White Paper

THE SALESFORCE DATA PROTECTION GUIDE

Addressing the critical gaps in Salesforce backup and recovery

Why Back Up Your Salesforce Data?

> *"It is important for customers to develop a data backup and recovery strategy as part of their overall data management and security model. The Salesforce Data Recovery service is an expensive and time-consuming process and should only be used as a last resort, when no other copy of the data is available."*
>
> *— Salesforce Cloud Services*

Take Salesforce at its word. It simply isn't designed for the long-term, policy-based data retention, search, management, and access that companies need. While most companies have built practices around protecting this data on-premises, they have not yet invested in protecting their business-critical information that is now being hosted in SaaS applications, especially in Salesforce. In fact, Enterprise Strategy Group's "2018 IT Spending Intentions Survey" showed that 40 percent of their respondents are using cloud infrastructures like Salesforce as a repository for backup or archiving data.

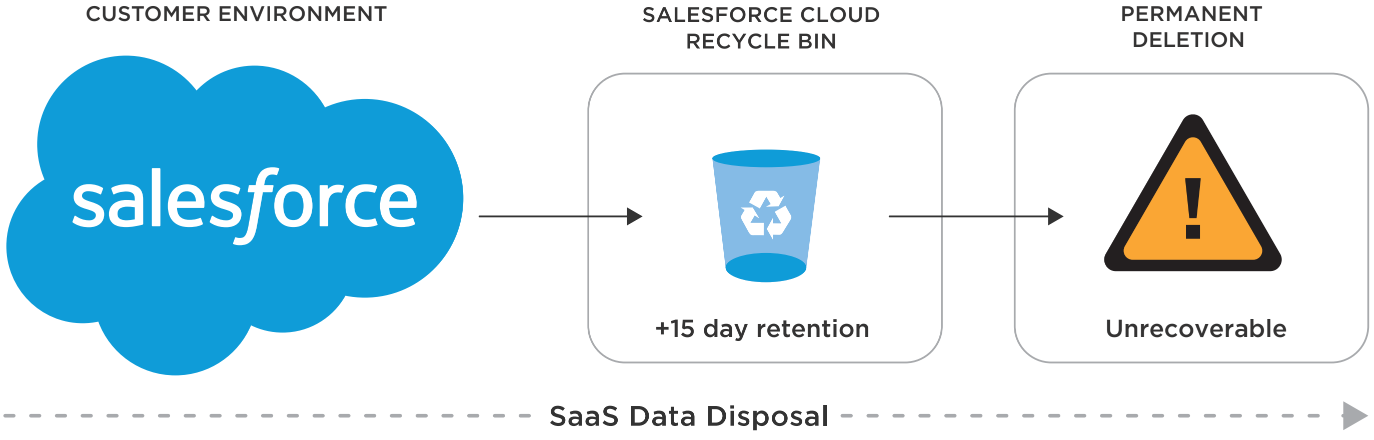
> *"The SaaS market will grow to $157 billion in 2020; some providers have more than $1 billion in revenue and are growing strongly. This rapid increase in SaaS usage means a proportional growth in the movement of customer business data from on-premises to cloud instances."*
>
> *— Forrester Research, "Back Up Your SaaS Data—Because Most SaaS Providers Don't. Cloud-To-Cloud Backup Is The Only Practical Option For SaaS Data Protection." January 25, 2018*

What Salesforce Provides

While Salesforce has an Admin Export feature to back up a full database, it's a manual, once-a-week-only process. Otherwise, records are permanently lost 15 days after being deleted—or sooner if the recycle bin is full. Deleted custom objects are immediately unrecoverable. A recovery service is available for data deleted in the prior three months, but it costs a minimum of $10,000 and can take weeks. Metadata, however, is not included, so it's up to the user to restore the data back to Salesforce via the CSV file they provide.

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 because the data is immediately removed 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.



> *“For customers who want to have additional backup/recovery functionalities, they may find it worthwhile to evaluate and adopt a third-party backup tool that offers more automation and simpler procedures than the native backup/restore functions.”*
>
> *— Gartner, “You May Need Additional Backup to Prevent Data Loss From Your SaaS Solutions” Refreshed 10 June 2016, Published 20 January 2015*

Why You Shouldn’t Rely Solely on Salesforce for Data Backup and Protection

Most organizations make the incorrect assumption that Salesforce has redundant and easily accessible copies of their data, and they don’t need any additional data protection. However, you should never rely solely on Salesforce to safeguard your critical data. Here are five reasons why:

- **Users make mistakes.** Salesforce automatically deletes records 15 days after they’re sent to the recycle bin. What’s wrong with that? One potential problem with that is if a project’s status changes. For example, an intern may try to show initiative and clean up records after a big campaign is canceled. A month later, the campaign is back on, but the data is no longer available.
- **Malicious users wreak havoc.** When an employee feels they’ve been treated badly and their job is in jeopardy, there’s no telling how they’ll react. If they are the proactive sort, by the time they are “walked out,” it’s too late. If they delete custom objects, it’ll cost a minimum of $10,000 and take weeks to restore the data if that’s even possible.
- **Corrupted data is ruined forever.** Salesforce offers at least some limited protection for accidentally deleted data. But what about corrupted data? A mishandled or corrupted bulk upload to Salesforce or a misconfigured integration could ruin the database that your organization has been carefully building for years.

