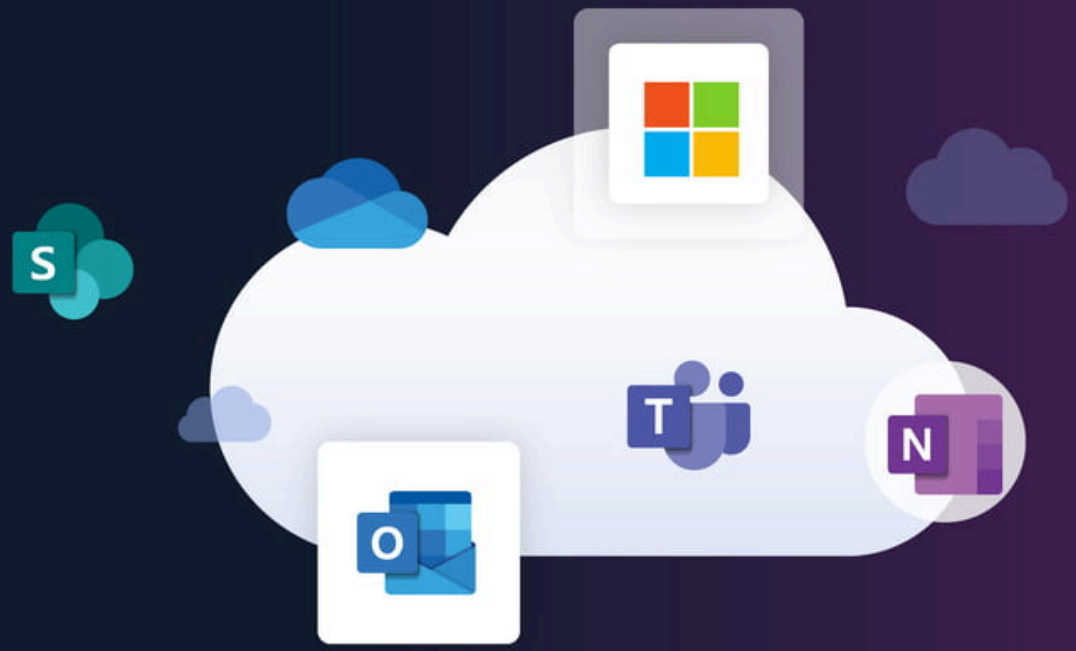
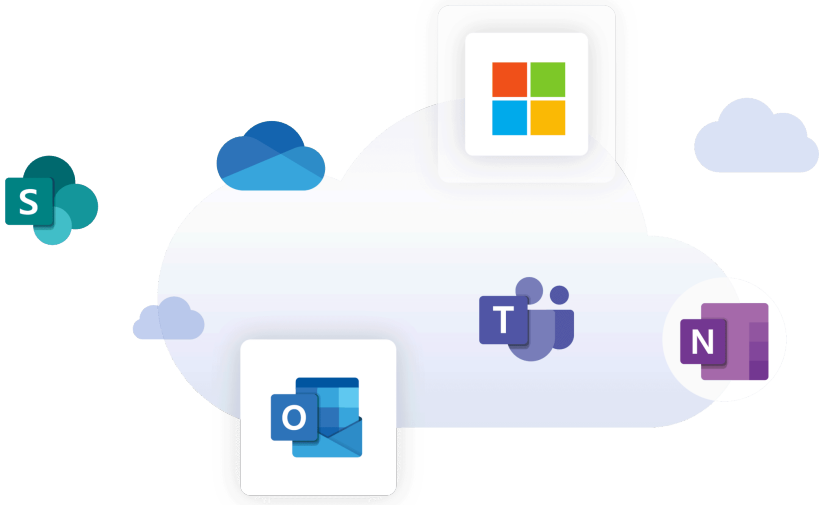
Protecting Microsoft 365 with Redstor as part of an automated, policy-driven, unified data management strategy.

*NEW - AI enables malware-free recoveries

Avoid the risk of storing all your data with one provider





Protect the Microsoft 365 data within your organisation - directly from Microsoft's cloud to the Redstor cloud - and manage it all through a single application

Microsoft's Service Agreement, Section 6 states: 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.

The new standard of data management and protection

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

Benefit from market-leading 365 coverage, featuring complete protection for SharePoint, OneDrive, Email, Teams, OneNote and even Class and Staff Notebooks.

Speed

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

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 manage your Microsoft 365 data via a single app as part of a centralised data management solution. Get backup and recovery, archiving and DR from a single vendor on a unified platform.

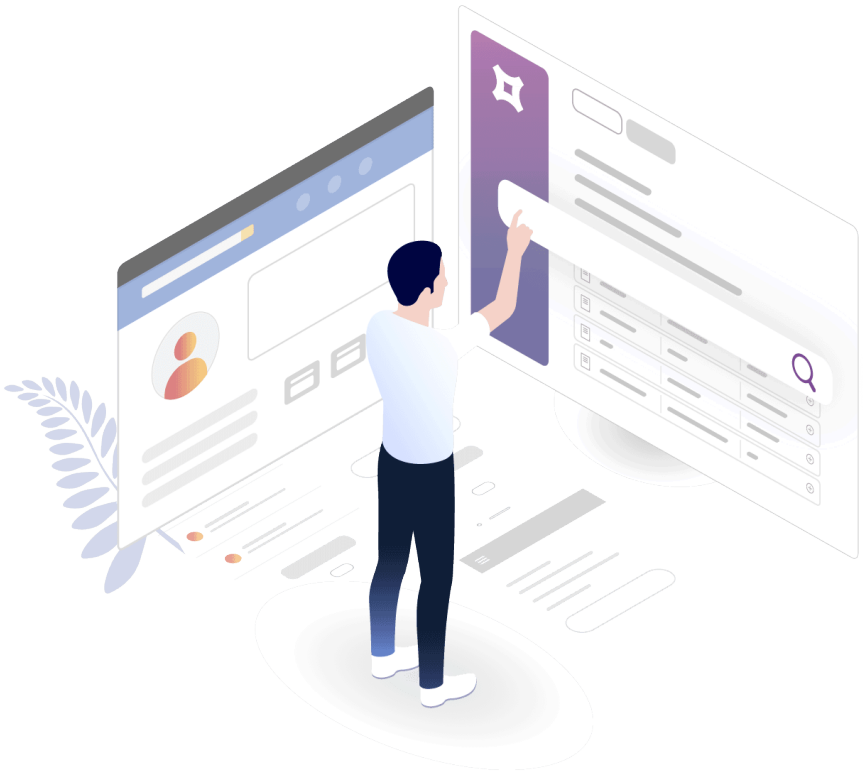
Smart

Automatically highlight risks and protect data against malware with Redstor's platform, which continuously learns and improves, based on community insights.

