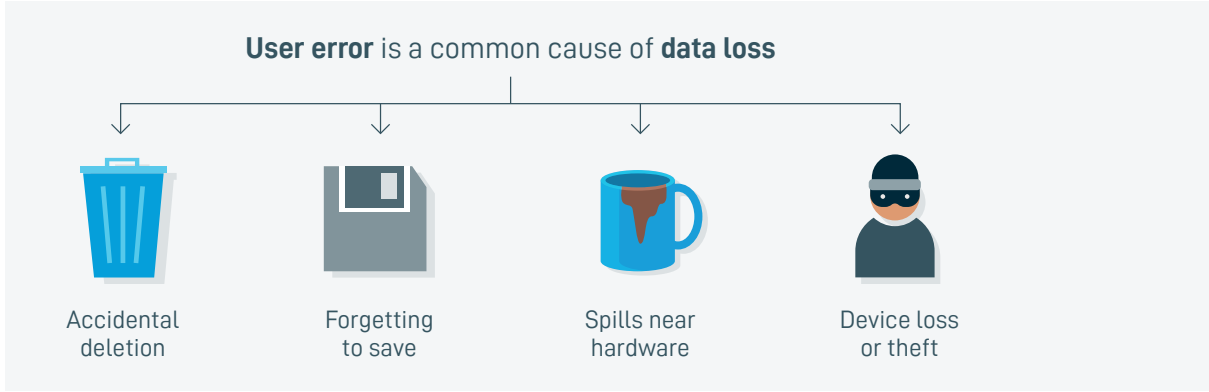


While accidental deletion of files is by far the most common form of data loss in SaaS apps, ransomware can be the most damaging.

4 Common SaaS Myths and Misconceptions

1. SaaS applications do not require backup

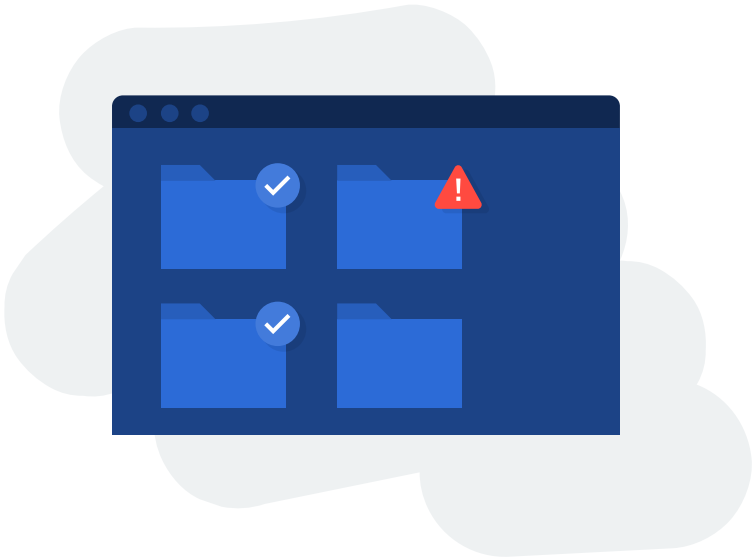
While SaaS applications do protect against data loss in their cloud servers, this doesn't protect against user error, accidental and malicious deletion, or ransomware attacks. While accidental deletion of files is by far the most common form of data loss in SaaS apps, ransomware can be the most damaging. That's because ransomware is designed to spread across networks and into SaaS applications, impacting many users.



Ransomware isn't only an on-premises problem. It can and does spread into SaaS applications, especially Microsoft 365. Businesses need a way to quickly revert files, folders, settings, and permissions in the event of an attack.

2. File sync is a replacement for backup

While file sync tools like Microsoft OneDrive or Google Drive do create a second copy of files and folders, they are not a replacement for backup. File sync automatically copies changes to synchronised files. So, if a file or folder is infected with ransomware, the malware will automatically be copied to all synced versions of that file.



Beyond simply lacking the restore capabilities of a backup solution, file sync can actually introduce ransomware to SaaS applications.

