SaaSAssure℠
powered by Asigra

WHITEPAPER

The Seven Deadly Sins of SaaS Backup

These days, many companies have turned to cloud-based, software-as-a-service (SaaS) solutions to organize data under one umbrella, provide easier access for their staff, and use best-of-breed services to run their organization. Even with more and more business-critical data stored in SaaS platforms, some IT leaders still believe that because their data is in the hands of a third party that it is protected by their service provider. They are often shocked when data loss occurs, and the provider is not able to recover their data and informs them they were never responsible for it.

If you want to ensure your SaaS data is recoverable in the event of an accidental or malicious data loss, then you'll want to avoid these seven deadly sins to adequately protect your SaaS data.

Sin #1: Not Realizing that SaaS Data is at Risk

One of the foremost issues with SaaS data is the potential for data loss. Data can be lost for all kinds of reasons, from accidental deletion to syncing errors to malicious actions. Deliberate attacks can be executed even with advanced SaaS & cloud solutions, such as ransomware attacks and other data loss or intrusion via cyber-attacks.

Another issue that many face with SaaS solutions is cloud service outages. It's no secret that cloud solutions can provide a much-needed extra layer of data protection and oversight compared to storing traditional data on-site. However, depending on an enterprise's vendor, cloud systems can still fail, and data loss can occur. When this happens, recovery time is essential, as well as the proper restoration of all files at every granularity, no matter the size and scope.

With cloud SaaS document services like Microsoft 365, Dropbox, Box and Google Drive, syncing issues are another common problem. Sometimes local files do not sync properly, and sometimes file errors are synced before they can be corrected. A user might delete files locally and discover the deletions have been propagated to the cloud service (a possible issue with Dropbox, OneDrive, etc.). Such issues do not only create data issues but can also enable ransomware to spread from one device to another within the cloud.

Sin #2: SaaS Data Protection Misconceptions

The biggest misconception is that your SaaS provider is backing up and archiving your data. In most cases there is some form of data retention policy, possibly some snapshots for a limited period but they do not constitute a proper backup. If a user deletes a file and only realizes that they've done so after 30 days, it may be too late to get a stored copy from the SaaS provider. In some cases, if a user account is deactivated, i.e., if they've been terminated or quit, their data is deleted along with the account. In fact, an average of 67% of companies have experienced data loss in SaaS environments due to accidents or malicious deletions.[1]

Most SaaS vendors work on a shared responsibility model, meaning you may not be protected against

[1] *Enterprise Strategy Group (ESG)

every contingency. Although this will often vary depending on the vendor, it has to do with where their responsibility ends (in terms of backup and protection) and where your enterprise is responsible for maintaining data protection integrity. You may have a SaaS provider that will handle all the physical aspects and applications related to cloud services and backup. However, protecting your data is still your responsibility.

Sin #3: Not Planning for Impacts to RPO & RTO

The negative impacts cloud SaaS services data loss can have on your company can present serious issues, as the stored data supports ever more important business functions. From finance and accounting systems to collaboration services, project management, human resources, ecommerce, and more, the loss of data in any one of these systems can cause a serious business outage that needs to be prevented.

Recovery point objectives (RPO) complications often arise. Essentially, RPO is defined as the amount of data your company can afford to lose before such losses seriously impact your enterprise's daily operations, resulting in invaluable losses. Many SaaS vendors do back up their own environments, but their overall RPO may not be as stringent as your requirements. If your data is only replicated internally once per day or week, it may not meet your RPO objective of 30 minutes if that's what is required for regulatory compliance.

A more serious issue is the Recovery Time Objective (RTO). For small data sets, your SaaS provider may be able to recover them immediately. For larger amounts of data, you are at the mercy of the SaaS provider especially if they've had a major outage.

Another thing to consider is that SaaS vendors typically do not provide individual account-level data protection, as per the shared responsibility model. They protect against system-wide outages but will not have the capability of recovering an individual customer's account.

If you have backed up your SaaS data externally – you must plan adequately for RPO and RTO. That means frequent enough backups and continuous data protection to meet your RPO and having enough bandwidth on hand to back up your data in a reasonable window. Recovery Time Objectives can also be harder to achieve because you are dependent on redelivering data to your SaaS provider over the internet. You might be able to meet your backup window using incremental backups – but when you must recover, it's going to be all your data at once. If it's terabytes, it's going to take a long time over the internet. And bandwidth is not the only issue you have to account for.

