Spin.ai

BUYERS GUIDE

Comprehensive SaaS Backup Buyers Guide

Table of Contents

Introduction

Data is the lifeblood of most hybrid environments. Businesses largely use processes and systems with applications that are data-driven. Even real-time business decisions are made based on data collected across on-premises and cloud environments. Also, SaaS environments are heavily used for modern productivity and communication. Users also use these for collaboration between departments and teams.

It is important to note that SaaS vendors don't take responsibility for protecting critical data found in these SaaS environments. Customers are ultimately responsible for their own data. Let's consider what items and features should be found in your SaaS backup evaluation criteria in order to make the right choice in choosing SaaS data protection.

SaaS apps are gaining popularity across the enterprise

What is SaaS Data Protection?

SaaS data protection backs up and restores the data in your SaaS environments like Microsoft 365, Google Workspace, and Salesforce. You are taking a copy of the production data as it is stored in the cloud and creating a separate copy of the data outside the SaaS environment. This helps to make sure if data is lost, it can be recovered.

However, not all SaaS data protection solutions are created equal. Businesses need to consider the details of each solution before making the decision it should be used to protect their SaaS environment.

Why are SaaS Backups Needed?

Despite the idea that SaaS environments are immune to things like ransomware and user error, this couldn't be further from the truth. Realistically, the exact same reasons for data loss on-premises can happen in the cloud.

Cloud data is subject to the same types of cyberattacks, accidental deletions, and hardware failures that happen on-premises. When it comes to cloud storage, ransomware can encrypt data that exists locally on a PC, and the encrypted (latest modified) data will be synchronized back to the cloud and overwrite the good copy of data. Cloud providers can also have security breaches and hardware failures that can result in data loss.

Shared Responsibility Model

There is another key consideration that makes SaaS backups necessary. Modern cloud providers operate in what is known as a "shared responsibility model." This model splits responsibilities for the customer's environment between the cloud provider and the customer.

Cloud providers are generally responsible for the physical infrastructure and its security as well as the software systems that underpin the SaaS environment. However, customers are ultimately responsible for protecting their data. If data loss happens, cloud providers are shielded from the responsibility of getting the data back.

SaaS Data Protection Considerations

Organizations need to consider key factors when implementing their SaaS data protection strategy. Note the following important concepts and requirements:

Who Owns the Data and is Responsible

Organizations need to understand that while SaaS vendors take care of the physical infrastructure and security, they have the responsibility for protecting their data, according to the shared responsibility model.

Access Policies for Data

Policies need to be defined to access and work with data. Implementing role-based access and knowing who has access to critical data is essential for compliance and security.

Compliance Regulations

Today, organizations must comply with many crucial compliance regulation frameworks like GDPR, HIPAA, and others. Non-compliance can lead to significant fines and damage to your organization's reputation. Customer confidence can lead to huge fiscal impacts. Businesses must regularly review and update compliance measures to align with regulations that can often change.

Data Loss Prevention (DLP)

Data loss prevention helps prevent accidental or malicious data loss. DLP tools help monitor for unusual data transfers, and then they can flag these for visibility or for applying policies. It goes a long way in preventing data breaches and data leaks to unauthorized users.

Understanding Data, Backups, & Other Important Metrics

Businesses must do their homework before understanding their SaaS backup and data protection needs. One of the first requirements is actually understanding the SaaS data itself. Note the following:

Discover & Understand Critical Data

Data discovery is an important part of selecting a SaaS backup solution. After all, if you don't understand your data, it will be challenging to understand which data needs protection. Data should be classified based on how important it is to the business. Businesses should consider the impact of losing critical data on business processes.

Assess Current Backup Solutions

Evaluate existing backup solutions and identify gaps in how effective data is protected. Understanding the SaaS capabilities of your current backup solution, if any, helps to understand the limitations or challenges with protecting your data. Only then will you be able to select a SaaS backup solution that can bridge your data protection gaps.

Define RPO & RTO

Establish a Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These allow you to understand how often data should be backed up and how quickly it needs to be restored. These two metrics are extremely important in determining the frequency and speed of backups, which can help to minimize data loss and downtime.

