SaaSAssure℠
powered by Asigra

WHITEPAPER

The Challenges of Backing Up SaaS Services

Why Proper Backups are Crucial

Shared Responsibility Model

Understanding the Importance of Backing Up SaaS Data and Overcoming Limitations

SaaS solutions are used by businesses the world over for everything from accounting, project management, customer relations, resource planning, and even large-scale data storage. Software as a Service, or SaaS, providers provide extensive protection for the data entrusted to them by their customers with enterprise grade backup systems and redundant data centers.

However, just because a SaaS provider has everything backed up in the cloud, doesn't mean that their customer's data can't be compromised, lost, damaged, or stolen by cyber attackers. This is because SaaS providers operate on a Shared Responsibility Model, where in most cases the provider is responsible for protecting their infrastructure and their clients' data against system wide issues, but their customers are responsible for protecting their own data against their own issues. (To read more about customer responsibilities under a Shared Responsibility Model – see the section titled "**The Shared Responsibility Model is Yours to Shoulder**" at the end.)

SaaS Customers *Really* Need to Back Up Their Data

One of the leading reasons to backup SaaS data is that it's extremely valuable. Many businesses host their most crucial data on the cloud, and if it's lost or falls into the wrong hands, it can be incredibly costly to recover. Additionally, most businesses nowadays use many different SaaS services for everything from payroll to ERP solutions; in some cases, a business could employ hundreds of services that generate business-critical information.

As mentioned above, although various SaaS providers do have enhanced security options, your customer's data is still at risk from several things, including:

Internal Factors: SaaS data can be put at risk internally in many ways. For example, staff could accidentally delete files without realizing it until later. Unfortunately, most SaaS vendors only allow a certain amount of time for deleted files to be recovered until they're automatically wiped. In fact, recent studies have shown that approximately 76% of companies experience data loss due to accidental deletions.

External Factors: There are also external risks to cloud data, such as cyberattacks or ransomware attacks that can be

incredibly costly and damaging to a company's reputation. For example, a cyber attacker could gain access to a SaaS customer's credentials remotely and hold their most valuable data for ransom, or threaten to release sensitive information to the public.

Malicious Actors: Malicious actors within a client organization can also compromise data. Disgruntled employees can leak passwords to cybercriminals, or delete or steal sensitive information themselves.

Vendor Outages: SaaS providers are not immune to service disruptions and outages. They are also just as vulnerable to attackers. Although most vendors have some level of protection in terms of backups and will take steps to safeguard and recover their data, many operate on a shared responsibility model, meaning, in the event of an outage, the client is ultimately responsible for protecting their own data on the cloud. That's why many recommend implementing third-party backup measures. In the event of a lengthy recovery, clients should have a copy of their data to access or bring to another provider as necessary.

E-Discovery: It's important for clients to have access to their data for e-discovery to meet ever-growing regulatory requirements.

Vendor Migration: To prevent vendor lock-in, clients should maintain easy access to their data to allow for a smoother transition to a different SaaS provider in the future.

SaaS Vendor Limitations

SaaS services have some innate limitations when it comes to allowing customers to protect their own

So, if businesses are storing business-critical data that their SaaS provider is not ensuring, why aren't those businesses backing up their data themselves?

data, and that's due to the nature of how these services are designed. Think about how any application is designed. An application is a combination of a code base that is designed to perform specific functions, such as managing projects. The application has settings that are customized to the business needs of the organization using it, and then user data is stored in a database within the application. In a traditional data center, the business can protect the application in several ways – including backing up the database or backing up the entire application and data as a set.

A SaaS service is designed as a multitenant service, or a service providing for multiple businesses at once, allowing isolated settings and user data to be stored independently for each business. There are obvious advantages to designing applications as SaaS services, but it makes it more difficult to allow each business to back up their own instance. There's no easy way to extract both an individual company's data and other settings stored in the application. That is somewhat by design. A SaaS provider generally doesn't have too many incentives to make it easy for their clients to take their data and move it to another SaaS provider. It creates vendor lock-in, which is good for the vendor but

creates some challenges for an organization looking to back up their data.

- **Lack of Built-In Backup Capabilities**

There is a lack of built-in backup capabilities for cloud SaaS vendors that pose many issues for businesses. Often, vendors will provide export functions to enable a client to take native backup measures. However, these functions will usually only allow users to export their data as several .CSV tables, and usually can't be automated. This can create further complications when these tables need to be recovered.

A good example of this is the capabilities offered by Zoho, a leading SaaS provider of customer relationship management, or CRM, software and related services for SMBs (small and medium-sized businesses). Their core product, Zoho CRM, has dozens of modules that can be used by their customers: from Contact Tables to Company Tables, to Tasks, Reports, and Dashboards. If a customer wants to back up their data, there are options available but limitations by payment tier. Their enterprise tier only allows a maximum of four backups per month. The backup is generated not as one file, but as a series of .CSV files representing each of the modules in the CRM. Once a backup is complete, they can be downloaded from a link.