> *"With the ecosystem of add-on applications for popular SaaS solutions growing by the day—Salesforce's AppExchange now boasts more than 3,300 apps and more than 4 million installations—we're seeing growing concern about rogue third-party applications causing damage. What happens when the app that's supposed to consolidate duplicate records accidentally deletes or corrupts unique records?"*
>
> *— Forrester report, "Back Up Your SaaS Data—Because Most SaaS Providers Don't," January 2018*

- **Data imports can go wrong.** Data imports done incorrectly can have a destructive impact. Automation tools designed to allow users to update large numbers of records in a single operation are great—unless something goes wrong. For example, an incorrect mapping can ultimately result in bad values for a large number of records.
- **In court, inaccessible data might as well be lost.** Throughout litigation, courts require data as part of the eDiscovery process. This data must be readily available, fully recoverable, indexed, searchable, and demonstrably unspoiled. If Salesforce data is hard to find because it is fragmented across different business units or unusable due to a partial recovery or download, an organization can incur fines or penalties and/or lose the court case.

What's at Stake?

> *"Some IT organizations wrongly assume that high-availability and disaster recovery capabilities offered by SaaS providers can recover data loss by user errors or malicious attacks."*
>
> *— Gartner, "Data Backup/Recovery Factors to Consider When Adopting SaaS," December 2016*

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

Organizations need to take into account the challenges and considerations around data availability, compliance, and security in order to adequately address the data protection and governance gaps brought about by Salesforce. For example, your organization must be able to do the following:

- **Ensure always-on data availability —** A common misconception among IT leaders and end users alike is that Salesforce data does not need to be protected because Salesforce is already backing up your sensitive enterprise information under their Service Level Agreement (SLA). Many people are not aware that the SLA provided by Salesforce 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.

Salesforce may not be able to help you recover deleted data older than 15 days, because they permanently purge the deleted information after that period. Even if Salesforce is willing to work with you, and the data still exists, they will charge you a sizeable fee and recommend that you use a cloud backup solution. And if the data is actually recovered, countless hours of productivity will most likely have been lost while trying to get it back. Furthermore, if critical data is not available during an audit, your organization will be vulnerable to large fines and strict regulations.

- **Meet legal obligations —** A business can face very serious consequences if they fail to produce data stored on Salesforce during litigation following a discovery request made by the courts. This requires legal teams within an organization to have immediate access to user data that may be critical for the defense of their case or to avoid serious penalties. In many cases, some or all of this data resides in Salesforce, which may not be recoverable or may remain completely unprotected throughout the litigation process and susceptible to deletion or mishandling by the users.

  At the core of legal discovery is the process of mining through the data to identify and isolate information that is relevant to the litigation. This assumes that information is properly indexed and that the search functionality is sufficiently flexible. In addition, during early case assessment, the ability to see results in real time and refine the search based on the results becomes essential. Legal teams can access the data that has been backed up for legal requests, but there is no way to put the data on a legal hold to maintain an immutable copy of the data. Plus, that data cannot be ingested directly to an eDiscovery platform.

  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 result in a negative outcome of a lawsuit. It is crucial for an organization and its legal team to have an effective way to collect data that resides on Salesforce while preserving and handling that data in a way that can be defensibly presented in court.

- **Address security and compliance in Salesforce —** A top concern for any Information Security (InfoSec) team is the risk associated with the leakage of sensitive and confidential data. A recent study performed by Dimensional Research indicates that close to 95%[1] of businesses have some form of sensitive data in the cloud. The cost of not protecting this data can be staggering, not just in the form of regulatory fines, but also the effect it would have on the reputation of the business and losing the trust of its customers.

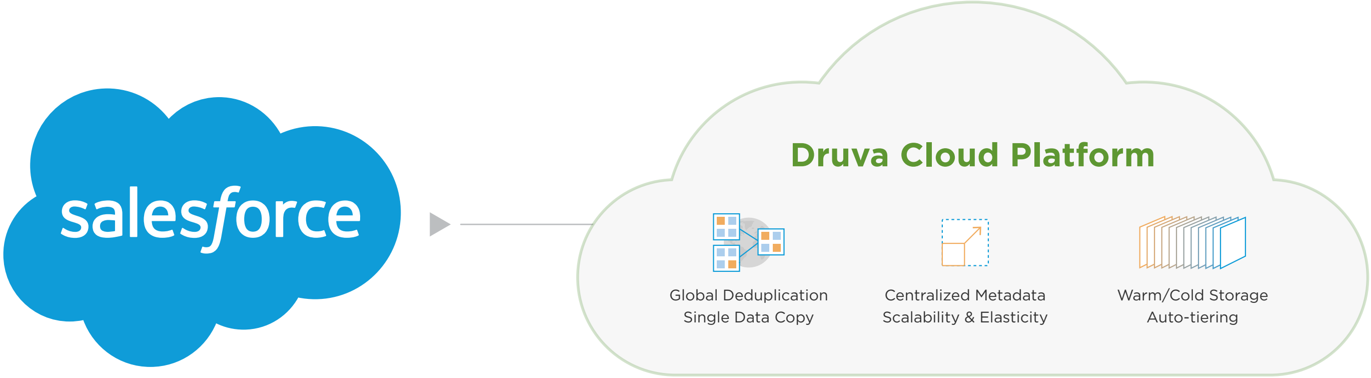
  With privacy laws constantly changing, the regulatory environment is becoming even more complex. For example, Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), and new data privacy regulations have forced businesses to drastically change how they capture, store, and secure data.

