The Complete Guide

Backup and Recovery for Microsoft Dynamics CRM and Power Apps

Own

Contents

A (False) Sense of Data Security

Scalable, cost-effective, and customizable, Software as a Service (SaaS) continues to dominate as the preferred method of enterprise application delivery. CRM, in particular, is the fastest-growing software on the market today, with revenues expected to exceed $96.5 billion by 2028.

Microsoft Dynamics CRM has become a force in the CRM space. In FY 2023, **Dynamics 365 grew 16% YoY** and was one of the fastest growing products at Microsoft.

But like all clouds, it comes with risk.

While companies like Microsoft provide cloud environments with hardened security controls and proven infrastructure far beyond what most enterprises can achieve with on-prem solutions, data resiliency and security remain real and present dangers for all companies using cloud services.

According to Gartner, **99% of cloud security failures and resulting data loss will be the customer's fault**[1] through 2025. This includes things like lax permissioning, social hacking, insider threats, poor physical security controls, and other vulnerabilities.

[1] **Is the Cloud Secure?**

Data Loss and Corruption Can Happen in Unexpected Ways

Every attack, line of code, and integration can result in losing access to your Dynamics CRM or Power Apps data in Dataverse.

Microsoft calls out the following **disruptive events** that can impact data availability and security in the cloud:

- Data corruption or deletion caused by a bug or human error
- Upgrade or maintenance errors that occur during planned maintenance
- Malicious attacks that successfully delete data or databases

Other data risks include:

- Migration errors when moving large volumes of data, consolidating data, or executing complex transformations
- Developers or admins releasing applications, workflows, or system updates into production without proper testing

It's important to remember the vast majority of data loss and corruption issues aren't tied to major events. Simple mistakes happen every day.

The Shared Responsibility Model in the Cloud

Many organizations assume that data stored in the cloud is automatically protected. While it's true that some responsibilities transfer to the SaaS provider as you move from on-prem systems to the cloud, data protection remains solely the end user's responsibility.

	Responsibility	SaaS	PaaS	Iaas	On-prem
Responsibility always retained by the customer	Information and data	●	●	●	●
	Devices (Mobile and PCs)	●	●	●	●
	Accounts and identities	●	●	●	●
Responsibility varies by type	Identity and directory infrastructure	◐	◐	●	●
	Applications	🟡	◐	●	●
	Network controls	🟡	◐	●	●
	Operating system	🟡	🟡	●	●
Responsibility transfers to cloud provider	Physical hosts	🟡	🟡	🟡	●
	Physical network	🟡	🟡	🟡	●
	Physical datacenter	🟡	🟡	🟡	●

🟡 **Microsoft**
● **Customer**
◐ **Shared**

Microsoft's website states:

"You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type)."

Microsoft's Service Agreement recommends that its Dynamics CRM customers use a third-party backup solution.

The Service Availability section of Microsoft's service agreement states:

"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."

> "When it comes to cloud computing and data protection, it is a shared responsibility between the cloud service provider and the customer that is analogous to the relationship between the car owner and car manufacturer."

DIANA KELLEY
FORMER CYBERSECURITY FIELD CTO
MICROSOFT

Dynamics CRM Backup Services

To help its customers hold up their end of the shared responsibility model, Microsoft offers **automated and manual backups** of Dynamics CRM and Dataverse cloud data.

SQL Managed Instance (Microsoft's fully managed instance hosted in Azure) uses Azure SQL combined with Azure BLOB storage and CosmosDB to create full backups, differential backups, and transaction log backups with the following frequencies:

Once a week

A full backup of all the data in the system is taken once a week

12–24 hours

Incremental backups are performed every 12 to 24 hours to capture data that has changed since the last full backup

5–10 min

Transaction Log Backups capture all modifications to the database in a virtual log file every 5 to 10 minutes

The backups are stored in read access, geo-redundant storage (**RA-GRS**) for at least seven days with a limited retention period for a point-in-time restore of up to **28 days**.

