

The necessity of a SaaS backup and archive solution

...and how it can offer value above and beyond recovery.

The Veritas logo is displayed in a bold, red, sans-serif font. It is positioned in the upper right corner of the page, to the right of the main title and subtitle. The background of the page features a light gray diamond-patterned grid and several thick, diagonal red lines that intersect the grid.

SOFTWARE AS A SERVICE (SAAS) FROM THE CLOUD - DO YOU REALLY NEED BACKUP?

Even before the increase in the number of employees working remotely, enterprises were starting to move away from on-premises applications and moving their data and workloads to SaaS platforms. Many people are using SaaS applications daily without even being aware of it.

IF MY DATA IS ALREADY IN THE CLOUD, WHY DO I NEED A BACKUP SOLUTION?

Many organizations have taken a similar position regarding SaaS application data. They point to multiple synchronous copies being automatically stored in multiple locations. They point to the native data protection built into the SaaS platform. These approaches seem good in theory, but in practice, too many organizations have paid heavy costs incurred from relying on them when data is lost.

WHY ARE ENTERPRISES ADOPTING MORE SAAS APPLICATIONS?

If you were to pose this question to the decision-makers at different organizations, you'd likely receive different answers, but at the core, their reasons for choosing SaaS over on-premises comes down to the following:

- Lower cost—SaaS costs for the organization will be less than the total of individual applications for each user.
- Ease of deployment—There's no actual software deployment needed. All users need is a web browser or a client they can download and install.
- Simpler purchasing process—Rather than having to count users to ensure the purchase of enough license keys, SaaS has a far simpler subscription pricing model.
- Simple support for remote users—From the SaaS platform's point of view, all users are remote, including those working on-premises, allowing all of them to receive the same support regardless of their location.
- Reduced management effort—On-premises or per-desktop software requires administrators spend time and effort monitoring and managing the software and its infrastructure. Management tasks associated with SaaS applications are minimal, and the SaaS provider manages the infrastructure.

SAAS APPLICATION NATIVE DATA PROTECTION

Nearly all SaaS platforms provide some form of built-in data protection capabilities, ranging from the bare minimum to specific tools often provided through an add-on subscription. Successful enterprises recognize their data is the lifeblood of their business. That's why no enterprise will be satisfied with "bare minimum" data protection and many of the add-on tools don't meet all of its requirements.

Here are some of the common SaaS approaches to data protection.

SYNCHRONIZED COPIES OF DATA

Nearly all SaaS application platforms protect their clients' data using multiple copies of the data, even if those copies are invisible to users and only accessible by the platform itself. Because enterprises' data is changing rapidly—sometimes 24/7—the SaaS provider needs to set its time interval between synchronizations very low, ensuring the copies are as up-to-date as possible to provide a low recovery point objective (RPO).

The problem, however, is that data deletions—either accidental or malicious—often aren't noticed right away. The same goes for files being corrupted either through a software crash or malware. When these events are noticed, most of the time the user who noticed doesn't have the access or permissions to do anything, and more time is spent contacting an administrator with the right privileges.

In the time it takes to become aware of the problem, the deletion or corruption will have been replicated to the other copies of the data, spreading the problem to the replicas as well.

RECYCLE BIN OR SIMILAR FUNCTION

On many SaaS platforms, when a user deletes data, the platform might not actually delete it, but will instead move it to the Recycle Bin or a similar reserved storage space. Depending on the platform and how it's configured, the user might not be aware of this process or might not have access to the Recycle Bin, eliminating the option for a self-service restore.

Additional issues with the Recycle Bin approach include the following:

If users do have access to the Recycle Bin, they could accidentally delete the data from it. Once data has been deleted from the Recycle Bin, there is no option to restore it.

A Recycle Bin usually has an expiration policy that sets a time limit on how long it will retain the data. This period could be anywhere from 3 days to 90 days, but once the time is up, the data is automatically and permanently deleted. Once the data has been purged from the Recycle Bin, there is no option to recover it.

Recovering files from the Recycle Bin can work for a small number of items, but bulk recovery scenarios are virtually unusable.

SAAS APPLICATION-PROVIDED BACKUP

Some SaaS applications do provide backup and recovery options, but it's notable that some providers have explicitly stated that backing up and recovering your data is not their responsibility. For those that do offer it, there's typically an add-on cost. Be careful when looking at the costs associated with their backup. You'll often end up paying double your current storage usage costs to have an extra copy of the data as well as additional bandwidth usage charges.

Also look at their Terms and Conditions very carefully before you sign anything. For most of these services you won't find a single mention of service-level agreements (SLAs) about how long a recovery might take—or even that they're able to recover data at all. Instead, you'll see phrases like "best effort" in reference to data recovery, which means the vendors are saying they'll try to recover your data, but you agree it's OK that they might not be able to recover anything at all. Also keep in mind that your definition of "best effort" will very likely differ from that used by the already-overworked person who will be responsible for putting in that effort.

