Redstor Microsoft 365 protection datasheet

Microsoft provides platform protection for M365 - but ransomware, user mistakes, malicious behaviour, sync or configuration errors all threaten an organisation's productivity.

Ensuring business continuity can be difficult and risky if IT staff rely on native protection since this is not only limited, but also complex and time-consuming to manage.

Organisations have a responsibility not only to protect critical data in Microsoft 365, but also to comply with regulations.

You can address these challenges by backing up data in Exchange, OneDrive, SharePoint, Teams and OneNote directly from Microsoft's cloud to the Redstor cloud.

Simplified data management

Protect your Microsoft 365 data as part of a unified, automated, policy-driven data management strategy, using Redstor's powerful, web-based control centre. With the complete visibility that Redstor offers, you can assign consistent protection policies across your entire data estate. Backup and recovery, archiving, disaster recovery, search and insight, and data migration can all be managed with one central, easy-to-use system.

True cloud-to-cloud protection
No on-prem servers required, no impact on local bandwidth or storage management.

Intuitive, user-friendly control centre
No need to splash out on user training. Protect in minutes - start restoring in seconds.

Customisable retention
Redstor retains M365 data for however long you want - the standard 60 days, seven years or even indefinitely.

GDPR compliance
Find and delete references to a data subject, enabling you to comply with Article 17 of the General Data Protection Regulation (GDPR), i.e. the "right to be forgotten".

Audit trail of user activities
Actively track and monitor all user activity across the cloud-to-cloud platform. Easily evidence restores.
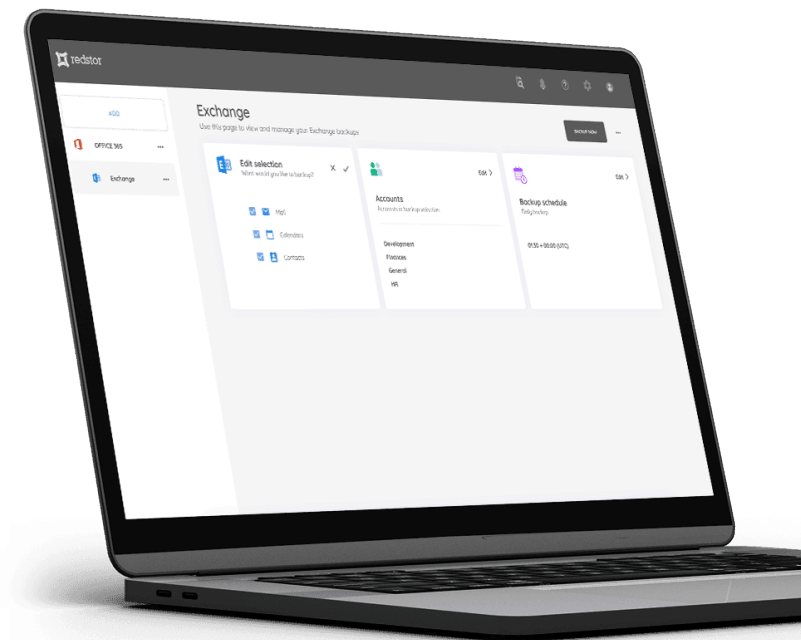
Full control, fast recoveries

OneDrive & SharePoint

For OneDrive and SharePoint, you have two recovery options: straight back to the cloud, or onto a physical machine using Redstor's InstantData™ technology. Both have single-item recovery options. Simply select the relevant accounts and where you want to recover to - the original location or a new folder/new site.

Recovering with InstantData™ onto a physical machine

Each selected account receives an email with a link to our InstantData™ agent. When you click on this link, an easy-to-use interface will appear from which you can configure your recovery, including how long you want access to the data to be available to other users.

OneDrive
SharePoint

InstantData™

As an admin, you are able to search across a OneDrive account and SharePoint site for specific files and select them individually to restore.

