

SOTERIA CLOUD SECURE FILE SERVICES

How to enable secure file access and collaboration

Secure file collaboration for teams that need control, access, and continuity.

File sync, share, and access

Acronis Cyber Files, Files Advanced, and Files Connect

STARTING POINT

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

For organizations that need secure file access and sharing without losing governance over business data.

Acronis Powered by Acronis



File collaboration and SaaS data protection view



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 Cyber Files, Files Advanced, and Files Connect capability into a practical service outcome.

01 Confirm objectives	Agree the business outcome, buyer priority, environment scope, and service owner.
02 Prepare access	Confirm the tenant, administrators, required integrations, and any customer approvals.
03 Apply the service	Enable the relevant Acronis-powered capability through the Soteria Cloud operating model.
04 Validate results	Check coverage, reports, alerts, exceptions, and user impact before broad rollout.
05 Review and improve	Use recurring service reviews to keep the protection model current and measurable.

KEY OUTCOME

Enable secure file access and collaboration.
The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Cyber Files, Files Advanced, and Files Connect

PROTECTION FOCUS

File sync, share, and access

SERVICE OWNER

Soteria Cloud

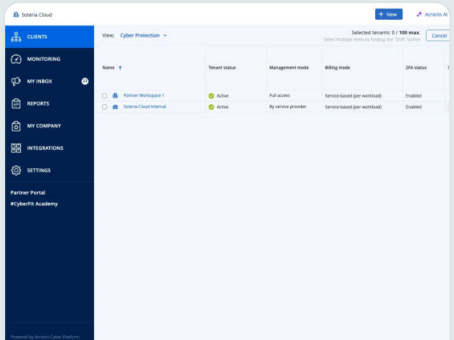
SCREEN CUES

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

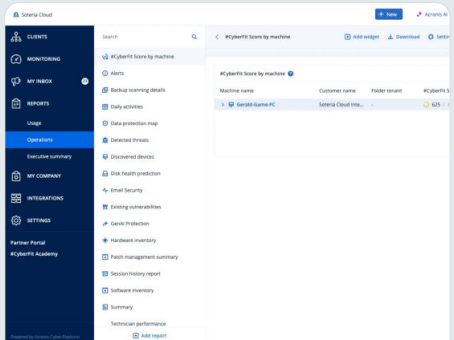
Secure file collaboration for teams that need control, access, and continuity. The screens below help buyers understand where scope, controls, and reporting evidence come from.



File collaboration and SaaS data protection view



Confirm services and scope



Review reporting evidence

File sync, share, and access 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

Enable secure file access and collaboration

02

Improve control over business file sharing

03

Support recovery and continuity for file workflows

Controls to put in place

- Cloud file sync and share
- Mobile and remote file access
- User and group controls
- File activity visibility
- Mac and Windows file service support
- Policy-based governance

Strong fit scenarios

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

SOTERIA CLOUD

Protection should be operational, not theoretical.

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