

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. In fact, according to Gartner, Inc., SaaS application spending will grow to over \$99 billion worldwide by 2020. While the enterprise has adopted SaaS at a rapid rate, SMBs are typically more agile than large companies with heavier investment in on-prem technology. This means MSPs have an immense revenue opportunity in moving end users to the cloud.



Grow Your MRR with Cloud Backup Sales

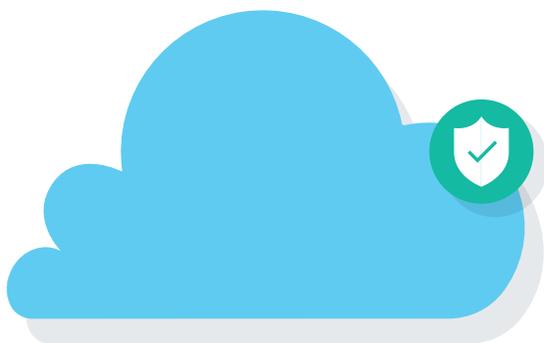
SaaS applications such as Google's G Suite and Microsoft Office 365 are popular because they're easy to use, highly scalable, standardize employees on the same applications like Word or Excel, and are relatively inexpensive. However, SaaS apps don't deploy and manage themselves. Additionally, SaaS applications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

In this eBook, you'll learn the importance of third-party backup of SaaS apps, how to pitch SaaS backup to customers 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-premise apps. Why? Because the #1 cause of data loss is human error. People delete stuff, 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 something like 85 percent 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



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

Other scenarios where customers 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, your techs need an easier way to efficiently manage these applications for clients. This brings us to why your MSP needs to mandate that SaaS backup become one of your main responsibilities.

Why Your MSP Needs SaaS Backup

Customers will blame their MSP for any data loss - even if it isn't their fault. As your clients' trusted advisor for all things tech, 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. The reason being that many vendors 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



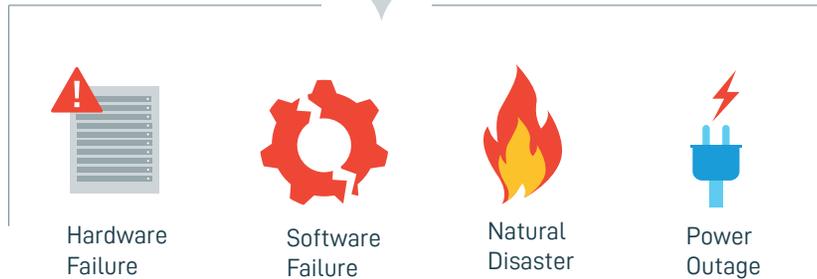
Microsoft

Application • OS • Virtualization
Hardware • Network



MSP

Users • Data • App Admin



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. Take, for example, this best practice advice from the Salesforce SLA:

Salesforce: Salesforce maintains a copy of customer data for disaster recovery purposes but it is important for customers to develop a data backup and recovery strategy as part of their overall data management and security model. The Salesforce Data Recovery service is an expensive and time-consuming process and should only be used as a last resort when no other copy of the data is available.

In addition, 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.



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, Office 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 in the [how it works page here](#).

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!"



One of the most overlooked areas of SaaS management is the most essential resource for your MSP: time.

Litigation hold or storing emails in Shared Mailboxes are two common shortcuts to backing up data in Office 365. However, these options do not give you a second independent copy of your data, which means there is risk associated with these storage methods. In addition, they can hinder your ability to recover quickly in a massive data loss scenario. For example:

- **Litigation hold** is about saving data over a long period of time for legal or regulatory compliance purposes, and involves a labor-intensive manual restore process
- **Shared Mailboxes** are limited in size and negate all organizational hierarchy in their restore process, also making for a time-consuming recovery

One of the most overlooked areas of SaaS management is the most essential resource for your MSP: time. SaaS applications are built to foster collaboration and make the users who use them more productive -- not help your MSP manage the data easily. 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 be so intuitive that training takes less than 10 minutes, if that.

Finally, generating recurring revenue for your MSP is paramount to your success, and SaaS backup can play an important role here. SaaS providers have not offered fantastic 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:



datto

Secrets to Selling Office 365 Backup with SaaS Protection

View Now

The graphic features a blue, organic-shaped background. At the top left, the word "datto" is written in white. In the center, the text "Secrets to Selling Office 365 Backup with SaaS Protection" is displayed in white. To the right of this text is a yellow shield icon with a white checkmark. At the bottom center, there is a green button with the text "View Now" in white.

Dollars and change aside, doing the right thing for your clients can be motivation enough for selling SaaS backup. 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.

