

SOTERIA CLOUD ADVANCED MANAGEMENT

How to make endpoint operations measurable

Bring endpoint visibility, patch awareness, inventory, and policy hygiene into a managed protection rhythm.

RMM and endpoint operations

Acronis Advanced Management

Total Data Protection

BEST FIT

MSPs and IT teams that need operational control across endpoints without losing the resilience context.

A protected device that is unmanaged, unpatched, or invisible can still become a business risk.

Acronis Powered by Acronis

Mode



☒ Observation mode ⓘ

☐ Allow all

RMM workflow and endpoint operations 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 endpoint groups need monitoring

02

What health signals require action

03

How patch and software status is reviewed

04

Which alerts matter to service teams

05

How inventory supports security and backup decisions

06

What monthly operations evidence matters

Readiness checklist

- Inventory endpoints, operating systems, and key software
- Group devices by business role and risk
- Set monitoring and alert thresholds
- Review patch, protection, and backup status together
- Track open actions through recurring reviews

Gaps to close

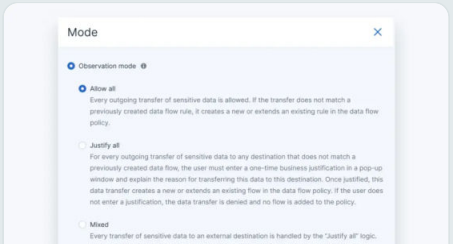
- Protected devices that are unmanaged or invisible
- Patch status reviewed outside security risk
- Inventory missing from backup and endpoint planning
- Too many alerts with no service priority

PRACTICAL PATH

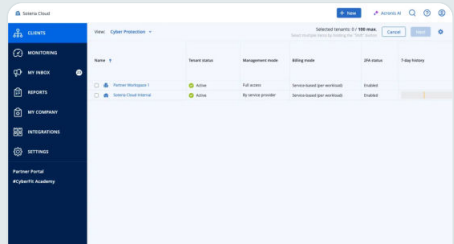
Turn the requirement into an operating model.

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

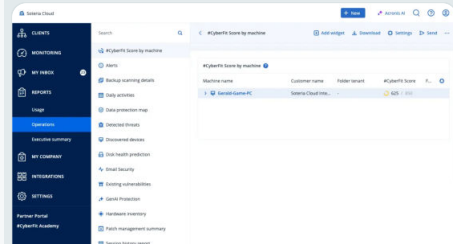
BUILD VISIBILITY	Create a usable view of endpoints, owners, locations, software, and operational status.
SET ACTION RULES	Define which health, patch, inventory, and policy signals need service-team action.
ALIGN POLICIES	Connect endpoint management settings to backup, security, remote support, and reporting needs.
CLOSE HYGIENE GAPS	Prioritize unmanaged devices, missing patches, repeated alerts, and outdated software.
REPORT OPERATIONS	Show endpoint health, protection posture, action closure, and trend improvements.



RMM workflow and endpoint operations view



Confirm services and scope



Review reporting evidence

SOTERIA CLOUD OFFER
Soteria Cloud Advanced Management

POWERED BY
Acronis Advanced Management

SERVICE FIT
Best for buyers that want endpoint operations connected to cyber resilience and measurable service improvement.

OUTCOME

Improve endpoint operational visibility. 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

Endpoint inventory accuracy

02

Patch or software actions closed

03

Policy compliance trend

04

Unmanaged devices found

05

Alert noise reduced

Business outcomes

- Improve endpoint operational visibility
- Make protection policies easier to maintain
- Connect management and security into one service package

Strong fit scenarios

- Managed endpoint operations
- Backup and security policy hygiene
- Customer environment standardization

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Operational management that supports protection, patching, and endpoint reliability. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.