File sync services do offer some restore capabilities via versioning, but they fall short of a true SaaS backup solution. Here's why:

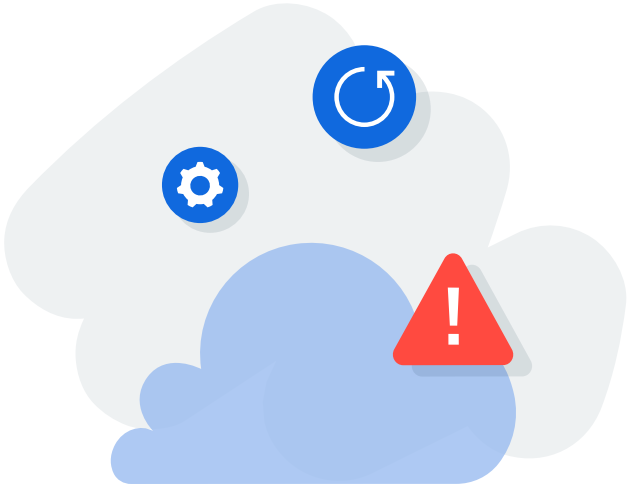
- If a file is deleted, older versions of the file are deleted as well.
- You don't have control over backup and recovery—it's left in the hands of end users.
- Large restores are a time-consuming, manual process.

Beyond simply lacking the restore capabilities of a backup solution, file sync can actually introduce ransomware to SaaS applications. File sync and backup are not competitive solutions, rather they can and should be used side-by-side. **Remember: file sync and share tools are for productivity and backup is for data protection and fast restore.**

3. SaaS applications are always available

While SaaS apps are highly reliable, outages do occur. In 2020 alone, Microsoft 365 had five significant outages in the space of six weeks that impacted businesses worldwide. Last year, Google applications suffered a global outage causing users in Australia, the US, Europe and Asia with no access to for several hours.

Outages and slow restore times aren't just an inconvenience. When businesses can't access important business data, productivity falls and revenue is impacted. Creating backups that are independent of a SaaS provider's cloud servers is the only way to ensure access to essential files in the event of an outage.



SaaS providers ensure they won't lose your cloud data. However, they do not take responsibility for restoring data if you lose it.

4. Microsoft and Google are responsible for backup

SaaS providers ensure they won't lose your cloud data. However, they do not take responsibility for restoring data if you lose it. Microsoft calls this the Shared Responsibility Model for data protection. That's why Microsoft recommends third-party SaaS backup in its user agreement. In the Shared Responsibility Model:

SaaS providers protect data against:

- Service interruptions due to hardware or software failure
- Loss of service due to natural disaster or power outage

Users must protect data against:

- Accidental deletion
- Hackers, ransomware attacks, other malware
- Malicious insiders

The Shared Responsibility Model places the onus of data protection squarely on businesses that rely on SaaS services. SaaS providers are responsible for keeping their infrastructure up and running, but businesses are responsible for the preservation and security of their data.

While Microsoft 365 and Google Workspace (formerly G Suite) may make collaboration more efficient, data protection and management remain a challenge.

Why SaaS Protection is Important

SaaS data is not immune to permanent data loss. Both Microsoft and Google make no guarantees when it comes to restoring deleted data whether it's inadvertent human error or a malicious ransomware attack. While Microsoft 365 and Google Workspace (formerly G Suite) may make collaboration more efficient, data protection and management remain a challenge.

While SaaS apps do include some basic recovery capabilities for lost data, there are a few major issues:

Data loss due to permanent deletion

If an employee accidentally deletes a critical spreadsheet from OneDrive or an entire folder of important emails passes the retention period in the Trash, Microsoft or Google will not be able to recover your data. Even if those files are within your retention period, locating and restoring lost data can cost you more time than you can afford.

Data loss due to a ransomware attack

If your business suffers a ransomware attack, no backup means you can't roll-back your data to a point-in-time before the attack occurred. This puts you at risk of losing not only your valuable business data, but also a hefty sum of money to criminals—without any guarantee your files will be unlocked, or any future protection from the same attack.

Time and money lost in recovering files

Retaining critical user data if employees leave a company can be costly without a backup solution in place. The time it takes to recover data from the cloud

might take longer than what your business can afford. It can take anywhere from minutes to weeks or longer to restore lost data.

Whether you're losing data or time, the impact to your bottom line can be significant. To address this challenge, you need a secure solution for this growing reliance on the cloud.

When selecting a SaaS backup product, look for solutions that offer protection for things like contacts, shared drives, collaboration and chat tools, and calendars.

Evaluating SaaS Backup Solutions

There are a variety of SaaS backup solutions on the market today. When evaluating products, you want to be sure it offers the data protection capabilities you need. We can help you find the right solution. At a minimum, a SaaS backup solution should offer the following.

Comprehensive Protection

Some SaaS backup solutions only protect email, files, and folders. However, there are solutions available today that offer more comprehensive coverage. When selecting a SaaS backup product, look for solutions that offer protection for things like contacts, shared drives, collaboration and chat tools, and calendars. SaaS protection solutions that offer this type of coverage are far more effective at maintaining business continuity than less robust offerings.

