



EBOOK —

Essential Guide to Choosing a SaaS Backup Solution

What You Need to Know



Table of Contents

[Key Considerations for SaaS Backup Solutions / 3](#)

[Choosing the Right SaaS Backup Provider / 5](#)

[Deep Dive on Recommended SaaS Backup Features / 7](#)

[Compliance and Security Features / 9](#)

[Backup and Recovery Capabilities / 11](#)

[Pricing Models and Cost-Effectiveness / 14](#)

[What are the common pricing models for these tools? / 16](#)

[How much do these SaaS backup tools typically cost? / 18](#)

[Are there any free SaaS backup software options available? / 20](#)

[Conclusion — Choosing a SaaS Backup Solution / 22](#)

A photograph of two men sitting at a table in a meeting. The man on the left is wearing a blue patterned shirt and is pointing at a laptop screen. The man on the right is wearing a dark blue polo shirt and is smiling. There are two white coffee cups on the table, one in front of each man. The background is a blurred office or meeting room with large windows.

Key Considerations for SaaS Backup Solutions

KEY CONSIDERATIONS FOR SAAS BACKUP SOLUTIONS

With the proliferation of SaaS applications used by businesses of all sizes, SaaS backup solutions are becoming an increasingly urgent necessity. There are dozens of different SaaS data protection offerings available on the market, but they are not created equally and may not be suitable for every organization's needs.

This e-book will provide you an overview of the core features that enterprises should consider when choosing a backup solution for their critical SaaS data.





Choosing the Right SaaS Backup Provider

CHOOSING THE RIGHT SAAS BACKUP PROVIDER

Of all things SaaS backup products do, at a bare minimum they need to backup and recover SaaS data. But to support enterprise workflows they need to do more than just that. There's lots of free utilities on the market to backup SaaS data, but these utilities lack the capabilities needed to maintain data integrity, service uptime, ensure security, and comply with regulations. Some of the general areas that SaaS backup solutions should have are as follows.

Comprehensive App Support (comprehensive in the app, and # of apps)

With the popularity of Microsoft 365 and Salesforce it's no surprise that there is a wide range of support for these SaaS services. But these are only two of the hundreds of SaaS services businesses use every day. A SaaS backup solution should have support for a wide range of SaaS services covering different business operational functions including HR, Finance, Marketing, Sales, Development, etc.

Advanced Security Features

SaaS backup services are frequent targets for cybercriminals because they store valuable company and consumer data. The data can be compromised

or stolen and used in ransom campaigns. Backup services should be protected against internal and external threats with advanced authentication, encryption, and role-based access controls.

Ease of Use / Modern UX

Care should be taken to choose a solution with a modern user interface that is easy for administrators to use, yet powerful enough to automatically backup and restore SaaS data in a uniform way across multiple target SaaS services.