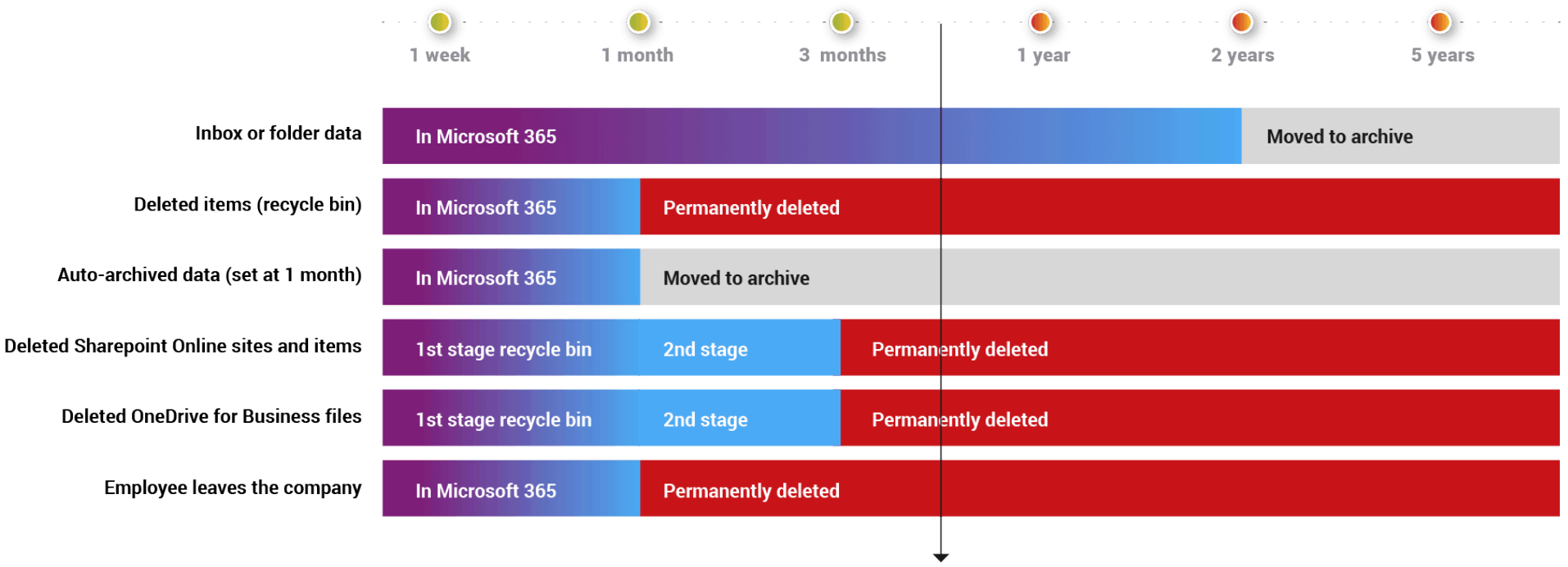
TRY FOR FREE

Simplify and automate your data management and assign consistent protection policies across your entire data estate with one central, easy-to-use application.

- **Establish a consistent data protection policy** across your whole estate, viewing cloud and onsite data in one place through a single app
- **Comply with the General Data Protection Regulation** with the timely access to data you need to avoid potential fines and reputational damage.
- **Define Microsoft 365 retention periods** and ensure they are aligned to your business requirements
- **Detect and remove malware from backups,** using artificial intelligence to quarantine suspicious files for an additional layer of protection against ransomware
- **Set up in minutes, and easily scale the protection you need** - without the need for capital expenditure
- **Deliver centralised management of data** in Microsoft 365 Exchange, SharePoint, OneDrive, Teams and OneNote without circumventing Microsoft 365 security and auditing
- **Benefit from faster, simpler recoveries** with on-demand access to data in the event of accidental deletion or a ransomware attack
- **Retain full control of your data** for business continuity by mitigating the risk of storing it with the cloud service provider
- **Avoid lock-in** by migrating data easily



Microsoft 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.

