



Selling SaaS Backup Made MSPeasy

Introduction

IT spending has been steadily shifting from traditional on-premises offerings to cloud services over the past five years, and it is continuing to grow. Considering that by 2022, 78% of businesses will run almost entirely on Software-as-a-Service (SaaS) applications and in 2021, the market for SaaS will reach \$113.1 billion—cloud is clearly [here to stay](#). While the enterprise has adopted SaaS at a rapid rate, the current emphasis on remote working has made SMBs rethink digital transformation with many of them more committed than ever to accelerate their use of SaaS applications. This means MSPs have an important role to play when it comes to guiding clients to make SaaS a strategic success for their business as well as an immense revenue opportunity in moving clients to the cloud.



Grow Your MRR with Cloud Backup Sales

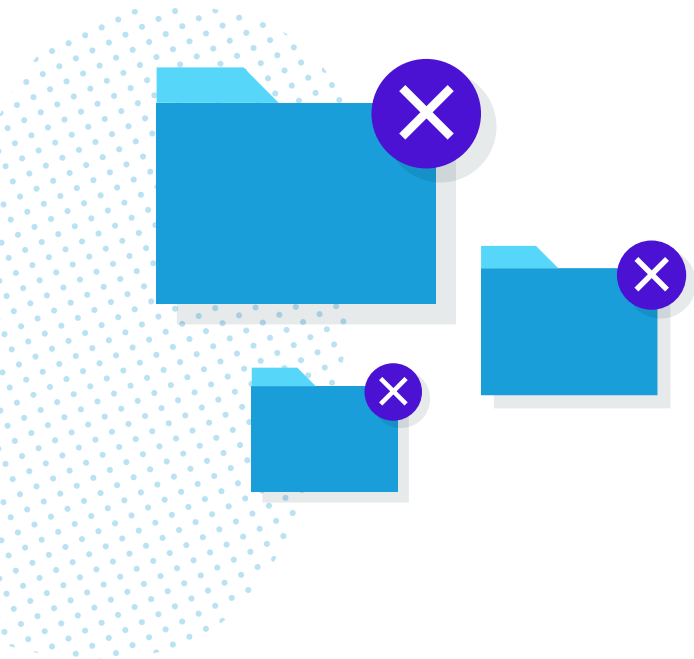
SaaS applications such as Google Workspace and Microsoft 365 are popular because they're easy to use, highly scalable, standardize employees on the same applications like Word or Excel, and are relatively inexpensive. However, SaaS apps don't deploy and manage themselves. Additionally, SaaS applications require more robust data protection for businesses just like any other mission-critical app—posing an opportunity for MSPs.

In this eBook, you'll learn the importance of third-party backup of SaaS apps, how to pitch SaaS backup to clients and prospects, and additional benefits of SaaS backup tools beyond data protection. You'll also learn about bundling strategies to build better margins and drive recurring revenue.

Why Your Customers Need SaaS Backup

There's a common misconception among SaaS users that backup isn't necessary for their data because it exists in the cloud. However, this is patently untrue. SaaS applications are just as vulnerable to data loss as on-premises apps. In fact, Gartner predicts that by 2022, 70% of businesses will suffer unrecoverable data loss in SaaS applications. Why? Because people delete files, open phishing emails, accidentally download malware, and more. SaaS vendors are unable to distinguish if certain user actions are done in error or deliberately.

"With 85% of a company's intellectual property flowing through Outlook, it's important for us to be able to provide the same backup potential that we could elsewhere in the cloud." - Frank M. DeBenedetto, Two River Technology Group



Other scenarios where clients could lose data include:

- Malicious deletion by a disgruntled employee or outside entity
- Malware damage or ransomware attacks
- Operational errors such as accidental data overwrites
- Lost data due to canceled app licenses

Aside from recovering from data loss, there needs to be an easier way to efficiently manage these applications for clients. This brings us to why SaaS backup needs to become one of your key service offerings.