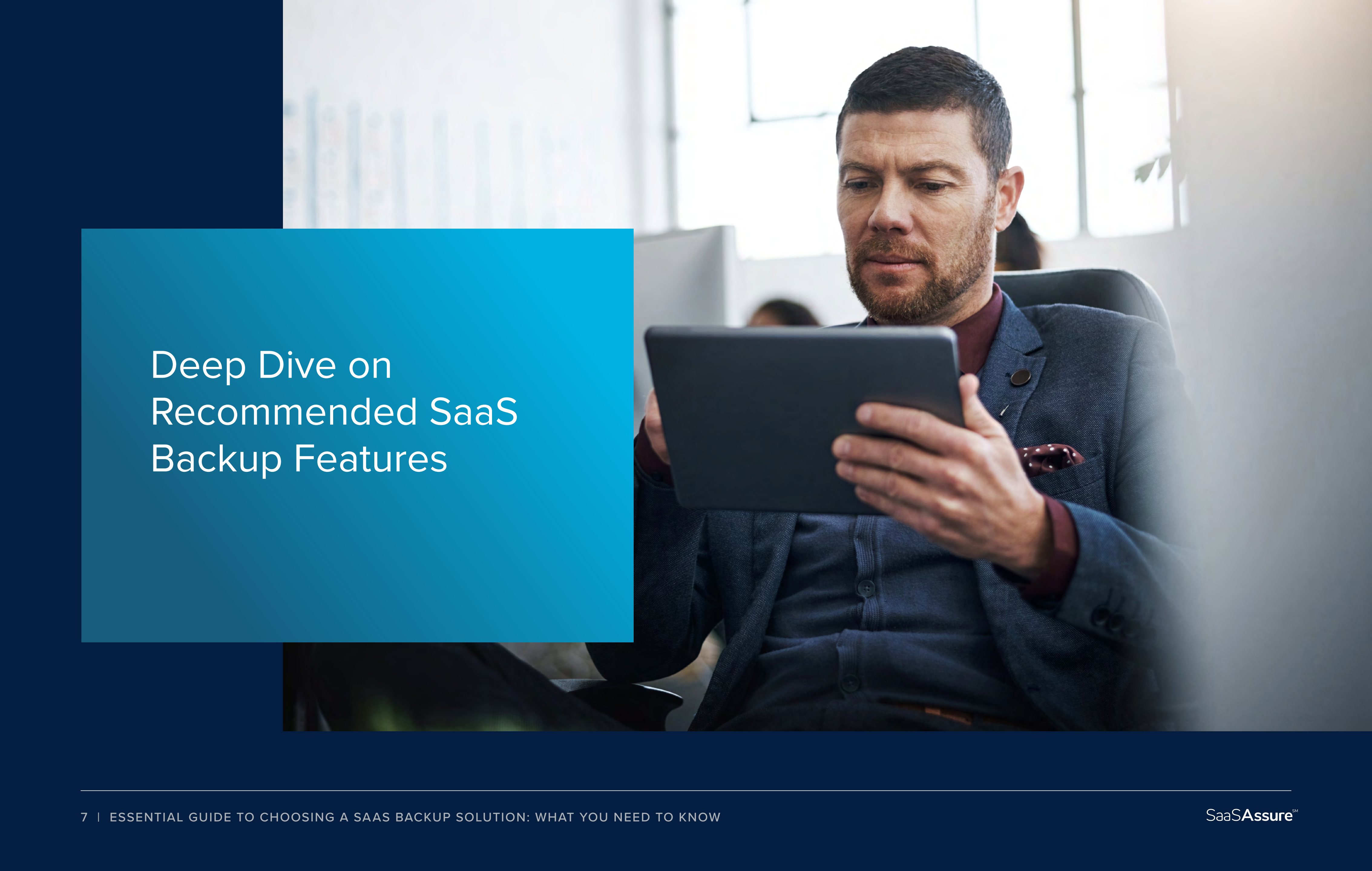
Managed Service Provider (MSP) Support

Since much of the work of backup processes is typically outsourced to MSPs, the software should be

designed with multitenancy features by default and include an ability for MSPs to delegate authority to segregated admins, provide dashboards and reports for clients, and provide an easy way to bill customers for use.

Cost Effective & Fair Pricing

Pricing for a SaaS backup service should be easy to understand and align with the type of SaaS service being backed up. SaaS apps with more users than data should be priced by the number of users, and apps with more data than users should be tiered by the amount of data to backup. There should be clear upfront pricing terms without hidden fine print and overage gotchas that surprise IT buyers.

A man with a beard, wearing a dark suit jacket over a maroon shirt, is sitting in an office chair. He is holding a tablet computer with both hands and looking at the screen. The background is a blurred office environment with windows and other people. A large blue rectangular overlay is on the left side of the image, containing white text.

Deep Dive on Recommended SaaS Backup Features



DEEP DIVE ON RECOMMENDED SAAS BACKUP FEATURES

With some of the larger categories covered, let's dive deeper into some of the specific features that IT leaders should consider as required features for their chosen SaaS data protection solution.



Compliance and Security Features

COMPLIANCE AND SECURITY FEATURES

Multifactor Authentication (MFA)

By default, any SaaS backup solution should be protected by a multifactor authentication solution. Given the prevalence of SMS hijacking attacks, and phishing campaigns a strong MFA solution would use an authenticator service like Microsoft or Google Authenticator.

