Key Scenarios for Safeguarding Salesforce Data

Why organizations need to be in control of their own Salesforce data

Introduction

Do you know if your Salesforce implementation is protected and secure? Do you know the difference between Salesforce data and metadata? If you were asked to name the responsible indivdual for protecting and securing Salesforce within your organization, what would your answer be?

Not knowing the answers to these questions is what tends to get organizations into trouble when their Salesforce data and metadata are compromised and not protected.

Salesforce is the #1 customer relationship management (CRM) platform in the world due to its advanced account and contact management, customization options, and third-party app integrations. While these options can be essential to the growth of a business, the potential loss of months and even years of customizations can throw a thriving business into a tailspin. Salesforce's primary focus is to manage the infrastructure and maintain uptime for its users, but as a user, you are responsible for backing up your own data.

While data loss is inevitable within any organization, whether that's due to human error, integration error or data breaches, being proactive about data protection is the first step to avoiding disruptions.

The following report will explore the importance of having a robust data resilience strategy in place when — not if — your data becomes compromised through loss, corruption, security events, and more.

The misconceptions of Salesforce backup

There is always confusion about what Salesforce actually protects, and how easily you can retrieve data that is lost or has been corrupt. Most organizations assume their Salesforce data is automatically protected in the cloud and is easily accessible if something goes wrong. Unfortunately, there are a few things wrong with this thought process:

There is no arguing about the growth and business criticality of Salesforce data and metadata, yet organizations rarely back it up. Even though Salesforce hosts the infrastructure, this doesn't replace your responsibility to protect your Salesforce instance from data loss and corruption.

Protecting Salesforce metadata is just as important as protecting your Salesforce data, but what exactly is metadata? Simply put, metadata is data that describes, connects or organizes other data. Metadata is kind of like a librarian, who knows the location of each book and how they all fit together—the data are the books. In Salesforce, metadata could be page layouts, code, custom fields or configurations. For example, when you create an account in Salesforce, your first name, last name, company name and phone number are all considered metadata. Not keeping your architecture safe and accessible in case of data loss can change a simple mistake into a major setback to an organization.

9 Reasons Why You Need to Safeguard Salesforce

Understanding that Salesforce protection is your organization's responsibility is the first step in solving the problem. The second is figuring out who in your organization makes sure your Salesforce instance is properly protected. More than once we have heard, "I assumed IT would have figured this out," and "I thought the Salesforce Admin was responsible," and "Why did our Salesforce Consultant not think about this?"

With so many people touching Salesforce within an organization, ranging from sales to marketing to IT, it can be hard to know what changes are being made. This is also the reason why sometimes it can take weeks or months for a data compromise to be discovered.

Salesforce data loss and data corruption can include:

Human error (admin)

Human error (user)

Human error (developer)

Human error (over-privileged user)

Human error (Salesforce)

Integration error

Data corruption (accidental)

Data corruption (malicious)

Poor data hygiene

1. Human error (administrator)

Even with deep Salesforce expertise, it's all too easy — and tempting — to upload or change data on the fly while in production. However, if a mistake is made, it can quickly propagate all throughout the application and ruin its relational integrity. When administrators use tools like Data Loader to change records, mass amounts of data can be overwritten in seconds. Data Loader can input, update, and completely delete up to five million records at one time.

Example

A Salesforce admin uses Data Loader to upload a large amount of data but accidentally maps a list of fields incorrectly, overwriting all existing data. Or, instead of using a sandbox, less-experienced admins may configure changes in a live environment to save time, accidentally erasing large amounts of data.

2. Human error (user)

Even users with regular permissions can cause major data loss incidents, and not everything can be restored from the recycle bin.

Example

A customer support representative in the call center deletes or alters data that was used in a report, which then feeds into an important team dashboard, and now the dashboard is reporting on incorrect data. Or, a support user merges two accounts that shouldn't have been merged, so it's impossible to separate their contacts, opportunities, and contracts.

3. Human error (developer)

While working within complex configurations, workflows, or formulas in Apex, the slightest mistake can wreak havoc across Salesforce objects. For large installations, configuration changes happen daily, and pressure from the business to make changes quickly might lead to skipping standard release protocols.

Example

Bad code wasn't tested properly, causing major issues when rolled to production. The entire Salesforce flow becomes flawed and needs to be rebuilt, and any impacted data must be restored. Or, when migrating the entire knowledge base in Service Cloud from the older Classic interface to the newer Lightning interface, you find that permissions and user access is different. As a result, a huge amount of data (which took nine months to build) is gone.

4. Human error (over-privileged users)

It's very common for someone in marketing, sales, or finance to have administrator access — when they really shouldn't. Not verifying user access and checking permissions can be detrimental to an organization's interface. For example, if a user accidentally has access to objects and is creating random records, unraveling the resulting mess could take days or weeks. System administrator privileges are often given to a group of people from different departments within an organization after implementation, and they're never taken back.

Example:

The vice president of sales decides they don't need a certain field and deletes it. This, which also deletes all the field history, and the changes are no longer tracked. Unfortunately, errors like this can sometimes take days or weeks to be discovered.