Frequent backups

Solutions that offer frequent backups enable you to restore to a recent point in time, minimising data loss. This makes restores faster and easier by reducing the amount of manual effort to perform restores and your users will be able to access data in the event of a SaaS outage.

Without a backup solution that goes beyond the basics you may not be able to recover valuable data and could experience business-threatening downtime.

Security/Compliance

Products that back up data in compliance with Service Organisation Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards can meet your HIPAA and GDPR compliance needs.

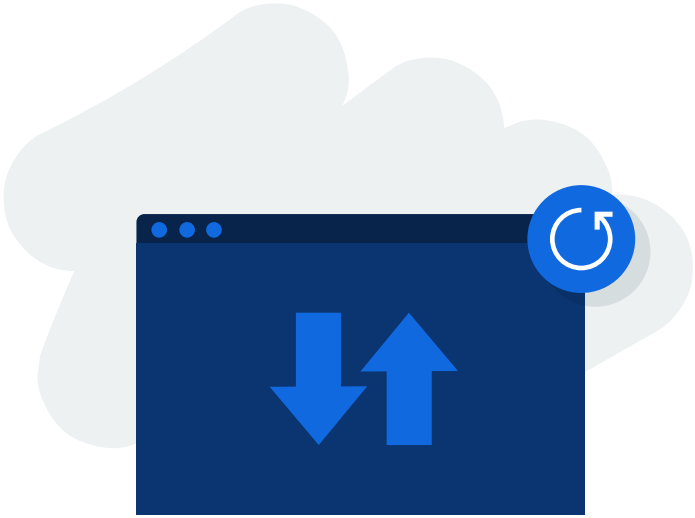
How We Can Help You

As we shift to a remote, digital workforce, businesses need tools that can quickly and effectively enhance how they handle new compliance, security and data loss risks. The benefits of collaboration and connection that SaaS applications offer is undeniable, but without the proper security measures in place, you could put your business at risk. Whether it's human error or a malicious attack, without a backup solution that goes beyond the basics you may not be able to recover valuable data and could experience business-threatening downtime.

Datto SaaS Protection can help. Datto SaaS Protection is a cloud-to-cloud backup solution that offers comprehensive backup and recovery for critical cloud data that lives in Microsoft 365 and Google Workspace applications.

Comprehensive Data Protection

Microsoft 365	Google Workspace
• Exchange • Tasks • OneDrive • SharePoint • Teams	• Gmail • Google Docs • Calendar • Contacts • Shared Drives



Eliminate stress with a SaaS backup solution that makes it easy to locate and restore the files and folders you need, right when you need them.

Robust, Automated Backup

Set and forget your SaaS backup to save you time

Data loss can happen for many reasons - human error, cyber attacks, and keeping up with new compliance measures can cost you valuable time and resources. Protect your business data efficiently and avoid the tedious day to day management of your backups with SaaS Protection.

- **Automated point-in-time backups 3X a day** captures your team's relevant changes across Exchange Online, Google docs, Sharepoint sites, and other relevant apps
- **New user detection and automatic archiving for departing employees** saves you money, critical information and administrator effort
- **Non-destructive restore** recovers data without overwriting existing files, folders or even site collections targeted at the same Sharepoint URL.
- **Cloud managed user interface** means no on-premise hardware is necessary for backups and admins can check-in on status anytime, anywhere

Fast, Easy Recovery

Go beyond your SaaS applications' native recovery capabilities

Eliminate stress with a SaaS backup solution that makes it easy to locate and restore the files and folders you need, right when you need them.

- **Granular restore function** to recover lost files and folders directly to a user's account or download them to your computer or device
- **Export to access cloud-based files** in standard formats if Microsoft 365 or Google Workspace go down

Intuitive IT Pty Ltd

yadal@intuitiveit.com.au

03 9044 4767

- **Robust search parameters** across all users to zero in on emails, contacts, files, and entire folders that you need
- **Full Service Restore** of individual items or complete folders of data maintained with its original format, file and label structure intact
- **Unlimited storage** option means that your data will be protected as you grow

Security Made Simple

Your data deserves more than industry-standard security

Go above and beyond industry standards to make sure your SaaS data is secure, easily recoverable, and protected.

- SOC 2 Type II audited
- Supports HIPAA and GDPR compliance needs
- Move data from one account into another with admin capabilities
- Data encryption both at rest and in transit
- Data controls and monitoring tools, including audit logs

Conclusion

We understand the collaboration and business operations needs of growing organisations, and Datto SaaS Protection will protect your cloud data from online security threats and downtime. Implementing the right SaaS Protection will make you feel safer and enable you to easily locate and restore the files and folders you need, right when you need them.

Contact us today to find out how we can help your business against permanent data loss.