To assist their customers with their shared responsibility model, Microsoft offers the following:

- All environments, except trial environments (standard and subscription-based), are backed up. System backups occur continuously.
- For production Dataverse environments that don't have Dynamics CRM applications enabled (ex: Power Apps), the default backup retention period is only seven days. However, for managed environments, admins can use PowerShell to change the setting and extend the backup retention period. The available options are 7, 14, 21, and 28 days.
- System backups for sandbox environments will be retained for seven days days.
- Production environments that are downgraded to sandbox will revert to a seven-day day retention policy and immediately lose 21 days of backup retention against the environment.
- You must restore an environment to the same tenant and region in which it was backed up.
- Currently, Activity Tracking audit logs are not restored.
- Power Platform Admin Center does not expose backup status nor completion time.

Dataverse Recovery Services

When a Dataverse environment is deleted or corrupted, it can be replaced with a previous version backed up at a specific point-in-time in the past and retained within the retention period using Power Platform Admin Center, Azure PowerShell, or REST API. **This applies to Sandbox environments only and requires available storage in the Power Platform tenant.**

Administrators have four recovery options:

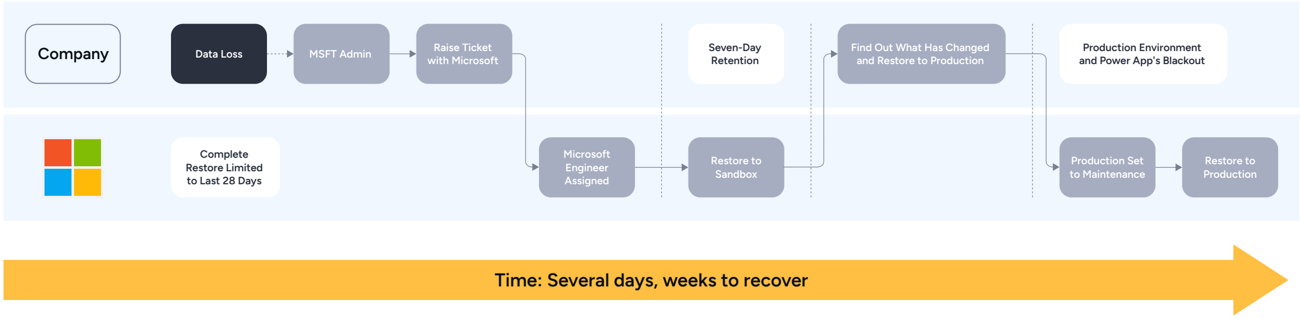
1. Restore an automated system backup to an existing Sandbox environment
2. Restore an automated system backup to a newly created Sandbox environment
3. Restore an automated system backup to a different environment that already exists
4. Restore in any of the three previous methods using a manually created backup

If specific data needs to be restored to recover from a user or application error, or any source that can manipulate data, (AI, automation rules, integrations, etc) administrators need to write and execute a data recovery script that extracts data from the restored database and applies it to the original database. Microsoft cautions this can take a long time to complete.

Limitations of Dataverse Backup and Recovery Services

Most backup and recovery approaches are still stuck in the era of disaster recovery centered around infrastructure failures, making them ill-suited for the data management needs of an always-on, digital world.

The backup and recovery service provided by Microsoft Dataverse presents several notable challenges:



Company
Data Loss
MSFT Admin
Raise Ticket with Microsoft
Seven-Day Retention
Find Out What Has Changed and Restore to Production
Production Environment and Power App's Blackout
Complete Restore Limited to Last 28 Days
Microsoft Engineer Assigned
Restore to Sandbox
Production Set to Maintenance
Restore to Production
Time: Several days, weeks to recover

Linear recovery process

Microsoft's recovery process requires administrators to revert to a specific date and time in the past when data was last believed to be correct, and lose everything that has been added since. This includes both data and metadata,[2] which will inherently revert any solution updates from the point of recovery. Performing a point-in-time restore with a subset of data is complex and prone to errors.

Recovery time

According to Microsoft, it takes about 30 minutes to restore every two gigabytes of data. Recovery is likely to take much longer[3] if there is a prolonged outage in a region and a high number of geo-restore requests are initiated for disaster recovery.

Retention periods

You can retain backups of your production instance with one or more Dynamics CRM or Dataverse environments for up to 28 days. System backups of your sandbox instances are retained for up to seven days, which you cannot extend within the Power Platform Admin Center.

