FieldTrust
INNOVATIVE SOLUTIONS

redstor

7 reasons why you need a separate backup strategy for Microsoft 365

How secure is your data?

To what extent do Microsoft's native tools support backup and recovery?

There is a common misconception held by some IT professionals that cloud services, such as Microsoft 365, do not need to have a backup.

But to believe that a SaaS vendor like Microsoft has taken care of your backup is a dangerous assumption - particularly when data has been deleted, but it's gone unnoticed for a while.

Here are seven reasons why it's important to have a diverse backup strategy:

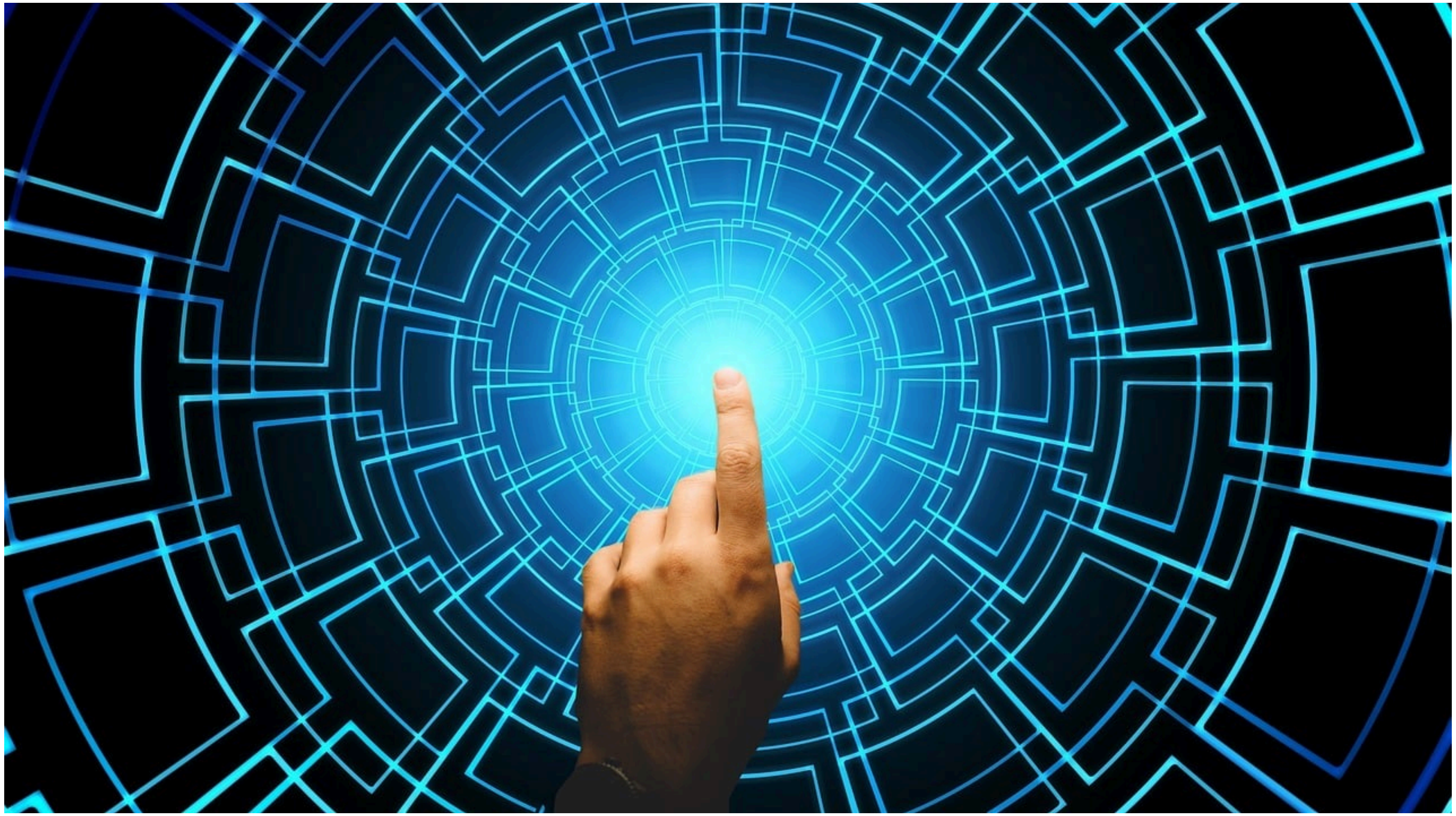
Retain control with a tailor-made solution

