druva

6 critical reasons for Salesforce data backup

Why you need a comprehensive third-party cloud data protection solution

Introduction

The ways you deploy application software have changed dramatically as the cloud has matured. Instead of locally installing programs, you leverage SaaS for Salesforce and other applications. Yet, you may not be aware of Salesforce's inherent limitations for data protection as a SaaS application hosting data in the cloud. Salesforce provides many benefits to organizations, but it natively lacks a backup and restore functionality. For this purpose, your organization needs a third-party cloud data protection solution.

With a comprehensive cloud data protection solution, you can — not only achieve complete protection for your valuable Salesforce data — but also gain high-quality test data for Salesforce sandbox seeding, while accelerating and protecting cloud projects. Your organization can ultimately accelerate development, optimize testing, and populate sandboxes quicker. It's automatic, astonishingly fast, secure, and easy.

Throughout this eBook, you'll discover the six critical reasons why your organization needs a comprehensive third-party Salesforce backup solution:

1. **Salesforce data is prone to user error**
2. **Ransomware prevention is a must-have**
3. **Migrating large data sets always involves risk**
4. **Data imports can overwrite the wrong fields**
5. **Data privacy regulations demand reliable backup**
6. **Sandbox seeding must be reliable and predictable**

#1 | Salesforce data is **prone to user error**

Ensure your data is protected when accidents occur

There's no question, end users and even admins occasionally delete records accidentally. They overwrite parent records as they create and collaborate, or they import data incorrectly, potentially leading to cascading corruption. Overall, without a true Salesforce backup solution, your valuable data is vulnerable.

Commonly, workers may not realize their business-critical data was accidentally deleted until months later. For example, a well-intentioned intern tries to tidy things up and purges accounts they think are closed, believing they're saving the company storage space and money. Their manager inattentively requests a physical delete. Months later, another group urgently wants the deleted data. Consequently, it's gone.

On the other hand, with an efficient third-party Salesforce backup solution, your organization can achieve:

- Regular point-in-time backups and unlimited retention vs. limited Salesforce data retention capabilities.
- Bulk and granular point-in-time restores vs. more complicated recovery options provided by Salesforce.
- SLA requirements that are met with quick recovery and self-serve options vs. Salesforce's slower recovery times.

So, the next time your business-critical data is accidentally deleted, you won't have to worry — a dedicated, third-party backup and restore solution is on your side.

> **"The vast majority of problems in Salesforce are your own mistakes — yes, as much as 70% of all data loss is the result of a human error!**
>
> — SalesforceBen

#2 | Ransomware prevention is **a must-have**

Be prepared with cyber resiliency and keep business on the move

If you manage an enterprise's IT team, you know that ransomware is a constant threat. For instance, a distracted executive will click on an innocent-looking link or a visitor will insert an infected flash drive.

Beyond perimeter security and protective hardware and software, you must be prepared with cyber resiliency and establish adequate recovery measures — ensuring your data can be bulk-recovered by IT reliably and quickly. As a result, users and organizations can continue to operate in the aftermath of a ransomware attack. Asking end users to manually recover sets of records, which may also be contaminated, isn't the answer. Your enterprise loses money every second that people can't work.

Effective SaaS backup solutions can do what Salesforce can't, enabling data protection that is:

- **Reliable** — quickly detect when an attack first occurred and identify which records were infected.
- **Comprehensive** — restoring an entire site is as easy and fast as restoring a single account.
- **Safe** — maintaining a copy of data in an independent, external location is a fundamental security rule.
- **Fast** — ransomware can cause widespread damages. Ensuring business continuity requires rapid bulk-recovery of pristine point-in-time data by IT.

If and when a ransomware attack strikes, you'll be armed and ready with the right third-party backup solution.

> **"The Cyber Catalyst designation signals that leading insurers believe Druva can help reduce cyber risk, and strongly merits consideration by organizations who seek solutions that yield meaningful improvements in cyber risk outcomes ...**
>
> — Marsh

#3 | Migrating large data sets **always involves risk**

Flexible and comprehensive backups are insurance against inevitable migration errors

Migrating data between orgs or from Classic to Lightning without any bad overwrites or other data loss can be tricky. Classic environments can be highly customized, with many unique objects and components, and all record relationships have to stay accurate. Experienced admins know to store original Salesforce IDs in a custom field in target records before a migration, but not everyone has that expertise. There's always a risk, even when you're using a third-party specialty tool.

Migrating data from a legacy CRM system into an initial SF deployment is even more complex, and there is an entire industry of consultants who specialize in it. Yet mistakes will eventually occur in any large migration. Extract, transform, load (ETL) tools will be misconfigured, fields will be mismatched, or relationships will be overlooked. The complexity is what dictates having insurance: third-party, enterprise-wide backup and restore in place before, during, and after any SF deployment.

What's essential:

- Reliable, automated, cloud-to-cloud backups of all Salesforce data.
- Quick recovery and restorations of data at any specific point-in-time.
- Protection of standard, custom, and managed package objects — and more.

The bigger and more complex the task, the more likely errors will occur. Your organization must be prepared.