System availability

During a restore, the Dataverse environment goes offline, requiring the admin to take it out of this mode when the restore is complete.

Data corruption detection

Unless a database is inaccessible or a user reports an issue, administrators have no way of knowing data has been deleted or corrupted.

Data change isolation

Restore processes are designed to replace an entire database. Recovering specific data requires the use of complicated and error-prone scripts.

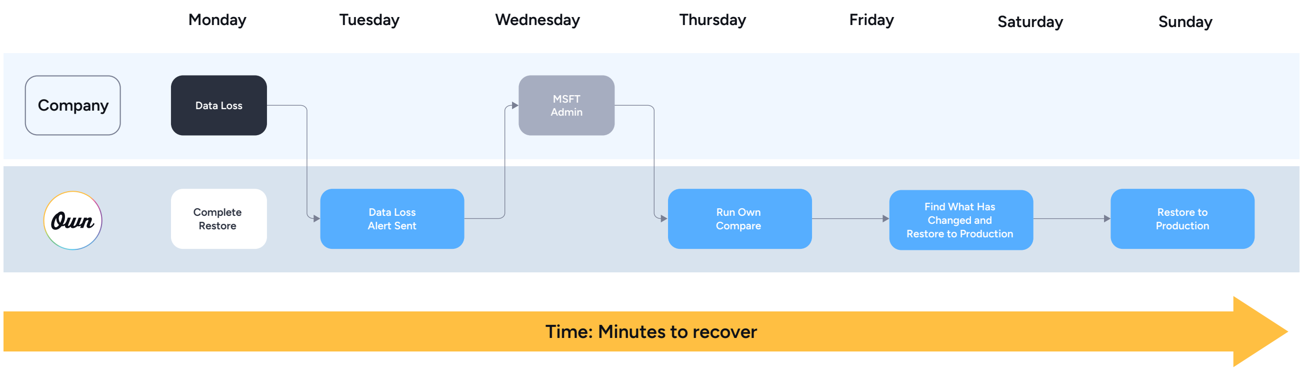
Cost

The more copies of your data you make, the more it costs, because in Microsoft, you pay for Dataverse storage whether it is for production or non-production usage.

[2] Solution history tables get truncated on restore, so histories of all solution releases are erased.

[3] Recovery Time Objective (RTO) varies depending on the nature of the outage, and could take up to 4 to 10 hours.

Own Recover for Microsoft Dynamics CRM and Power Apps



Gain visibility into changes to your environments

Easily investigate data incidents and streamline time to recovery. Quickly compare backups and data changes to your production and sandbox environments by leveraging visual tools to zero in on changed tables, rows, and fields.

Stay connected to backup data anytime, anywhere

Ensure business continuity during cloud service disruptions by accessing your data independently of your Dynamics CRM or Power Apps subscription.

Ensure regulatory compliance

Easily meet and process regulatory compliance requirements with GDPR, SOC2 Type II, HIPAA, and GDPR Article 17 certifications. Tailor retention policies for every instance to keep immutable copies for exactly the right time period.

Restore only what's needed, quickly

Isolate corrupted data, and reinstate data hierarchies in just a few clicks. Easily identify unwanted changes and restore to production — without any downtime or impacting new data from your previous backup.

Easy to use and deploy

A simple, intuitive, and easy-to-use web interface eliminates complexities to configuring Dynamics CRM or Dataverse backups. No installation is required; get up and running within minutes.

Proactively monitor data

Don't be caught by surprise. Be the first to know about suspect data changes that can disrupt your business and stakeholders. Get notified about unusual levels of data changes and deletions.

Retain backups for as long as you need

Design a retention policy tailored to your business needs by taking advantage of unlimited storage and flexible backup scheduling.

A single solution to protect your growing SaaS footprint across the commercial and Public Sectors

Tap into a comprehensive platform of SaaS data protection solutions that span data security, archiving, and seeding for ServiceNow and Salesforce. Public Sector environments can now securely authenticate to the US Government Community Cloud (GCC).

OWN YOUR OWN DATA

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, ServiceNow, and Microsoft Dynamics CRM, 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