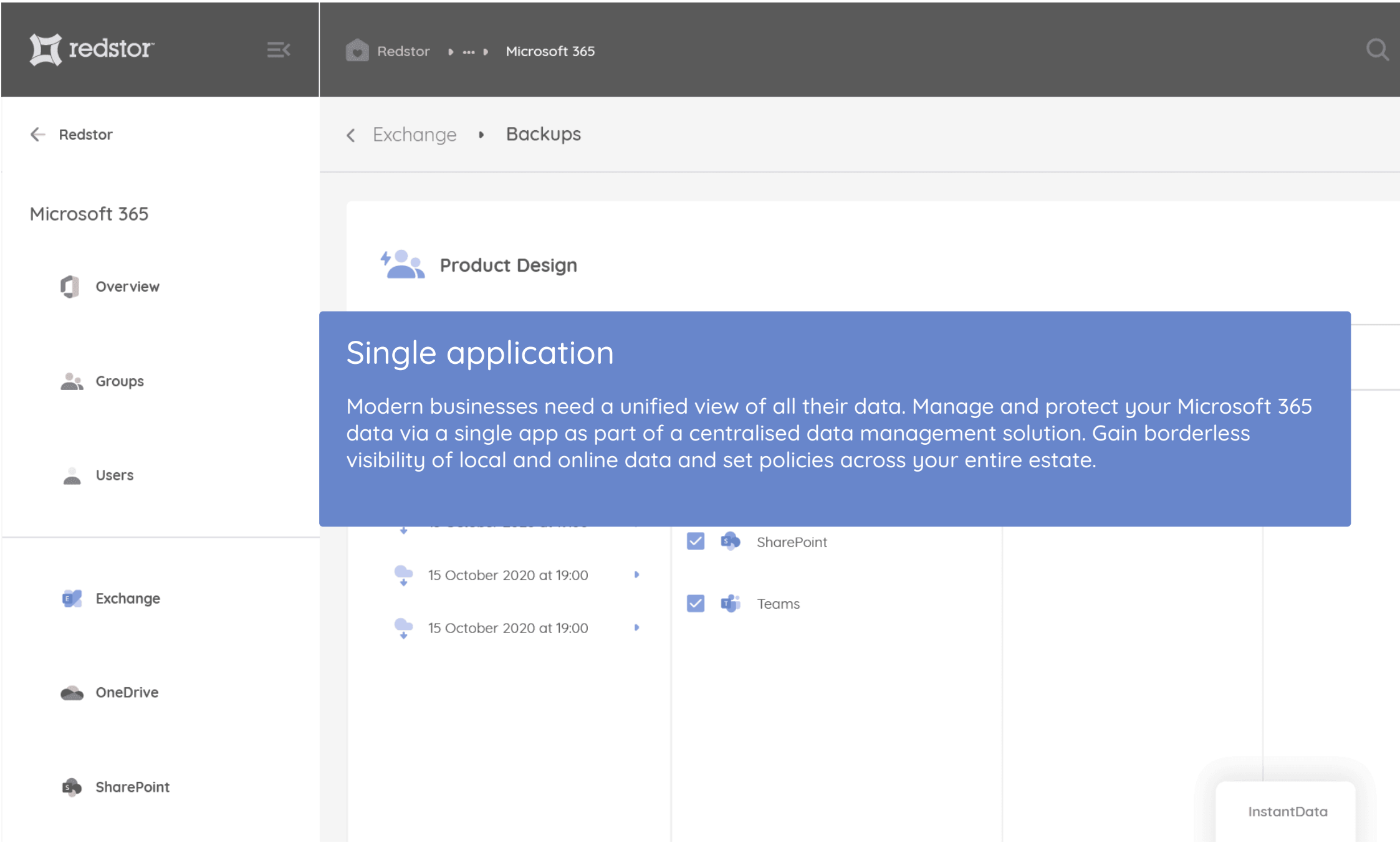
Microsoft 365® data recovery restrictions:

Outlook:
Deleted emails can be recovered within 14 days, but are permanently deleted and cannot be recovered after 30 days.

OneDrive / SharePoint:
Items are retained for 93 days from the time of deletion from their original location. Administrators can contact Microsoft Support to request or restore within 14 days, but items are permanently deleted and cannot be recovered after 14 days.

Outlook Calendar:
The calendar and all events recorded in it are permanently deleted and cannot be recovered after deletion.

Outlook Contact (People):
Deleted contacts can be recovered within 14 days, but are permanently deleted and cannot be recovered after 30 days.


redstor
Redstor
Microsoft 365
Redstor
Microsoft 365
Exchange
Backups
Product Design
Overview
Groups
Users
Exchange
OneDrive
SharePoint
Single application
Modern businesses need a unified view of all their data. Manage and protect your Microsoft 365 data via a single app as part of a centralised data management solution. Gain borderless visibility of local and online data and set policies across your entire estate.
SharePoint
15 October 2020 at 19:00
Teams
15 October 2020 at 19:00
InstantData

Easily evidence compliance

Gain comprehensive oversight across an entire estate with real-time reporting and insights to proactively highlight data risks. Restrict permissions, track search sessions and monitor all data deletions.

Automated, simple management

Get up and running in minutes and benefit from intelligent, policy-driven automation, powerful monitoring and sophisticated reporting. Fast to deploy and easy to manage, our pioneering solution requires zero human intervention on a daily basis.

Built to scale for maximum cost savings

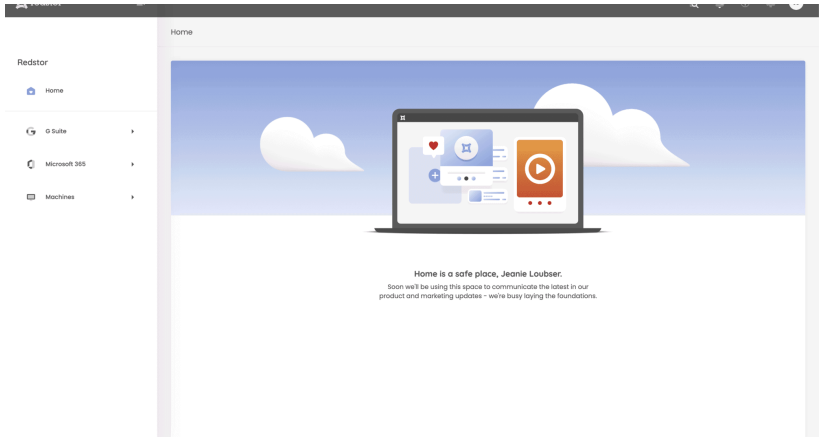
Scales seamlessly in line with your Microsoft 365 needs. Unlike some services for protecting Microsoft 365, Redstor provides true cloud-to-cloud protection for your data without the requirement for any on-prem hardware. Transparent and predictable pricing. No hidden costs, no surprises.

Move data transparently, with no downtime

Avoid lock-in by having the capability to move data easily back on premises if required and access data anywhere, using InstantData™ to stream data to the user on demand.

