OPERATIONAL HOW-TO

ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to keep audit-ready evidence for security and recovery activity

Create a repeatable evidence trail for incidents, policy changes, restore tests, admin actions, and service review decisions.

Buyer-ready | Operational evidence | Total Data Protection

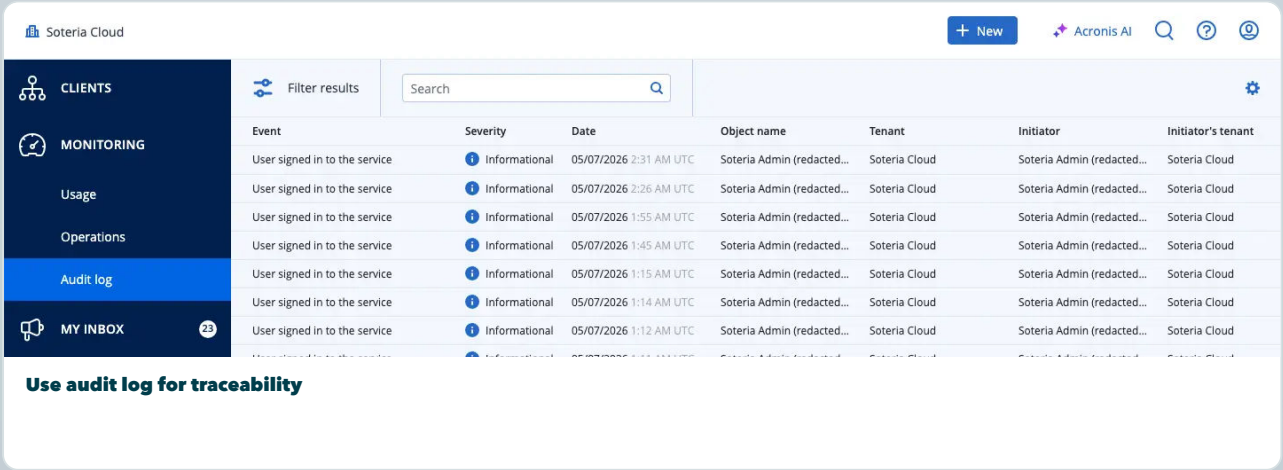
BEST FIT

Compliance teams, MSPs, resellers, security owners, customer executives, and IT leaders under audit or insurance pressure.

The buyer needs to prove what was protected, what happened, who acted, and which recovery or security actions were completed.

Powered by Acronis

Soteria Cloud delivered



Use audit log for traceability

BUYER NEED

Make the commercial requirement operational.

Incident response and recovery expectations increasingly emphasize governance, communication, traceability, and completed documentation.

BUYER TRIGGER

The buyer needs to prove what was protected, what happened, who acted, and which recovery or security actions were completed.

PRODUCTS INVOLVED

Cyber Protect Cloud, Advanced Backup, EDR, DLP, RMM, Microsoft 365 Protection, Email Security

CONSOLE SURFACES

Audit log, Reports, Executive summary, Users, Roles and permissions

01

Evidence should be gathered as the service operates, not recreated after pressure arrives.

02

Keep the audit story simple: scope, event, action, owner, outcome, and next control.

03

Restore evidence and admin access evidence are both part of resilience.

04

Use reports for trends and audit log for traceability.

05

Do not bury buyer decisions in ticket chatter; summarize accepted risk and approved actions.

06

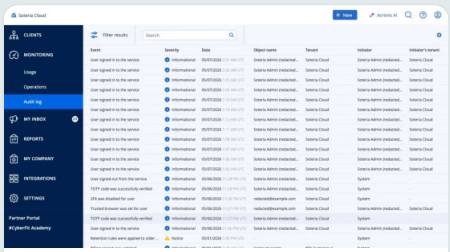
Review evidence monthly so gaps are found before renewal, audit, or claim events.

PRACTICAL PATH

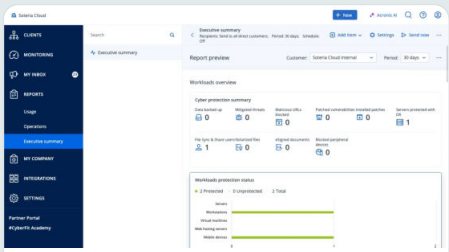
Turn the offer into a repeatable service motion.

Soteria Cloud positions Acronis technology around buyer outcomes, support ownership, recurring review, and evidence that can be explained without product jargon.

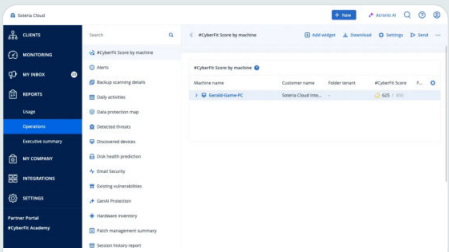
DEFINE EVIDENCE CATEGORIES	Separate evidence for backup status, restore tests, incidents, policy changes, admin access, DLP exceptions, patch actions, and service decisions.
COLLECT SYSTEM RECORDS	Use Audit log, Reports, Monitoring, and Executive summary to collect traceable system evidence for each category.
ADD BUSINESS CONTEXT	Attach owner, business impact, decision, accepted risk, remediation action, and target date so evidence is buyer-readable.
REVIEW COMPLETENESS	Check whether evidence answers who, what, when, why, result, and next step for the activity being reviewed.
PACKAGE FOR REVIEWS	Use recurring service reviews to confirm evidence, close gaps, and prepare for compliance, insurance, or executive requests.



Use audit log for traceability



Summarize evidence for buyers



Support evidence with operational reports

BUYER OUTCOME

Create a repeatable evidence trail for incidents, policy changes, restore tests, admin actions, and service review decisions.

EVIDENCE

Show the proof buyers expect to see.

Soteria Cloud service reviews give buyers visible status, known exceptions, agreed actions, and a reviewable record of protection activity.

Evidence to keep

- Audit activity record
- Restore and backup evidence
- Incident response summary
- Access and role change evidence
- Approved risk and remediation actions

Measures to review

- Evidence categories covered
- Audit events reviewed
- Restore evidence current
- Access changes traceable
- Open evidence gaps closed

01 **Evidence categories covered**

02 **Audit events reviewed**

03 **Restore evidence current**

04 **Audit activity record**

05 **Restore and backup evidence**

06 **Incident response summary**