Security & Compliance

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

SOC 2® Type II

CloudCapsule is committed to your privacy and security. As part of that commitment, we have completed our SOC 2 Type II examination and have been independently audited against AICPA Trust Services Criteria for Security, Availability, and Confidentiality. Continuous monitoring with automated evidence collection ensures controls stay effective between audits.

AUDIT SCOPE

Security, Availability & Confidentiality

MONITORING

Continuous with automated evidence collection

REPORT ACCESS

Available under mutual NDA

Data Handling & Privacy

CloudCapsule is designed to keep your data under your control. You choose where your data resides at sign up, with support for US, EU and AUS data centers.

Data is retained on a rolling one-year basis and can be deleted on demand by revoking access. Access to stored data is governed by role-based controls, and all data is ecrypted at rest and in transit. Periodic Vulnerability scanning is performed on the database. The data is not aggregated or used to train a larger model.

For full details, see our Privacy Policy at cloudcapsule.io/privacy.

DATA CENTERS

US data is hosted in GCP: East US
EU data is hosted in GCP: europe-west1
AU data is hosted in GCP: australia-southeast1

DATA RETENTION

Data is retained for a rolling one year and can be deleted on demand by revoking access in CloudCapsule.

ACCESS CONTROL

Role-based access control is enforced on the database with row-level access control. All access is gated by MFA at restricted locations

DATA ENCRYPTION

All data is encrypted at rest and in transit.

Microsoft App Registrations

CloudCapsule uses two separate app registrations in Microsoft, depending on your plan and the level of access you choose to grant within a given tenant.

Neither application requests more access than is needed for its specific function, and CloudCapsule never automatically pushes changes to a tenant.

Every remediation and policy action must be explicitly initiated by a user within the app. All actions are recorded in a full activity log, giving you complete visibility into what was changed, by whom, and when.

CLOUDCAPSULE (Analyze)

The core assessment and visibility application. Analyze operates on a read-only model wherever possible. The small number of write permissions it holds are used exclusively to manage CloudCapsule's own access, including the ability for you to revoke permissions or remove the app from a tenant entirely. Analyze does not modify tenant configuration.

CLOUDCAPSULE-MANAGE (Manage)

A separate app registration that adds remediation and policy management on top of the base Analyze permissions. Manage follows the same least-permissive philosophy, requesting only the additional write permissions required to take action on your behalf. You remain in control of what is deployed and when. Consenting to Manage replaces the need to separately consent to Analyze.

CloudCapsule (Analyze) Permissions

Analyze is a fundamentally read-only application. The vast majority of its permissions are scoped to reading configuration data, audit logs, security signals, and policy information across Microsoft 365 services. This allows CloudCapsule to perform a thorough security assessment without modifying anything in the tenant.

Read Permissions

Analyze holds a broad set of read-only Microsoft Graph permissions covering identity, device management (Intune), Conditional Access policies, security alerts, SharePoint and Teams configuration, audit logs, and user authentication methods.

It also includes read access to Windows Defender ATP for threat and vulnerability data, and Exchange Online via Exchange.ManageAsApp, which is used in read-only mode to retrieve Exchange policies where Microsoft does not provide a dedicated read-only API.

Permission	Type	Purpose
AuditLog.Read.All	Read	Read all audit log data for sign-in information and suspicious user activity.
DelegatedAdminRelationship.Read.All	Read	Read Delegated Admin relationships with customers. Used to pull in all tenants under an MSP partner tenant.
DeviceManagementApps.Read.All	Read	Read Microsoft Intune apps.
DeviceManagementConfiguration.Read.All	Read	Read Microsoft Intune device configuration and policies.
DeviceManagementManagedDevices.Read.All	Read	Read Microsoft Intune devices.
DeviceManagementScripts.Read.All	Read	Read Microsoft Intune scripts. Used to assess deployed Intune script configurations.
DeviceManagementServiceConfig.Read.All	Read	Purpose: Read Microsoft Intune configuration. email Purpose: View users' email address. Used for SSO.
GroupMember.Read.All	Read	Read all group memberships.
IdentityRiskEvent.Read.All	Reed	Read all identity risk event information.
MailboxSettings.Read	Read	Read all user mailbox settings.
offline_access	Read	Maintain access to data you have given it access to. Used for SSO.
openid	Read	Sign users in. Used for SSO.
Organization.Read.All	Read	Read organization information.
OrganizationalBranding.Read.All	Read	Read organizational branding information.
OrgSettings-AppsAndServices.Read.All	Read	Read organization-wide app and service settings. Used to assess org-level app configurations.
Policy.Read.All	Read	Read your organization's policies such as Conditional Access.
profile	Read	View users' basic profile. Used for SSO.
Reports.Read.All	Read	Read all usage reports.
SecurityAlert.Read.All	Read	Read all security alerts.

Permission	Type	Purpose
SecurityEvents.Read.All	Read	Read your organization's security events.
SharePointTenantSettings.Read.All	Read	Read SharePoint and OneDrive tenant settings.
Sites.Read.All	Read	Read all site collections. Used to pull in details about SharePoint sites.
Team.ReadBasic.All	Read	Get a list of all teams.
TeamSettings.Read.All	Read	Read all teams' settings.
User.Read	Read	Sign in and read user profile. Used for SSO.
User.Read.All	Read	Read all users' full profiles.
UserAuthenticationMethod.Read.All	Read	Read all users' authentication methods.

