



CONNECTWISE™

CONNECTWISE
EBOOK SERIES

SaaS Data Backup

Everything You Need to Know (and Do) About It

Don't Leave Your Customers' Data At Risk In The Cloud

When SMBs move to SaaS, backup & recovery is up to the MSP

For years, businesses have relied on MSPs to protect their on-premises data. Now, as SaaS solutions like Microsoft Office 365, Salesforce.com, and Google Workspace gain popularity, most companies assume their SaaS providers take the same responsibility for data in the cloud. But they don't—and that misconception can leave critical data at risk. Of course, if something does go wrong, it's the MSP who'll most likely take the blame anyway. To ensure the best results for their customers, and avoid unproductive finger-pointing after the fact, MSPs need to take the lead on backup and recovery for SaaS data just as they do for data stored on-premises. After all, when customers lose data, nobody wins.

MSPs need to take the lead on backup and recovery for SaaS data just as they do for data stored on-premises.

Data moves offsite—and away from Standard Operating Procedures—as SMBs flock to the cloud

MSPs know as well as anyone how critical technology is for helping small and midsize businesses level the playing field against larger competitors. That's a key force driving the rapid adoption of SaaS solutions like Microsoft Office 365, Salesforce, and Google Workspace.

For enterprises, cloud-based tools for email, collaboration, file storage, and business productivity make it possible to compete more effectively by increasing mobility and agility. For SMBs, the impact is even greater. By making work seamless across locations and devices, a company can make a smaller team feel bigger—like serving customers in more locations, becoming productive more easily in more scenarios, putting personal technology to work for business, and so on.

The economic benefits of SaaS are especially compelling for small businesses. For a big company, a more flexible and efficient cost model is a good way to improve the balance sheet. For a smaller one, it can be a financial lifeline. Instead of allocating scarce resources to in-house infrastructure and IT staff, they can let a SaaS provider handle the back end at a fixed monthly cost. In fact, the factors that lead SMBs to work with SaaS providers have a lot in common with their reasons for relying on MSPs.



SaaS Data Backup

Everything You Need to Know (and Do) About It


However, as small and midsize businesses move to the cloud, they don't always fully understand the implications of this shift for their data. Before the transition, they relied on their MSP to provide backup and recovery for their on-premises data. In moving their data to the cloud, they might assume that this responsibility will shift along with it, from their MSP to Microsoft, Salesforce, Google and whoever else delivers their SaaS services. But that's simply not the case.

While some SaaS solutions do provide rudimentary capabilities for data recovery, such as the recycle bins and file version histories in Office 365, that's far from a comprehensive native backup and recovery service. If data goes missing—a CEO accidentally deletes a crucial email, a disgruntled former employee corrupts a ShareFile directory, a hacker locks down business-critical data with ransomware—the company is on their own to try to get it back. And they quickly find this to be a costly and time-consuming effort with no guarantee of success.



Only 34% of small businesses have policies in place for storing and disposing of confidential data.

Microsoft and other SaaS providers don't exactly hide their abdication of responsibility for backup and recovery. Their Service Level Agreements make clear that it's up to customers to handle this themselves. But one way or another, the message isn't getting through; according to Shred-it!, only 34% of small businesses have policies in place for storing and disposing of confidential data. Furthermore, half of C-Suites



7 out of 10 companies had been hit by a cyberattack with a data recovery cost of \$150,000

say human error or accidental loss by an insider cause a data breach. In the lack of a regular data backup and recovery plan in place, companies are exposed to a major data loss or even more concerning, vulnerable to a ransomware attack. For smaller companies, the resulting damage from these to customer relationships, market credibility, and business continuity can be too much to survive.

The many perils facing SaaS data

These are dangerous times to leave data at risk. A recent Cost of a Data Breach report from IBM found that 83% of companies have had more than one breach—with the average total cost of a data breach is USD \$4.35 million.

Today's cyberthreats come in more forms than ever, including:

- **Ransomware** attacks that forcibly encrypt vital data and hold it hostage, rendering it inaccessible by employees and customers
- **Phishing** attacks that circumvent defensive technologies and often deliver targeted malware to unsuspecting users

And hackers aren't the only ones posing a danger to data.

SaaS Data Backup

Everything You Need to Know (and Do) About It

Companies have just as much to worry about inside their own organization. As SaaS gives users greater control over the data within an application, it becomes far more difficult for IT and security teams to maintain protection. Similarly, the complexity of SaaS architecture increases the likelihood of security gaps and misconfigurations. All it takes is one malicious insider—a disgruntled, corrupt, or simply mischievous employee—to wreak havoc.

Even well-intentioned but negligent employees can do considerable harm. In fact, such individuals cause the most damage of all: according to the Shred-it Report, the lack of training and human error are major contributors to data risk, with 51% of small business owner in the United States identifying employee negligence as their biggest information risk.