1) Avoid dependency
2) Set your own retention policies
3) Address compliance issues

1) Avoid dependency

It is a big mistake for an organisation to be wholly dependent on a single cloud vendor. If organisations do not have control of their data, they will struggle to act immediately once an issue becomes apparent.

Even when data is retrievable, the process could end up being long and complicated, and there is the added problem of all-or-nothing destructive restores.

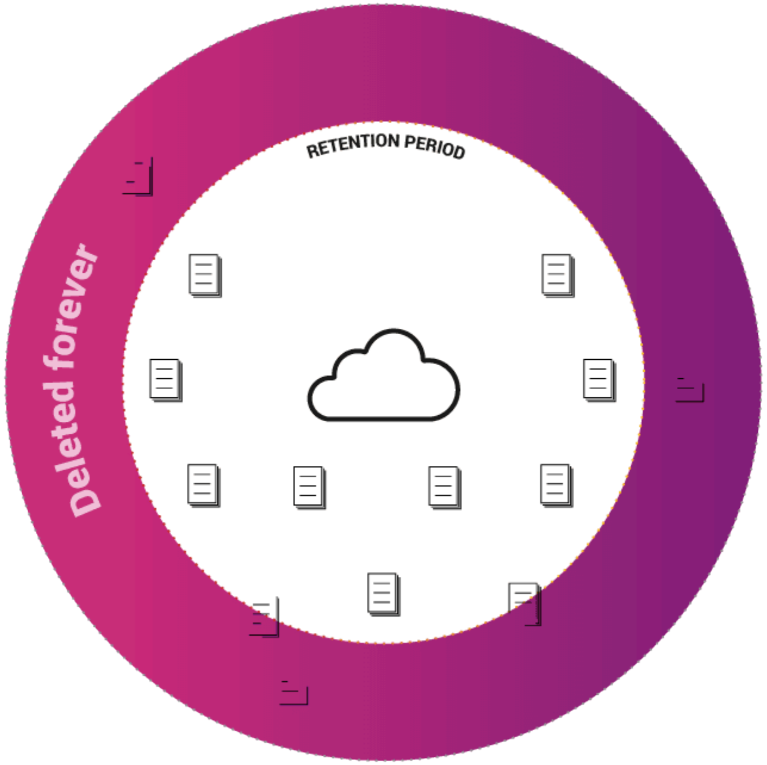


2 Set your own retention policies

Microsoft 365 is not intended to be an all-encompassing backup solution.

A simple recovery can be a massive problem if data has fallen out of the retention period and Microsoft 365 has deleted it forever.

You can avoid this with a data management service that allows you to set your own retention policies very easily and whose sole purpose is to ensure that your data can be recovered directly back to Microsoft 365, regardless of the state of your live data.



3 Address compliance issues

If employees leave a company, can you prevent their files leaving with them?

When someone deletes a user or users from Active Directory - intentionally or otherwise - once they are outside of retention their Sharepoint sites and OneDrive data are also deleted.

What if you need those files during legal action in months or years to come?

If you are to retain access to data after a user has been removed from Microsoft's Active Directory, it's imperative to have a backup to a third-party backup provider, not least for compliance purposes.

Avoid adverse impact on business

4) Recover everything in the event of deletion
5) Prevent delays due to data loss

4) Recover everything in the event of deletion

What happens when users accidentally or intentionally delete or overwrite files? Recycle bins and version histories in Microsoft 365 provide only limited protection.

