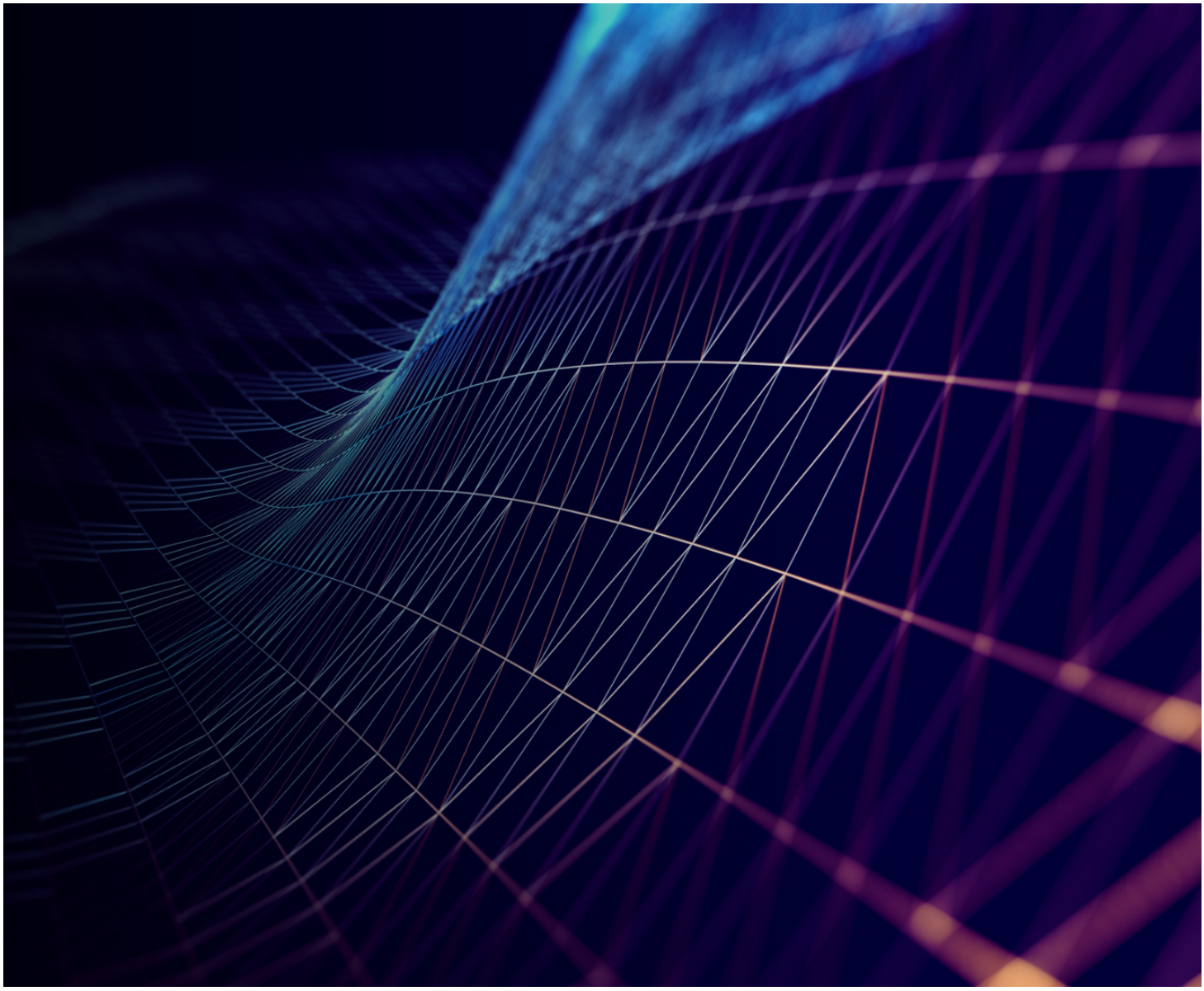
druva

White paper



The SaaS apps data protection handbook

Addressing the critical gaps in data backup, recovery, and archival

Q222-20282

Why back up your cloud data?

