

SOTERIA CLOUD CYBER INFRASTRUCTURE

How to plan resilient storage for protection services

Create storage infrastructure that supports backup growth, service resilience, and recoverable data.

Storage and infrastructure

Acronis Cyber Infrastructure

Total Data Protection

BEST FIT

Service providers and organizations building storage for backup, file, and cyber resilience workloads.

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

Acronis Powered by Acronis



Amazon Web Services



Microsoft

Reports



+ Add widget ↓ Download ⚙ Settings ✉ Send ...

CyberFit Score distribution

Vulnerable machines

Activities for 7 days

100

● Secured 64

Infrastructure reporting and protection visibility 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 services the storage layer must support

02

How capacity growth will be forecast

03

What resilience level is required

04

Where backup gateway or object storage fits

05

How operational monitoring is handled

06

Who owns lifecycle and expansion planning

Readiness checklist

- Estimate protected data, retention, and growth
- Define resilience requirements by service
- Plan node, network, and storage architecture
- Confirm integration with backup and file services
- Review capacity, health, and lifecycle regularly

Gaps to close

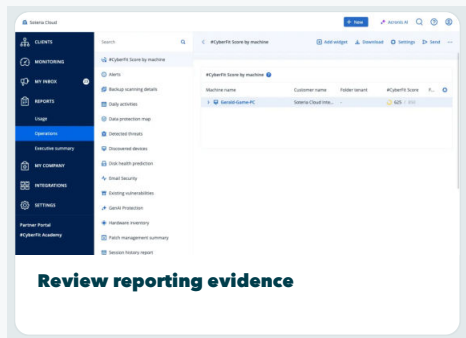
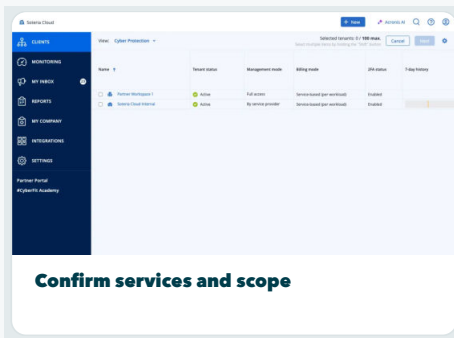
- Storage sized only for current data volume
- Resilience assumptions not matched to service promises
- Growth planning disconnected from customer onboarding
- Monitoring focused on capacity but not recoverability

PRACTICAL PATH

Turn the requirement into an operating model.

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

MODEL DEMAND	Estimate backup, file, object, retention, and customer growth across the expected service life.
DESIGN RESILIENCE	Plan storage architecture, nodes, networking, and redundancy around the service impact of failure.
CONNECT SERVICES	Align storage with backup gateways, file workloads, and cyber resilience requirements.
MONITOR OPERATIONS	Track capacity, performance, health, alerts, and lifecycle risks through Soteria Cloud reviews.
PLAN EXPANSION	Set triggers for capacity growth, hardware refresh, and service expansion before pressure arrives.



SOTERIA CLOUD OFFER
Soteria Cloud Cyber Infrastructure

POWERED BY
Acronis Cyber Infrastructure

SERVICE FIT
Best for buyers that need resilient infrastructure beneath backup, file, and protection services.

OUTCOME

Support protected storage growth. 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

Capacity forecast accuracy

02

Storage health trend

03

Resilience targets met

04

Expansion triggers defined

05

Service integration verified

Business outcomes

- Support protected storage growth
- Improve resilience for backup and file services
- Create infrastructure that supports recurring cyber resilience services

Strong fit scenarios

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

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Resilient storage infrastructure for backup, file, and service provider workloads. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.