It should be noted that native backup tools and most SaaS backup tools will back up and recover your entire database and not individual user accounts, which may make up most of the recovery requests. However, if you do need to recover a specific user account, you will likely need to recover the entire dataset no matter how large it is.

Another factor affecting recovery time is recovery complexity. Most recovery operations involve multiple data tables that must be recovered in a precise order. An example of this is Jira, a development collaboration and project management system. It includes tables for project data, and tables for attachments, as well as tables for user accounts. The data must be backed up manually, and recovery takes several complex steps. The manual processes take more administrative time and introduce a higher risk of data loss during recovery.

Sin #4: Not Planning for Adequate API Calls

Cloud SaaS solutions can present frequent issues when it comes to Application Programming Interfaces (APIs). They can quickly become a bottleneck where SaaS services are concerned. In addition, managing recovery can be incredibly complex because backup services rely on API calls.

Since all SaaS services are multitenanted, there is a limit of API calls enterprises can make in 24 hours to ensure they have the proper access to the resources they need. When formulating a comprehensive backup plan, API caps need to be considered because the backup and restoration process, as well as API usage, not only impacts the integration solutions of other applications, but can also result in the breakdown of apps and other critical services.

Another important consideration is that choosing the correct RPO metrics and considering API limits can enable a faster restoration and boost RTO. Cloud SaaS service providers must also consider the different API call limits and speeds. Some API caps will be based on the license agreement with your cloud SaaS backup provider, but not always.

Sin #5: Not Understanding Your SaaS Vendor-Specific Challenges

Piggybacking off the contract point above, some of the vendor specifics to keep in mind when considering potential cloud SaaS vendors include assessing the different systems and applications connected with your cloud backup services, as well as the problems you may encounter and the vendor's solutions for specific applications/ systems, such as:

- **Microsoft 365:** Although Microsoft 365 does provide data encryption and offline remote backup, these things will occasionally differ from application to application. Microsoft 365 does local flash copies and near-time replication. However, the downsides are that it doesn't offer complete backup solutions or adequate malware file scanning and only provides 30–90-day data retention periods depending on the data type.

- **Google Workspace:** Multiple issues can arise when it comes to Google Workspace backup and recovery. First and foremost, Google's solution doesn't include a native backup service. Additionally, it only has a 30-day retention policy and doesn't retain copies of deleted emails or mailboxes.
- **Salesforce:** Many companies use Salesforce as a CRM and data management system. However, Salesforce has some common issues that cloud SaaS vendors need to account for and reconcile. First, Salesforce's backup tool only provides a weekly data backup/export tool, meaning it cannot back up data in real time or every hour. It can also cause downtime when it comes to receiving data due to other requests in the system. There are also seven steps to restore recovered data, causing further recovery time complications.

Sin #6: Only Protecting the "BIG THREE" SaaS Services

In many cases, there are already solutions to backup these big 3 SaaS / Cloud services because they are commonly used. Most backup vendors have a solution, including Asigra in their Tigris Ultra Secure Backup solution. But that ignores the fact that the average organization has over 137 SaaS applications in use today. The average person uses nine. Business-critical information is being stored in these services as well, typically unprotected by traditional backup solutions. Some examples of the complexity of protecting SaaS data are below:

- **Atlassian Jira:** Jira provides a 1hr RPO on its entire infrastructure but will not rollback individual accounts. Account data is only retained for 30 days. They recommend that all users backup their databases. Backup requires at least 3 separate tables that must be recovered in a specific sequence. Users must manually back up their service which can be time-consuming without some form of automation.
- **QuickBooks Online:** Like other SaaS tools you'll have to initiate a manual backup of the service, but you can set up automated backups. However, you can't back up and recover all your data. Some of this is non-critical, but others can be very inconvenient and require significant time to rebuild, like recurring transactions, reports, and bank feeds.