Cloud-based applications have become critical to businesses and operations around the globe. But do leading software-as-a-service (SaaS) providers such as Microsoft, Google, and Salesforce protect their customers' data with equally-critical backup options? And can they quickly and easily recover deleted data when needed, or is it just lost?

There is a misconception that cloud data is protected across SaaS applications, but without a comprehensive data protection strategy you run the risk of the following:

- Exposing your organization to data loss, breaches, and internal attacks — especially if you have a legacy data backup solution
- Increasing costs of managing cloud data
- Delaying cloud benefits
- Facing compliance and audit penalties

In order to overcome these challenges with SaaS application data protection, you need a single, comprehensive data protection strategy that follows best practices, and supports new cloud workloads and initiatives. When implemented, your business will be able to focus resources on higher-value functions, deliver expected SLAs, achieve predictable data protection costs, reduce data risk, and stay compliant with industry standards.

The missing layers of SaaS apps data protection

SaaS apps retention capabilities are not intended to make all versions of all data, from every point in time, available to customers whenever they need it. The simple fact is that SaaS applications such as Microsoft 365, Google Workspace, and Salesforce are not designed for the long-term, policy-based data retention, search, management, and access that companies need. Cloud services that do have limited backup capabilities may charge customers a sizable fee to retrieve even a small fraction of their stored data. Ask yourself, would you consider the Recycle Bin on your computer a backup solution?

> *"We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services."*[1]
>
> — Microsoft

Here are a few key reasons why having a third-party cloud data protection solution to back up your SaaS apps data is critical, and provides major benefits (capabilities and positive business outcomes) to any organization.

Data recovery

Leading SaaS application providers such as Microsoft, Google, and Salesforce do offer cloud-based data storage capabilities. For example, Microsoft 365 users can use OneDrive, retention policies, and versioning to retain their data in the service. Users can also recover their data if it is deleted accidentally, or even intentionally by rogue employees and administrators,

[1] Microsoft Services Agreement, April 1, 2021

within a certain timeframe. However, native restore options have several limitations and do not always guarantee full recovery of your data in the event of a breach or accidental deletion. It is important to remember that these services are designed for productivity, not data restoration, and the applications that do have backup capabilities may charge customers considerable fees for data retrieval. Generally speaking, with most SaaS applications, the only backup you have for your organization's data is via the Recycle Bin, which is automatically purged after a fixed period of time. After that, your data is gone forever.

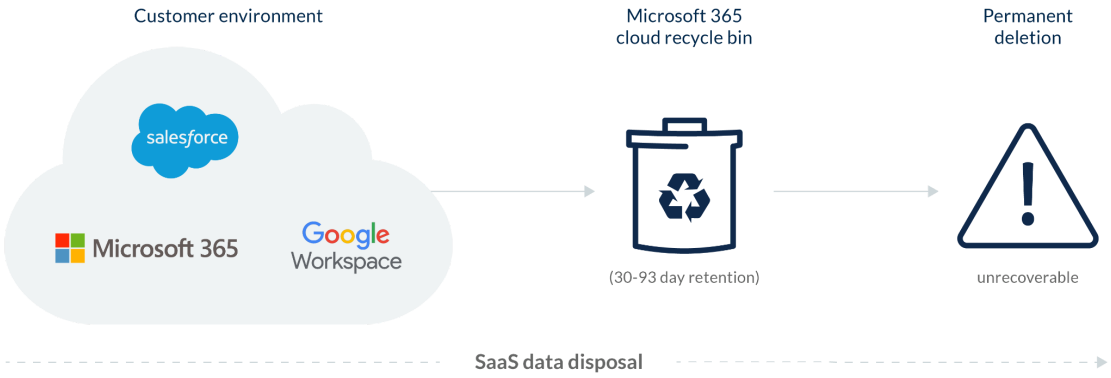
The truth is that once your data is deleted, altered, or corrupted — whether accidentally or intentionally — there is very little a system administrator can do to recover it.