This data is extremely valuable, and it begs the question: why would they limit the number of backups that can be done? One of the limitations that SaaS providers have is bandwidth. If customers could perform as many backups as they want, this could put an unreasonable amount of strain on their available resources. Unfortunately, this isn't sufficient for most organizations' Recovery Point Objective (RPO) policies, which may be as little as 30 minutes of data loss. Note – some of these policies may be driven by regulatory compliance requirements, or customer contractual agreements that a SaaS customer may be in violation of.

In addition to the limitations above, when it comes to backup capabilities offered by SaaS providers, they also have API limits that restrict the amount of data they can export daily.

- **Lack of Built-In Restore Capabilities**

To restore business-crucial data in the event of a deletion or attack, SaaS providers have limited built-in restore capabilities. Usually, the process involves manually reimporting .CSV files. As files are being imported, the service may be unavailable, meaning end users won't be able to go about business as usual, creating costly downtime.

Just like many vendors have daily API limits for exporting data, they also have limits for importing it as well. A client could be in a situation where they can't access their content for multiple days if they have an excessive amount of data to restore. Lastly, there's the chance that their only recourse is to restore all their data at once, potentially overwriting any new data put into the SaaS service after the last backup was done. The result is lost data and more downtime.

- **Not All Data is Included in Exports/Backups**

Each SaaS vendor has limitations as to what types of data can be accessed. A good example of this is the cloud accounting and bookkeeping service QuickBooks, which backs up standard transactions but doesn't back up recurring transactions. Another example is Zoho, which does not allow backup solutions for workflows, but it does for CRM data.

Another type of data often not included in native backups is metadata – information about the information stored in a SaaS service – which can

sometimes be just as vital as the data itself. The cloud SaaS vendor Box, for instance, allows users to create custom metadata for organizing client files and projects, but when they perform native backup solutions from the cloud, this information isn't exported with the rest of their data.

- **Data is Unencrypted In-Flight and At-Rest**

The native backup options that SaaS vendors make available have another big flaw. By allowing customers to download their data as .CSV files, those files are sent across the internet as unencrypted, non-password protected files.

Unencrypted data that's in transit or at rest can be easily compromised. Files can be intercepted by middleman attacks. Files are usually downloaded to a customer's downloads folder. They may be copied or moved to a destination folder, but an unencrypted version of the file may be easily accessed or recovered. A resourceful attacker can easily find these files and have access to sensitive customer data.

- **Limited Third-Party Backup Provider Catalogues**

There are, of course, third-party tools that exist to backup SaaS services, but these are not without their limitations. For example, some of the most popular enterprise backup vendors provide SaaS backup solutions, but often only for a few leading services like Google Workspace, Salesforce, and Microsoft 365. There are a few SaaS backup providers that have more options, but usually fewer than 10 services, and limited ability to protect more. There are many point solutions for individual SaaS services. Unfortunately, there is no "standard" today for unified SaaS backup.

Considering businesses have an average of 137 SaaS applications in use, this means that many of those services are unprotected. And if they are, they may have dozens of different backup interfaces to contend with to provide a comprehensive backup solution.

One Platform for Unified, Simplified, and Secure SaaS Backup

With **SaaSAssure℠ powered by Asigra**, customers can safeguard their most business-crucial data. The platform allows for fully managed backup capabilities, tying directly into some of the most popular SaaS services (including CRM, HR, Project Management, Collaboration, File Management, Financial Services, etc.) on the market.

Core features clients expect from an enterprise backup solution are available, including fully automated backup and recovery, a unified management interface, backup job reporting, role-based access, and more. Some SaaS services will allow for incremental backups and granular restores (depending on the SaaS vendor API). For managed service providers, Asigra SaaSAssure℠ offers built-in billing and multitenant capabilities, as well as simple payment models. They can use their own S3-compatible storage repository to store and protect their client's backed up data.

With AES 256-bit data encryption algorithm both in flight and at rest. as well as **multifactor authentication (MFA)** and **multiperson authorization (MPA)**, customers' most crucial in-flight and at rest data always remains protected. Multiparty authorization is an industry first approach providing critical protection against motivated attackers. An attacker with access to backup service credentials can create tremendous damage, setting clients up for ransomware (and double ransomware)attacks. With MPA, an attacker using

compromised credentials can only initiate specific data-destructive tasks when other authorized individuals also provide consent. This service can stop attacks in motion and provide a warning that an attack is underway.

Most importantly, Asigra is developing a pathway to standardize SaaS backup across the industry. Asigra is providing a software development kit (SDK) along with the platform to enable managed service providers, system integrators, and SaaS vendors to easily and quickly create plug-ins for SaaS platforms, eliminating a weakness from other third-party backup offerings. By providing an SDK, theoretically, any SaaS service with an accessible API will be able to bring itself into the SaaSAssure platform.

