cloudcapsule

Security & Compliance

Empowering MSPs to elevate Microsoft 365 security — safely, privately, and in compliance.

SOC 2® Type I Attested

Independently audited against the AICPA Trust Services Criteria for Security, Availability, and Confidentiality. Type II scheduled to complete summer 2025.

Continuous monitoring with automated evidence collection ensures controls stay effective between audits.

Latest report available under Mutual NDA—contact support@cloudcapsule.io.

Our Permissions in the Tenant

The app is composed primarily of read-only permissions. While we maintain a model of least-privileged access, there are certain API limitations that require us to have write access we outline specifically here:

- **Policy.ReadWrite.AuthenticationMethod** -- this is currently the least possible permission to be able to retrieve data regarding the authentication flow. There is no read only method for this data.
- **RoleManagement.ReadWrite.Directory** -- Used for Teams and Exchange because Microsoft doesn't have Graph APIs to retrieve policy data which requires write permissions for the role assignment. The solution uses an app consent model to then retrieve data through PowerShell: App-only authentication in Exchange Online PowerShell and Security & Compliance PowerShell

  NOTE This permission can be removed off the Enterprise app after the initial consent.
- **Reports.ReadWrite.All** -- Used to anonymize report data if it is not already enabled.

You can find the full list of app permissions we use on our Privacy and FAQ page.

Data Handling & Privacy

Select your Data Center upon sign up — we support US and EU datacenters where customer data resides.

Role based access control is enforced on database with row-level access control. All Data is encrypted at rest and in transit.

The data is only retained for a rolling one year and can be deleted on demand by revoking access in CloudCapsule

For more info, please see our Privacy Policy: https://www.cloudcapsule.io/privacy