# Entra ID back-up and recovery solution

Why Redstor?

Entra ID is the foundation of your IT estate and if this is compromised, your entire Microsoft suite can go down. The problem with Entra ID is often users assume the built in protection is enough but that's not the case. Microsoft offers some security features but not long-term data recovery for Entra ID, with data and configurations only being stored for a maximum of 90 days. Without additional protection in place, your data is vulnerable, putting you at risk to cyberattacks and insider threats.

Redstor have addressed the critical protection gaps in Entra ID, developing an Entra ID backup and recovery solution that goes beyond simple data backup. The solution not only ensures that your data is stored safely but that it can be fully restored in seconds if the worst were to happen.
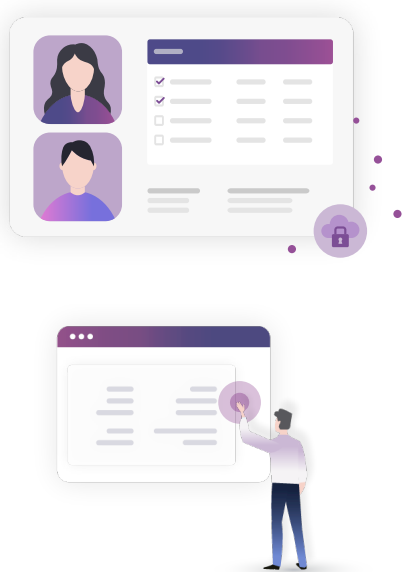
Challenges Redstor solves

Data is at the centre of your IT. If your Entra ID is compromised, whether through cyberattacks, system failures, or human error, it will cause significant disruption to your business. Even Microsoft recommends using third-party backup services to avoid the above scenarios.

Redstor's backup and recovery solution secures your Entra ID data, including user attributes, groups, and roles, with reliable off-site backups that allow for rapid recovery without the threat of data loss. You can monitor changes over time, compare configurations, and restore settings in seconds. Whether human error or corruption, Redstor's solution guarantees full recovery of user attributes, licenses, and relationships, helping maintain workflow continuity.

With the ability to recover quickly and address access issues effectively, you can minimise downtime and remain compliant with global regulations.

Benefits of Redstor Entra ID backup

Recover data, attributes, and relationships for full workflow continuity

Secures against credential stuffing, zero-day vulnerabilities, and phishing threats

Restore all user attributes and licenses instantly

Re-establish memberships, roles, and management links

Reduce downtime, recovering essential data in seconds

Maintain compliance with extended data retention

Reverse unauthorised changes to preserve critical configurations