HOW-TO

SOTERIA CLOUD MANAGED DETECTION & RESPONSE

How to improve visibility into suspicious activity

Detection, response, and recovery guidance for organizations that cannot watch everything themselves.

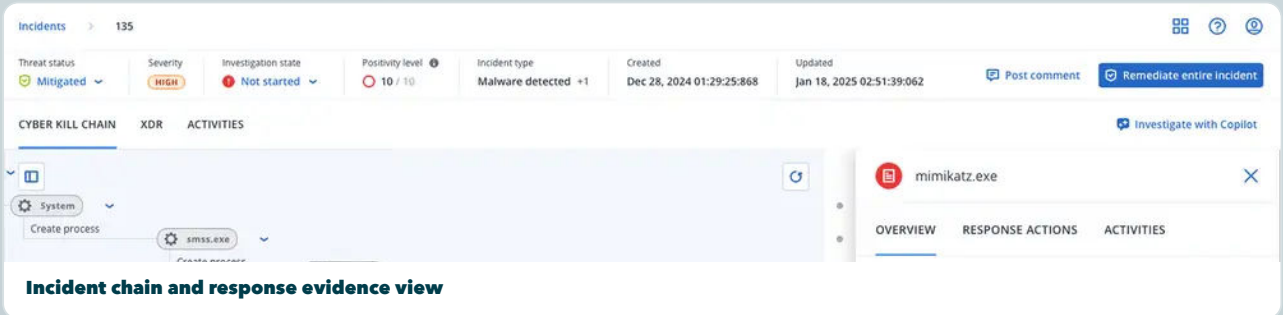
Managed security **Acronis MDR and EDR capabilities**

STARTING POINT

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

For customers that need stronger security monitoring and incident response confidence without building a full security operations team.

Acronis **Powered by Acronis**



Incident chain and response evidence view

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 MDR and EDR capabilities 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

Improve visibility into suspicious activity. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis MDR and EDR capabilities

PROTECTION FOCUS

Managed security

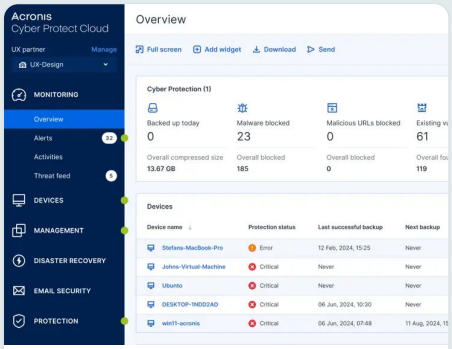
SERVICE OWNER

Soteria Cloud

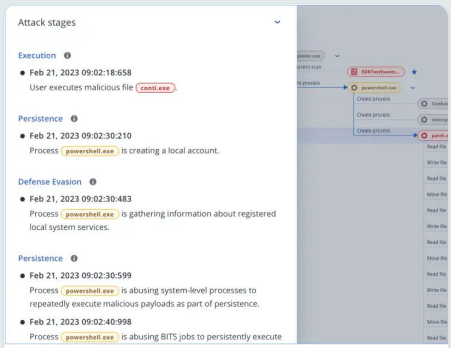
SCREEN CUES

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

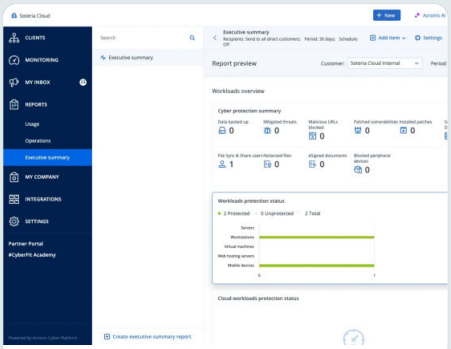
Detection, response, and recovery guidance for organizations that cannot watch everything themselves. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Review detection status



Check incident evidence



Report action and outcome

Managed 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

Improve visibility into suspicious activity

02

Create a clearer response path for endpoint incidents

03

Connect response decisions to backup and recovery options

Controls to put in place

- Threat detection workflows
- Endpoint response actions
- Security event review
- Incident escalation support
- Protection policy improvement
- Reporting for stakeholders

Strong fit scenarios

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

SOTERIA CLOUD

Protection should be operational, not theoretical.

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