Multiperson Approval (MPA)

Another innovation in authentication security is Multiperson Approval. SaaSAssure is a SaaS data backup solution that created this security advancement. If an account is successfully hijacked, or if a backup admin has gone rogue, they can do a lot of damage to backup data. Ultra secure solutions can be set up to require multiple admins concurrent approval to perform data destructive actions like deleting a backup job or canceling a backup job set. This not only protects against insider threats but can also mitigate the risk of human error.

Encryption

Because of the sensitivity of backup data, the backup solution should be protected with AES 256-bit encryption for data in-flight and at-rest.

Role-Based Access Controls

Simple backup tools let one administrator have access to all data. An enterprise solution should have support for multiple admins with the ability to separate access controls by administrator and by admin role. For example, backup admins may be able to create backup jobs and recover data but may not be given the ability to delete backup sets, cancel jobs, or make any other administrative changes. It's especially important in multitenant environments where different admins are assigned to different clients or operational groups.

Compliant with Regulatory Frameworks

The backup solution should help organizations comply with an ever-changing regulatory environment, specifically by ensuring that data is discoverable, protected, and recoverable.

A man with a beard and glasses, wearing a light blue shirt and a lanyard with an ID badge, is holding a tablet. A woman with glasses, wearing a light blue shirt and a lanyard, is looking at the tablet. They are in a server room with racks of servers in the background.

Backup and Recovery Capabilities

BACKUP AND RECOVERY CAPABILITIES

While the primary function of SaaS backup solutions is data backup and recovery, the methods and range of features offered can vary significantly. Here's more detail on what should be considered for enterprise solutions.

Smooth Integration into Apps

The backup service should have a smooth, seamless integration process into the target app. The most you may have to do is to get an API code from the target app. The more complex the connection process, the more chances there are for human error which could lead to data backup errors or an inability to recover data as needed. Ideally, the backup service should work seamlessly with the app as well, and not require you to acquire extra "API" call credits from the target app to work.

Comprehensiveness

The backup service should be comprehensive in two senses of the word. First, it should back up all data in the service necessary to do a full recovery. For example, in a CRM, this would encompass all tables, and in the case of an image gallery, all image files. In an office application, it includes all files and records of collaborative communications.

Secondly, as mentioned above, it should cover more than just Microsoft 365 and Salesforce. A good solution would have support for popular apps in finance, HR, development, marketing, sales, and other operational areas.

Metadata Backup

In addition to collecting all data in a backup, there's also the concept of metadata, the data about your data. All but a few SaaS backup services exclude this data, which can

create problems during the recovery process, and some of the data may be requested for compliance auditing purposes.

Incremental Backups

There should be support for incremental backups. If the SaaS service performs a full backup each time, backups will take longer and have a higher risk of failure when dealing with large volumes of data. Incremental backups can dramatically reduce the time to backup, and with the right technology can be merged into an initial full backup indefinitely.

Storage Flexibility

Some SaaS backup services provide no choice of where the data is backed up. In those cases, it's on the same storage infrastructure that the SaaS backup vendor runs its service on, which does not necessarily guarantee a secure environment. An enterprise SaaS backup solution will provide flexibility to allow customers to choose the target storage environment, which ideally will have a choice of region to satisfy compliance requirements.

Scalability

The backup solution should be scalable and able to handle a growing customer base with many users and significant amounts of storage. It should also be able to handle multiple simultaneous backup jobs and recovery operations across thousands of clients.

BACKUP AND RECOVERY CAPABILITIES CONT'D

Granular Recovery Options / Flexible Recovery Options

Flexible recovery options should be available for all protected services, allowing backup admins to either do a full recovery should they need to recover all data, or to selectively recover a single user or group of users who may have accidentally deleted data.

Point-in-time Recovery

Because data errors can happen at any time, and not be discovered until much later, it's possible for users to request a recovery of a record from weeks or months prior to the request. Your SaaS backup service should be able to perform a point-in-time recovery of a record.