Minimize downtime. Even Microsoft and Google experience downtime, which can negatively affect your clients' productivity and compromise their ability to access important business documents. Keep your clients' businesses running without interruption— even in the event of a massive outage. Datto SaaS Protection provides a simple way to export Microsoft and Google Workspace files to ensure “offline” productivity.

Increased use of collaboration tools. Microsoft Teams now has 75 million daily active users, adding 31 million in just over a month with the global shift to remote work. Given the shared responsibility model for data protection and the impact of an outage on Microsoft Teams, it should be considered essential to protect Teams.

As your clients' trusted advisor for all things tech, protecting customer SaaS data should be standard for your business.

You may also be interested in:



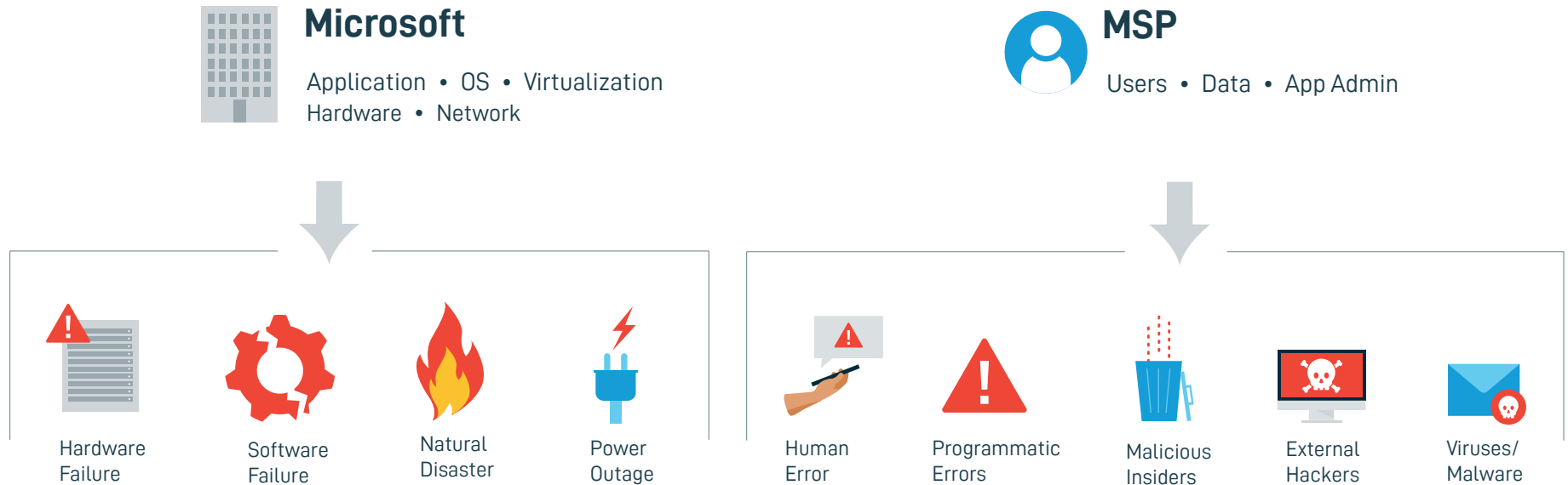
Microsoft Teams has become such a critical tool for many businesses to discuss, share, and collaborate on projects. Without the proper tools in place to protect Teams data against cyber threats, businesses are extremely vulnerable to a data disaster. Datto SaaS Protection supports Microsoft Teams, including public channel content, conversations, and calendar meetings.

Why SaaS Backup is Your Responsibility

As your clients' trusted advisor, protecting customer SaaS data should be standard for your business. In addition, you should have an efficient means of managing data and be compensated for the work you put into setup and management of SaaS applications.

SaaS apps provide limited protection against accidental data loss scenarios, and sometimes even less so when it comes to ransomware attacks or malicious end user activity. Many vendors, including Microsoft and Google, operate under the "Shared Responsibility Model" - they only claim responsibility for areas that they have complete control over. Microsoft and Google must maintain the availability of their applications and protect their servers from disaster scenarios, but the end user is responsible for the data being created within their applications.