FIVE CRITICAL FEATURES YOU DON'T WANT TO COMPROMISE ON IN YOUR SAAS BACKUP AND ARCHIVE SOLUTION

Not all data protection solutions are created equal, so it's important to identify your actual requirements before you even begin the conversation. At a bare minimum, you'll require a solution that offers full coverage for your SaaS data with flexible recovery options, high-level performance, automation and scalability, so the solution grows as your data grows. Beyond that, there are additional advanced features to consider that will enhance your ability to protect, recover, archive, ensure compliance and even manage all your organization's mission-critical SaaS data.

1 - FULL COVERAGE

Most enterprises are relying on more than one SaaS application and on offerings from more than one SaaS provider. There are many solutions that only protect specific SaaS applications or even only specific aspects of those applications.

A full-coverage backup solution should be able to back up and archive data from multiple data sources as well as have the intelligence to treat different types of data differently. For example, there are some solutions that can protect specific Microsoft mailboxes, but require you to use a separate solution or add-on software to also protect Microsoft SharePoint collections and files stored in Microsoft OneDrive or Google Drive. You'll also need to protect the data in your organization's messaging platform like Microsoft Teams or Slack. These often require separate point solutions.

Full-coverage solutions don't cover your full data if they don't allow for configuring default data protection policies for each data source or even for different groups of data from the same data source. When covering all sources with default policies, your SaaS backup solution should auto-discover and automatically enroll new users, new site collections and new messaging groups, thus providing automatic data protection for the new data without requiring an administrator to take any action. No more losing sleep wondering whether the data for the new employees or projects that were added today will be protected.

If you're looking for a complete, full coverage SaaS backup solution, you need something that can handle all:

User mailboxes

(Microsoft 365 Outlook and Exchange)

- All active and archived mailboxes
- Any shared mailboxes
- Any and all message attachments
- Message journaling

File collections

(Microsoft SharePoint and OneDrive, Google Drive, Box)

- All content types
- Site hierarchies
- Permissions and access control lists (ACLs)

Messaging solutions

(Microsoft Teams, Slack)

- Conversations
- All files sent through conversations
- Document libraries
- Wikis

2 - FLEXIBLE RECOVERY

With a SaaS backup solution that gives you flexible recovery options, you'll have the ability to easily address unanticipated or unconventional recovery requirements. Being able to do so can be particularly important when managing data through changing roles, staff turnover, mergers and acquisitions and other organizational changes.

Ensuring you have flexible recovery options in your backup solution will give you peace of mind that you'll be able to provide efficient, effective and rapid recovery support for your entire organization.

Examples of flexible recovery options:

- Restore items, folders, mailboxes or sites with multi-level recovery—Get your data back no matter what.
- Reinstate multiple mailboxes or collections in a single operation—Resolve large-scale data loss affecting multiple users or sites.
- Recover data to a preferred location, including cross-tenant recovery, data migration or restore to an on-premises location—Gain flexibility for users who need access to the data, have changed roles or don't have access to the original location of the data such as in an acquisition or merger, tenant-to-tenant migration or as part of an exit plan from the cloud.
- Apply filters to your recovery—Recover an entire mailbox, except for the user's contacts, or recover all files from an entire site or collection only within a specific date range, by file type, by owner and so on.
- Maybe you don't need to recover—Access data from accounts after employees are no longer with your organization or in the case of audits without having to maintain an additional active license.

3 - PERFORMANCE AND SCALABILITY


Your organization is already managing increasingly large volumes of data. The cloud makes this process easier and more cost-effective—if it's able to accommodate the level of performance and scalability your organization needs as it grows. You need a solution that will allow you to manage your volumes of data today, tomorrow and in the years to come.

When it comes to choosing based on performance and scalability, your SaaS backup solution needs to be able to:

- Scale to petabytes of data and billions of objects.
- Capture data at rates of multiple terabytes per hour.
- Augment incremental backups with continuous data protection.

Making the shift from on-premises applications and storage to applications and data hosted in the cloud is an investment that needs to be usable and sustainable. That's why it's essential for your chosen SaaS data protection solution to be able to handle all your needs as your organization grows.

Direct benefits of performance and scaling:

- Ability to meet the continuous data protection (CDP) needs of rapidly changing data.
 - Blazingly fast search results.
 - Reduced recovery time objectives (RTOs).
 - Reduce costs with a pay-as-you-grow pricing model.
 - Reduce costs further with automated data tiering policies.
 - Metadata and content indexing at scale.
- 

4 - AUTOMATIC COMPLIANCE ENFORCEMENT

Regardless of what industry your organization is in or where it's located, there are very likely multiple regulations with which you need to comply.

