

eBook

datto

SaaS Protection Buyers Guide



Introduction

SaaS application adoption has spiked with the increase in remote work due to the global health pandemic. These tools have become essential in today's remote work world. Even before work-from-home became the norm for many, the benefits of easy access to documents from any device and improved collaboration are obvious.

Unfortunately, many organisations still believe that these tools make 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, talking points for discussing SaaS data loss and downtime with clients, what to look for when selecting a SaaS backup solution, and how you can use SaaS backup to build margin and grow your business.

Common SaaS myths and misconceptions

SaaS applications do not require backup

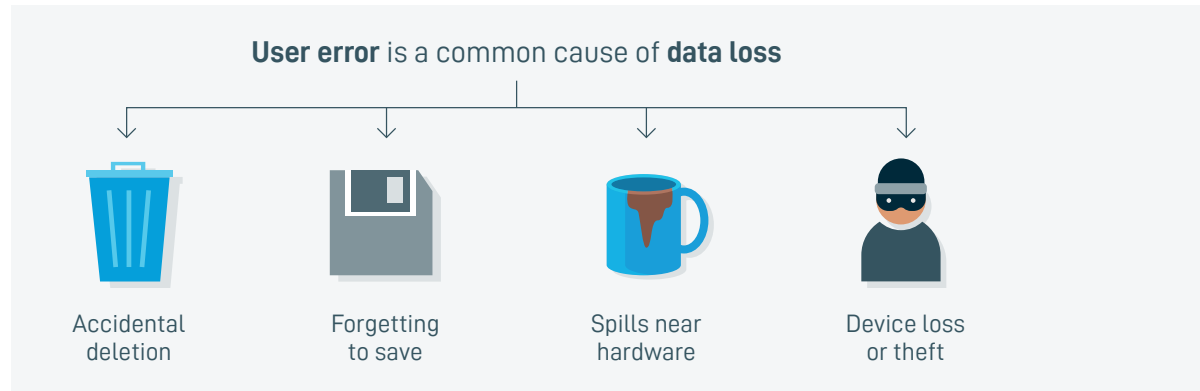
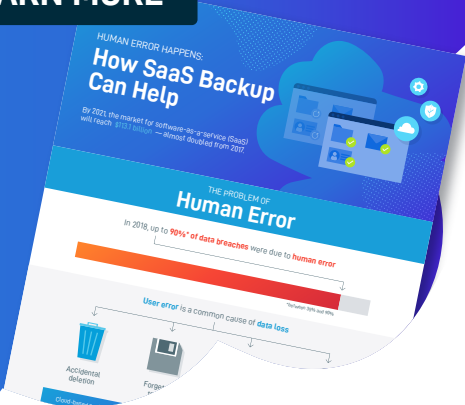
While SaaS applications have built-in redundancy that protects against data loss in their cloud servers, this doesn't protect against user error, accidental and malicious deletion, or ransomware attacks. While **accidental deletion** of files is by far the most common form of data loss in SaaS apps,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

You may also be interested in:

Infographic

Human Error Happens: How SaaS Backup Can Help

LEARN MORE



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.

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.

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

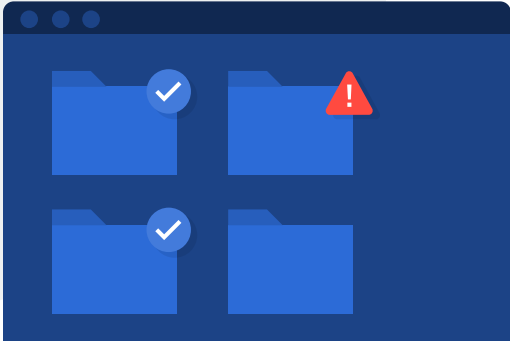
- **Versions are not immutable recovery points.** So, if a file is deleted, older versions of the file are deleted as well.
- **Versioning doesn't enable centralised management of user data.** In other words, you don't have control over backup and recovery—it's left in the hands of end users.
- **Versioning doesn't maintain recovery points across files, folders, settings and users.** If you only need to restore a couple of files, no big deal. But, 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 is for productivity and backup is for data protection and fast restore.

SaaS applications are always available

While SaaS apps are highly reliable, outages do occur. In October 2020 alone, [Microsoft 365 had three significant outages](#) that impacted businesses worldwide. Last year, [a massive Google outage](#) affected nearly one billion Gmail, G Suite, and YouTube users.

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.



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

Microsoft and Google are responsible for backup

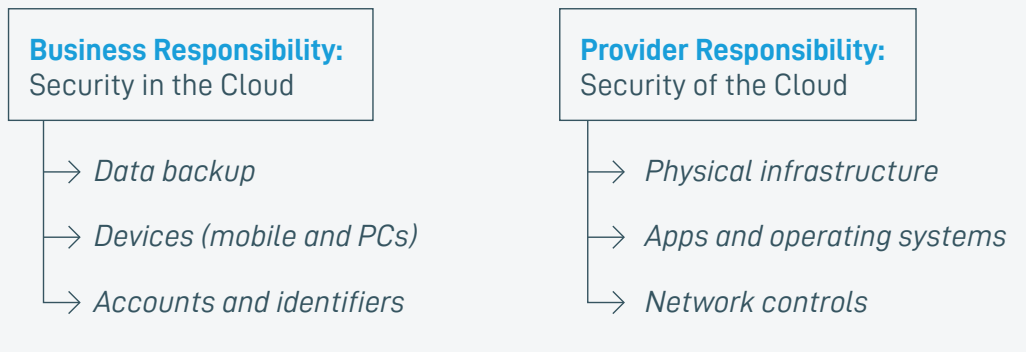
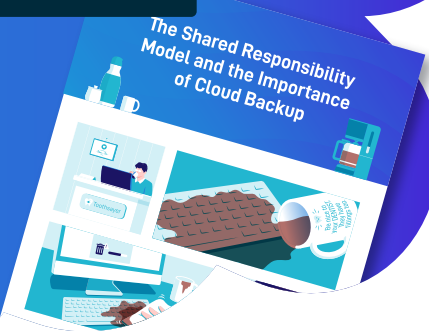
SaaS providers ensure they won't lose your cloud data with built-in redundancy and other high availability measures. However, they do not take responsibility for restoring data if you lose it. Microsoft calls this the [Shared Responsibility Model](#) for data protection. That's why Microsoft recommends third-party SaaS backup in its user agreement. In the Shared Responsibility Model:

You may also be interested in:

Infographic

The Shared Responsibility Model and the Importance of Cloud Backup

LEARN MORE



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.

Evaluating SaaS Backup Solutions

There are a variety of SaaS backup solutions at competitive price points on the market today. However, there is disparity in exactly what these products protect. So, when evaluating products that can be a good place to start.

You may also be interested in:

Recovery Time & Downtime Cost Calculator

LEARN MORE



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 (more on that below).

RPO/RT0

Recovery point objective (RPO) and recovery time objective (RTO) are also critical considerations. These metrics refer to the point in time you can restore to and how fast you can perform a restore, respectively. When it comes to SaaS backup these are largely dictated by the frequency of backups and what specifically is being protected. Solutions that offer frequent backups address RPO since they enable you to restore to a recent point in time, minimising data loss. As noted above, these make restores faster and easier by reducing the amount of manual effort to perform restores. Plus, they enable users to access data in the event of a SaaS outage.

Ease of Use/Management

Ease of use is critical for MSPs. Increasing efficiency can expand margins on services delivered, so finding a product that is easy to deploy and manage should be considered essential. Look for SaaS backup products that are designed specifically for MSPs. That might mean streamlined onboarding, native reporting capabilities, intuitive seat management, and flexible retention

policies. Consider partnering with vendors that offer not for resale programs, sales-based discounts, and 24x7x365 tech support. Finally, products that integrate with other tools you also increase your ability to deliver SaaS backup services efficiently.

Security/Compliance

Many MSPs serve clients in verticals with significant security and compliance requirements. So, choosing a SaaS protection solution that can address these needs is essential. Look for products that back up data in compliance with Service Organisation Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards that can meet clients' HIPAA and GDPR compliance needs. Solutions that enable automated retention management to meet compliance standards can reduce the need for manual intervention—streamlining management and ensuring client data is stored for the right length of time.

Business Growth

No discussion of product evaluation for MSPs is complete without considering profitability. Look for products that have the features and functionality you need at a price point that allows you to build margins on your services. Consider products that offer pricing benefits for MSPs such as sales-based discounting and flexible 'pay for what you use' licensing. As noted above, products that increase efficiency can also grow margin and increase revenue, since they require less manual intervention. You may also want to bundle SaaS protection on top of SaaS services you already deliver—this has proven effective for some MSPs. This isn't necessarily part of the product evaluation process, but it's worth noting when discussing business growth.



Solutions that enable automated retention management to meet compliance standards can reduce the need for manual intervention

Datto SaaS Protection

[Datto SaaS Protection](#) is a cloud-to-cloud backup solution that offers comprehensive backup and recovery for critical cloud data in Microsoft 365 and Google Workspace. It is designed specifically for MSPs to protect their clients' SaaS data efficiently and manage client data retention, licenses, and cost.

SaaS Protection protects against permanent data loss and allows MSPs to easily recover clients' data following a ransomware attack with 3x daily, point-in-time backups. Backups are stored securely in the Datto Cloud with files, folders, settings, and permissions intact for fast restores whether you need to restore a single item or an entire user account.

SaaS Protection delivers backup, search, restore, and export for:

Microsoft 365

- Exchange
- Tasks
- OneDrive
- SharePoint
- Teams

Google Workspace

- Gmail
- Google Docs
- Calendar
- Contacts
- Shared Drives

As you know, delivering profitable managed services is all about increasing efficiency and maximising return on services. Datto SaaS Protection improves MSP efficiency with streamlined onboarding that gets new clients up and running fast. Single pane of glass management gives you complete visibility into client backups, further increasing efficiency.



Datto SaaS Protection also offers:

- **Simple, per-license pricing:** Deploy licenses across end clients, and redeploy them as needed.
- **Aggregated, volume-based discounting:** Discounts are based on total licenses sold across all of your clients.
- **Flexible subscription options:** Choose the best fit for each client with standard month-to-month contracts or discounted longer-term commitments.
- **Margin building opportunities:** Build margin and add multi-layer protection for your Microsoft 365 clients by bundling Microsoft 365 and Datto SaaS Protection.
- **Unlimited NFR Program:** Pilot the Datto SaaS Protection product with your clients and add a new NFR client in minutes with our streamlined onboarding process.
- **SaaS Protection marketing and sales campaigns:** Launch pre-built SaaS Protection campaigns, access a library of co-branded content, and manage your leads from prospect to sale.

You may also be interested in:



Datto SaaS Protection for Google Workspace →



Datto SaaS Protection for Microsoft 365 →

Datto SaaS Protection By The Numbers:



Billions of Backups



Tens of Thousands of Recoveries



Hundreds of Thousands of Teams Protected