

WHITE PAPER

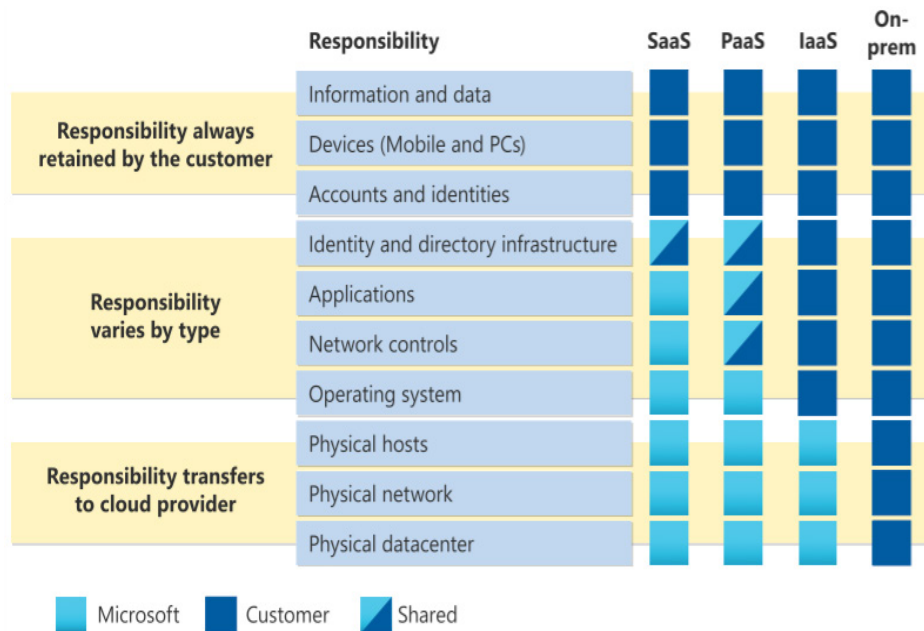
Why Dedicated Backup for Dynamics 365 CE Data

DOES MICROSOFT BACKUP MY DATA?

When it comes to SaaS applications, industry-leading cloud service providers (including Microsoft), follow a ‘Shared Responsibility Model’. Unlike an on-premises datacenter, where you own the whole stack, some responsibilities transfer to Microsoft as you move to the cloud, such as the uptime, performance, and continuous availability of Dynamics 365. However, some responsibilities still lie within your organization, such as protecting the data living within your favorite Customer Engagement (CE) apps.

The following diagram illustrates the areas of responsibility between you and Microsoft, according to your type of deployment:

Microsoft Shared Responsibility Model¹



For all Microsoft cloud deployment types, including Dynamics 365 and the Power Platform, the customer owns their data and is responsible for protecting identities, on-premises resources, and the cloud components you control (which varies by service type).¹

Regardless of the type of deployment, the customer always retains responsibility for the following:

- Data
- Endpoints
- Account
- Access management

And while Microsoft provides native options to back up and restore Dynamics 365 environments,¹ many organizations still turn to dedicated data protection. These third-party solutions enrich native capabilities offering extended retention of the backups, robust recovery controls, and comprehensive tools to meet operational, regulatory, and data governance requirements.

¹ <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility#division-of-responsibility>

EXTENDING BEYOND NATIVE CONTROLS

Microsoft Dynamics 365, like their other SaaS products, offers geo redundancy, which is often mistaken for backup. Backup takes place when a historical copy of data is made and then stored, so if data is lost, accidentally deleted, or maliciously attacked, there will be an easily accessible copy from which to restore. Geo redundancy, on the other hand, protects against site or hardware failure, fulfilling Microsoft's responsibility of continuous availability.

It is established that Microsoft does maintain a backup of Dynamics 365 data, but shared responsibilities clearly put the customer in charge of managing and protecting their OWN data (and rightfully so!). This includes managing it from loss, corruption, or accidental deletion. What the enterprise needs to be aware of is how long Microsoft keeps copies of their data. Data in production environments will be retained for 28 days and data in sandbox environments and most Power Apps will be retained for just 7 days.² Why would an enterprise need a longer retention period? We're glad you asked...

ACCIDENTAL DELETION

Native backup included within Dynamics 365 can only protect from data loss that hasn't left the system. This can turn a simple recovery of human error into a challenge. After 28 days for production, and 7 days for sandboxes, Dynamics 365 hard deletes data from the system—then it's gone forever. If there was an accidental deletion caused by a mistake in the Power Platform Admin, or an errant update/import and the mistake is caught after the 28th day, it is unrecoverable. Period. Unless there is a backup solution at work in the background.

