HOW-TO

SOTERIA CLOUD ADVANCED SECURITY + EDR

How to detect and respond to endpoint threats faster

Endpoint protection and detection connected to recovery, not isolated from it.

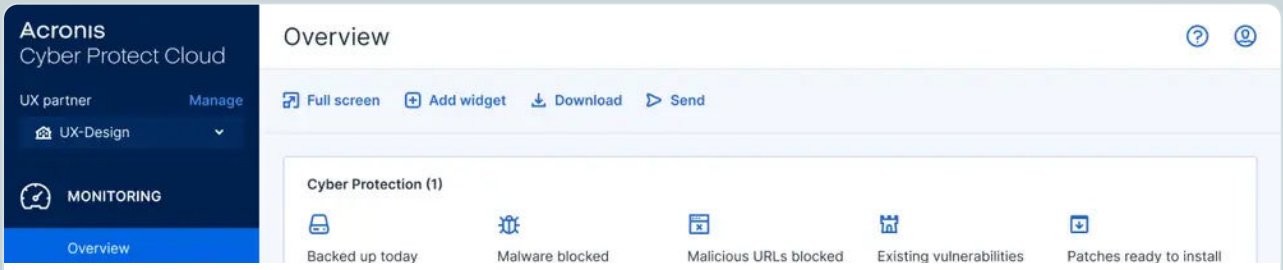
Endpoint security | Acronis Advanced Security and EDR

STARTING POINT

Security incidents become business incidents when detection, containment, and recovery are not connected.

For teams that need modern malware protection, behavioral detection, and response capability without adding another disconnected console.

Acronis **Powered by Acronis**



Endpoint detection and response overview

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 Security and EDR capability into a practical service outcome.

01 Group endpoints	Separate executives, finance users, servers, remote staff, and other high-risk devices.
02 Apply protection	Enable prevention, behavioral detection, ransomware protection, and EDR settings by group.
03 Connect response	Define when to isolate, investigate, run remediation, recover from backup, or escalate.
04 Review incidents	Use the incident chain, timeline, and response actions to understand what happened.
05 Report improvement	Track blocked threats, unresolved events, repeat-risk devices, and recovery readiness.

KEY OUTCOME

Detect and respond to endpoint threats faster. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Advanced Security and EDR

PROTECTION FOCUS

Endpoint security

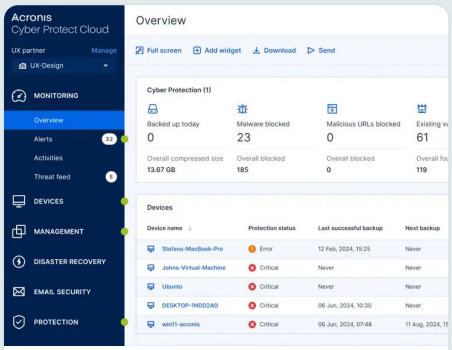
SERVICE OWNER

Soteria Cloud

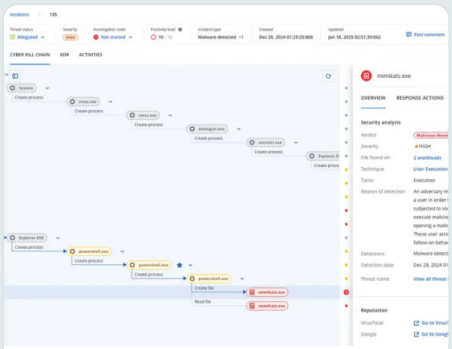
SCREEN CUES

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

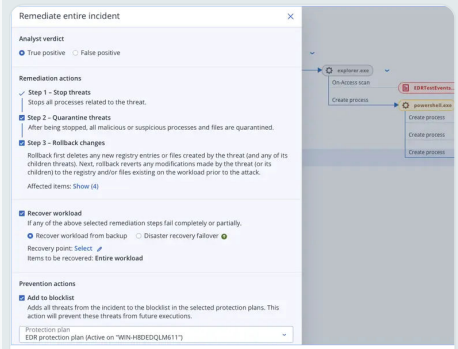
Endpoint protection and detection connected to recovery, not isolated from it. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Review endpoint risk and active incidents



Follow the attack sequence



Prepare response actions

Endpoint security 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

Detect and respond to endpoint threats faster

02

Reduce ransomware impact through protection and recovery alignment

03

Give customers a clearer security service story

Controls to put in place

- Anti-malware and exploit prevention
- Behavioral and ransomware protection
- Endpoint detection and response options
- Investigation and response workflows
- Policy management
- Security reporting

Strong fit scenarios

- Endpoint security modernization
- Ransomware risk reduction
- Managed security add-on for backup customers

SOTERIA CLOUD

Protection should be operational, not theoretical.

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