Fully auditable

Protect your entire organisation in a couple of clicks without compromising on security. The history of all Microsoft 365 search and delete sessions is stored. The erasure of relevant data is simple, monitorable, and auditable throughout the deletion process.



Maintain full control for business continuity

Avoid relinquishing control and relying on the cloud provider for restores in the event of an issue. With a separate backup policy, you can confidently manage and access 365 data with Redstor.

Strong security and guaranteed data sovereignty

With zero downtime and preservation of data sovereignty, your data remains 100% safe in our dedicated, highly secure, local data centres. Our engineers are available 24/7/365 to provide expert advice wherever you are in the world. Encrypted at source using Advanced Encryption Standard with a 256-bit key length, your data remains protected with a customer-defined key.

Rapid restores

Radically reduce the impact of accidental deletion, malicious activity or corruption with granular recovery. For OneDrive and SharePoint, select the specific file or folder and whether you want to recover back to the cloud or onto a physical machine. For Exchange, select a mailbox, then choose whether to restore messages and attachments, calendar events, contacts or the whole mailbox. Restore Teams, channels, posts, files and tabs. Protect OneNote, Class and Staff Notebooks - and restore to whatever M365 app they were created in.

Detect and remove malware from backups

With automated malware detection as an added feature, your M365 backups will be checked for suspicious files. Our machine-learning model enables you to isolate and delete malware from backups, providing you with an additional layer of protection and peace of mind that you can perform malware-free recoveries.

AI enables malware-free recoveries

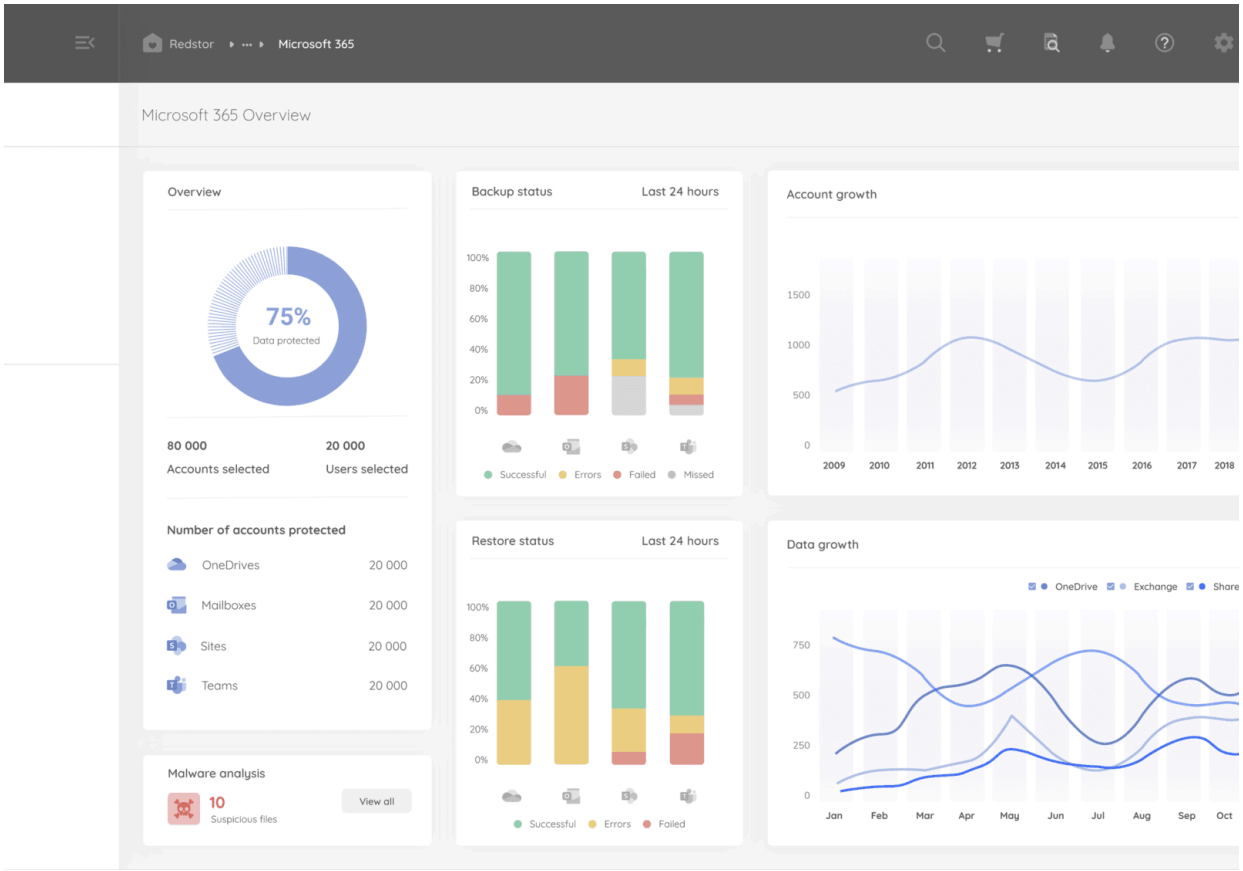
Most organisations will have a form of anti-virus and anti-malware protection in place, but the time it takes to uncover a malicious attack is often longer than typical retention policies.

In this case malware will be present within all backups as well as the live environment. This makes it extremely difficult to perform a malware-free recovery.

With Redstor you can detect, isolate and delete malware from backups for that additional layer of protection and peace of mind.

Our artificial intelligence-infused solution enables you to:

- **Mitigate risk** – ensure you can recover safely, even if your Microsoft 365 data has been infected, by ring-fencing your backups in a known safe state
- **Eliminate downtime** – avoid end-user frustration and loss of productivity with malware-free recoveries
- **Flag threats** – suspicious files are automatically quarantined after EVERY backup

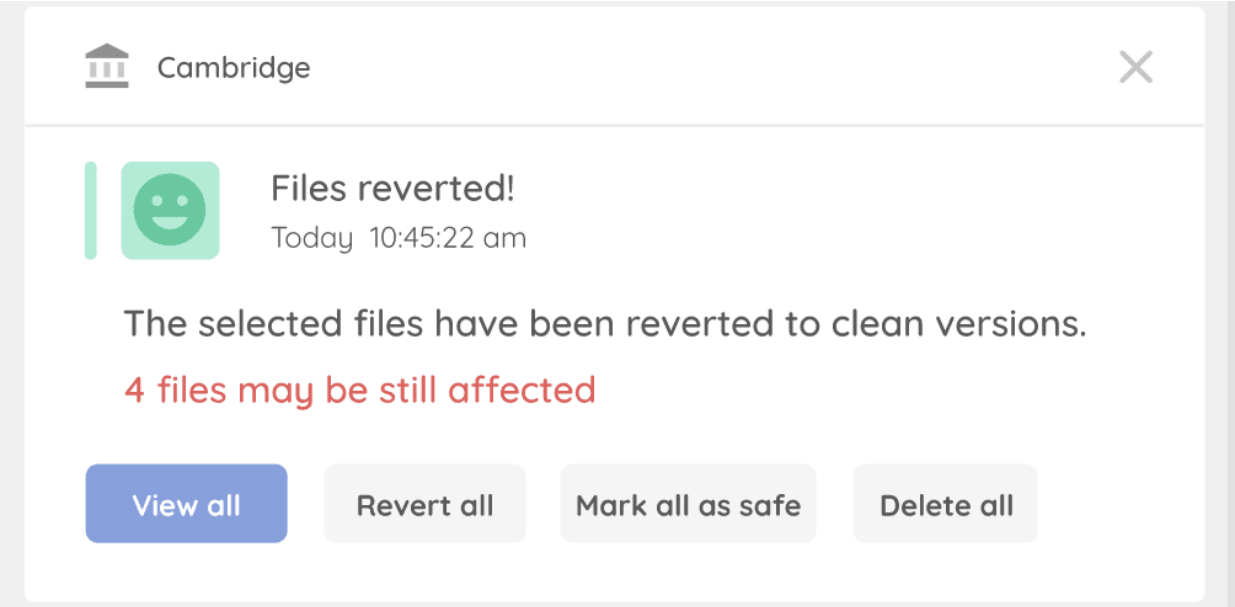


Detect malware in M365 backups

Our machine-learning model:

- searches for key indicators exhibited by malware
- checks for malware outside your environment, so there is no impact on your resources
- avoids the need for a user to configure or install anything or carry out upgrades

When you purchase Redstor's malware detection for backups as an add-on, it will quarantine suspicious files in backups from SharePoint, Exchange (including attachments), OneDrive, Teams. If an attachment is flagged as suspicious, the entire email will be quarantined. The option is also available to check backups from servers, laptops and any other end-point machines or devices.



Constantly improving its accuracy, based on shared community insights, Redstor's machine-learning model provides enhanced protection against 'zero-day' threats, leaving you free to make malware-free recoveries.

Removing suspicious files

Manual intervention is only required when a suspicious file is detected. A notification then gives the option to:

- delete the file
- revert to a previous safe version
- mark it as safe
- leave it in quarantine

These actions can be taken in bulk by selecting multiple files or done for a single file.