If you delete a user, whether you meant to or not, that deletion is replicated across the network. Once an item is purged from the mailbox database, it is unrecoverable. This could have far-reaching effects if a rogue employee decided to delete incriminating emails or files.

Microsoft's backup and retention policies can only protect you from data loss up to a certain point, and can't take the place of third-party data management solutions.

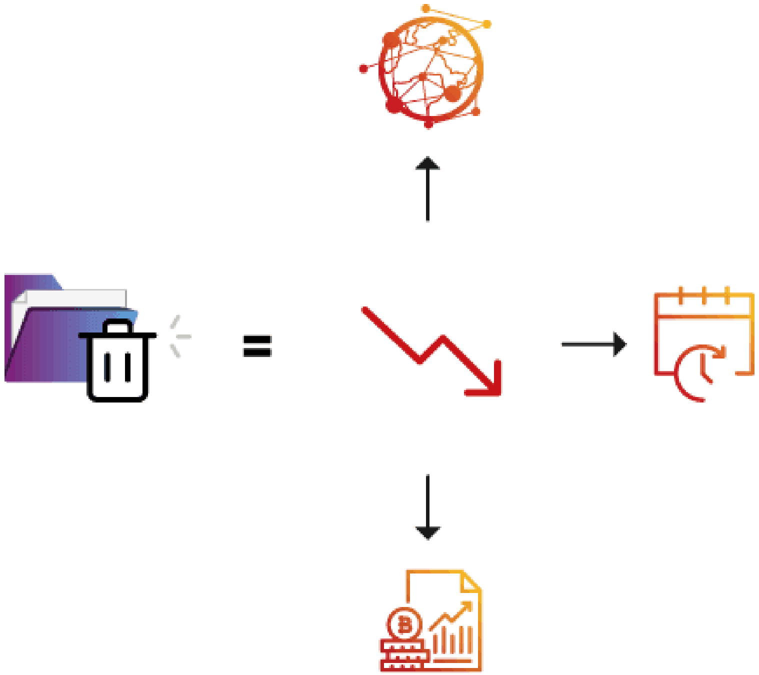
5) Prevent delays due to data loss

When data is deleted or corrupted, businesses face three major problems - loss of data, loss of time and loss of money.

Microsoft provides exceptional availability and cannot be expected to focus elsewhere on extended retention or old user data.

Being solely reliant on Microsoft Support for help recovering lost data can be very time consuming.

The best way to avoid an issue impacting severely on business continuity is to find a third party that offers streamed, on-demand access to data at a moment's notice.



