

SOTERIA CLOUD CYBER BACKUP SCS

How to design secure backup for controlled environments

Support stricter control, sensitive workloads, and disciplined backup operations with a secure protection model.

Secure backup platform

Acronis Cyber Backup SCS

Total Data Protection

BEST FIT

Organizations with sensitive data, controlled architecture needs, or stricter operational requirements.

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

Acronis Powered by Acronis

WORKSTATIONS



Windows



Mac

Secure backup workload coverage 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 workloads require a controlled backup model

02

Who administers backup and restore activity

03

How access and policy changes are governed

04

Where backup data is stored and protected

05

How restore testing evidence is retained

06

Which compliance expectations influence design

Readiness checklist

- Identify controlled workloads and data sensitivity
- Define administrative roles and access boundaries
- Set backup, retention, and restore policies
- Confirm storage and security expectations
- Review restore evidence and operational changes

Gaps to close

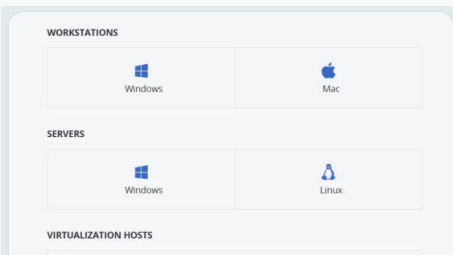
- Administrative access broader than business need
- Sensitive workloads protected with generic policies
- Restore evidence missing from compliance reviews
- Backup architecture not matched to control requirements

PRACTICAL PATH

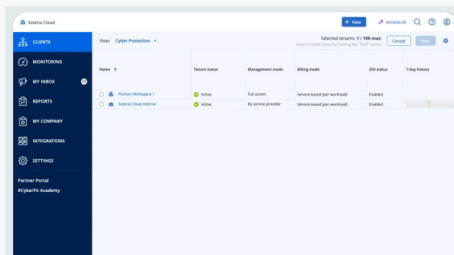
Turn the requirement into an operating model.

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

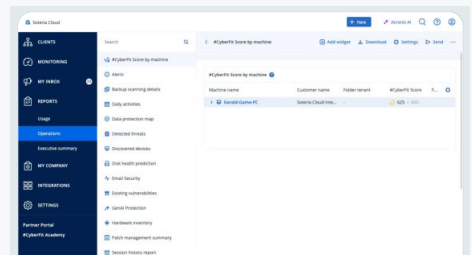
CLASSIFY SCOPE	Identify the workloads, data types, and control requirements that make standard backup insufficient.
DESIGN CONTROLS	Define administrative roles, policy authority, storage expectations, and restore approval paths.
APPLY PROTECTION	Roll out secure backup policies for priority workloads with clear monitoring and exception handling.
VALIDATE RECOVERY	Test restores and retain evidence that recovery works inside the controlled operating model.
REVIEW CHANGE	Track policy, access, storage, and restore changes through recurring Soteria Cloud reviews.



Secure backup workload coverage view



Confirm services and scope



Review reporting evidence

SOTERIA CLOUD OFFER
Soteria Cloud Cyber Backup SCS

POWERED BY
Acronis Cyber Backup SCS

SERVICE FIT
Best for buyers that need secure backup discipline for sensitive or tightly controlled environments.

OUTCOME

Protect sensitive workloads with a controlled backup platform. 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 workloads protected

02

Administrative access reviewed

03

Restore evidence retained

04

Policy exceptions approved

05

Security changes tracked

Business outcomes

- Protect sensitive workloads with a controlled backup platform
- Support stricter operational and compliance requirements
- Keep recovery strategy aligned to security posture

Strong fit scenarios

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

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Secure, controlled backup for environments that need stricter deployment and operational boundaries. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.