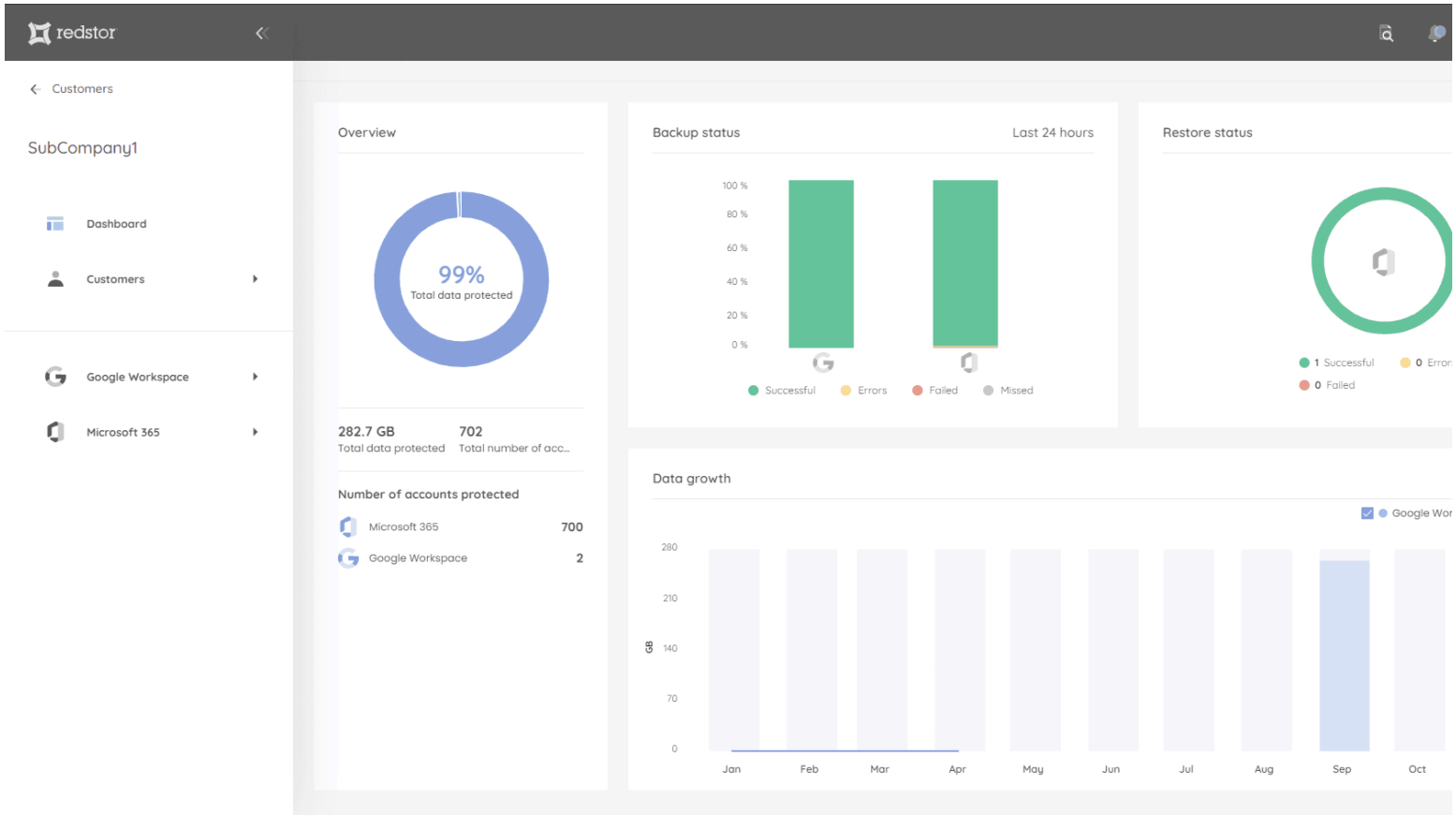
Pricing

Pricing is per seat per month with discounts for between 1,000 to 10,000 seats, and even lower rates for more than 10,000 seats.

You can choose to enable malware detection on individual services (e.g. Sharepoint, OneDrive, Teams etc). The backups of all users protected on that service will then automatically benefit from malware detection.

Take control with a single application

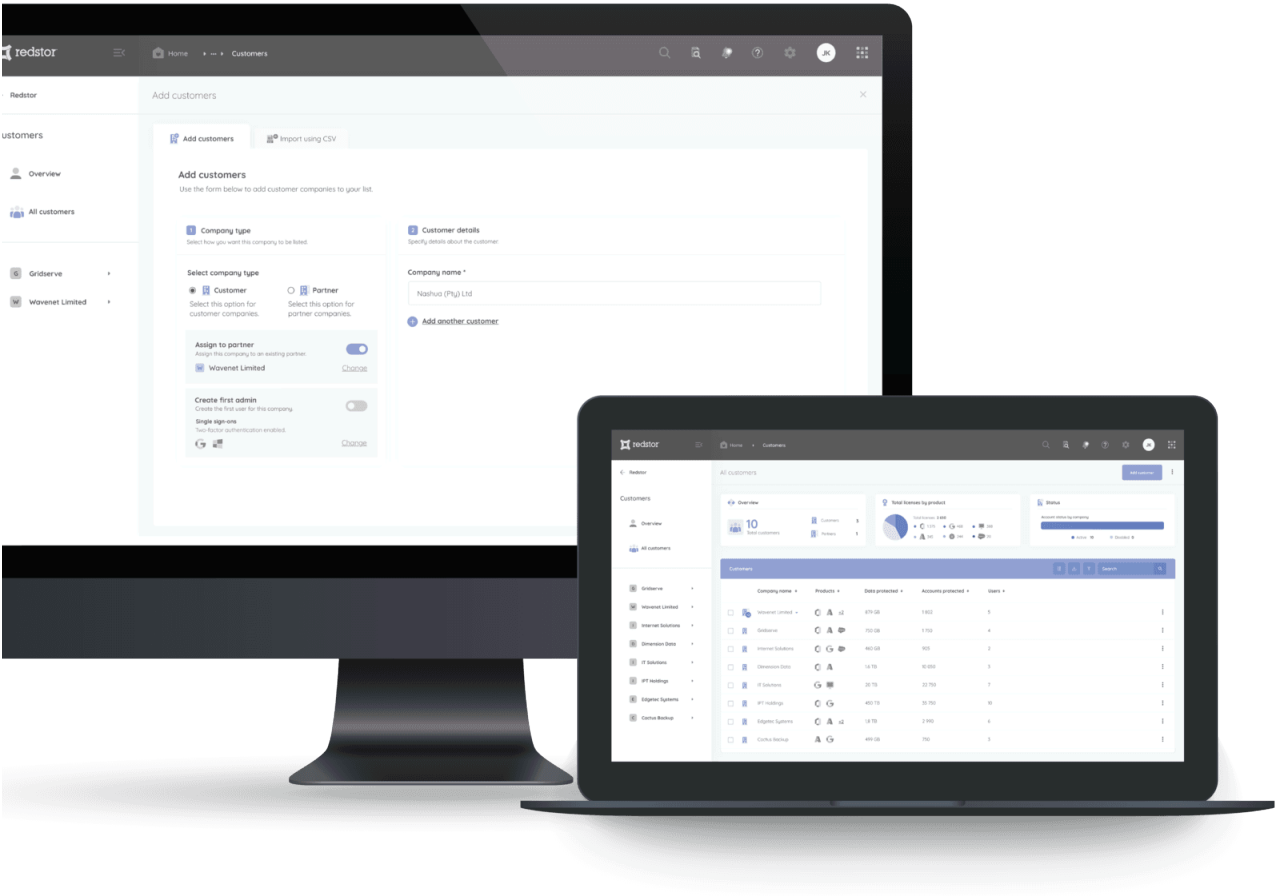
A comprehensive overview of everything you are protecting with Redstor



Drill down and take action without switching between different products and credentials.

- Capture key metrics of data in M365 and wherever else Redstor protects it
- Monitor status of backups and recoveries for protected products
- Measure growth of data in M365 and other sources Redstor protects
- Verify, remove or revert to previous versions of suspicious files detected in backups from M365 - and anywhere else in your environment

User Access Management for complete control



Redstor delivers a **whole new level of control and security** to organisations seeking greater visibility into backing up and managing their own data as part of their managed service.

The RedApp, Redstor's app for smart data management and protection, has been specifically designed for granular, configurable Identity and Access Management. This enables you to:

Set up strong security

Protect against data breaches, identity theft and forbidden access to confidential information. Prohibit the spread of compromised login credentials. Block unauthorised entry to your organisation's network. Bolster your defences against ransomware, hacking, phishing, and other cyber-attacks.

