

SOTERIA CLOUD MICROSOFT 365 PROTECTION

How to protect Microsoft 365 beyond native retention

Add independent protection for Exchange Online, OneDrive, SharePoint, Teams data, and identity-related risk.

SaaS data protection

Acronis Microsoft 365 backup and security capabilities

Total Data Protection

BEST FIT

Microsoft 365 customers, MSPs, and resellers that need better SaaS recovery confidence.

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

Acronis Powered by Acronis



Microsoft 365 protection and risk dashboard

DECIDE FIRST

Make the business choices clear before rollout.

Useful protection starts with the workloads, users, data, recovery targets, and risk decisions that shape the service.

01

Which Microsoft 365 data is business-critical

02

How retention differs from recoverable backup

03

Which users and sites need priority protection

04

How granular restores will be requested

05

How account compromise affects data recovery

06

What SaaS recovery evidence leadership needs

Readiness checklist

- Map Exchange, OneDrive, SharePoint, and Teams priorities
- Identify executives, finance users, and shared sites
- Set backup frequency and retention requirements
- Confirm restore approval and request paths
- Review security posture and backup coverage together

Gaps to close

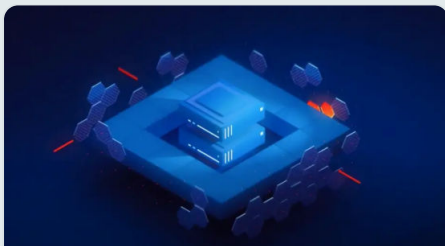
- Assuming native retention equals backup
- Shared sites missing clear ownership
- Granular restore expectations undefined
- Security posture and data protection reviewed separately

PRACTICAL PATH

Turn the requirement into an operating model.

Soteria Cloud surrounds Acronis technology with assessment, policy design, onboarding, review, and support ownership.

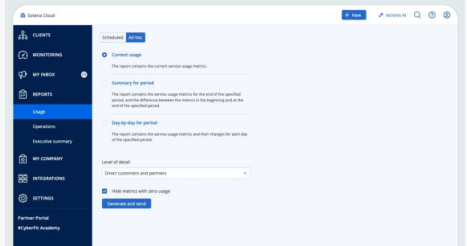
MAP COLLABORATION DATA	Identify the mailboxes, drives, sites, and teams where loss would disrupt work.
SET PROTECTION RULES	Assign backup, retention, and recovery expectations by user, department, and site.
PREPARE RESTORES	Clarify how mailbox, file, folder, and site restores are requested and approved.
REVIEW IDENTITY RISK	Connect backup planning to account compromise, access changes, and security posture findings.
MEASURE COVERAGE	Use Soteria Cloud reporting to show protected data, restore readiness, and remaining gaps.



Review Microsoft 365 posture



Explain collaboration data protection



Confirm usage and backup reporting

SOTERIA CLOUD OFFER

Soteria Cloud Microsoft 365 Protection

POWERED BY

Acronis Microsoft 365 backup and security capabilities

SERVICE FIT

Best for buyers that rely on Microsoft 365 every day and need recoverability beyond platform retention.

OUTCOME

Protect collaboration data beyond native retention. The plan is stronger when controls, recovery expectations, and reporting evidence are connected from the start.



EVIDENCE

Measure the things that prove protection is working.

Good cyber resilience is visible. Buyers need coverage, exceptions, recovery confidence, and service actions they can understand.

01

Protected mailboxes and sites

02

Priority users covered

03

Restore requests completed

04

Retention exceptions reviewed

05

Security posture actions closed

Business outcomes

- Protect collaboration data beyond native retention
- Recover mail, files, and user data more confidently
- Strengthen Microsoft 365 security posture conversations

Strong fit scenarios

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

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Independent protection for Microsoft 365 data, identity risk, and collaboration workflows. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.