File sharing is not data protection

People often assume that because they're using a cloud-based file-sync-and-share solution that their data is protected. It's an old argument: "We already have cloud file sharing, can't you just store your files there and call it a day?" The short answer is there are significant and important differences between these types of online services. While file-sharing and data-protection technologies have some overlapping features, they are fundamentally different in their approaches. **Here's what you need to know:**

- File sharing is built for real-time collaboration with user content. It is not designed for data recovery in the case of user error, data corruption, or ransomware. It also does not address archiving, compliance, or eDiscovery challenges.
- Enterprise backup software differs from file sync and sharing, in that the backup software automatically makes a copy of every user's data available for fast recovery. Endpoint and cloud application data are protected in their entirety, and if a device is lost or stolen, additional features such as remote wipe and geotracking help organizations trace the device and/or remotely delete corporate data. In addition, backing up a user's system and application settings ensures that new or replacement devices can be set up quickly while preserving the user's familiar working environment.

The many causes of data loss



Accidental deletion and user error — Sometimes, data is deleted by an employee, only for that same employee or their organization to later realize that it is still needed. For example, a collaborator might accidentally delete a shared project, or you might delete a scrapped project and later learn it is starting up again. Information can also be unknowingly overwritten or corrupted by users and third-party apps.

Malicious actions — People might delete data before they quit a job if they suspect they are going to be fired, or to spite a boss or coworker. Hackers can also be the culprits, surpassing security systems to delete, corrupt, or lock up data with ransomware. Whether internal or external, untrustworthy people are a reality.

Data corruption — Applications can hold extremely large data sets that are constantly updated. Overwriting data is a common problem that occurs when large data sets are imported into the application via bulk uploads. This can also happen when integrated third-party applications are used to manage the data inside the base SaaS application. What if your project management app purges all your calendar events or overloads your inbox with redundant, malformed messages? What if your expense report app paves over your tax-records spreadsheets with tampered data? What if your marketing analytics tool corrupts your CMS database, destroying all your carefully coded web designs?

Ransomware in the cloud

Today, ransomware is not only commonplace, it's on the rise.[2] What most organizations don't realize is that SaaS applications are equally at risk, with hackers constantly employing new strategies and turning this form of intrusion into its own mature industry. The ransomware threat now affects all organizations and industries. At the same time, the threat is no longer limited to physical devices, but is now a major concern for users of cloud applications. Companies are quickly finding themselves struggling to understand this unsettling new threat and how to adequately plan their response to an attack.

The findings of a survey conducted by Sophos revealed that the average cost of recovering from a ransomware attack had doubled from 2020 to 2021, and the average ransom paid by organizations was $170,404.[3] Because these criminals continue to operate with few consequences, these crimes will continue to increase in frequency and severity as a standard part of a company's daily threat landscape. According to the Federal Bureau of Investigation's Internet Crime Report, there were nearly 2,474 complaints registered, representing over $29.1 million in adjusted damages.[4] But the true numbers are far higher.

What's at stake?

Many organizations fail to understand that the cloud is just an extension of a user's operating environment. Data in SaaS applications is just as susceptible to loss, theft, or malicious attack as anywhere else. Enterprises are still responsible for managing data in the cloud, and failing to comply with rules and regulations can result in hefty fines, or worse yet, loss of reputation.

> *"65 percent of enterprise data lives in collaboration and business software-as-a-service (SaaS) applications."*[5]
>
> — McAfee

Organizations need to take into account three new challenges and considerations around data availability, compliance, and security to adequately address the data protection and governance gaps brought about by the rise of SaaS apps.

Ensuring always-on data availability — A common misconception among IT leaders and end users alike is that SaaS data does not need to be protected because the SaaS vendor is already backing up this sensitive, enterprise information under their Service Level Agreement (SLA). However, many people are not aware that the SLA provided by their SaaS vendor probably only covers data loss if the provider is at fault (e.g., a service outage). The SLA typically does not cover data lost due to accidental deletion, migration errors, data corruption, or malicious attacks. SaaS vendors may not be able to help you recover deleted data older than 30 days because their service, as a part of their standard, permanently purges the deleted information after that period. Even if the SaaS provider is willing to work

[2]Harvard Business Review, Ransomware Attacks Are Spiking. Is Your Company Prepared?, 21 May 2021
[3]Sophos, The State of Ransomware 2021, April 27 2021
[4]U.S. Federal Bureau of Investigation, 2020 Internet Crime Report, 17 March 2021
[5]McAfee, Cloud Adoption and Risk Report, 18 June 2019

with you, and the data still exists, they may charge fees — Microsoft itself recommends you use a third-party cloud backup solution for Microsoft 365 data. Even if the data is actually recovered, countless hours of productivity will most likely be lost trying to get it back.