Physical recovery can be:

Permanent - Work on whatever files you need, while Redstor restores the rest of the data in background

Temporary - Access backups temporarily on a virtual drive (no local disk space required)

Exchange

Search for individual items online. Select a mailbox and then choose whether to restore messages and attachments, calendar events, contacts or the whole mailbox.

Recovering back to Microsoft 365 Exchange

In this scenario, data is restored into a new 'Redstor' folder which appears in your M365 Outlook client.

Within this folder is a separate folder, named with the date of the restore point. From here, you can move individual email items to

Granular recovery
Select individual emails, contacts, or calendar events from backup and restore instantly

Rapid restores
With Redstor, downtime in the event of a disaster will be seconds rather than days. Simply restore the data you need to carry on working - as soon as you need it

Point-in-time versions
Restore historical point-in-time versions of data so administrators and end users can see the data in its exact context

Full control
End users and IT admins restore data via a web-based control centre

wherever they need to go,
such as the original mailbox
or a different location.

Teams

Back up and restore teams, channels, posts, files and tabs.

Recovering to Teams

There are several options.

1) Recover a team's data to its original location, to a new team or recover using single-item recovery to the original team.

2) Recover to a physical machine, using InstantData™. A recovery link is sent to the email address associated with each channel. The user can then use the InstantData™ link to recover the files they need.

OneNote

Redstor protects your OneNote notebooks in whatever M365 app they were created in. Restores back to OneDrive, SharePoint sites or Teams are conducted in the same way as any other files restored to those locations.

A notebook in OneDrive or SharePoint can be recovered straight back into M365 or onto a physical machine, using Redstor's InstantData™ technology.

Physical recoveries can be conducted on a permanent basis or can be temporary with backup data presented

as a virtual drive.

InstantData^{TM} recovers the notebook in its entirety but displays the content within it as separate folders and files.

If a notebook is created within a team's data in Teams, you can recover it to its original location, to a new team or, using Teams' single-item recovery, to the original team. Alternatively you can recover the team's data and the notebook to a physical machine, using InstantData^{TM}.

Class Notebook and Staff Notebook

Class and Staff notebooks have additional settings to OneNote notebooks and require extra backup and recovery permissions, but they are protected and restored to Teams and OneDrive in the same way as other files in those M365 apps.

Once again InstantData$_{TM}$ will display these notebooks and their content as separate folders and files, but will recover a Class or Staff notebook in its entirety to a physical machine, along with its associated team in Teams.
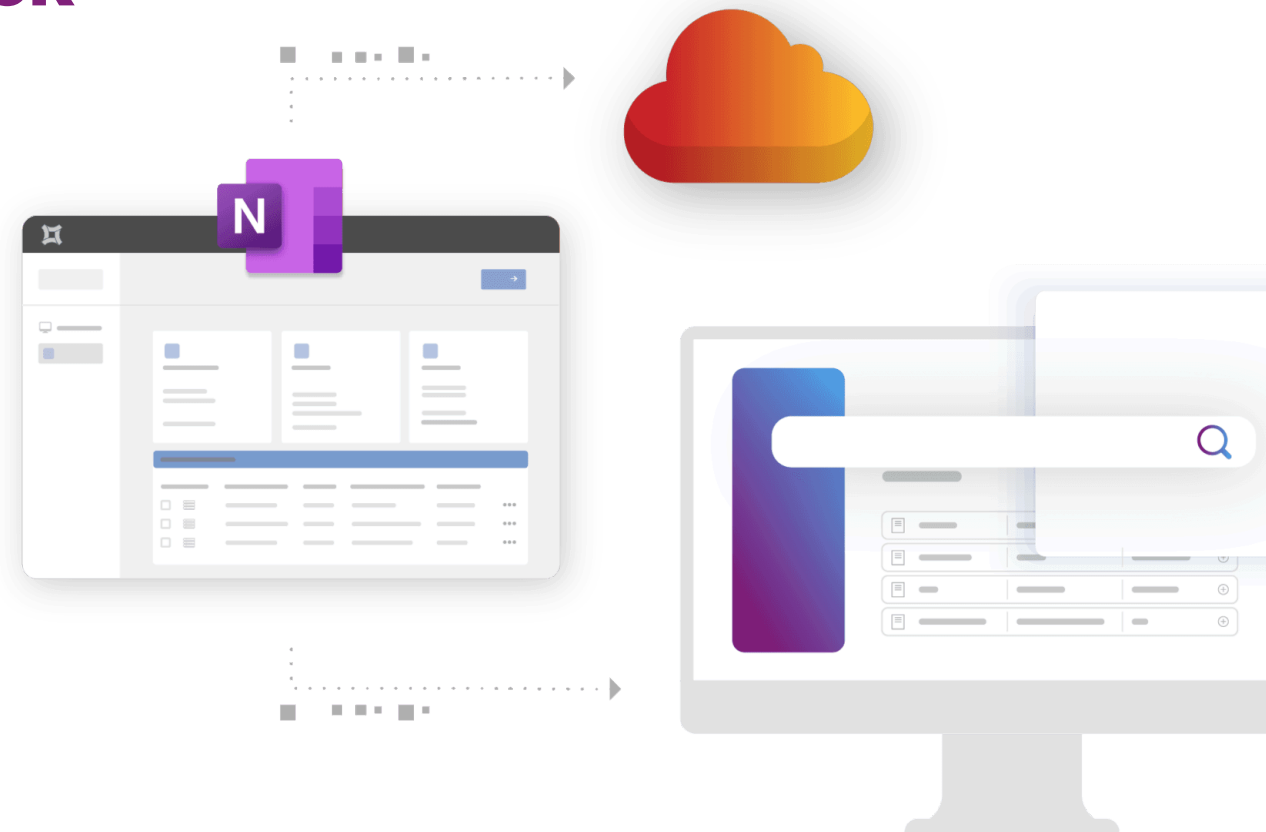
See the future of data management. Now.

Protect your Microsoft 365 data today and see how fast and easy it is to manage

Compare Redstor now with any existing data management solution you may have

Speed

Set up, trial and scale fast - what may have taken days in the past, now takes hours. No hardware, no professional services costs, no management overhead, no complex licensing models.

TRY FOR FREE

Control

A powerful, self-service portal eliminates vendor bottlenecks - leaving you free to deploy, manage and scale Microsoft 365 protection quickly and easily (24/7 support remains on hand if required).

Value

If you protect your wider estate with Redstor too, you can do it all via a single control centre and manage your Microsoft 365 data as part of a centralised data management solution. Get backup and recovery, archiving, DR and Search and Insight from a single vendor on a unified platform.
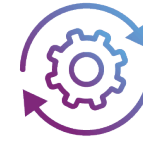
Smart