Office 365 Exchange Online	Type	Purpose
Exchange.ManageAsApp	Read	Manage Exchange as Application. Used to retrieve Exchange policies. Read-only calls are made in the Analyze SKU.

Windows Defender ATP	Type	Purpose
Alert.Read.All	Read	Read all alerts.
Machine.Read.All	Read	Read all machine profiles.
Score.Read.All	Read	Read Threat and Vulnerability Management score.
SecurityRecommendation.Read.All	Read	Read Threat and Vulnerability Management security recommendations.
Software.Read.All	Read	Read Threat and Vulnerability Management software information.
Vulnerability.Read.All	Read	Read Threat and Vulnerability Management vulnerability information.

Analyze Write Permissions

Analyze holds four write-scoped permissions. In each case, the write scope is either the minimum permission level available from Microsoft to accomplish the task, or is scoped specifically to CloudCapsule's own app registration.

None are used to make unsolicited changes to your tenant:

Application.ReadWrite.All

Used to read all Enterprise Applications and, if needed, to programmatically remove CloudCapsule from the tenant, giving administrators a clean, complete removal path.

Policy.ReadWrite.AuthenticationMethod

The minimum permission available from Microsoft to retrieve authentication flow data. No read-only equivalent exists 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 retrieve data through PowerShell: App-only authentication in Exchange Online PowerShell and Security & Compliance PowerShell.

This permission can be removed from the Enterprise app after the initial consent.

Reports.ReadWrite.All

Used to anonymize report data if it is not already enabled.

CloudCapsule-Manage (Manage) Permissions

CloudCapsule-Manage includes all read permissions from the base Analyze registration, plus a set of elevated and new write permissions required to support remediation and policy management workflows. These additional permissions are only present when the Manage app registration is deployed.

The guiding principle is the same as Analyze: permissions are scoped as narrowly as possible to the actions being taken, and CloudCapsule never pushes changes automatically. Every remediation action must be explicitly triggered by a user in the app and is captured in the activity log.

Write Permissions

Remediation is the core purpose of Manage. To disable a stale device, update a Conditional Access policy, modify group memberships, or revoke compromised user sessions, Microsoft requires corresponding write permissions at the policy or directory level. The permissions below represent the minimum set needed to cover those operations across the Microsoft 365 surface area.

Permission	Status	Purpose
Device.ReadWrite.All	New	Read and write devices. Used to take remediation actions on managed devices such as disabling stale devices.
DeviceManagementConfiguration.ReadWrite.All	Elevated	Read and write Microsoft Intune device configuration and policies. Required to apply and update device configuration policies as part of remediation.
DeviceManagementServiceConfig.ReadWrite.All	Elevated	Read and write Microsoft Intune service configuration. Required to manage Intune service-level settings during remediation.
Directory.ReadWrite.All	Elevated	Read and write directory data. Required to apply directory-level changes such as group and user modifications as part of remediation actions.
Domain.ReadWrite.All	New	Read and write domains. Used to support domain-level configuration changes during remediation.
Group.ReadWrite.All	New	Read and write all groups. Used to create, modify, or remove groups as part of policy or remediation workflows.
GroupMember.ReadWrite.All	Elevated	Read and write all group memberships. Used to manage group membership changes during remediation.
GroupSettings.ReadWrite.All	New	Read and write all group settings. Used to apply group-level configuration changes.
OrgSettings-AppsAndServices.ReadWrite.All	Elevated	Read and write organization-wide app and service settings. Used to apply changes to org-level app configurations during remediation.

Permission	Status	Purpose
Policy.ReadWrite.ApplicationConfiguration	New	Read and write your organization's application configuration policies. Used to manage app-level policy settings.
Policy.ReadWrite.Authorization	New	Read and write your organization's authorization policy. Used to manage authorization policy settings during remediation.
Policy.ReadWrite.ConditionalAccess	New	Read and write your organization's Conditional Access policies. Used to create or modify Conditional Access policies as part of policy management workflows.
Policy.ReadWrite.ConsentRequest	New	Read and write your organization's consent request policy. Used to manage consent request policy settings.
Policy.ReadWrite.DeviceConfiguration	New	Read and write your organization's device configuration policies. Used to apply device policy changes during remediation.
Policy.ReadWrite.PermissionGrant	New	Manage consent and permission grant policies. Used to control permission grant policies as part of remediation.
User.ReadWrite.All	Elevated	Read and write all users' full profiles. Used to apply user-level changes during remediation workflows.
User.EnableDisableAccount.All	New	Enable and disable user accounts. Used to take action on compromised or non-compliant user accounts as part of remediation.
User.RevokeSessions.All	New	Revoke all sign-in sessions for a user. Used to immediately terminate active sessions for compromised accounts.

CloudCapsule Dedication to Security & Privacy

Security and privacy are our top priority, and the data privacy of a tenant is of utmost importance to our team.

Our SOC 2 Type II attestation is available for review with a mutually signed NDA that we're happy to provide.

Our team is also available to answer any questions or concerns about security or privacy when using CloudCapsule. Simply contact us at cloudcapsule.io/contact or support@cloudcapsule.io.