To ensure your organization is in full compliance, you need a SaaS backup and archive solution that allows you to create policies that will have all data subject to these regulations assigned data retention and permission policies to all your backup copies and your archived data. At scale, this process is not something your employees can do. Instead, you need a backup solution that will automatically apply these rules to the data as it is backed up and archived. This approach will ensure your organization will have no problems during any compliance audits.

Global enterprises operating in multiple countries may also have to comply with data sovereignty regulations that require data be subject to the laws and governance structures of the nation within which it is collected and stored. These regulations also apply to your backup and archived data.

Many SaaS backup solutions don't make it easy to meet this requirement. The Veritas solution allows customers to select their hosting Azure region or even scale across regions. It also automates the enrollment of user mailboxes and site collections into policies that map their content to the appropriate backup storage region, ensuring data residency control.

Compliance features you need:

- Immutable, tamper-proof storage for your data.
- Security, including multi-factor authentication, role-based access controls (RBAC) and end-to-end encryption.
- Data residing in a SOC 2–compliant platform.
- Flexible retention policies based on numerous criteria, allowing you to ensure preservation of the data throughout the required time frame.
- Near-infinite scaling.
- Personally identifiable information (PII) detection, allowing isolation of private and sensitive data.
- Enhanced discovery capabilities, including optical character recognition (OCR), transcription of audio and video files and searches based on multiple factors such as keywords, phrases, proximity relevancy ranking, Boolean and regular expressions.
- Ability to run a search across multiple data sources simultaneously.
- Ability to apply a legal hold quickly and easily.
- Ease in working with a designated third party (D3P) during regular audits.

5 - A SINGLE, UNIFIED MANAGEMENT CONSOLE

Enterprises today need to provide data protection for a near-overwhelming amount of information. This information is created by many different sources in many separate locations. You need the same level of protection and compliance applied to all your data regardless of source and location.

Enterprises need a single solution that can meet all their SaaS backup, recovery, archive and compliance requirements. That solution must allow all backup, recovery and archive jobs to be monitored and managed through a single, simple, intuitive graphical user interface (GUI). And that solution should allow administrators to monitor and manage all those jobs—regardless of the data source, regardless of the location, regardless of the compliance policies being applied—from anywhere they have an Internet connection.

With a single management console, administrators can collect the requested data from all relevant data sources quickly with a single search query. They can also place a legal hold on all that data with a single command. Last, but by no means least, a good solution makes it easy to export a copy of the discovery data to a specified location.

Advantages of unified management:

- Monitor and manage all backup, recovery and archiving jobs across all data sources and locations from anywhere.
- Configure and edit backup, archive and tiering policies from anywhere.
- Enables simple management for enterprises using a “follow-the-sun” IT support model.
- Perform discovery across specific or even all data sources with a single search query.
- Easily standardize policies across all business units and locations.
- No need to learn different interfaces or switch between consoles, as required with point solutions.
- Unified activity log simplifies auditing processes.

ADDITIONAL ADVANCED FEATURES

Finding a SaaS backup and archive solution that meets all five of the requirements detailed in this brief will enable your organization to have a strong data protection profile. Here are some additional features to look for in the solution you choose that will enhance your ability to protect, recover and archive your data in a way that goes above and beyond those five requirements.

Enterprise-grade security

It's no longer enough to protect your data from loss due to mistakes or software crashes. Today you also need to protect your data from being stolen, maliciously deleted, modified or held for ransom.

To protect your data from being stolen or even viewed by anyone, you need a SaaS backup solution that offers end-to-end data encryption. This approach means any data in transit is encrypted and your backup data is encrypted when it's stored.

The Veritas SaaS Backup solution also includes tight integration with Azure Active Directory, enabling single sign-on (SSO), multifactor authentication (MFA) and unified password controls.

Continuous data protection

A SaaS backup solution that provides continuous data protection (CDP) will actively monitor your data and automatically capture modifications in a near-real-time manner. Unlike normal incremental scans or snapshots, which happen at scheduled intervals, CDP is always running to capture any changes as they occur.

Features like CDP are useful for augmenting your SaaS backup strategy by applying it to high-priority site collections, users and/or processes to ensure the continuity and integrity of your mission-critical data.

Archive storage for former employees' data

Today's workers are increasingly transient, which leaves IT dealing with a data challenge when it comes to archiving inactive SaaS user accounts' data. The ability to do so has become particularly important with the emergence of compliance regulations such as the European Union's (EU's) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Finding a backup solution that provides automatic archiving of all SaaS data—mailboxes, site collections and messaging systems—means you can avoid unnecessary licensing costs when someone leaves your organization.

Plus, with a backup and archive solution that offers flexibility around long-term retention, you can restore user data in the future.

CHOOSE THE RIGHT SAAS BACKUP AND ARCHIVE SOLUTION FOR YOUR ORGANIZATION

Knowing what's possible and the benefits to your organization can make all the difference when evaluating solutions that allow you to protect, recover and archive your SaaS data.



ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS™