

FAQ

Arrow's cloud backup for Microsoft 365

Version 1.0, May 2024

What is Arrow's cloud backup for Microsoft 365?

Arrow's cloud backup for Microsoft 365 is a SaaS offering provided by Arrow ECS, offering a secure backup solution for Microsoft 365 data, including Exchange, OneDrive for Business, SharePoint, and Teams. Data is safeguarded by IBM Cloud data centres and managed through a self-service portal.

How does Arrow's cloud backup for Microsoft 365 ensure data security?

Arrow's cloud backup for Microsoft 365 employs air-gapped storage with AES256-bit encryption in transit and at rest in IBM Cloud data centres, ensuring data integrity and protection against ransomware, other malicious intent, and accidental errors.

Why is the service built in IBM Cloud?

Arrow's cloud backup for Microsoft 365 is built in IBM Cloud to deliver a cloud-to-cloud solution. In addition, IBM Cloud is utilized for higher security and compliance delivering ISO certifications along with SOC 2 and 3 certifications for data centres.

Why should I use a SaaS offering compared to building my own?

Utilizing a SaaS offering like Arrow's cloud backup for Microsoft 365 minimizes hacker incidents and provides segregation of duties. In addition, the service complies with cybersecurity regulations of NIS2, which requires organizations to have effective backup and recovery procedures in place.

How is my data stored?

IBM Cloud data centres provide access to different data centre sites worldwide. IBM Cloud data centres are minimum tier 3, which ensures 99.9999% availability 24/7. In addition, the data centres have SOC 2 and SOC 3 certifications and are EU and GDPR compliant. Data can be placed on regional sites and thereby be distributed across 3 independent IBM Cloud data centres that are spread across a metropolitan area a minimum of 10 km apart. Data can also be stored in a single site, and thus distributed in many physical storage appliances and is contained within a single data centre.

How do I access my data?

The data is accessible through the Arrow portal. The solution is managed through three portals: the management portal for administration, the self-service restore portal for user-initiated restores, and the restore portal for backup retrieval. The portal utilized Microsoft credentials for login methods.

What does Arrow's cloud backup for Microsoft 365 include in the backup?

Arrow's cloud backup for Microsoft 365 supports backup for Microsoft Exchange Online, OneDrive for Business, SharePoint Online, and Microsoft Teams.

How is pricing determined for Arrow's cloud backup for Microsoft 365?

Pricing is based on a subscription model per active Microsoft seat based on Microsoft Exchange Online, SharePoint, OneDrive for Business, and Teams accounts. The Arrow Cloud Backup for 365 for license is not required for shared, resource, and group mailboxes and external SharePoint users.

Do I pay for my deleted users and shared resources?

No. You only pay for active Microsoft 365 seats that are backed up. Deleted users are kept in the retention period.

Do I pay for my deleted users and shared resources?

No. You only pay for active Microsoft 365 seats that are backed up. Deleted users are kept in the retention period.

Is Arrow's cloud backup for Microsoft 365 compliant with industry standards and regulations?

Yes, Arrow's cloud backup for Microsoft 365 is compliant with ISO 27001, GDPR, and other industry standards, ensuring data security and regulatory compliance.

Does the solution support the right-to-be-forgotten (EU GDPR) rule?

Yes, Arrow's cloud backup for Microsoft 365 offers a feature for "right to be forgotten," allowing users to request deletion of specific data. Note, it is only possible to request a deletion of a user after the 30 days.

What happens if I accidentally or maliciously have data deleted?

Arrow's cloud backup for Microsoft 365 provides insider threat protection. The ITP feature fully protects users from malicious or accidental deletion for 30 days. This means the deletion is reversible within the 30-day period.

What happens when users are deleted in 365?

Deleted users are kept within the entire retention period selected in the backup solution. Unless you actively delete a specific user through the right-to-be-forgotten feature.

Can I delete active backup users?

No.

Can I remove deleted users from the retention period?