Features When Choosing a SaaS Backup Solution

When looking for a modern SaaS data protection solution, there are key features that need to be considered. Note the following:

○ **Comprehensive Coverage:** Make sure the chosen solution protects all SaaS applications used by your organization. For instance, in Microsoft 365, it may back up OneDrive, but not SharePoint. A comprehensive solution should be able to back up data from all SaaS applications such as Google Workspace, Microsoft 365, Salesforce, and Slack to avoid data protection gaps.

○ **Automated Backups:** Automated backups reduce the likelihood of human error and it makes sure backups are performed regularly.

○ **Data Recovery:** Choose a backup solution that allows granular restores (ability to restore individual files) of email and files without needing to restore everything. This feature keeps restore operations efficient and reduces the time needed to recover from a disaster caused by deleting only a few critical items.

○ **Security & Compliance:** Security is an absolutely critical aspect of modern data protection. These need to use encryption, access controls, and align with compliance frameworks to be effective. Compliance with these regulatory frameworks helps to avoid legal woes and makes sure organizations can uphold data security best practices in data protection.

○ **Data Locality:** Does the SaaS data protection solution allow backup data to be stored in a way that aligns with data locality requirements and industry best practice standards? For example, it would be best practice to store cloud data outside the same cloud from which the data is backed up (i.e., Microsoft, Google, etc).

○ **Scalability:** The solution should be able to scale with your business needs without performance impacts or architecture challenges. The backup solution should be able to handle any increase in data as your data use grows.

○ **Easy-to-Use Interface:** Make sure the SaaS data protection solution has a user interface that is easy to use and provides efficient backup management. An interface that is challenging to navigate could lead to backup inefficiencies or even data loss if data that is expected to be backed up is not backed up.

○ **Proactive Malware Protection:** Look for solutions to proactively stop malware attacks, like ransomware, and offer data leak prevention. It helps to add an extra layer of security to your data protection strategy.

○ **Use of Official APIs:** Make sure the chosen data protection solution uses official APIs for data extraction and restoration. It reduces the risk of breaking the backup solution or disruption to data backups and recovery by changes in the SaaS application.

SaaS Backup & Application Governance

Governance helps to make sure that SaaS applications and their data are administered securely and are in compliance with regulatory frameworks. Governance helps establish policies and procedures for data protection, regular audits, and employee training.

Best Practices for Governance

Regular Audits

Organizations need to regularly audit their environments to ensure compliance with data protection policies. It can help identify vulnerabilities and ensure that backup practices are up-to-date.

Policy Development

Create data protection and backup policies that provide a clear framework for data management. This helps to make sure all stakeholders understand their roles and responsibilities.

Employee Training

Train employees on the importance of their role in ensuring data security. Threat actors can often compromise data due to the actions of unsuspecting end users. Regular training sessions can keep employees informed about the latest security threats and what to look for.

Continuous Monitoring

Continuously monitor the effectiveness of backup solutions. Monitor which data is backed up and look for any gaps in coverage to make any needed adjustments. Monitoring tools can provide real-time insights into backup operations and highlight areas for improvement.

Built-In Backup Capabilities are Often Not Enough

Some SaaS applications offer built-in backup capabilities, but these are often not enough to cover all aspects of data protection needed. It is crucial to ask SaaS providers about their backup guarantees. Is there compensation for data loss? What is the granularity with which data backups can be achieved?

SaaS backups are crucial for data protection

Third-Party SaaS Backups

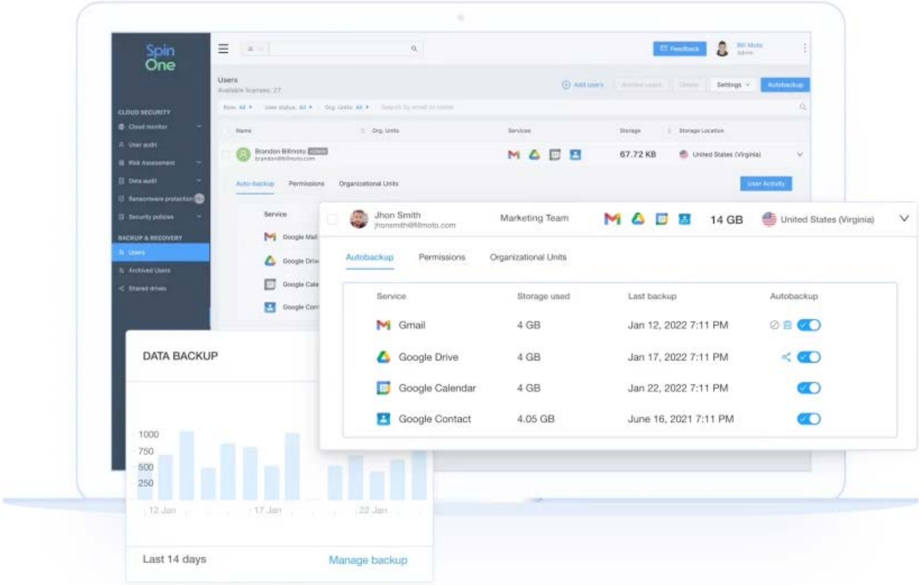
Third-party backup solutions are generally more powerful and contain robust features and capabilities not found in built-in backup solutions from SaaS vendors. What are some critical factors to consider when choosing third-party options?

When considering third-party options, evaluate where the backup data is stored. Also, consider whether the solution uses official APIs and whether it is vulnerable to breaches. Does it have built-in cybersecurity features, like data leak prevention, ransomware protection, and others? What is the SLA to get data back?

How SpinBackup Tops the SaaS Backups Buyer’s Guide

SpinBackup is a top solution for businesses looking to protect their critical SaaS data and “check the boxes” needed for security and compliance. SpinBackup takes the approach that backups and cybersecurity are one and the same and not separate solutions for protecting your data.

It integrates features like automated backups, ransomware protection, and granular recovery options. It makes sure that organizations can protect their critical data across multiple SaaS platforms, and not just one. It provides an industry-leading SLA to recover your data following a ransomware attack in 2 hours.



Brandon Billmoto ADMIN — 67.72 KB — United States (Virginia)

Jhon Smith
jhonsmith@fillmoto.com — Marketing Team — 14 GB — United States (Virginia)

Autobackup | Permissions | Organizational Units

Service	Storage used	Last backup	Autobackup
Gmail	4 GB	Jan 12, 2022 7:11 PM	✓
Google Drive	4 GB	Jan 17, 2022 7:11 PM	✓
Google Calendar	4 GB	Jan 22, 2022 7:11 PM	✓
Google Contact	4.05 GB	June 16, 2021 7:11 PM	✓

Note the following additional features:

Backup Automation

SpinOne provides backup automation and allows you to schedule backups for continuous data protection without manual human-driven processes.

Proactive Ransomware Protection

It can detect ransomware attacks in real time and take immediate action to stop the attack and recover any data affected.

Granular Recovery Options

You can restore individual files, email items, or entire datasets. This allows for flexibility and minimizing downtime.

Compliance & Security

SpinOne helps organizations comply with industry compliance frameworks like GDPR and HIPAA. It provides robust security features like encryption and multi-factor authentication.

Intuitive Interface

It has an intuitive interface that helps simplify backup management. It also reduces the learning curve for admins.

Scalability

SpinOne can scale infinitely based on the growing data needs of organizations. It is suitable for small to large organizations of all sizes.

Real-Time Monitoring & Alerting

It provides continuous monitoring of data and system activities. You can think of it like an automated security operations center protecting your environment 24×7×365. It provides real-time alerts and reports to identify potential threats promptly.

API-Based Backup & Restore

It uses official SaaS vendor APIs for data extraction and restoration. This helps to ensure future compatibility and reliability.

SpinBackup is part of SpinOne, the all-in-one SaaS security platform for mission-critical SaaS apps. SpinOne provides SSPM, DSPM, Risk Assessment, Ransomware DR, Backup, and Archive. It helps enterprises enhance cyber resilience, streamline security operations, and reduce security costs.

Conclusion

Selecting the right SaaS backup and data protection solution is absolutely critical for modern organizations to protect their important data. The features and capabilities of how well you can protect your data are often directly related to the backup solution chosen. Choose a solution that meets your requirements, including backups and built-in security and compliance features. Sound governance strategies help make sure of compliance and protect against security risks associated with data loss.

Request a demo of SpinBackup today.

BOOK A DEMO

About Spin.AI
Spin.AI is an innovative provider of SaaS security solutions for mission-critical SaaS apps (Microsoft 365, Google Workspace, Salesforce, and Slack). Our all-in-one SpinOne platform helps organizations mitigate risk, save time, reduce downtime, and improve compliance.