Streamline IT workloads

Update a security policy easily and comprehensively. Change all access privileges across your organisation in one action and save IT time by automating more tedious tasks e.g. password reset requests.

Comply with regulations

Quickly implement IAM best practices to meet the requirements of industry regulations e.g. Health Insurance Portability and Accountability Act and General Data Protection Regulation.

Enable secure collaboration with third parties

Achieve greater productivity by giving external parties (customers, suppliers, and visitors) access to your network without jeopardising security.

Simplify user experience

Free users from having to remember and enter numerous, complex passwords. With tighter IAM control, you can allow them to access multiple systems under Single Sign On and make use of biometrics or smart cards.

Secured by the very latest multi-factor authentication technology, UAM enables you to:

- Create and manage user identities within a single interface
- Customise and control who has access to your data
- Protect key processes with multi-layer security

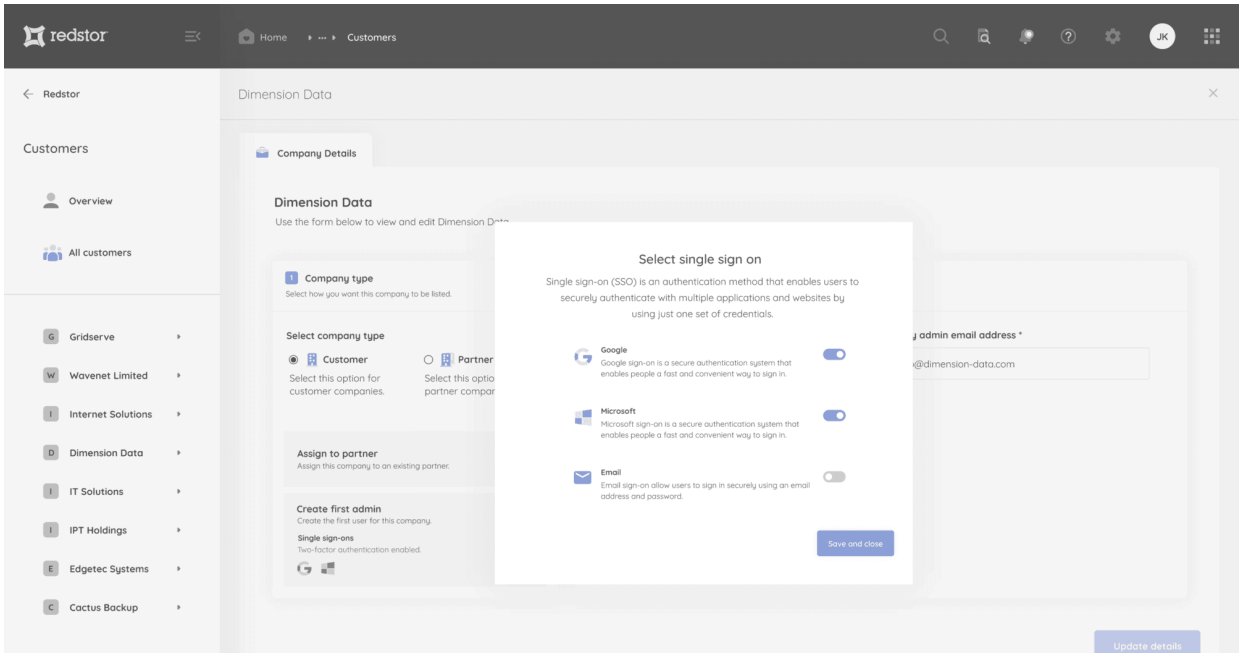
If your data is spread over many sites or multiple regions, but you wish to delegate permissions to regional offices, you can restrict and allow access accordingly.

To avoid any risk of unwanted deletions, roles can also be customised in the RedApp to remove the ability to delete accounts and data.

By delivering greater control of user accounts, Redstor's UAM avoids having to divide up an estate and assign admins with more access than is deemed secure.

Administrators can lock down specific users if an employee leaves the organisation or a login is compromised.

The introduction of mandatory 2FA using the more secure TOTP (time-based, one-time password) method also protects against malicious activity.



Granular Control

Administrators can choose from a wide variety of roles depending upon their access needs and can customise the granular permissions of each role for customers and products.

