

SOTERIA CLOUD SECURE FILE SERVICES

How to govern secure file collaboration

Enable team, customer, and mobile file access while keeping control over business data movement.

File sync, share, and access

Acronis Cyber Files, Files Advanced, and Files Connect

Total Data Protection

BEST FIT

Organizations that need secure file workflows for remote work, customer sharing, and controlled access.

File sharing spreads data quickly. Without the right controls, productivity can become a visibility and compliance gap.

Acronis **Powered by Acronis**



File collaboration and SaaS data protection view

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 file workflows need secure sharing

02

Who owns access approval

03

How external sharing is governed

04

Which mobile or remote users need access

05

How file activity is reviewed

06

Where file recovery fits into the workflow

Readiness checklist

- Map departments, shared folders, and external workflows
- Set access groups and sharing expectations
- Define controls for mobile and remote access
- Confirm recovery expectations for key file areas
- Review file activity and access changes

Gaps to close

- External sharing handled through unmanaged channels
- File access rights never reviewed after role changes
- Mobile access treated as convenience only
- File recovery disconnected from collaboration risk

PRACTICAL PATH

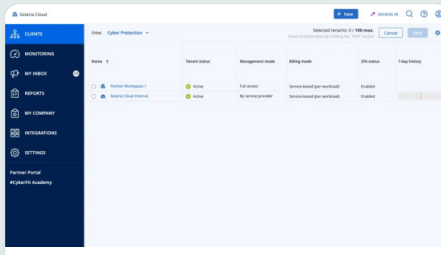
Turn the requirement into an operating model.

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

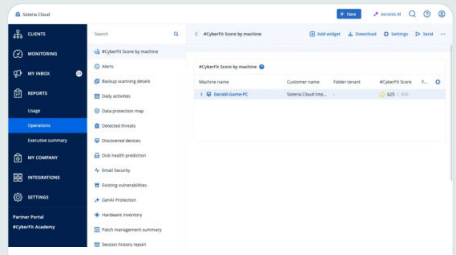
MAP WORKFLOWS	Identify the files, teams, external parties, and devices involved in everyday collaboration.
SET ACCESS RULES	Apply user, group, sharing, and mobile access controls that match business need.
ENABLE COLLABORATION	Roll out secure file access for priority workflows without opening uncontrolled sharing paths.
CONNECT RECOVERY	Align file service governance with backup and restore expectations for critical file areas.
REVIEW ACTIVITY	Track access changes, sharing activity, exceptions, and recovery needs in service reviews.



File collaboration and SaaS data protection view



Confirm services and scope



Review reporting evidence

SOTERIA CLOUD OFFER

Soteria Cloud Secure File Services

POWERED BY

Acronis Cyber Files, Files Advanced, and Files Connect

SERVICE FIT

Best for buyers that need secure collaboration with control, visibility, and continuity.

OUTCOME

Enable secure file access and collaboration. 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

Controlled file areas onboarded

02

External sharing reviewed

03

Mobile access governed

04

Access exceptions closed

05

Recovery coverage confirmed

Business outcomes

- Enable secure file access and collaboration
- Improve control over business file sharing
- Support recovery and continuity for file workflows

Strong fit scenarios

- Secure remote work
- Controlled customer and team file sharing
- Modernization of legacy file access

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Secure file collaboration for teams that need control, access, and continuity. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.