

SOTERIA CLOUD MICROSOFT 365 PROTECTION

How to protect collaboration data beyond native retention

Independent protection for Microsoft 365 data, identity risk, and collaboration workflows.

SaaS data protection

Acronis Microsoft 365 backup and security capabilities

STARTING POINT

Native retention is not a complete backup strategy, and Microsoft 365 risk spans data loss, account compromise, and configuration drift.

For organizations that rely on Exchange Online, OneDrive, SharePoint, Teams, and Entra ID every day.

Acronis Powered by Acronis



Microsoft 365 protection and risk dashboard



STEP-BY-STEP PATH

Move from scope to validated service without losing the buyer's objective.

These are the decisions and checks Soteria Cloud uses to turn Acronis Microsoft 365 backup and security capabilities capability into a practical service outcome.

01 Inventory the tenant	Confirm Exchange, OneDrive, SharePoint, Teams, priority users, and retention needs.
02 Protect data	Apply backup and security policies that match department risk and recovery requirements.
03 Validate restores	Test mailbox, file, and collaboration-data recovery before relying on the service.
04 Review posture	Check identity, endpoint, and collaboration risk signals alongside backup status.
05 Report clearly	Show protected users, recovery tests, open gaps, and next actions in one service review.

KEY OUTCOME

Protect collaboration data beyond native retention. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Microsoft 365 backup and security capabilities

PROTECTION FOCUS

SaaS data protection

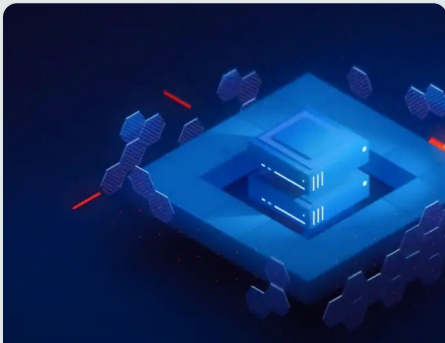
SERVICE OWNER

Soteria Cloud

SCREEN CUES

Use the console views to confirm progress and explain the service clearly.

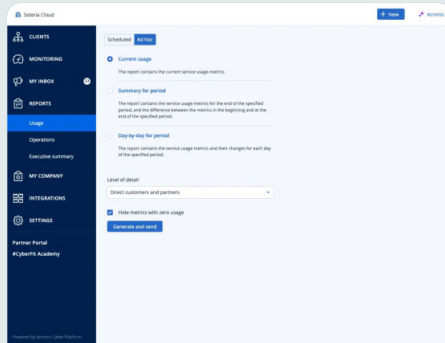
Independent protection for Microsoft 365 data, identity risk, and collaboration workflows.
The screens below help buyers understand where scope, controls, and reporting evidence come from.



Review Microsoft 365 posture



Explain collaboration data protection



Confirm usage and backup reporting

SaaS data protection scope has named owners and clear exclusions.

Required administrator access and customer approvals are confirmed.

Policies match the workload, user, data, and recovery risk profile.

Reports show coverage, exceptions, and action owners in plain language.

Soteria Cloud review rhythm is agreed for changes, incidents, and renewals.

BUYER CHECKPOINT

Before expanding the service, confirm that the buyer can see what is protected, what is excluded, what needs action, and how Soteria Cloud reports improvement.

OPERATIONAL FIT

Clear coverage, visible progress, and support when it matters.

The result is a protection approach customers can understand, fund, and measure through recurring Soteria Cloud reviews.

01

Protect collaboration data beyond native retention

02

Recover mail, files, and user data more confidently

03

Strengthen Microsoft 365 security posture conversations

Controls to put in place

- Exchange Online backup
- OneDrive and SharePoint backup
- Teams data protection where supported
- Granular restore
- Security posture assessment
- Identity and endpoint integration options

Strong fit scenarios

- Microsoft 365 backup replacement
- SaaS recovery assurance
- M365 security posture improvement

SOTERIA CLOUD

Protection should be operational, not theoretical.

Soteria Cloud brings Acronis-powered capability together with onboarding, support, and recurring review.