Put simply, SMBs who lack third-party backup and recovery for their SaaS data are on thin ice. And when it breaks, they're all too likely to point their fingers in the wrong direction.

Cost of a Data Breach report

Common Types of Cyberthreats

Ransomware: holds data hostage

Phishing attacks: delivers malware to users



The lack of training and human error are major contributors to data risk.

When Microsoft's shortcomings put MSP relationships at risk

As any IT professional knows all too well, the assignment of blame can be an inexact science. If data is lost beyond hope of recovery, an SMB is mostly likely to turn to their primary technology partner for answers: the MSP. Never mind that the customer's contract covers only data residing in the data center, or that the MSP had no way of accessing the SaaS data to back it up in the first place, or that the customer refused the additional charge to back up SaaS data. If you're the provider they most rely on, they'll ask why they couldn't rely on you this time. "You should have read your Microsoft agreement more carefully" is an answer no customer will be happy to hear.

In a way, the customer has a point. MSPs differentiate their services by promising to make life simpler for customers. They provide the reliability companies need to do business with confidence. The fact that the customer's move to SaaS has made it harder to deliver on this promise is beside the point.

As the customer's technology environment evolves, so must the MSP's services.

MSPs differentiate their services by promising to make life simpler for customers.



What your customers need now to keep their SaaS data safe

While some MSPs already offer limited SaaS backup services, they tend to be limited to simpler use cases like email-only and OneDrive files. Shared data like SharePoint and Microsoft Teams pose a greater challenge requiring a deeper integration into Office 365. For both MSPs and their customers, the key is to make data backup and recovery both comprehensive and simple—as well as fast. When critical data goes missing, time is of the essence.

As you introduce backup and recovery services for SaaS data, focus on the features and capabilities that matter most to your customers.

Full protection of SaaS data and metadata

There's more to backup than files. Business teams use SharePoint to create custom sites that play a key role in productivity and collaboration. If all you're doing is backing up the files themselves, customers will have to spend valuable time recreating the columns, views, lists, and permissions that make this data truly useful. By backing up metadata as well as data, you can restore their SaaS services to exactly the way they were— ready for business.

Comprehensive SaaS backup should include:

- SharePoint sites, including metadata
- Mailboxes (all types)
- In-place archives
- Calendars, tasks, and contacts
- Microsoft OneDrive folders
- Office 365 Groups, including conversations, plans, files, sites, and calendar
- Microsoft Teams, including wiki and chat

Fast and easy find & restore

The faster customers can restore their missing data, the better for their productivity. In a full disaster recovery scenario, this can mean recovering an entire site or service. In many cases, though, the data needed might be a single file or message. In that case, customers need a quick and easy way to find and restore just that specific item.

Your SaaS backup and recovery service should make it simple for people to browse current and deleted files across time without needing to load multiple snapshots. A preview feature can let people confirm that they've found the right file or message before they initiate the restore. To help customers most efficiently, you should provide multiple methods of recovery, including the ability to download a email locally, send a link to a recovered file, or restore an item back to the SaaS production location. From beginning to end, the search and recovery process shouldn't take more than a minute.



Daily automated backup

Nothing is more frustrating than discovering that the file you need wasn't included in the most recent backup. To give customers confidence, the solution should automatically run at least one complete backup every day, and ideally several.

Compliance

Many companies, especially in highly regulated fields like legal, finance, and healthcare, face complex requirements for data governance. Your solution should meet enterprise audit requirements for backup, search, and recovery to help customers comply with these rules. Customers may also want to set specific retention periods by data type (email, OneDrive, SharePoint, etc.) ranging from 30 days to unlimited.

As international regulations like the E.U. General Data Protection Regulation (GDPR) expand the rules covering data sovereignty, your solution should offer flexible options for where customer data is stored. Even smaller businesses need to pay attention to rules like these. A company with even one customer located in Europe will need to ensure compliance, and every business should plan for success with a future-proof data protection strategy.

Your customers are counting on you

Even as companies expand their relationships with the major corporations that provide their SaaS services, their MSP retains a special place. Microsoft, Google, and Salesforce are vast and faceless entities, but the MSP represents a more personal connection based on a real, human relationship. When something goes wrong, a smaller business will feel more comfortable turning to the MSP for help—in large part because of the trust you've built as a partner and advisor. By helping them ensure the safety of their SaaS data, you can extend that relationship once more with a promise that you'll be there for them when the big companies aren't. It's one more way you can differentiate your role as an indispensable part of your customer's success.

ConnectWise SaaS Backup™ provides a single portal to protect your clients' SaaS application data, including Microsoft 365®, SharePoint® and Microsoft Teams®, Microsoft Dynamic 365, Google® Workspace, and Salesforce®. [Watch this demo](#) to see how to reduce the risk of SaaS data loss for all your clients.

The MSP represents a more personal connection based on a real, human relationship.