Customizable Retention Policies

Because different regulations have different retention requirements for different types of organizations and data, the SaaS service should have some flexibility in the retention periods it can set by backup job.

Historical Dashboard, Reports, Alerts & Audit Log

A user-friendly dashboard should be available to make it easy for administrators to check on the status of their backup and recovery jobs, and to quickly re-initiate them if the job has failed. Alerts should be made when problems with jobs arise, and there should be an audit log for senior administrators and management to inspect what tasks backup admins have performed.

MSP Friendly Features

Managed Service Providers (MSPs) should carefully evaluate the capabilities of SaaS backup products before use, as many products claiming to support MSP features may not perform as expected. For example, it should support increasing workloads and the addition of new clients without requiring extensive redesign or reconfiguration. Some solutions, like SaaSAssure, are built specifically with the MSP in mind.

Multitenancy

There should be built-in support for multitenancy. It should be straightforward to set up multiple admins, separate their access rights, and create separate jobs by clients. Clients should not be able to see other client's data, and assigned admins should only be able to access the clients they are assigned to.

Built-in Pricing & Billing

Along with multitenancy, there should be built-in support for displaying service pricing to clients, adding or modifying users, and logging usage for billing purposes. The service should integrate with existing MSP invoicing tools to allow them to simplify the billing process for their end clients.

Admin Dashboard

A nice thing to have is a dashboard that admins can access to see the performance of their backup jobs and to review any other relevant data. At the very least admins should be able to see job status reports that are client specific. regulatory environment, specifically by ensuring that data is discoverable, protected, and recoverable.



Pricing Models and Cost-Effectiveness



PRICING MODELS AND COST-EFFECTIVENESS

There's a wide variety of SaaS backup services available and just as wide a variety of pricing models, subscription schemes, and costs. Some services are very upfront about the pricing available, and others hide the pricing between opaque quoting processes. Special care should be taken to ensure that there are no hidden costs like excessive overage fees or especially long terms with punitive cancellation policies.



