

SOTERIA CLOUD CYBER INFRASTRUCTURE

How to support protected storage growth

Resilient storage infrastructure for backup, file, and service provider workloads.

Storage and infrastructure

Acronis Cyber Infrastructure

STARTING POINT

Protection services depend on storage that is resilient, scalable, and operationally manageable.

For service providers and organizations that need scalable storage infrastructure under a cyber resilience strategy.

Acronis Powered by Acronis

 Amazon Web Services

 Microsoft

Reports



+ Add widget Download Settings Send ...

CyberFit Score distribution



Vulnerable machines



Secured 64

Activities for 7 days

100



Infrastructure reporting and protection visibility 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 Infrastructure 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

Support protected storage growth. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Cyber Infrastructure

PROTECTION FOCUS

Storage and infrastructure

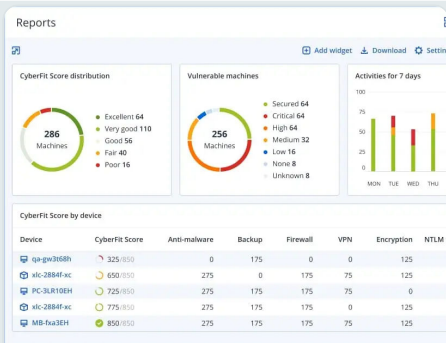
SERVICE OWNER

Soteria Cloud

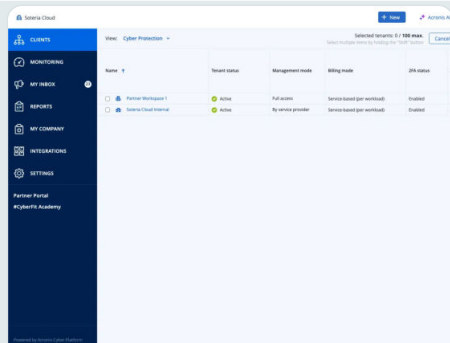
SCREEN CUES

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

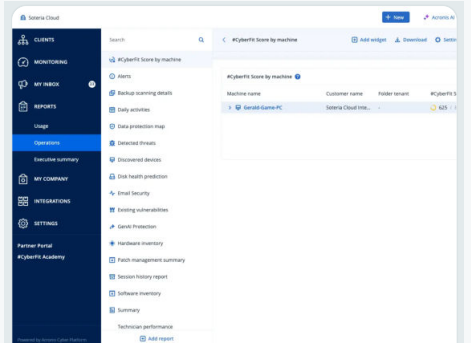
Resilient storage infrastructure for backup, file, and service provider workloads. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Infrastructure reporting and protection visibility view



Confirm services and scope



Review reporting evidence

Storage and infrastructure 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

Support protected storage growth

02

Improve resilience for backup and file services

03

Create infrastructure that supports recurring cyber resilience services

Controls to put in place

- Software-defined storage
- Backup gateway options
- S3-compatible storage use cases
- Storage appliance support
- Multi-node infrastructure design
- Operational monitoring

Strong fit scenarios

- Backup storage platform
- Service provider storage layer
- Private or hybrid cyber resilience infrastructure

SOTERIA CLOUD

Protection should be operational, not theoretical.

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