RETENTION POLICY GAPS AND CONFUSION

The fast pace of business contributes to constantly evolving data governance policies, including retention policies that are difficult to keep up with, let alone manage. Dynamics 365 backup and retention capabilities are not intended to meet demanding data governance needs.

For example, several industries require that customer and field service records be maintained for much longer than 28 days. Utilities is a prime example of this. Conversations such as service interactions with customers and the field must be maintained for 2 years or more. In addition, changes to the account must be kept for 7 years and if requested in an auditory process must be restored. This is where extending the native capabilities of Dynamics 365 backup provides a significant benefit for businesses.

INSIDER THREATS

Hackers and viruses are the general idea of a security threat. However, businesses experience threats from the inside, and they happen with increasing frequency. Organizations fall victim to threats posed by their very own employees, both intentionally and unintentionally. Access to files and contacts changes so quickly, it can be hard to keep an eye on those in which you've installed the most trust. Microsoft Dynamics 365 has no way of knowing the difference between a regular user and a terminated employee attempting to delete critical company data before they depart. In addition, some users unknowingly create serious threats by downloading infected files. Of course, a certain level of education is needed to combat these issues, but human error and malice will always pose a threat. These deletions or corruptions if not caught within the 28-day limit won't be recoverable. If caught within the 28-day window it is a manual process, that flows through a sandbox, to recover the data.

² <https://learn.microsoft.com/en-us/power-platform/admin/backup-restore-environments>

With third party backup, data is safeguarded in isolated locations, outside of source environments. This provides an air-gapped copy of Dynamics 365 data that cannot be tampered with by internal and external threats. By isolating this critical data, dedicated backup solutions preserve data and ensure it is rapidly recoverable to production environment's, on a moment's notice.

LEGAL AND COMPLIANCE REQUIREMENTS

Sometimes you need to unexpectedly retrieve transactional data and interactions or other types of data amid legal action. This is a risk that enterprises try to safeguard against, but it is always a burden when it happens. Microsoft Dynamics native backup capabilities hold deleted or changed information for a limited timeframe. When facing audits and litigation requests, businesses are commonly outside of this 28-day window. Legal, compliance requirements and access regulations and requirements vary between industries and countries—but fines, penalties and legal disputes are three areas where enterprises must reduce risk. An extended backup that, when searched doesn't disrupt your production environment is a benefit to the enterprise compliance officer and can avoid costly fallout.

PRECISION RESTORES

'Can't we just roll the production environment back a couple of hours and everything will be OK?' Well, if you could stand the loss of any data entries made after the restore point, that would of course be an option. The fundamental problem here of course is that the Dataverse backup always contains the entire database. There is no built-in way to restore records just from a specific table, rather it's all or nothing.

If this environment was just a single CRM database, as it was before Power Platform came along, then the direct restore operation on top of an existing database might be feasible. Now, this is not a good option, as there's no going back after clicking the Restore button in Dynamics 365.

Take a Power Platform for example. This production environment doesn't just contain Dataverse tables and Model-driven Power Apps, but a wealth of internal tools built on Power Apps Canvas apps and Power Automate cloud flows that run in this system. What would happen to those elements if we'd restore the environment database?

If using Microsoft natively, there's a list of validation steps needed to ensure flows are working as expected after environment restore. Flows may be stopped, triggers and actions may need to be adjusted. Connection References will require new connections. Custom Connectors may need to be deleted and reinstalled. Oh, and speaking of Power Apps Canvas apps, their app IDs will be different in the restored environment, thus breaking bookmarks, embeds, and a whole host of other things. As the icing on the cake, also apps shared with everyone need to be re-shared.

COMMVAULT® CLOUD BACKUP & RECOVERY FOR MICROSOFT DYNAMICS 365

Commvault Cloud, powered by Metallic AI, delivers proven data security and cyber recoverability for your Marketing, Sales, Customer, and Field Service CE applications. Keep Dynamics 365 data protected, compliant, and recoverable from today's threats. With proven, hardened security protocols built-in, you'll enjoy enterprise-grade coverage, with the ease, simplicity, and scale of SaaS.

- Safeguard entities records, forms, field attributes, and more
- Optimize operations with automated backups
- Store and retain data for unlimited timeframes
- Seed and replicate sandboxes to accelerate dev/test
- Mitigate risk with air-gapped backups, and zero-trust user access
- Recover rapidly with immediate and flexible restore options
- Protect Dynamics 365, Office 365, and Azure from a single solution

For more information on Commvault Cloud Backup & Recovery for Microsoft Dynamics 365, please visit the [following page](#).