3-STEP GUIDE TO SAAS DATA PROTECTION

Moving critical data from on-premises apps to cloud-based apps like Salesforce, Office 365, or G Suite? Congratulations! Your data is in good hands, with your SaaS provider providing a reliable platform to keep it available. But you need to do your part to keep it safe.

Follow this 3-step guide to protect your data in SaaS apps against everything from accidental deletion to getting hacked.

STEP 1: MAKE ACCESS EASY - YET SECURE

Follow these best practices in identity and access management to get data to the right people – and keep it out of the wrong hands.

Simplify data access: Adopt repeatable onboarding/offboarding processes, including keeping data in a restorable format post-offboarding.

Control data access: Institute strong password policies and multi-factor authentication, leveraging security mechanisms in your SaaS platform.

STEP 2: SECURE DATA AGAINST LOSS.

Prevent data loss by following best practices for data security.

Know what's at risk: Use data classification tools to help you understand what data you're keeping and sharing (via APIs) in SaaS apps.

Limit data exposure: Develop data security policies that limit risk by limiting the types of sensitive data kept in SaaS platforms.

Keep your guard up: Institute both preventive and real-time policy enforcement, using SaaS platform tools as well as third-party tools.

STEP 3: PROTECT DATA WITH THE RIGHT BACKUP.

Choose a backup solution that doesn't just back up your data, but enables you to restore it quickly, easily, and effectively. Look for a solution with these capabilities.

Enterprise-level scalability: Both large enterprises and smaller organizations will benefit from a robustly scalable solution.

Automated and on-demand backups: Daily "set it and forget it" operations are crucial, but you should also have the option to back up data at any time you choose.

Quick, easy point-in-time restores: Admins need the ability to retrieve data and put it back exactly as it was at any point in time - and the option to extend that ability to users.

Multiple-layer security: Multiple layers of operational and physical security are essential to ensure the integrity and safety of your data.

CASE IN POINT

Here are three great examples of how your SaaS data can be vulnerable to loss – and how a Spanning Backup solution can protect it.

- An admin importing data into a SaaS app accidentally overwrites good data with bad; Spanning Backup lets her easily go back to a point in time before the error and restore what was overwritten.
- An application sync error overwrites SaaS app data with incorrect data and empty fields; Spanning Backup's point-in-time restore capability quickly returns the overwritten data to the app.
- Ransomware encrypts critical files in a shared collaboration folder; an admin uses Spanning Backup to go to the "last known good" point in time backup and restores data and metadata, so the data goes back into users' accounts exactly as it was before the attack.

ABOUT SPANNING

Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, protecting more than 10,000 organizations from data loss due to user error, malicious activity and more.
Learn more about how Spanning Backup protects business-critical data from loss at spanning.com.