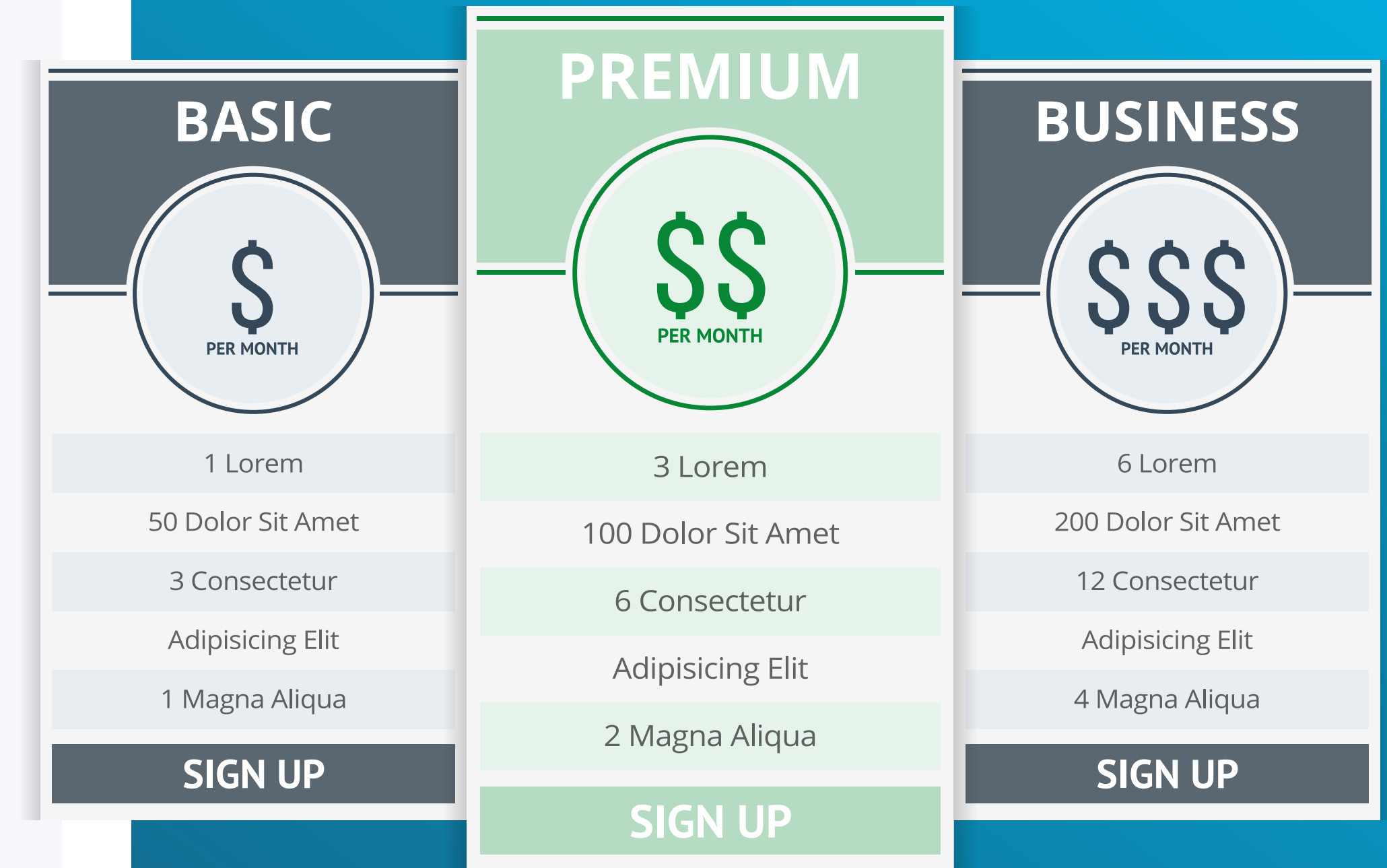
What are the common pricing models for these tools?

WHAT ARE THE COMMON PRICING MODELS FOR THESE TOOLS?

There are a few common pricing models that exist for SaaS backup services. The first is a simple per user pricing model. These are fairly predictable and scale up or down with the number of users protected.

Another model is a storage-based model, where the cost is rated by the amount of data being backed up. This is less predictable, especially when the amount of storage being used by clients is highly variable. This model might make more sense for apps like HR services where there is a small number of users in an organization, but a large amount of data important to all employees that need to be protected.

Another model we've seen is a "per app" model, where each app protected adds to the overall cost. These models tend to be overpriced for most customers based on their typical usage though.





How much do these SaaS backup tools typically cost?



HOW MUCH DO THESE SAAS BACKUP TOOLS TYPICALLY COST?

Again, there's a wide range of costs, but typically these tools will range from as low as about \$3 to as high as \$7 per user. Services that have lower per user rates than these usually do not include many of the features necessary to support enterprise or MSP use cases.

Are there any free
SaaS backup software
options available?



ARE THERE ANY FREE SAAS BACKUP SOFTWARE OPTIONS AVAILABLE?

There are a few utilities on the market that are free, however, they tend to focus only on a single service, and have very few features required by enterprise customers.





Conclusion —
Choosing a SaaS
Backup Solution

CONCLUSION — CHOOSING A SAAS BACKUP SOLUTION

In summary, selecting the right SaaS backup solution is crucial for enterprise businesses relying on a variety of SaaS applications. This article explores the essential features that should guide enterprises in choosing a backup provider, emphasizing the importance of comprehensive app support, advanced security measures, user-friendly interfaces, and MSP compatibility.

SaaSAssure will solve many of the challenges that customers face in protecting their SaaS data. SaaSAssure is designed to make SaaS backups extremely easy to manage. It is fully automated, meaning more efficient oversight and restoration when data disasters strike.

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 many SaaS services,

efficiently and quickly. 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 use 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, RTO will improve dramatically.

Join the forefront of SaaS data protection with SaaSAssure.



www.saasassure.com