> **Druva is much faster than OwnBackup Anonymization — ten hours vs. three hours with Druva and it provides consistent results with all of [our organization's] anonymization templates.**
>
> — Fortune 50 Technology Leader

#4 | Data imports can **overwrite the wrong fields**

Prepare for mistakes by new users and experienced admins

Importing data into Salesforce can be deceptively easy. It typically involves using either the Data Import Wizard or the Data Loader. The Wizard is designed for relatively simple imports of up to 50,000 records. The Data Loader, a client app, isn't so easy, but it can handle huge datasets. Most anyone can figure out the Wizard, but the Data Loader is often used with a command-line interface leveraging the Salesforce API.

Easy to use or not, with either tool, users have to specify a number of configuration parameters such as field mappings and data sources. Incorrect mapping such as mismatching types can result in overwriting the wrong records, and restoring lost data can be time consuming and surprisingly costly. If, in fact, you can restore it. Some mistakes made during imports result in overwrites that lose data permanently.

If your data is properly backed up and can be easily restored, these inevitable instances are tedious. But otherwise, things can get expensive. You can pay Salesforce $10,000 to fix it, but only if:

- The overwrites occurred within three months in a production instance.
- The overwrites occurred within one month in a sandbox instance.
- You're prepared to wait weeks.

Considering all users from interns to database admins make mistakes eventually, reliable third-party backup is a must.

> **"Druva was the only cloud-native data protection solution we found which would also backup our Salesforce implementation. Our Salesforce admin identified the product's key advantages for protecting critical customer and donor-related data.**
>
> — IT Infrastructure Manager, OHEL

#5 | Data privacy regulations **demand reliable backup**

Meet compliance requirements and avoid fines

Your organization's Salesforce orgs must comply with any number of data privacy regulations — state (such as California's CCPA), federal (such as HIPAA), regional (such as Europe's GDPR and Brazil's LGDP), as well as corporate data governance policies. Regulatory penalties can be stiff: the EU imposed nearly[1] $200M in fines in 2020.

The regulations typically demand high-performance Salesforce data governance, which can mean anything from preserving records for fixed periods of time (or indefinitely) to deleting data after a fixed period of time. Personal information fields may have to be protected or simply not be present. Data may have to reside in a particular location.

Configuring compliance is complex and varied, but all compliance efforts require bulletproof backup and fast restore capabilities. When you have the right third-party backup solution in place, you will:

- Have precise options for how long different data is archived.
- Flexibly fulfil residency requirements.
- Rest assured that all your Salesforce data is securely replicated independently of Salesforce servers.

Ensuring Salesforce data protection lets your organization fully satisfy compliance requirements.

> **"Our CRO and I know that the business impact of not protecting SaaS applications data like Salesforce is high. Druva enables us to maintain sales operations efficiency in case of Salesforce data loss. It minimizes the risk of data corruption, accidental deletion, or insider threats.**
>
> — Deputy CISO, Expel

[1] GDPR Fines Exceeded €170 Million in 2020, Eduard Kovacs in SecurityWeek, January 2021

#6 | Sandbox seeding must be **reliable and predictable**

Test faster and with greater confidence by reducing the time to prepare sandboxes

Seeding a Salesforce sandbox with reliable, high-quality test data from your company is an essential best practice. Yet exporting data and metadata from Salesforce is time consuming and can delay other business critical projects. Sensitive information and email addresses have to be masked or invalidated for governance and compliance. Significant mistakes can result in bugs or errors slipping into production.

Some enterprises choose to buy multiple full sandboxes based on replications of your Salesforce production data, at significant cost. However, there is one comprehensive data protection solution for Salesforce provided by Druva that, in addition to backup and restore, also enables sandbox seeding. The capability is built directly on the Salesforce platform and provides quality test data through:

- Handling all standard and custom objects.
- Automatically discovering related child records.
- Preserving parent/child relationships.
- Migrating all or subsets of relational data.
- Automatically disabling and re-enabling metadata.

> “We used Druva for a major and complex data migration between two Salesforce orgs for five Salesforce applications and several hundred GB of data. The data mappings were complex and the data copy had to be 100% accurate.
>
> — Linde

Salesforce requires a third-party data backup solution

A comprehensive, scalable, and cost-effective cloud data protection solution can protect Salesforce data, and other workloads, from major threats. Accidental overwrites, file corruption, migration errors, ransomware, and regulatory non-compliance are mitigated:

1. **If users overwrite records, they're restored quickly.**
2. **If ransomware corrupts data, pristine and uninfected versions are readily available.**
3. **If migration errors result in any loss data, all source content, Salesforce or other, is still safe.**
4. **If imports are misconfigured with mismatched fields and incorrect relationships, it's easily fixed.**
5. **If data privacy regulations dictate strict data governance, you've got it.**
6. **Additionally, multiple sandboxes can be automatically, quickly, and securely seeded with your own data.**

Druva's cloud data protection does all of the above, while providing true data isolation in an air-gapped environment (outside the Salesforce environment) — which is critical from a risk and compliance standpoint.

druva.com/solutions/salesforce

salesforce appexchange

aws marketplace

Find Druva in AWS Marketplace

Get started

druva

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

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