Enhance security

6 Protect against ransomware attacks
7 Separate roles as security standard

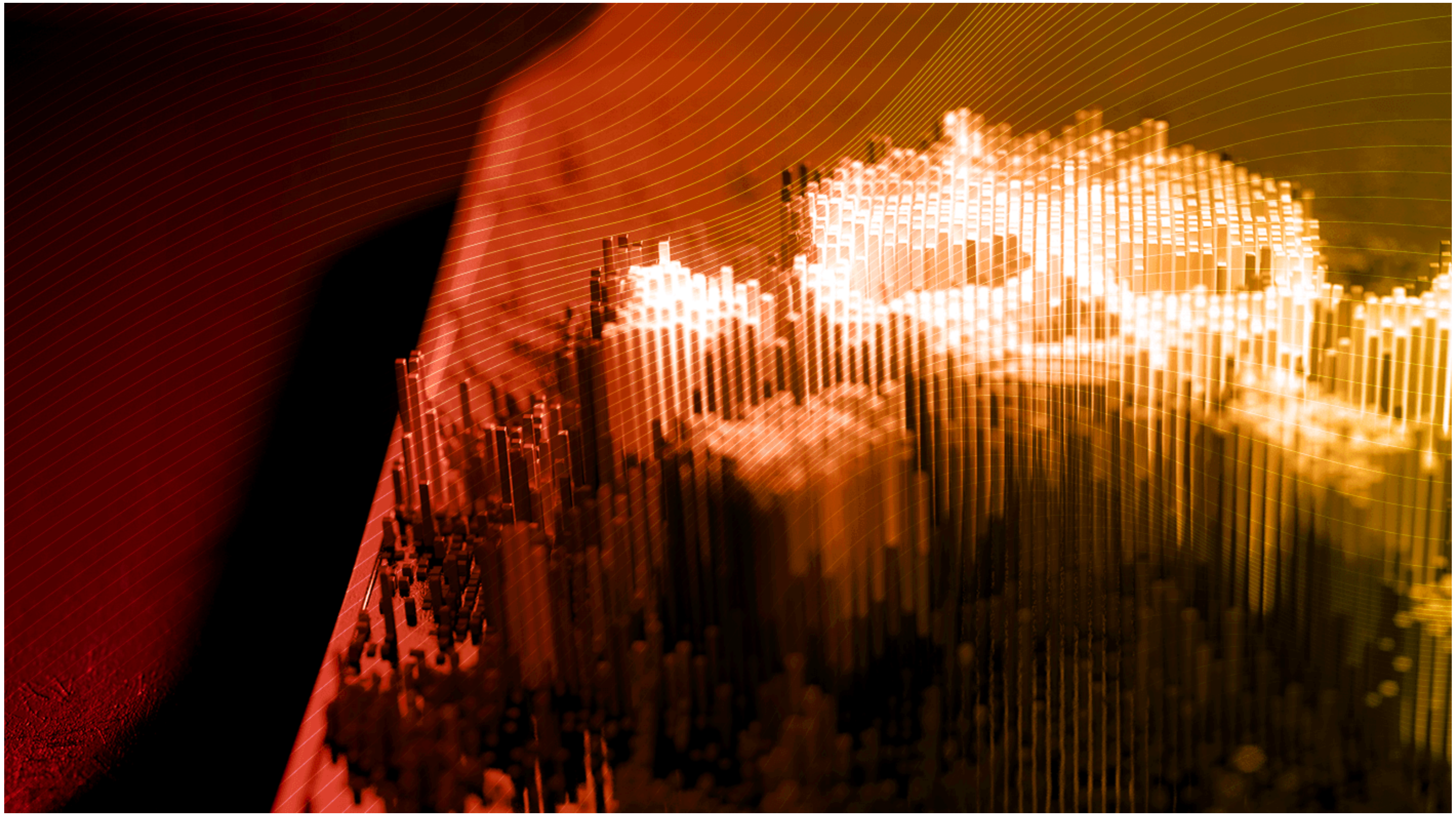
6) Protect against ransomware attacks

How can organisations be protected from app outages, misconfigured workflows or ransomware attacks?

Microsoft explicitly states that point-in-time restores of data are not in the scope of the Exchange service.

Regular backups will help ensure a separate copy of your data is uninfected and that you can recover mailboxes quickly to an instance before the attack.

The best data management providers offer streamed, on-demand access to all data instantly.