Data Protection Responsibilities



This Shared Responsibility model means that many providers don't offer any guarantees around restores and that you're on your own should attacks like ransomware strike. In fact, most advise their customers to implement a backup strategy using native or third-party tools. Microsoft makes it clear where their responsibility ends when it comes to things like deprovisioned user account data:

Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so

that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data. The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data as described in [this section](#).

The biggest limitation of native tools is that they do not create a secondary copy of your data independent of your SaaS provider—so you have a single point of failure.

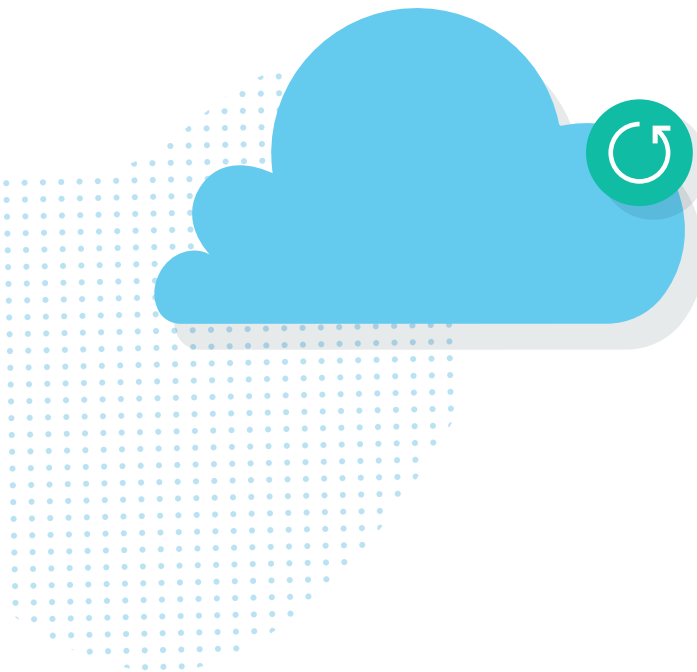


Recently, Google announced that starting October 13th, 2020, retention policies for items in the Trash in Google Drive will change. With this new policy, any file that is put into a Google Drive Trash will be automatically deleted after 30 days. Previously, trashed items would be retained indefinitely until the trash was emptied by the user. These changes affect items that are trashed from any device and any platform.

With this in mind, you will need to decide whether you will use a SaaS provider's native tools (if they exist), or opt for a third-party backup product. The biggest limitation of native tools is that they do not create a secondary copy of your data independent of your SaaS provider—so you have a single point of failure.

Many organizations take a “3, 2, 1” approach to backup (3 copies, 2 formats, 1 offsite copy). Third-party tools like Datto SaaS Protection enable this approach by storing data in Datto's private cloud, purpose-built for backing up and recovering data.

Some native tools might seem suitable to use for backup, but have serious limitations when it comes to restores. For example, Microsoft 365 apps like Exchange or OneDrive allow up to 30 and 93 days respectively to recover deleted user data, which admins may take to mean that data is backed up and easily restorable. Recovering that data from Microsoft is often a cumbersome process and past the retention period, your data is purged. Google Vault [cautions](#) against the potential “irreversible purging of data from user accounts” associated with their own retention tools.



If the lost data is recoverable via native means, you may not get exactly what you need. Matt Maines of Worksighted explains, "If you have 250 folders in your email and it gets accidentally deleted, I can recover all the emails, but it comes back to you as if I took that entire file folder and dumped it all over your desk! Is that any good for you? No!"

File sync and share tools are designed for collaboration and productivity—not data protection. Since OneDrive stores Microsoft 365 files in the cloud, many mistakenly believe that it eliminates the need for backup. However, using OneDrive as a form of backup is not enough. Here's why: If a file is deleted or infected on a local device, that change is automatically synced in OneDrive. In other words, the file is automatically deleted or infected on both sides.

Backup solutions are designed to recover lost data fast, and they can also make the day-to-day management of client SaaS data much more efficient for your techs. Datto SaaS Protection's UI aims to mimic native functionality and is so intuitive, training requirements are minimal.