Our automated portal provides a single place to view and manage cloud and on-prem data, saving on time and operational overheads.
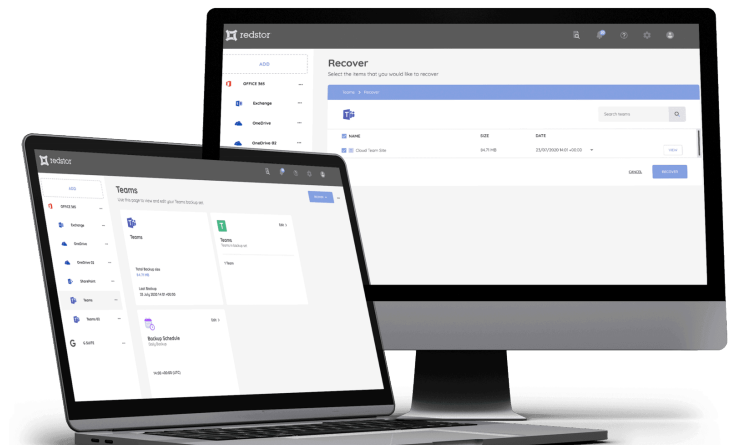
See how to set up your M365 environment :
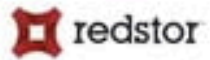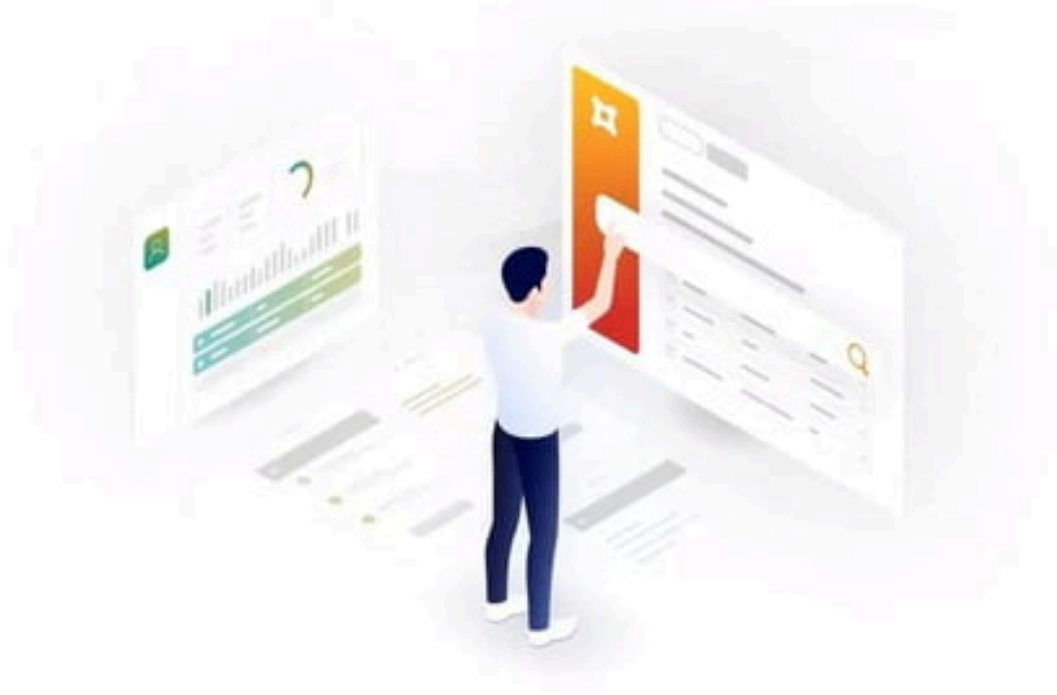
How to recover a single email item:

How to perform a OneDrive recovery:

How to recover OneDrive using InstantData:

How to set up Teams for backup:
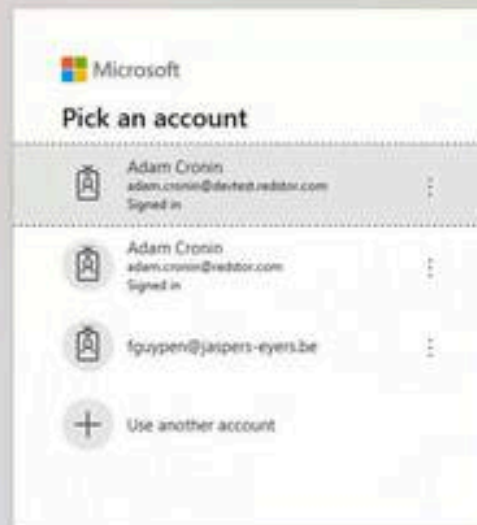
How to perform a Teams recovery:
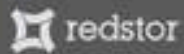
How to recover Teams using InstantData:
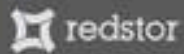
How to back up and recover OneNote:

Microsoft 365
OneNote recovery

What's protected

What's protected with Redstor

OneDrive - Safeguard files and folders.
SharePoint - Secure site collections, team sites and communication sites.
Exchange - Protect emails and attachments. calendar events and contacts.
**Teams** - Back up and restore teams, channels, posts, files and tabs.