Meeting legal hold obligations — Today, businesses can face very serious penalties if they fail to produce data stored in SaaS platforms during litigation following a discovery request made by the courts. Discovery requires legal teams within an organization to have immediate access to user data that may be critical for the defense of their case. In many cases, some or all of this data resides in cloud services and may not be recoverable. Or, it may be unprotected throughout the litigation process and susceptible to deletion or mishandling.

The core of legal discovery is the process of mining through data to identify and isolate information that is relevant to litigation. This assumes that information is properly indexed and that search functionality is sufficiently flexible. In addition, during early case assessment, the ability to see results in real time and refine searches becomes essential.

Not having timely and easy access to current and historical data for collection and review purposes could cost an organization millions of dollars in legal fees or even the outcome of a lawsuit. Collecting data residing in SaaS applications while preserving and handling it in a way that can be defensibly presented in court (with no data spoliation) is crucial for organizations and their legal team.

Addressing security and compliance in the cloud — A top concern for information security (InfoSec) teams is the risk associated with the leakage of sensitive and confidential data. According to an article on TechRepublic, 41% of companies have 1,000+ sensitive files open to every employee.[6] The cost of not protecting this data can be staggering, not just in the form of regulatory fines, but also by the effects it could have on a business's reputation.

With privacy laws changing regularly, the regulatory environment is becoming increasingly complex. The General Data Protection Regulation (GDPR) and Privacy Shield, adopted by the European Union (EU), demonstrated data-visibility mandates that went far beyond what most organizations had in place. Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), and new data privacy regulations have likewise forced businesses to drastically change how they capture, store, and secure data.

The business case for third-party SaaS apps

SaaS applications offer a range of valuable capabilities that organizations rely on every day to be more productive in achieving business goals. However, these powerful tools are not the purpose-built products needed to address the key concerns highlighted above. An increasing number of organizations have taken action to address the gaps in end-user data protection, data recovery, legal hold and eDiscovery, as well as third-party management of archived data.

> *"Organizations that assume SaaS applications don't require backup, or that the SaaS vendor's data protection is good enough, may place critical data at risk."*[7]
>
> — Gartner

Microsoft 365 data recovery

The core capabilities of Microsoft 365, while powerful, are not built to be a comprehensive solution for companies' data availability and governance requirements.

---

[6]TechRepublic, Report: 41% of companies have 1,000+ sensitive files open to every employee, 8 April, 2018
[7]Gartner, Assuming SaaS Applications Don't Require Backup Is Dangerous, Nik Simpson, 8 May 2019

- In Microsoft 365 Exchange, deleted items are moved to the Deleted Items folder where they remain until either manually or automatically deleted based on a retention policy that, by default, is 30 days. Once deleted from the Deleted Items folder, items remain recoverable for a minimum of 14 days.
- Microsoft offers Exchange Online Archiving as part of its E3 and E5 plans or as a separate add-on with a per-user fee. This is an email-only archive option that must be set for each individual mailbox, and it does not include archiving of Calendar, Contacts, or Tasks data. Although individual email messages can be recovered, it does not provide the ability to restore an entire mailbox from a specific point in time.
- Deleted items in SharePoint Online and OneDrive for Business first go to the site's Recycle Bin, automatically removed after 93 days. Once the items are automatically or manually purged from the Recycle Bin, they will go to the Site Collection Recycle Bin and remain for a set number of days (specified by the system administrator) before being completely purged from SharePoint.