Sin #7: Not Having SaaSAssure℠ as Your Backup Solution

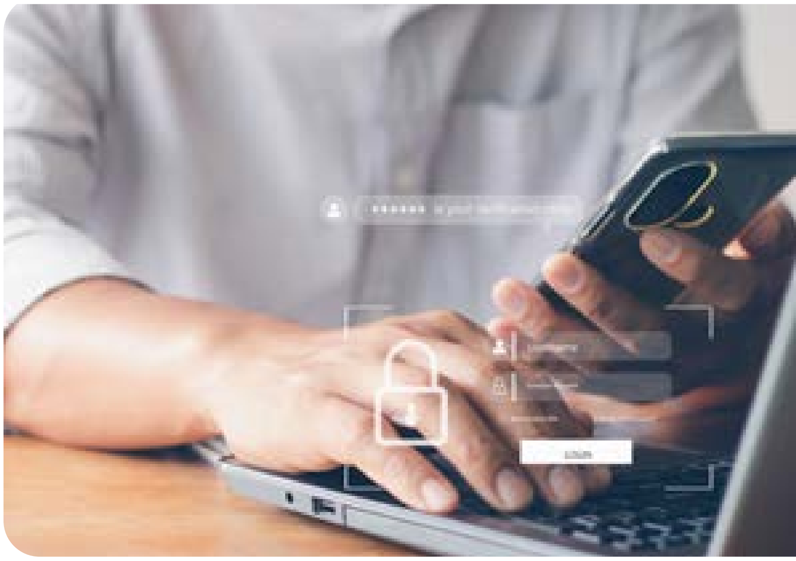
When it comes to comprehensive cloud SaaS backup solutions, Asigra is introducing a new platform to build an ecosystem of support for the thousands of SaaS apps that have no backup support today.

SaaSAssure℠ powered by Asigra has deep integration into dozens of SaaS services providing the benefit of continuous data protection and advanced recovery options for a wide array of business-critical systems, and more SaaS services are on the way. Partners will ultimately have access to an SDK (Software Development Kit) to enable backups for new SaaS apps. The platform will solve many of the challenges that customers face in protecting their SaaS data. In particular, it's designed to make SaaS backups not only possible, but extremely easy to manage. SaaSAssure is fully automated, meaning more efficient oversight and restoration services in the case of an issue. It's multitenanted and built for Managed Service Providers (MSPs), integrators, and other IT providers. Through a single console, an administrator can back up and recover across different SaaS services and different customers. There's no software or agents to install and no need to rip and replace existing software. Backup data can be stored in AWS or any S3-compatible storage that service providers already utilize, to minimize storage costs.

The goal is to simplify restoration steps to improve recovery speed. In addition to a simplified, rapid restoration process, select services will have granular restoration capabilities. For those services where granular restores are available, recovery time objectives will improve dramatically.

Most importantly, SaaSAssure provides the most secure environment for your SaaS data. Cybercriminals are directly targeting backups as a rich source of actionable data and SaaS data is particularly at risk, especially if it's manually backed up as a series of CSV files. A recent example is coming from ongoing revelations about the LastPass hack. Attackers were able to steal the credentials of a senior developer, then use those credentials to access their backup service where they then stole the master vault of all their users stored credentials.

With SaaSAssure, your data is protected by features that make it much harder for attackers to access your critical backup data. These include:



- **Multiperson Approvals (MPA)** – an industry first, you can require multiple people to approve a potentially destructive action that can result in data loss. This means that even if an attacker has access to your backup admin credentials, they will not be able to proceed with harmful actions without additional approvals from other specified users.
- **Multifactor Authentication (MFA**) – you can require users to authenticate using a six-digit Time-based one-time password (TOTP) application, such as Google or Microsoft Authenticator when signing in or attempting to perform a potentially destructive action that can result in the loss of data. MFA is a great first step at protecting systems but fails if an attacker has remote access to a system that an admin has logged into. Once the admin has logged into a service, someone with remote access could take control. Additional MFA requests prevent attackers from proceeding unnoticed.
- **Encryption** – SaaSAssure uses 256-bit encryption in flight and at rest to protect your data with the highest security and compliance standards.

In Summary

SaaS data is more at risk than ever before. The average company uses 137 different SaaS services to run its business, and that data, if lost can result in significant downtime. SaaS vendors do not provide the protection you need to ensure that you can recover your data in the event of a user error, outage, or malicious actor. Native backup tools are difficult to manage and time-consuming to use. Existing 3rd party tools do not provide adequate protection for your backups to ensure that criminals can't steal them. Only SaaSAssure has the breadth of support, ease of backup and recovery, and security to protect your SaaS services.

The average company uses 137 SaaS services

Contact Asigra for cloud SaaS backup solutions and more!

Contact Us

For more information about our SaaSAssure platform, visit www.asigra.com/saasassure.

SaaSAssure℠
powered by Asigra