SOTERIA CLOUD ADVANCED SECURITY + EDR

How to reduce endpoint risk with EDR and recovery alignment

Treat endpoint security as a resilience workflow that connects prevention, detection, response, and recovery.

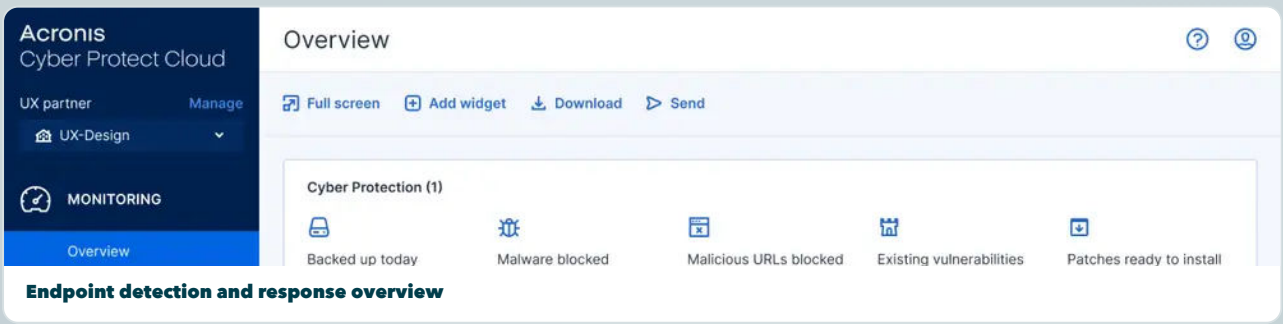
Endpoint security | Acronis Advanced Security and EDR | Total Data Protection

BEST FIT

Security-minded buyers that need stronger endpoint protection without separating response from recoverability.

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

Acronis **Powered by Acronis**



Endpoint detection and response overview

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 carry the highest business risk

02
Which events need containment or escalation

03
How response actions affect backup and recovery

04
What visibility executives need during incidents

05
How exceptions are approved and reviewed

06
Which users need added protection or coaching

Readiness checklist

- Group endpoints by role, location, and risk
- Set prevention and detection policies by group
- Confirm backup coverage for high-risk endpoints
- Define containment and escalation expectations
- Review security events with recovery readiness

Gaps to close

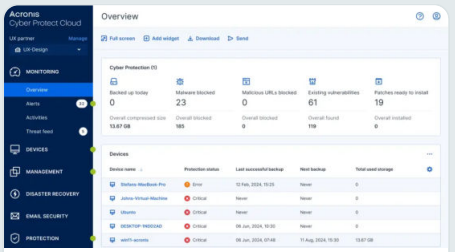
- Endpoint tools running separately from backup strategy
- Alerts that do not trigger business response decisions
- High-value endpoints with weak recovery coverage
- No review of repeated risky behavior

PRACTICAL PATH

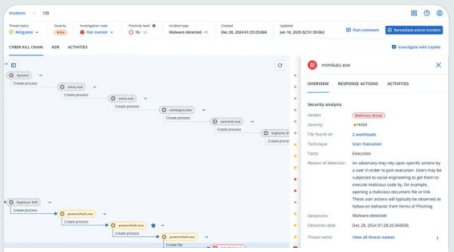
Turn the requirement into an operating model.

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

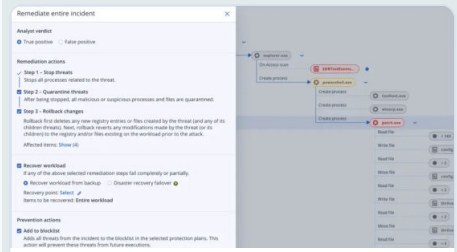
PROFILE ENDPOINT RISK	Identify executives, finance users, remote staff, servers, and devices with sensitive data.
SET CONTROLS	Apply anti-malware, exploit prevention, ransomware defense, and EDR settings aligned to each group.
CONNECT RECOVERY	Confirm protected backups for systems where containment or rebuild may be required.
TUNE RESPONSE	Agree when Soteria Cloud response actions move from monitoring to containment and escalation.
REVIEW EVIDENCE	Track blocked threats, suspicious behavior, unresolved events, and recovery readiness together.



Review endpoint risk and active incidents



Follow the attack sequence



Prepare response actions

SOTERIA CLOUD OFFER

Soteria Cloud Advanced Security + EDR

POWERED BY

Acronis Advanced Security and EDR

SERVICE FIT

Best for buyers that want endpoint security decisions connected to recoverable systems and practical response.

OUTCOME

Detect and respond to endpoint threats faster. 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 protection coverage**

02 **High-risk devices backed up**

03 **Events reviewed and closed**

04 **Policy exceptions approved**

05 **Repeat-risk users identified**

Business outcomes

- Detect and respond to endpoint threats faster
- Reduce ransomware impact through protection and recovery alignment
- Give customers a clearer security service story

Strong fit scenarios

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

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Endpoint protection and detection connected to recovery, not isolated from it. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.