Streamline management

- Data in OneDrive, SharePoint, Exchange Mail and Teams is automatically backed up in the background every day, while you can perform additional backups as needed at any time. New users and sites are automatically protected.

- Set-up is quick and easy

1) Log into Redstor's cloud portal
2) Select accounts or sites that need protecting
3) Start backing up immediately
4) Schedule subsequent incremental backups to occur daily or on specific days
5) Monitor backup progress from cloud portal
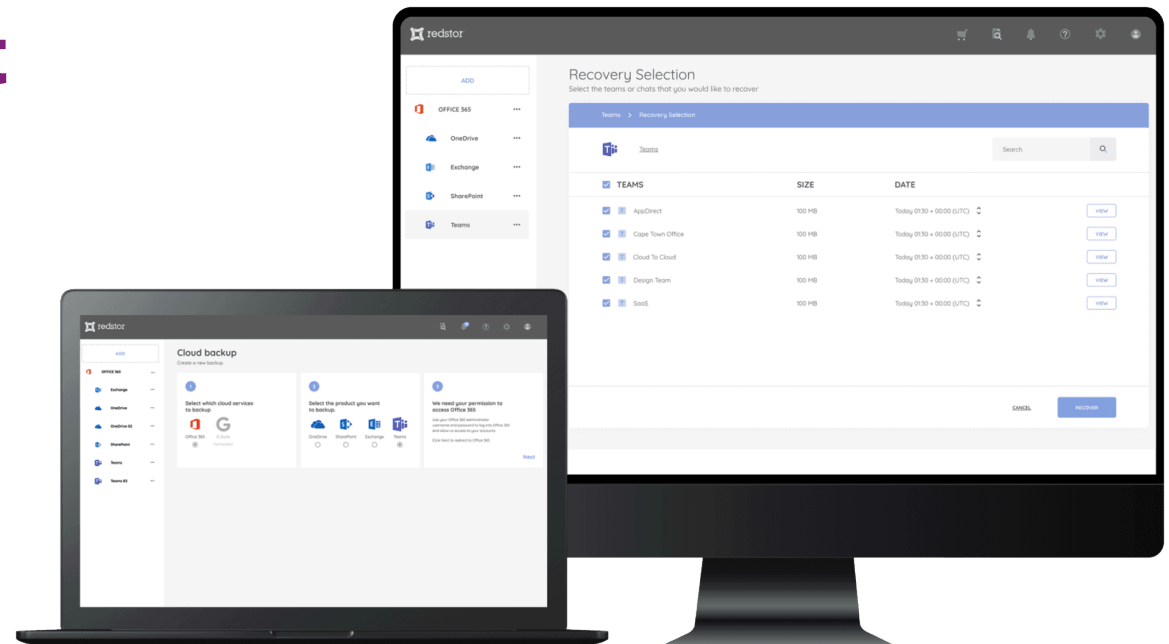
Strong security

Perform centralised management of your data without circumventing M365 security and auditing. Whenever you add a new backup set, Microsoft will ask your permission for Redstor to access your data.

Role-based permissions
Only your relevant IT staff will have the ability to download mailboxes. Microsoft will not have access to any of your organisation's mailboxes.

Advanced Encryption Standard
Before data is transferred during backup or recovery, it will be encrypted with 256-bit AES. Furthermore, all communication between Redstor's cloud backup service and its storage platform (where your data is stored) is secured with Transport Layer Security (TLS)

Data sovereignty
Local data centres are used to ensure you comply with data residency or data sovereignty regulations

Activity log
Logs provide a full record of administrator and user actions.

MFA (Multi-Factor Authentication) support

Without MFA, your users' passwords will be the only method of restricting access to your data. With Redstor, you can add an additional layer of security, like authentication via a trusted device or fingerprint.

Demo video

How to set up your Microsoft 365 environment

Thank you for reading

Factsheet - Backing up Microsoft 365 with Redstor