Finally, offering SaaS backup generates recurring revenue. SaaS providers have not offered compelling reseller margins on their products, so your bundle of services around the protection of those applications must make up for this. Once you have a client and can keep them satisfied, that consistent revenue can only increase. The recurring revenue associated with SaaS backup may seem small at first, but over time, it can become a key player in increasing your profitability.

Independent SaaS backup should be considered essential.

You may also be interested in:



More importantly, doing the right thing for your clients can be motivation enough for selling SaaS backup. Frank DeBenedetto at Two River Tech recalls a time when an accounting firm needed critical data associated with a deprovisioned user. "They were more than thrilled to realize that although we did delete the mailbox they wanted us to when the employee left, we could still go back and grab that data that they needed. We looked like heroes."

Ultimately, the tools you choose to protect your customers' SaaS data will be dictated by their specific business needs. Whatever tools you choose, independent SaaS backup should be considered essential. If your customers don't immediately understand the importance of SaaS backup, it is your responsibility to educate them about the risk of leaving SaaS data unprotected.

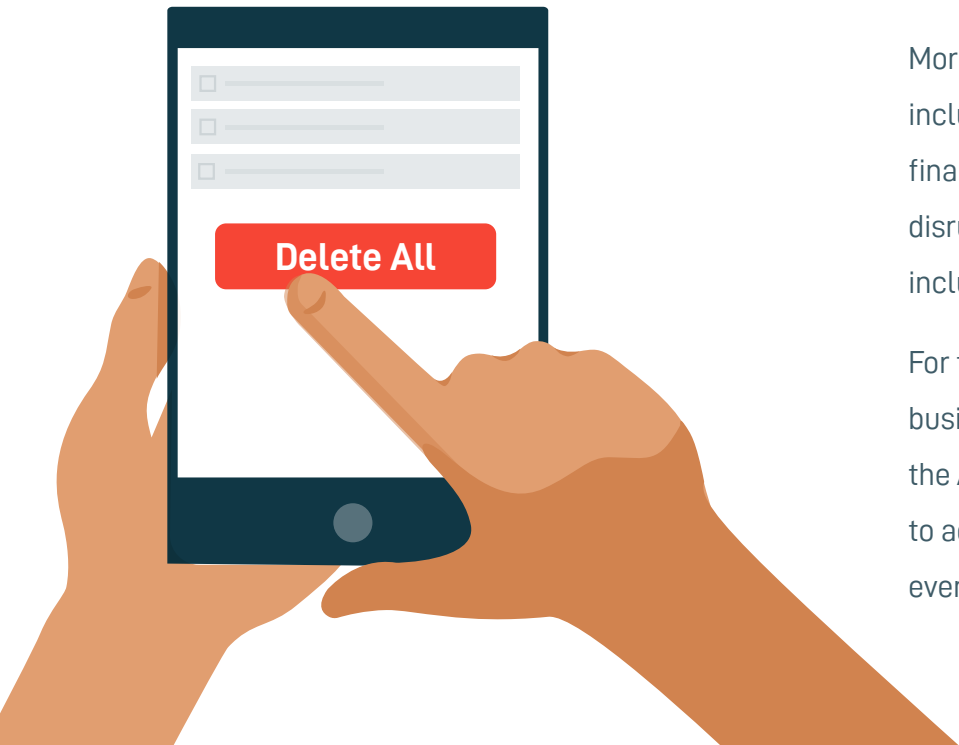
Talking to Your Customers About SaaS Backup

You may have already implemented SaaS solutions for your clients or are in the process of onboarding new clients to the cloud. Whatever the case, educating your clients about the risks they face for data loss within these applications is part of your role - even if they were skeptical of moving to the cloud in the first place. Some tools to help you broach the topic with both new and existing clients regarding SaaS backup include:

Data loss stories & Data loss statistics

Rather than focusing on the technology, share stories to make the risks real for your clients and prospects. Ask your clients and prospects, "how much do you value your data?" and take that to the next level with real-life examples.