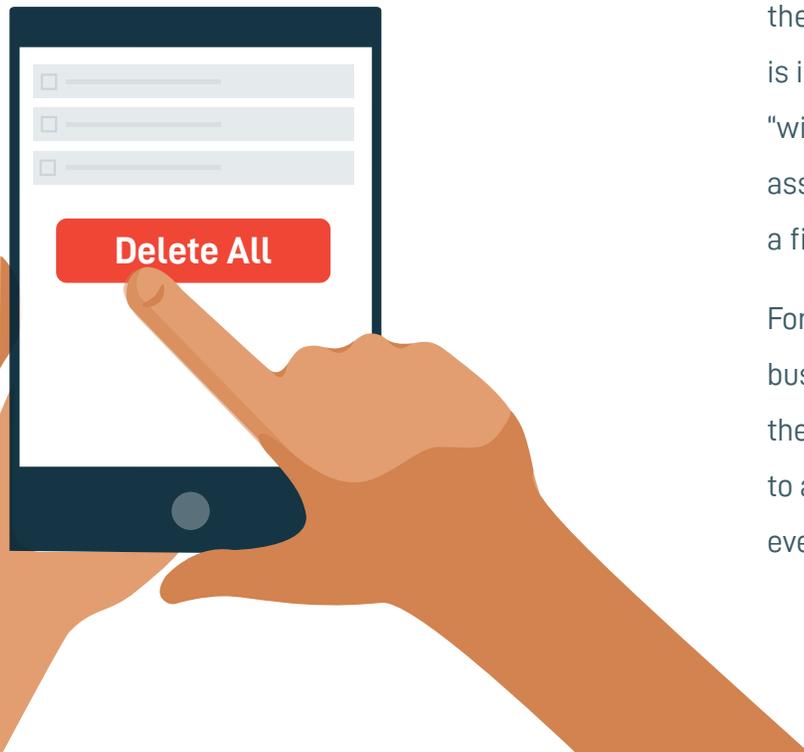
Talking to your customers about SaaS backup

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 of the risks they face within these applications can be simple - 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:

Ask:

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



Data loss stories & Data loss statistics

Rather than focusing on the technology, use 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. 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 prominent partners Kevin Damghani of ITPartners+ elaborates on this point by saying, "anyone you talk to will say their business email is important. That's then 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."

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 stating 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

No business owner will ever refuse a way to save money. One of Datto SaaS Protection's ancillary benefits is in its ability to save user data without the need for an active application license.

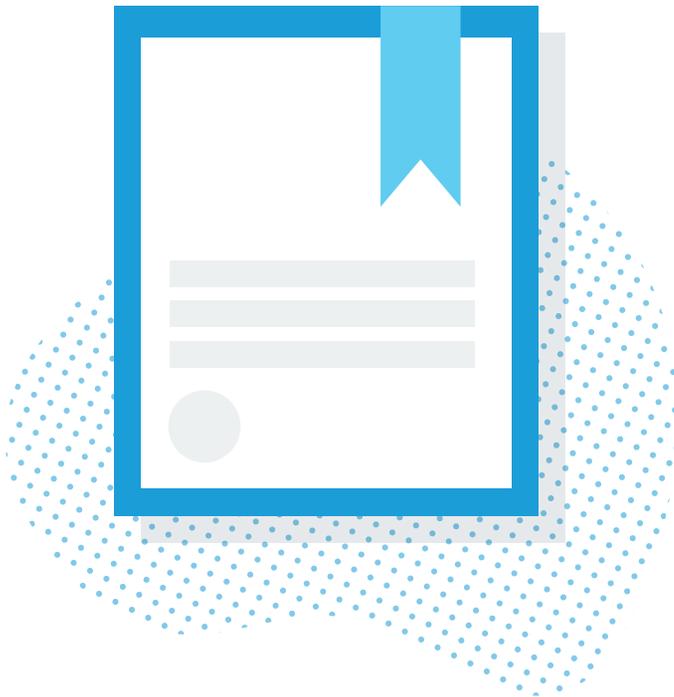
When asked how he pitches Datto SaaS Protection, Maines says, "Employees leaving the company is another great example for using the product - it's cheaper to maintain that account in backup than pay for something like an Office 365 E3 license."

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. A few dollars here and there goes a long way, but 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 Salesforce, Office 365 or G Suite. 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 by per user price per month. Be ready to defend your choices and explain in full the benefits of those services to the business you're selling to.

Ultimately you need to do what feels right for your business. Regardless, SaaS Protection should be automatically included in your Office 365 bundles for the simplest sale.



When all else fails: Requiring clients to sign a waiver

Even some of the most talented salespeople can't argue around a stubborn business owner that refuses to pay for SaaS backup. In situations like this, it's best to ensure that your business and reputation is protected by requiring your user to sign a disclaimer document outlining the fact that they refused the service. This maneuver can be a little scary and may feel aggressive for some MSPs, but with a calm approach, this method could be a wake-up call for an end user that hasn't understood the magnitude of data loss.

Talk to your legal counsel for help creating a waiver. Already a Datto partner? Check out the Datto Partner Portal for an example disclaimer ([linked here](#)) to use in this situation.

Conclusion

No matter what stage of growth your MSP is in, SaaS backup should be an important part of your service portfolio. The move to the cloud may seem to be happening slowly, but the big picture story that Microsoft and Google are telling says that there's still a world of opportunity for MSPs. 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. SaaS Protection delivers benefits outside of insuring your business against data loss and generating recurring revenue - it saves you time and gives you peace of mind.

For those who are still unconvinced, consider what one MSP thinks about SaaS Backup: "It shows a sign of an immature MSP who doesn't use SaaS Protection. If you have to tell a client 'oh sorry I can't do anything' if data is deleted in Office 365, that's not an acceptable answer. Data is so important to customers; *you* as the keeper of that data need to protect it." - Kevin Damghani