Yes, through the right-to-be-forgotten feature.

Where can I find support and documentation for Arrow's cloud backup for Microsoft 365?

Arrow's cloud backup Microsoft for 365 provides a knowledge base and changelog for common questions, technical errors, and updates. Additionally, support can be accessed through the management portal.

What is the true cloud-to-cloud model in Arrow's cloud backup for Microsoft 365?

The true cloud-to-cloud model ensures that data residing in Microsoft 365 is safely backed up and transferred to IBM Cloud for storage, providing data availability and restoration in case of data loss.

How does Arrow's cloud backup for Microsoft 365 handle data encryption during transit and at rest?

Data in transit is encrypted with AES256-bit encryption, and data at rest is equally encrypted, ensuring the security of data during transfer and storage.

What options are available for restoring data with Arrow's cloud backup for Microsoft 365?

Users can choose to restore data to its original location or to another location within the same tenant, ensuring flexibility and convenience in data restoration. Additional features include, but are not limited to, downloading files, folders and restoring previous Microsoft versions.

Does Arrow's cloud backup for Microsoft 365 offer item-level indexing during the restore process?

Yes, Arrow's cloud backup for Microsoft 365 provides a search tool to help locate specific data for restoration, indexing data by sender, receiver, subject, file type, file name, and date ensuring privacy and data integrity.

What can the Arrow's cloud backup for Microsoft 365 API be used for?

The Arrow's cloud backup for Microsoft 365 API is used to integrate own systems with the backup portal, making it possible to setup and close customers, download consumption reports, and much more.

How is pricing adjusted for shared, resource, and group mailboxes in Arrow's cloud backup for Microsoft 365?

Shared and resource mailboxes do not consume licenses unless assigned a Microsoft Office 365 license, ensuring fair and efficient pricing for organizational mailboxes.

What level of uptime can be expected from Arrow's cloud backup for Microsoft 365 data centres?

Arrow's cloud backup for Microsoft 365 utilizes minimum tier-3 data centres with an expected uptime of 99.999% per year, ensuring reliability and availability of backup services.

What is ITP (Insider Threat protection)?

ITP is an additional protection for end-customers' users, so if a user is deleted at the customer's end, the end-customer has 30 days to reverse this and cancel the deletion. The insider threat protection feature is created to prevent single point of failure.

Does Arrow's cloud backup for Microsoft 365 offer a web portal where end-users can restore their own personal data?

Yes, Arrow's cloud backup for Microsoft 365 offers a "Self-Service Restore" portal, allowing users to restore their own personal data. This feature needs to be activated in the management portal.

What is Role-based access control (RBAC)?

Role-based access control is a feature that allows for the segregation of access for different departments. To activate this feature, a minimum of 200 active seats is required.

Do I pay for my storage consumption in Arrow's cloud backup for Microsoft 365 solution?

In Arrow's cloud backup for Microsoft 365, end-customers do not pay for their storage consumption. In this solution, our end-customers have unlimited storage, no extra charge.

How detailed are my backup job reports?

A backup job report includes a variation of information including a list of objects backed up, if the objects have a warning during the backup, and duration of each object in the backup. In addition, a list will be provided of each object backup and the duration.

What types of backup jobs does Arrow's cloud backup for Microsoft 365 offer?

It is possible to set up both group backup jobs and entire backup jobs. Entire backup jobs include all users using MS365 services including Teams, SharePoint, OneDrive for Business, and Exchange Online. Group backup jobs allow for excluding specific users from the backup.

Is it possible to exclude users from one's backup jobs?

Yes, it is possible to exclude users directly within the end-customer portal in the Arrow's cloud backup for Microsoft 365 solution

Is it possible to invite new users to one's end-customer portal in the Arrow's cloud backup for Microsoft 365 solution?

Yes, it is possible to invite new users into a customer's portal under "User/Settings," where you also have the option to grant separate permissions to the invited users.