

SOTERIA CLOUD CYBER BACKUP SCS

How to protect sensitive workloads with a controlled backup platform

Secure, controlled backup for environments that need stricter deployment and operational boundaries.

Secure backup platform

Acronis Cyber Backup SCS

STARTING POINT

Some environments require backup control, deployment discipline, and security posture that goes beyond standard cloud SaaS.

For organizations with sensitive workloads, stronger control requirements, or self-managed backup architecture needs.

Acronis Powered by Acronis

WORKSTATIONS



Windows



Mac

Secure backup workload coverage 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 Backup SCS capability into a practical service outcome.

01 Confirm scope	List servers, endpoints, SaaS data, NAS, hosting workloads, and business owners that need protection.
02 Set recovery targets	Agree retention, recovery point expectations, recovery time expectations, and approval owners.
03 Apply policies	Group workloads, apply backup plans, enable required storage, and check that the first jobs complete.
04 Test recovery	Run file, folder, and system recovery checks before the service is treated as production-ready.
05 Review evidence	Use reports to show coverage, failures, exceptions, and restore-test outcomes.

KEY OUTCOME

Protect sensitive workloads with a controlled backup platform. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Cyber Backup SCS

PROTECTION FOCUS

Secure backup platform

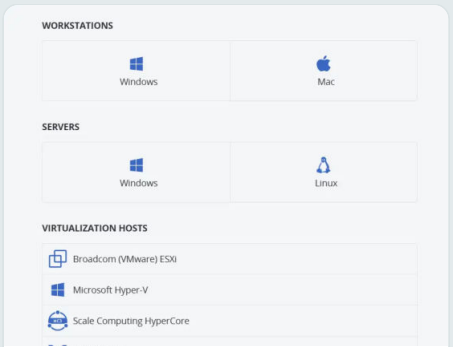
SERVICE OWNER

Soteria Cloud

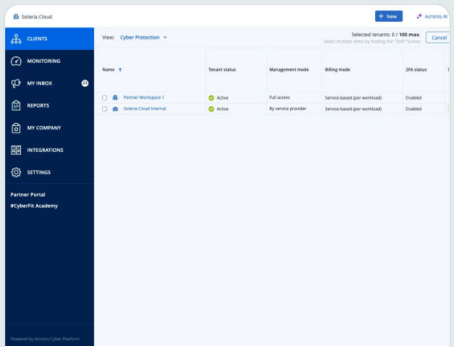
SCREEN CUES

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

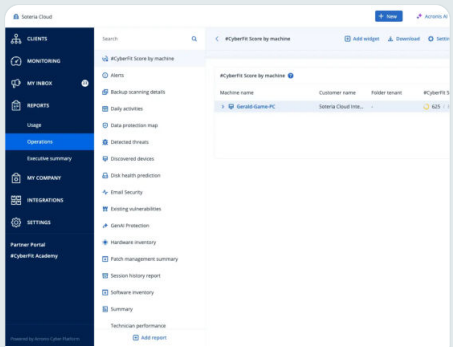
Secure, controlled backup for environments that need stricter deployment and operational boundaries. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Secure backup workload coverage view



Confirm services and scope



Review reporting evidence

Secure backup platform 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 sensitive workloads with a controlled backup platform

02

Support stricter operational and compliance requirements

03

Keep recovery strategy aligned to security posture

Controls to put in place

- Secure backup management
- Controlled deployment model
- Workload backup and recovery
- Administrative policy controls
- Evaluation and onboarding guidance
- Operational reporting

Strong fit scenarios

- Sensitive workload backup
- Controlled backup architecture
- Security-led backup modernization

SOTERIA CLOUD

Protection should be operational, not theoretical.

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