



A Guide to Fortifying ServiceNow® Data Resilience





Continuity—the ability to mitigate damage and rapidly recover from data corruption and loss—is critical to every organization. Today, almost every business has some sort of continuity solution in place for corporate data. However, many don't have one for data in SaaS applications like ServiceNow since they are under the impression that the SaaS vendor automatically protects their data. In reality, the protection these SaaS vendors provide extends only to their platform. Recovering from accidental data loss or corruption is fully the customer's responsibility.

That's why it's crucial for ServiceNow administrators and platform owners to have the tools to protect the data in their production and sub-production instances. In this guide, we explain the impact and risks of data loss in ServiceNow and provide strategies to ensure compliance and operational resilience.

How data loss happens in ServiceNow

Within SaaS applications like ServiceNow, data loss isn't just a possibility; it can often be an unfortunate reality. Events that can impact data availability and security in the ServiceNow include:

- Migration errors when moving large volumes of data, consolidating data, or importing data
- Developers or admins releasing applications, workflows, or system updates into production without proper testing
- Errors in integrations that inadvertently corrupt data
- Errors that occur during planned maintenance or during system upgrades
- Malicious attacks that successfully delete or corrupt data

Impact on business operations

ServiceNow is pivotal in managing mission-critical business processes, often housing highly sensitive and regulated data. The impact of data loss can be significant:



Operational disruption:

ServiceNow's role across IT, customer support, legal, HR, finance, health, safety, and more means data loss can paralyze multiple departments, leading to productivity and revenue losses.



Regulatory compliance:

Losing regulated data can lead to severe penalties and compliance issues.



Trust and reliability:

Data loss undermines trust in the platform's reliability, affecting overall business confidence and customer satisfaction.



from Salesforce

A Guide to Fortifying ServiceNow Data Resilience



Strategies to protect data in ServiceNow

Now that you are aware of the risks and impacts of data loss in ServiceNow, how can you prevent it? Having a backup of your ServiceNow data is a good first step, but the real challenge is restoring the data back into Salesforce exactly how and when you need to. Two elements are critical to accomplishing this: being able to detect data loss quickly and restoring lost or corrupted data to its previous state.

Let's take them one at a time.

Build a proactive data detection mindset

The first step to recovering from a data loss is knowing one happened in the first place. Organizations can experience weeks or months of data corruption or loss until one of their users notices something is amiss. If you're unaware of loss or corruption, you may not be able to address the issue before it disrupts your business, undermines trust in the data, or creates exposure to compliance issues.

Because of the shared responsibility model, you—the customer—must realize and monitor the health and integrity of your data. The problem is that data loss - especially when it's specific tables, columns, or records that were impacted - isn't always detectable. **ServiceNow does not provide any native capabilities to proactively alert you of data loss or corruption.** And even if you do detect something is amiss, you will need to work

with ServiceNow Support to attempt to recover the affected data.

When it comes to data loss detection, [Forrester](#) says plainly that "Humans are no longer the watchdog for spotting data loss or corruption. Data must be continuously monitored, and administrators and/or IT need to be instantly notified when anomalies are spotted by the backup and recovery system."



Humans are no longer the watchdog for spotting data loss or corruption

NAVEEN CHHABRA, RESEARCH SENIOR ANALYST, FORRESTER

Having tools to proactively monitor for data loss or corruption is key. Here are some things to consider when it comes to anomaly detection:

Do you have a way to be alerted to any significant changes to your ServiceNow data and, if so, how?

Can you be notified when activity levels are out of the normal ranges?

Can you set thresholds that will trigger an alert to be sent?

De-risk operations with faster, more precise recovery

Just like the shared responsibility model means you are responsible for detecting data loss, it also means you are responsible for ensuring you can recover as well.

Restoring lost or corrupted data is one of the most stressful situations a ServiceNow admin will face. While it's important to do it quickly, you also must do it correctly, otherwise, you'll risk making a bad situation even worse.

The problem is, restoring data correctly is hard. A report from Raconteur found that 1 in 3 organizations are unable to restore all of their data after experiencing data loss. In ServiceNow particularly, errors can cascade either because of the relationships between tables, or automations you've built that update and add data to the system.

In ServiceNow, backups are retained for only 14 days. For some customers, the 14-day retention of ServiceNow's native backups supports their business needs. However, for those who have more rigorous data resilience and retention requirements, detecting data loss or corruption early on is critical to ensuring data recovery.

With ServiceNow's native backup, if you discover a data loss or corruption after more than 14 days have elapsed, you will no longer have a backup to restore your data from. Furthermore, if you do experience a data loss or corruption within the 14-day period, there are no available self-service tools to recover your data.

One of the only options for recovering your data may be to do a full rollback of your ServiceNow instance, which would potentially result in a complete loss of all the changes (even valid ones) that had occurred since the backup was taken.

1 in 3

organizations are
unable to restore all
of their data after
experiencing data loss

A backup won't do you much good if you can't recover from it. Here are some things to consider when it comes to recovering data in ServiceNow:

How much downtime can you handle in ServiceNow, and how much data can you afford to lose before business is impacted?

Can you specify the set of records that need to be restored, even if those impacted records number in the hundreds or more?

Can you fix unwanted changes without affecting valid data?

How Own can help

As we outlined above, ServiceNow does have some out-of-the-box, native backup capabilities, but their limitations could prevent you from fully recovering in the event of a data loss.

That's where we can help. [Own Recover for ServiceNow](#) improves data resilience and compliance by equipping organizations with more control over backup timing and retention, proactive alerting of unusual data loss or corruption, and the ability to quickly restore data—from entire instances down to individual records—entirely through self-service.

An [IDC study](#) found that after adopting Own's continuity solution, customers experienced a 71% reduction in average data recovery time. One organization seeing the value of protecting its ServiceNow data with Own is [LightEdge](#), which initially bought Own's backup and recovery solution for Salesforce and has since expanded into ServiceNow.

71% reduction in average data recovery time



When it came to data—specifically around off-the-shelf tools provided by Microsoft, Salesforce, and ServiceNow—we were trusting that the vendors themselves were resilient enough. It wasn't super granular, and obviously, that's not a safe way to do business. For the price, [Own] made sense out-of-the-box: it does exactly what we need it to do, and using it has been an easy decision. Own's suite of services makes it a no-brainer: minimal management relative to the cost of building it internally.

MICHAEL HANNAN, CIO AND CSO AT LIGHTEDGE

Start protecting your ServiceNow data today

Looking for the right ServiceNow backup and recovery solution for your business? Download our Buyer's Guide for Backup and Recovery for ServiceNow, which includes all of the criteria to consider.

DOWNLOAD GUIDE

Want to see Own Recover for ServiceNow for yourself?

SCHEDULE A DEMO

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.



O W N Y O U R O W N D A T A

About Own

Own is the leading data platform trusted by thousands of organizations to protect and activate SaaS data to transform their businesses. Own empowers customers to ensure the availability, security and compliance of mission-critical data, while unlocking new ways to gain deeper insights faster. By partnering with some of the world's largest SaaS ecosystems such as Salesforce and Microsoft Dynamics 365, Own enables customers around the world to truly own the data that powers their business.

It's their platform. It's your data. Own it.

Learn more at owndata.com.