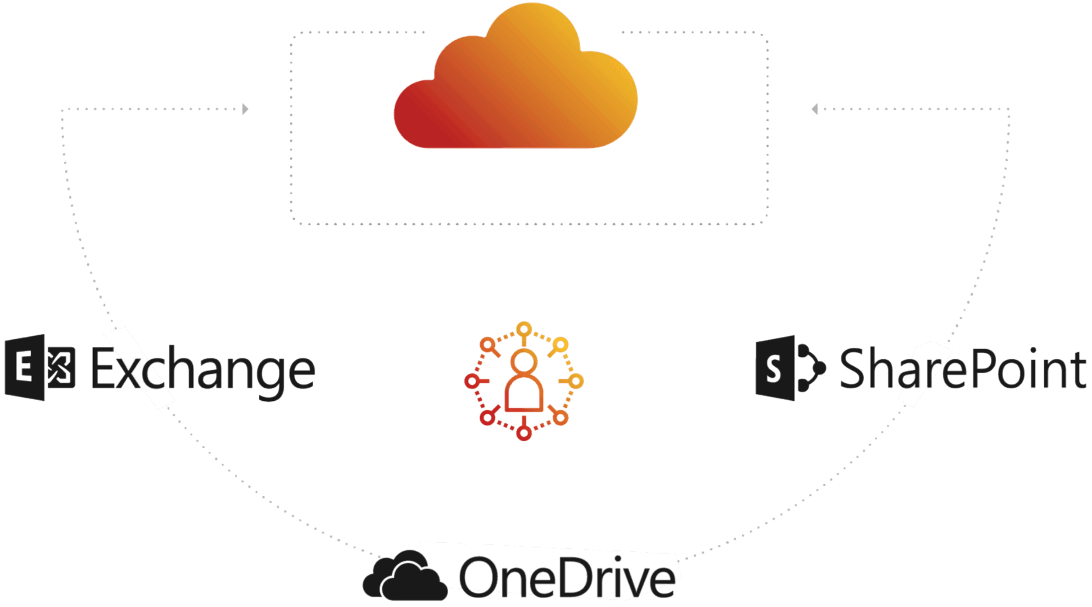
7 Separate roles as security standard

Companies nowadays require a separation of roles as a security standard.

Having your backup in the production platform allows for a single point of failure.

Microsoft 365 administrators could also potentially assign themselves full access to search and export from Exchange mailboxes, SharePoint folders, and OneDrive locations.

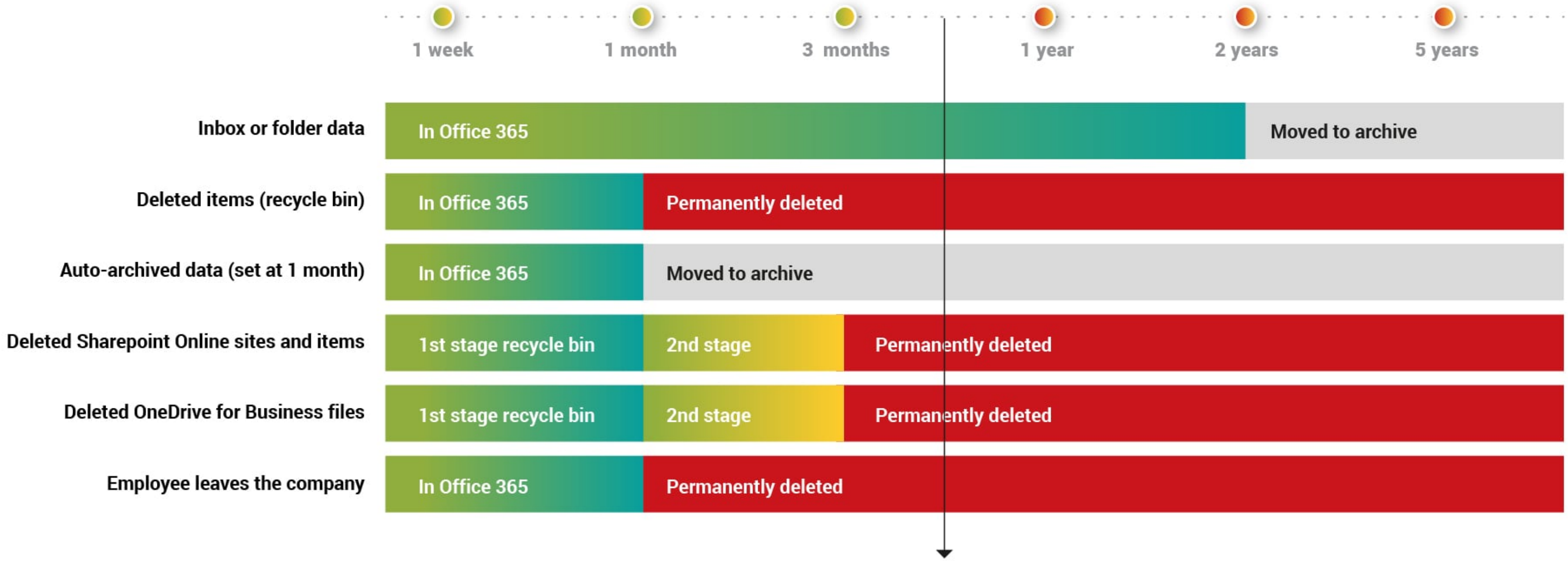
This would enable them to delete a file. Without third-party backup, that file, depending on the retention policy, may be irretrievable.