According to Gartner, "Organizations cannot assume that SaaS providers will offer backup as part of the service or provide interfaces that backup vendors can use to access the data."[8]

Google apps data recovery

Google data retention and recovery varies by service; the following are a summary of data retention policies from a variety of Google Help documents:

- **Gmail:** An email is gone forever 30 days after moving it to the trash, or immediately after clicking on "Delete Forever."
- **Google Contacts:** A contact is gone forever 30 days after deletion.
- **Google Calendar:** Once an event is deleted, its full details can't be recovered.
- **Google Drive:** Once a document has been deleted from the Trash file, a Google apps administrator can recover the data for up to 25 days. However, after 25 days, it's gone forever.
- **Google Sites:** A deleted site can be recovered from the Deleted Sites folder for 30 days, after which it's gone forever.
- **Google Account:** An account can only be recovered "within a short period of time after deletion." If a Google apps administrator deletes an end user's account, all documents and files owned by that person will no longer be accessible by collaborators and viewers.

Google users can manually download copies of selected files to their local PCs, but the process is not particularly scalable and may be difficult to manage centrally.

Salesforce data recovery

Salesforce data recovery is primarily based on the Recycle Bin as follows:

- Deleted Salesforce records can be recovered from the Recycle Bin for 15 days before they are permanently deleted.
- Once the Recycle Bin storage limits have been reached, Salesforce automatically removes the oldest records if they have been in the Recycle Bin for at least two hours.
- A deleted custom object is unrecoverable as the data is immediately deleted from the database.
- Salesforce offers an Admin Export function for their Enterprise and Unlimited Editions, but the export can only be run once a week and requires a system administrator to manually download and archive the data to local storage each week.

---

[8]Gartner, Assuming SaaS Applications Don't Require Backup Is Dangerous, Nik Simpson, 8 May 2019

Salesforce offers a data recovery service if the data has been deleted within the last three months. This service costs a minimum of $10,000 and generally takes 15 business days to recover the data. Metadata, however, is not included, so it's up to you to restore the data back to Salesforce using the CSV file they provide. Additional backup/recovery capabilities will need to come from a third-party solution that can provide more automation and simpler procedures.

Closing the gaps in SaaS apps data protection

Until now, IT has used labor-intensive, costly, and complicated processes to access and manage data. SaaS applications have changed much of that old paradigm by revolutionizing the way organizations manage and consume the software that generates the majority of their critical data. However, organizations must change the way SaaS apps data is protected and governed if they want to meet today's real-world business needs.

While solutions are available to solve individual challenges, it's essential that you adopt a comprehensive, integrated platform that manages data regardless of device type, service provider, or physical location. This integrated platform should also provide a single, centralized view of data that's created and stored across SaaS applications, endpoints, and data centers. This lets organizations better conduct analyses, assess risks, improve compliance, and meet other needs. Thus, a unified level of data protection across all data sources is an emerging standard.

How Druva fits in

An all-inclusive cloud data protection solution should address the above challenges for all user data regardless of where it is located — on a laptop, a mobile device, or a cloud service like Microsoft 365, or Google Workspace.

Druva helps some of the world's largest organizations protect their investments in Microsoft 365, Google Workspace, and other SaaS environments from data loss and compliance violations. Druva provides a cloud-based data protection service, ranging from backup/recovery to cyber resilience. Customers also take advantage of all-inclusive services with no need to manage hardware, software, or the associated cost and complexity.

With Druva, your organization receives:

- Unique cloud architecture and expertise
- Backup and recovery to ensure a clean copy of data is always available
- Data stored in an air-gapped, highly available environment with the highest level of security, guaranteeing data availability and durability
- Management via a unified interface empowering admins to manage data, not infrastructure
- Transparent business model that ensures customers have predictable, controllable costs
- On-demand data protection enabling customers to scale up and down for improved business agility

Key takeaways

Understanding and acknowledging that your SaaS applications aren't fully protected is the first step to improving your data protection strategy. Implementing a single, comprehensive strategy that follows best practices will help you get one step closer to better protecting and managing your cloud data and SaaS applications. Consider leveraging an all-inclusive cloud data protection solution that will enable you to:

- Lower IT budgets
- Refocus IT on innovation
- Quickly respond to business needs
- Reduce the risk of a security incident

Learn how you can achieve comprehensive SaaS apps data protection at druva.com/use-cases/saas-backup

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva® delivers Data Protection and Management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted by thousands of companies worldwide, including over 50 of the Fortune 500. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Viking Global Investors, CDPQ, Neuberger Berman, Tenaya Capital, Riverwood Capital, and Nexus Partners. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.