Ask:
Is your email backed up?
Well what would happen
if someone deleted all
their emails and walked
out the door?



Make your examples personal and try to use analogies the customer understands. A good rule of thumb: Email is typically the lifeblood of any business.

One of Datto's partners, Kevin Damghani of ITPartners+, elaborates on this point by saying, "Anyone you talk to will say their business email is important. That's a no-brainer for SaaS backup. We ask customers, 'Is your email backed-up? Well what would happen if someone deleted all their emails and walked out the door?'"

Don't be afraid to get creative and explicitly spell out the potential risks associated with data loss by industry. Proper planning involves outlining all of the possible data loss scenarios relative to the industry the client or prospect is in. For example, if you're pitching to an attorney's office, you can start with "without an independent backup solution, you can lose important information associated with a trial should one of your users accidentally delete an email or a file related to the case."

More network outages are on the rise across different business platforms, including Google and Microsoft, which affects millions of users and causes financial consequences. Downtime impacts productivity and can cause massive disruption. Even a small incident can cost businesses between \$18,000-\$35,000, including [productivity loss and reputation damage](#).

For those who may be more numbers oriented, you can use statistics to help sell business owners on the need for a backup solution. A good example: A report by the Aberdeen Group states that over 70% of data loss in cloud applications is due to accidental or malicious deletion by end users. A simple Google search reveals even more useful anecdotes and statistics for you to make your pitch your own.



SaaS backup can serve as both insurance for user data and a cost savings tool in the future.

Cost savings

One of Datto SaaS Protection's biggest benefits: Its ability to save user data without the need for an active application license. When asked how he pitches Datto SaaS Protection, Maines says, "Employees leaving the company is another great example for using the product - it's cheaper to maintain that account in backup than pay for something like a Microsoft 365 E3 license." Explain to your prospect or client that there's an easy way to save SaaS license costs should employees leave the company - simply store their data in a backup state until a replacement is hired. The investment in SaaS backup can serve as both insurance for user data and a cost savings tool in the future.

Smart bundling

MSPs vary in their approach to selling SaaS Protection - some sell a la carte, but the vast majority of successful MSPs include SaaS in some form of a security bundle for Microsoft 365 or Google Workspace. Another option is to bundle backup with other Microsoft 365 services. If you already provide Microsoft 365 administration and management to clients, adding backup as a line item or simply as a part of the service can be a relatively easy sell.

Keep in mind that your competition is also selling SaaS application licenses, so you need to differentiate your offerings and be clear about what's included in the package. For some, that may mean separate line items outlining the services included in the bundle, or it may mean bundle tiers priced per month, per user. Be ready to defend your recommendations and clearly explain the benefits of those



services to your client or prospect. Ultimately, you need to price and offer services based on what's best for your business. For the simplest sale, SaaS Protection should be automatically included in your Microsoft 365 bundles.

When all else fails: Requiring clients to sign a waiver

In situations where you aren't able to convince a client about the importance of SaaS backup, it's best to ensure that your business and brand are protected by requiring your client to sign a disclaimer document outlining that they have refused the service. This tactic may feel aggressive for some MSPs, but with a calm approach, this method could be a wake-up call for clients that don't understand the potential magnitude data loss could have on their business. Talk to your legal counsel about creating a waiver. Already a Datto partner? Check out the Datto Partner Portal for an [example disclaimer](#) to use in this situation.

Conclusion

No matter what stage of growth your business is in, SaaS backup should be an important part of your service portfolio. The move to the cloud has been accelerated in recent months as organizations become more mobile and the need for collaboration tools increases. If you want to protect the reputation of your brand, build more profitability, and do the right thing for your clients, Datto SaaS Protection is your best bet. For those who are still unconvinced, consider what Kevin Damghani of ITPartners+ sees as the value of SaaS Backup: "If you have to tell a client, 'oh, sorry I can't do anything,' if data is deleted in Microsoft 365, that's not an acceptable answer. Not having SaaS backup is a sign of an immature MSP. Data is so important to customers; as the keeper of that data you have to be able to protect it."