SOTERIA CLOUD MANAGED DETECTION & RESPONSE

How to move from unmanaged alerts to managed response

Give suspicious endpoint activity a clearer operating path with monitoring, escalation, response, and recovery context.

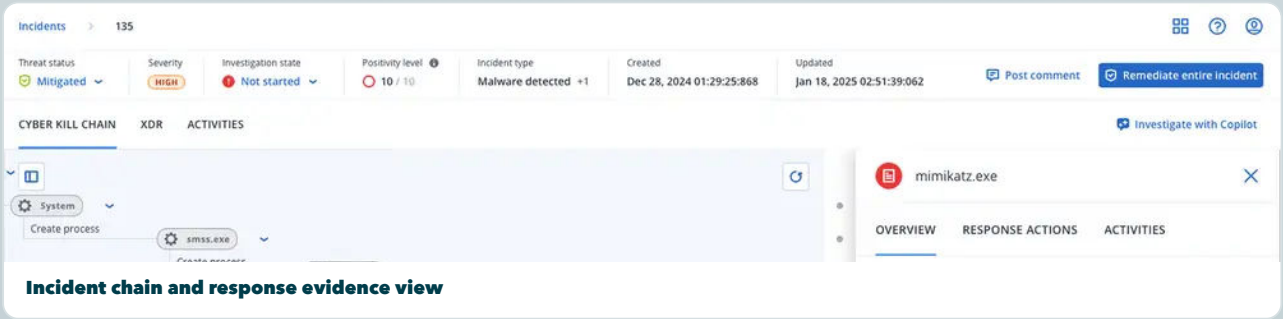
Managed security | Acronis MDR and EDR capabilities | Total Data Protection

BEST FIT

Organizations that need stronger security confidence without building a full security operations team.

Alerts have little value if nobody has the time, context, or process to act on them.

Acronis Powered by Acronis



Incident chain and response evidence view

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 alerts require immediate escalation

02
Who receives business-impact notifications

03
Which response actions are pre-approved

04
How containment decisions are captured

05
When recovery actions become part of response

06
What monthly security evidence matters

Readiness checklist

- Define alert severity and escalation contacts
- Confirm endpoint and workload coverage
- Agree response permissions and notification rules
- Connect incident handling to recovery planning
- Review monthly trends and improvement actions

Gaps to close

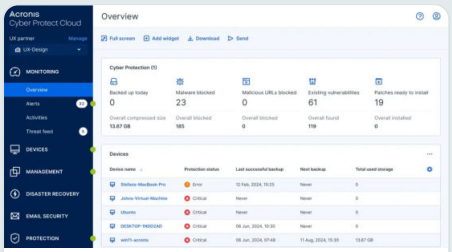
- Alerts seen after business impact is already visible
- No agreed route from detection to containment
- Response decisions made without recovery context
- Security posture reports missing business actions

PRACTICAL PATH

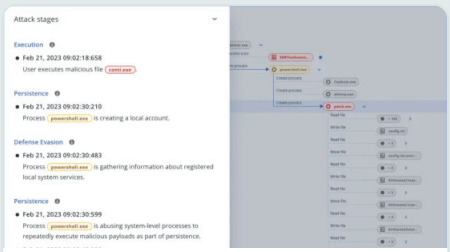
Turn the requirement into an operating model.

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

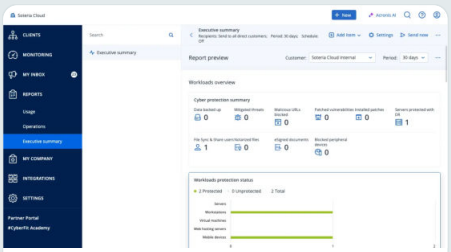
SET ESCALATION RULES	Agree what Soteria Cloud escalates, when, and to whom based on risk and business impact.
TUNE VISIBILITY	Make sure endpoint telemetry, protection status, and backup coverage can be reviewed together.
PREPARE ACTIONS	Pre-approve containment, isolation, investigation, and recovery consultation where appropriate.
REVIEW INCIDENTS	Turn incidents and near misses into policy improvements and user-risk actions.
REPORT OUTCOMES	Show alert trends, response activity, coverage, and actions in a consistent executive rhythm.



Review detection status



Check incident evidence



Report action and outcome

SOTERIA CLOUD OFFER

Soteria Cloud Managed Detection & Response

POWERED BY

Acronis MDR and EDR capabilities

SERVICE FIT

Best for buyers that need response capability, security visibility, and business-level escalation without extra complexity.

OUTCOME

Improve visibility into suspicious activity. 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 **Alert coverage by endpoint group**

02 **Escalations acknowledged**

03 **Incidents contained or closed**

04 **Policy improvements applied**

05 **Recovery gaps identified**

Business outcomes

- Improve visibility into suspicious activity
- Create a clearer response path for endpoint incidents
- Connect response decisions to backup and recovery options

Strong fit scenarios

- Managed endpoint security
- Ransomware response planning
- Security service uplift for existing backup customers

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Detection, response, and recovery guidance for organizations that cannot watch everything themselves. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.