5. Human error (Salesforce)

Outages and data loss are a risk to any system, even for a world-class CRM system like Salesforce.

Example

A few years ago, Salesforce made a mistake on their end, and permissions for thousands of companies were affected. Each company had to manually rebuild their organizational profiles.

6. Integration error

Salesforce has hundreds of plugins and integration options that alter or move data, many of which are consistently rolling out updates. As a result, data loss or corruption of data and metadata is common. It's often the smallest data corruptions that are the hardest to identify. Depending on the application that's being installed, items like custom objects and fields can be added or modified. These, in turn, cause problems with overwriting data, duplicating data, or having the same field in different places.

Example

Integrating third party applications like Hubspot can cause issues if all the properties, including contacts and leads, are not mapped correctly. Salesforce has records for both contacts and leads and Hubspot only has contacts, so the decision on how this process should flow is crucial.

7. Data corruption (accidental)

Salesforce administrators can move large volumes of data or consolidate data quite easily, but this means that mistakes are just as easy to make. Accidental data overwriting or deleting during these processes are very common.

Example

An administrator mass-transferred opportunities based on new territory splits, and as a result, named accounts got removed from the account executives that need them. Or, an administrator used a spreadsheet to build a file for data loading, but the spreadsheet was accidentally corrupted by deleting a field, which then caused all the other data to move into the wrong row. As a result, John Smith's email and phone number now gets updated with Jane Jones's info.

8. Data corruption (malicious)

In just a few clicks, any user can overwrite customer information. A disgruntled employee with administrative access with a few clicks can easily change large amounts of key information before leaving a job, or a computer virus could delete a large amount of data. These are two scenarios that most organizations are not prepared for.

Example

The sales representative responsible for named accounts exports contacts from a top account. Then, they alter all names, phone numbers, and email addresses within that account. This information now leaves for a competitor.

9. Poor data hygiene

Often within Salesforce, an administrator can identify fields or datasets that are either duplicative, incorrect, or no longer needed. But they are afraid to delete them, in case of a mistake. To avoid data sprawl and unnecessary fees, Salesforce must be kept clean. Examples of poor data include duplicate or outdated records, formatting for phone numbers and addresses, missing values in fields and import/export errors. This can impact an organization's pipeline, which can lead to their sales forecasting to be over or underestimated.

Example

The wrong list from an event was uploaded to the wrong place. Instead of properly deleting it, a duplicate list was uploaded to a different place. A group of contacts were mistakenly marked as accounts, which created duplicate records. Thus, due to inconsistencies, decisions are being made with flawed information.

How Often Do These Reasons Happen?

By now, you understand the risk behind not protecting and securing your Salesforce data for timely recovery. But how often do these scenarios actually happen? More often than you might think, and from both internal and external sources.

Here are some other everyday possibilities that could boil down to simple human error.

- You have just onboarded five new sales representatives. One of them assures you he is a Salesforce expert. He then decides to merge multiple accounts in his territory, belieing he was just moving everything into one place.
- Your Salesforce Admin is given the direction to unqualify 3,000 leads due to numerous reasons. They use Data Loader and overwrite the wrong data.
- Someone on the marketing team has administrative privileges because they have worked in Salesforce in the past. They decide to delete a custom field because they can't figure out how to remove it from an automation journey. This results in all field history data being deleted.
- A new integration is added to an organization's Service Cloud instance and a large number of agent workspaces are overwritten. These agents have now lost the ability to track their customer data, including assets, order history, and support history.

These types of mistakes can happen in organizations both large and small. But the larger the company, the more people have access, so the mistakes tend to be larger and more costly.

Safeguard Salesforce Data

No matter the size of your organization, protecting and securing your Salesforce data and metadata is something that should not be put off or ignored. It is your Salesforce data, you control it, and it is your responsibility to protect it.

A simple mistake can happen at any time. But not being prepared can result in massive data loss and heavily impact your organization. Being proactive and having the right resilience solution in place can help lessen these unexpected occurrences.

As an industry leader in data resilience, Veeam understands how important your data is to your organization. Veeam knows what it takes to protect and secure it properly. With Veeam Data Cloud, a single cloud platform that unifies resilience for all SaaS apps and data, your teams will have better management over their Salesforce environment while freeing up their time.

What's more, Veeam Data Cloud *for Salesforce* protects, secures, and restores critical data and metadata to keep your business running. Better yet, advanced data management and monitoring capabilities empower you to meet compliance confidently while lowering TCO.

With Veeam Data Cloud *for Salesforce*, you will also be able to:

- Eliminate Downtime: Maintain productivity with automated, high-frequency backup, and precise, fast recoveries of data and dependencies.
- Mitigate Risks: Secure all your data while maintaining compliance through access control, encryption, and data masking.
- Unlock Value: Leverage archiving, unlimited storage and sandbox seeding to lower TCO, all included in one predictable price.

To see Veeam Data Cloud *for Salesforce* in action, schedule a demo with one of our specialists!

Learn more veeam.com