An isolated backup strategy is vital for compliance purposes

Extend retention and cater for deleted users

Office 365: What is backed up?



The average length of time from **data compromise to discovery is over 140 days,** yet default settings only protect 30 - 90 days.

Protect all the Microsoft **365 data within your organisation, directly from Microsoft's cloud, all through an intuitive web interface.**

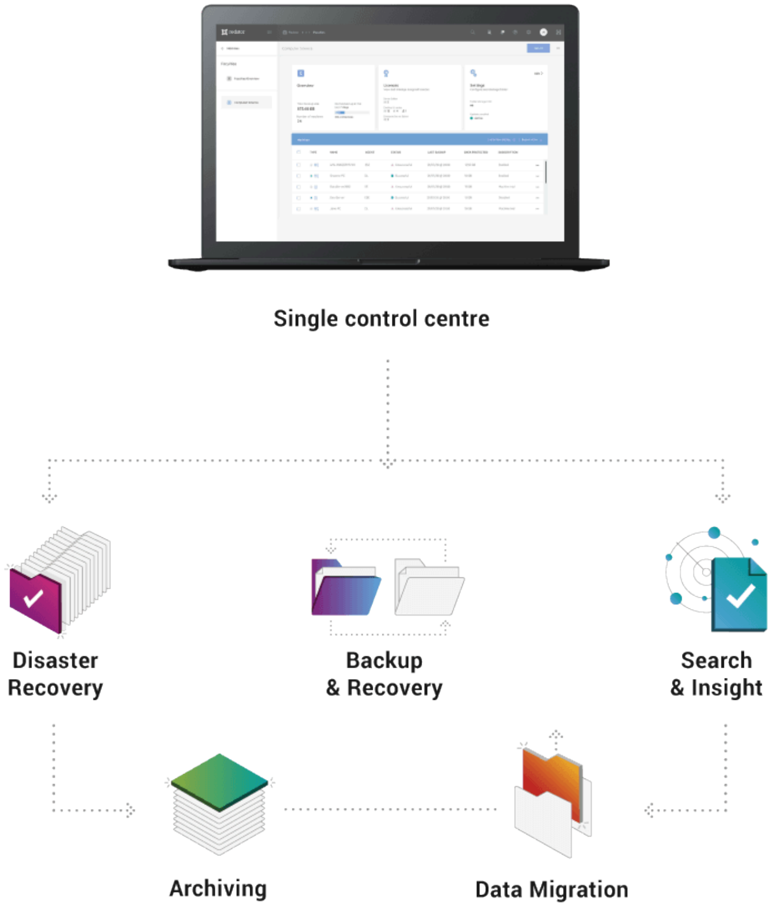
Extend retention and cater for deleted users with a diverse backup strategy that addresses compliance issues as well as simplifying your data backup systems with one central, easy-to-use system. InstantData™, Redstor's unique streaming technology, provides on-demand access to all of your data, wherever it is stored.

Gain borderless visibility of your entire data estate at any time, on any device. Our web-based control centre gives you a centralised view of multiple sites, wherever you are

Manage by exception and easily evidence compliance.

Redstor's data management solution includes role-based access control and auditing, which helps companies to comply with current and upcoming data protection laws, while also allowing a different department or administrator to hold the rights for restores.

See how the Brandon Trust improved business continuity and made cost savings by choosing Redstor to complement Microsoft Azure.



Thank you for reading

Microsoft 365 backup strategy

Contact us at redstor@fieldtrust.be

FieldTrust