Summary

SaaS customers can face many difficulties when attempting to back up their data stored on SaaS platforms. While SaaS providers offer some level of data protection, clients are responsible for safeguarding their own data from accidental deletions, cyberattacks, malicious insiders, and vendor outages. SaaS services often lack built-in backup and restore capabilities, fail to include all data types in exports, and send unencrypted data across the internet. Third-party backup providers have limitations as well, typically covering only a few popular services. SaaSAssure℠ aims to address these challenges by offering unified, simplified, and secure backup solutions for all SaaS services.

The Shared Responsibility Model is Yours to Shoulder

Any SaaS service is made up of two critical components: the SaaS vendors application (and the infrastructure to run it), and the customer's data. Because of this, they share the responsibility of protecting the infrastructure and the data. Each party has to protect their aspect of the service.

A common misconception is that the SaaS vendor is protecting the client's data because they are protecting their infrastructure. The distinction is that they are protecting the client's data only when data loss could be caused by an infrastructure problem. So, if the SaaS vendor's servers go down, resulting in data loss, they will recover their platform using their latest backups. They have a service level that they agree to meet in the terms and conditions.

Because of this, clients often assume that they are also protected against all potential data losses or breaches. However, when looking at the fine print of many SaaS contracts, the responsibility for data loss often falls on the customers' side if it results from their action or inactions. For example, if an employee accidentally deletes important files like a set of projects they were working on, or a malicious actor gains access through an employee's compromised credentials, the SaaS vendor might not be obligated (or able to) recover the data.

Let's consider some examples:

The Terms of Service for Google Workspace, for example, states that Google "will not be responsible for any harm to your computer system, loss or corruption of data, or other harm that results from your access to or use of the Services".

Microsoft's Service Agreement similarly states, "Microsoft isn't responsible for the loss of your data or for the backup or recovery of your data".

BambooHR's Terms section 4.4 state "4.4 Your Responsibility. You are solely responsible for your Data, and all uses of your Data that occur through your account or any actions taken by your employees, admins, consultants, agents etc. in your account."

Xero's Terms are almost helpful "36. Data loss: Data loss is an unavoidable risk when using any technology. You're responsible for maintaining copies of your data entered into our services. For information on how to do that, check out how to export data out of Xero on Xero Central."

Some SaaS vendors don't specifically mention responsibility for backups in their terms and conditions, but cover the responsibility in the "limitation of liability" section of their terms, which includes data.

Confluence's Terms state "WITHOUT LIMITING OUR EXPRESS OBLIGATIONS IN THESE TERMS, WE DO NOT WARRANT THAT YOUR USE OF THE CLOUD PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, THAT WE WILL REVIEW YOUR DATA FOR ACCURACY OR THAT WE WILL PRESERVE OR MAINTAIN YOUR DATA WITHOUT LOSS."

Dropbox's Terms state "IN COUNTRIES WHERE EXCLUSIONS OR LIMITATIONS OF LIABILITY ARE ALLOWED, DROPBOX, ITS AFFILIATES, SUPPLIERS OR DISTRIBUTORS WON'T BE LIABLE FOR: ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF USE, DATA, BUSINESS, OR PROFITS, REGARDLESS OF LEGAL THEORY."

The point is, if one reads and reviews the terms and conditions of any SaaS service, one will see language like this that explicitly or implicitly places the burden of responsibility for data, and therefore data protection, onto the customer.

Moreover, in the case of cyber-attacks like ransomware, even if the SaaS provider has security measures in place, it's possible that the customer's data could still be impacted, and recovering it might not be the vendor's obligation.

Therefore, businesses using SaaS platforms should not solely rely on their vendors for data protection. They should adopt an active approach in understanding the Shared Responsibility Model and implementing a comprehensive backup strategy. This could involve using third-party services that specialize in SaaS data backup for their critical SaaS services, or maintaining separate, secure backups of their data independently.

About Asigra

Asigra has been providing secure backup and recovery solutions for organizations of all sizes, including managed service providers, for over 37 years. The company prioritizes innovation, consistently launching new advances to protect your data. Their solutions cover servers, virtual machines, endpoint devices, and SaaS-based applications. Asigra was most recently recognized as CRN's coolest data protection vendor for 2023 and CRN's 2023 MES midmarket top 100 vendors that support the growth and innovation of midmarket organizations.

Contact Asigra for cloud SaaS backup solutions and more!

Contact Us

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

SaaSAssure℠ powered by Asigra

© 2023 Asigra Inc. Asigra, the Asigra logo, and Attack-Loop are trademarks of Asigra Inc. All other brand and product names are trademarks of their respective owners. [10/23]