> ***“Third-party backup tools for SaaS applications tend to offer more data restore options and give some control back to user organizations.”***
>
> *— Gartner, “You May Need Additional Backup to Prevent Data Loss From Your SaaS Solutions,” June 2016*

[1] ”State of Data Privacy in 2015: A Survey of IT Professionals” April 2015

The Business Case for Druva

Salesforce offers a range of valuable capabilities that organizations rely on every day to be more productive in achieving their business goals. However, it does not address the key concerns highlighted in this white paper. According to Enterprise Strategy Group's "2018 IT Spending Intentions Survey," the number one reason for justifying IT investments to management was for "improved security/risk management." This is why it's imperative that businesses supplement the native capabilities of Salesforce with Druva to establish a strong data protection solution in the cloud.



Druva helps some of the world's largest organizations protect their investment in Salesforce and address the gaps in end-user data protection, data recovery, legal hold, and eDiscovery. Druva's cloud-native data-management solution is the essential layer of data protection functionality, where administrators can continuously track and monitor data within Salesforce as well as mobile and laptop endpoints. Furthermore, the Druva solution can be set up to quickly alert system administrators to potential data risks associated with sensitive information—such as Personal Healthcare Information (PHI), Personal Credit Information (PCI), Personally Identifiable Information (PII), and Intellectual Property (IP)—so they can take appropriate action.

> ***"It's not practical to custom-develop adapters or connectors that protect SaaS application data. You must engage cloud-to-cloud backup providers, as they can leverage their experience to add support for new services quickly."***
>
> *— Forrester report, "Back Up Your SaaS Data—Because Most SaaS Providers Don't," January 2018*

Druva inSync can help automate your Salesforce data protection policies to address both availability and governance requirements by providing the following:

- **An integrated solution —** Druva inSync provides a single, integrated platform for data collection, recoverability, and governance so organizations don't have to manually access separate data sources using disparate solutions. This integrated approach automates and unifies backup, archival, and governance capabilities across multiple cloud applications like Salesforce and other data sources.
- **Aggregated end-user data —** Druva inSync efficiently aggregates end-user data, whether it resides on servers, mobile endpoints, or cloud applications such as Salesforce, giving enterprises improved

visibility and control of their data. In fact, Druva is the only data protection provider that enables enterprises to have a comprehensive, centralized view of end-user data regardless of its source.

- **Always-on data backup and availability —** With its new converged approach to backup, Druva inSync enables organizations to protect data, do quick restores, and take point-in-time snapshots from Salesforce for data recovery. Druva inSync also enables IT to restore objects, individual records, files, and attachments, including metadata.
- **Turnkey data governance —** Druva inSync helps organizations achieve and effectively govern Salesforce data so they can comply with privacy, financial, or other requirements. With Druva inSync, organizations can also search and track data across cloud applications and endpoints, and receive automated alerts of potential data risks. Druva inSync also provides organizations with automated compliance management, built-in legal hold workflow for eDiscovery, federated searches, tamper-proof audit trails, forensic-based collection, and chain of custody reporting.
- **Simplified backup and recovery —** Druva inSync provides time-indexed backup of standard and custom Salesforce objects and metadata, on-demand granular restore with the ability to compare snapshots before and after an incident, and unlimited retention to store data as long as regulated. With Druva inSync, organizations can be assured that data is will be on hand when needed and storage regions are configurable per site to meet regional data-privacy requirements.

Leveraging an Integrated Approach with Druva

It's crucial that your organization adopts a comprehensive, integrated platform that converges and manages data regardless of its device, service, or location. With Druva's cloud-native Data Management-as-a-Service solution, you get an integrated platform that provides a single, centralized view of data created and stored on Salesforce, endpoints, servers and other SaaS applications. As a result, your organization can better conduct analysis, assess risks, improve compliance, and meet other imperative needs.

To learn about how the Druva cloud can help, visit our Salesforce Solution Page.

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data management-as-a-service solution that aggregates data from endpoints, servers and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance and intelligence—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations, and protects over 40 petabytes of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44 (0) 203-7509440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729
sales@druva.com
www.druva.com