Audit trail

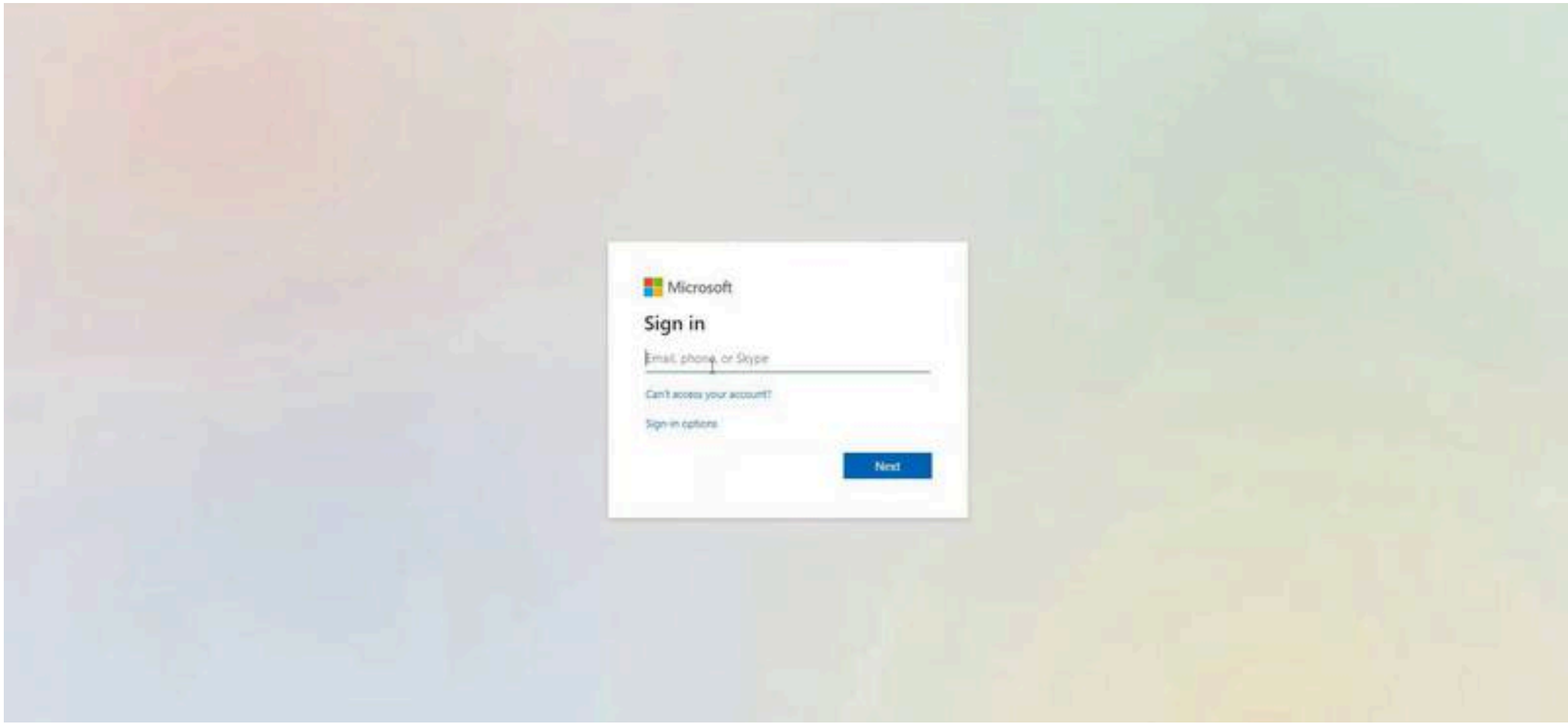
Administrators have an audit trail of who uses the platform with respective roles and actions. They can also manage users in bulk if required and obtain insight into user activity.

Designate responsibility

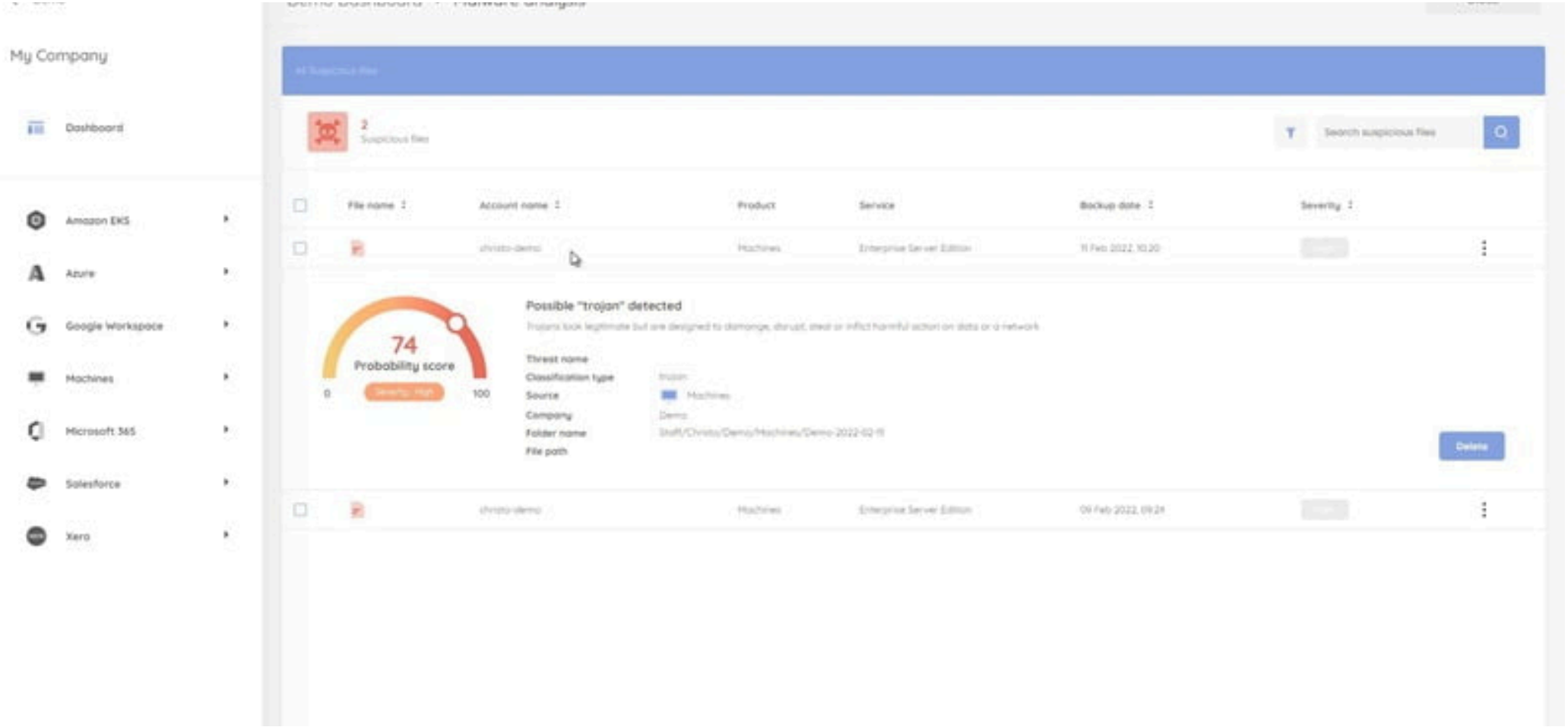
Easily enable the right person to take swift, comprehensive action in the event of human error, malicious activity or cyber-attack, while avoiding alerting an attacker or creating internal confusion.

Demo video

How to set up your Microsoft 365 environment



How to set up malware detection for backups



Thank you for reading

Protecting Microsoft 365