



SOTERIA CLOUD ADVANCED MANAGEMENT

How to improve endpoint operational visibility

Operational management that supports protection, patching, and endpoint reliability.

RMM and endpoint operations

Acronis Advanced Management

STARTING POINT

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

For MSPs and IT teams that need endpoint visibility and management inside the same cyber resilience conversation.

Acronis Powered by Acronis

Mode

☒ Observation mode ⓘ☐ Allow all

RMM workflow and endpoint operations 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 Advanced Management 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

Improve endpoint operational visibility. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Advanced Management

PROTECTION FOCUS

RMM and endpoint operations

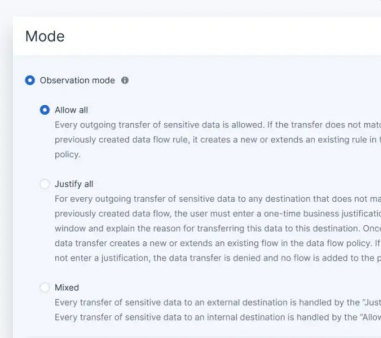
SERVICE OWNER

Soteria Cloud

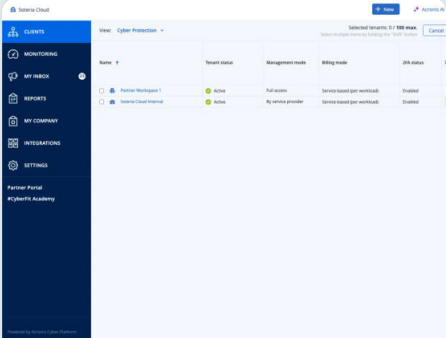
SCREEN CUES

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

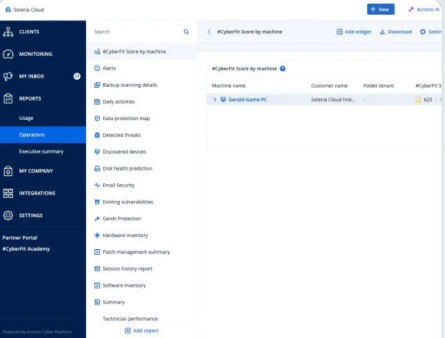
Operational management that supports protection, patching, and endpoint reliability. The screens below help buyers understand where scope, controls, and reporting evidence come from.



RMM workflow and endpoint operations view



Confirm services and scope



Review reporting evidence

RMM and endpoint operations 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

Improve endpoint operational visibility

02

Make protection policies easier to maintain

03

Connect management and security into one service package

Controls to put in place

- Remote monitoring and management
- Patch and software management options
- Hardware and software inventory
- Policy-based operations
- Alerting and reporting
- Service workflow support

Strong fit scenarios

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

SOTERIA CLOUD

Protection should be operational, not theoretical.

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