



ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to reduce endpoint exposure with patch and RMM evidence

Use Soteria Cloud to connect endpoint inventory, vulnerability visibility, patch actions, backup safety, and buyer-ready reporting.

Buyer-ready

Operational evidence

Total Data Protection

BEST FIT

MSPs, resellers, IT managers, and endpoint operations teams reducing exposure across customer devices.

The buyer wants fewer exploitable endpoints and a clearer way to see which patch or vulnerability actions are still open.

Acronis

Powered by Acronis



Soteria Cloud delivered

Mode

☒ Observation mode ⓘ☐ Allow all

Every outgoing transfer of sensitive data is allowed. If the transfer does not match a previously created data flow rule, it creates a new or extends an existing rule in the data flow policy.

Use RMM workflow for endpoint operations

BUYER NEED

Make the commercial requirement operational.

Endpoint resilience is now a combined operations issue: asset visibility, patch timing, safe rollback, security status, and reporting.

BUYER TRIGGER

The buyer wants fewer exploitable endpoints and a clearer way to see which patch or vulnerability actions are still open.

PRODUCTS INVOLVED

RMM, Advanced Backup, EDR, Cyber Protect Cloud

CONSOLE SURFACES

Monitoring, RMM dashboards, Reports, Audit log, Executive summary

01

Patch management should be tied to backup status so failed updates have a recovery route.

02

Group devices by business impact before setting patch windows.

03

Show exposure by customer, device group, and criticality instead of a raw patch count.

04

Use maintenance windows and rollback expectations to reduce buyer fear of disruption.

05

Connect repeated patch failures to support tickets or lifecycle replacement recommendations.

06

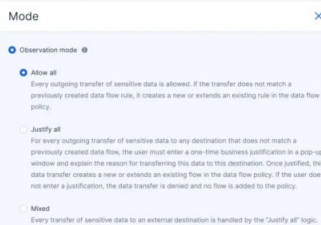
Report closed exposure and open exceptions every month.

PRACTICAL PATH

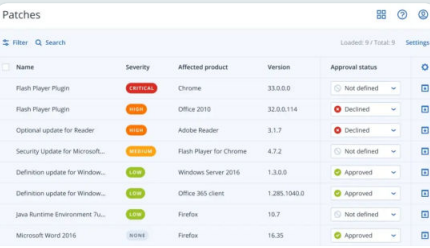
Turn the offer into a repeatable service motion.

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

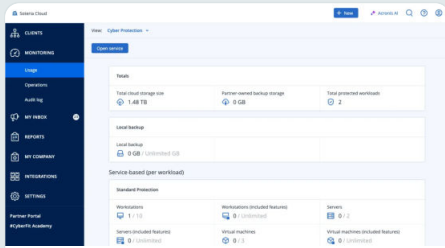
BUILD DEVICE GROUPS	Group endpoints and servers by role, risk, maintenance window, business owner, and backup requirement.
REVIEW EXPOSURE	Use RMM and monitoring views to identify missing patches, vulnerable applications, unmanaged devices, and repeated failures.
CONFIRM ROLLBACK READINESS	Check backup coverage or pre-patch safety options before applying changes to higher-risk systems.
APPLY AND VALIDATE	Deploy patches by group, validate endpoint health, confirm reboot outcomes, and isolate failed updates for remediation.
REPORT EXPOSURE TREND	Show patched systems, remaining critical exposure, failed updates, exceptions, and lifecycle recommendations.



Use RMM workflow for endpoint operations



Explain patch automation and risk scoring



Track endpoint and protection status

BUYER OUTCOME

Use Soteria Cloud to connect endpoint inventory, vulnerability visibility, patch actions, backup safety, and buyer-ready reporting.

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

- Device inventory
- Patch and vulnerability status
- Backup readiness before patching
- Patch deployment result
- Open exposure report

Measures to review

- Critical exposure reduced
- Patch success rate
- Failed patches remediated
- Protected devices before patch
- Exceptions approved

01

Critical exposure reduced

02

Patch success rate

03

Failed patches remediated

04

Device inventory

05

Patch and vulnerability status

06

Backup readiness before patching

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Acronis-powered protection packaged with Soteria Cloud onboarding, service ownership, reporting, and recurring buyer-ready review.