OPERATIONAL HOW-TO

ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to prepare a ransomware recovery runbook

Connect prevention, detection, backup, recovery decisions, and stakeholder evidence before a ransomware event forces rushed choices.

Buyer-ready | Operational evidence | Total Data Protection

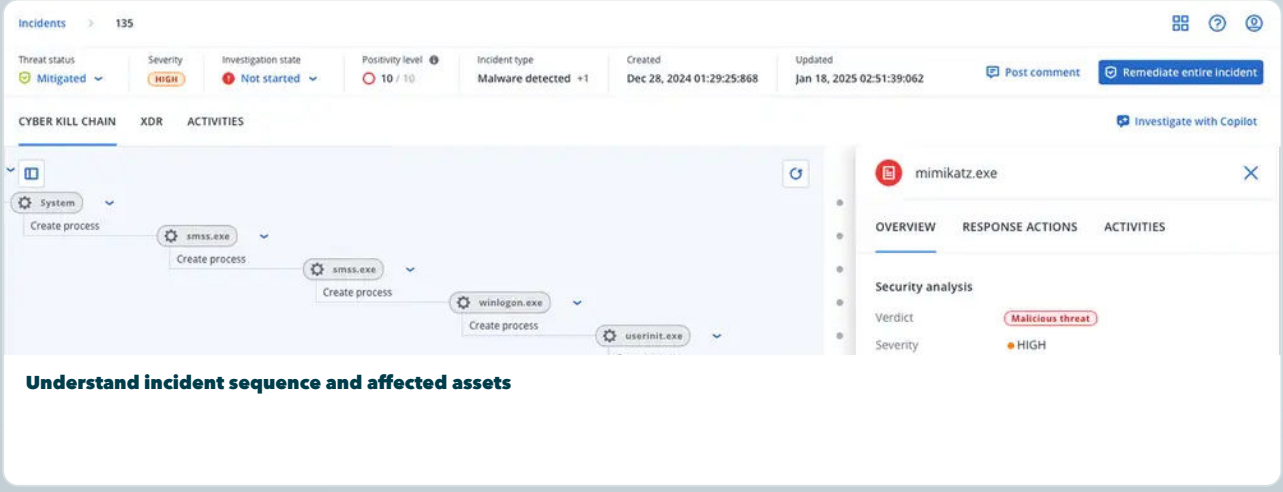
BEST FIT

Business leaders, MSPs, security teams, and IT operations teams preparing for ransomware impact.

The buyer needs confidence that Soteria Cloud can support containment, clean recovery, and executive reporting during a ransomware event.

Powered by Acronis

Soteria Cloud delivered



Understand incident sequence and affected assets

BUYER NEED

Make the commercial requirement operational.

Cyber resilience guidance increasingly expects tested recovery, verified restoration assets, incident communication, and post-incident evidence.

BUYER TRIGGER

The buyer needs confidence that Soteria Cloud can support containment, clean recovery, and executive reporting during a ransomware event.

PRODUCTS INVOLVED

Advanced Backup, Advanced Disaster Recovery, EDR, MDR, Cyber Protect Cloud

CONSOLE SURFACES

Monitoring, Dashboards, Audit log, Reports, Executive summary

01

A ransomware runbook is only useful if the recovery points and decision owners are known before the incident.

02

Backup success is not enough; buyers need evidence that clean restore paths have been tested.

03

Separate containment decisions from recovery decisions so response does not damage recoverability.

04

Keep executive updates simple: impact, protected assets, recovery sequence, and remaining risk.

05

Use audit evidence to show what changed, who acted, and when recovery criteria were met.

06

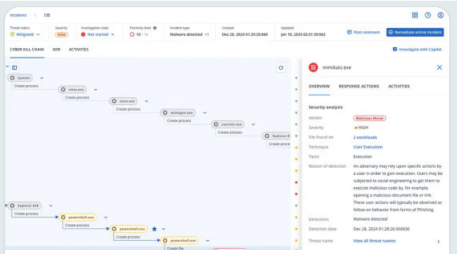
After the incident, turn lessons learned into policy and service review actions.

PRACTICAL PATH

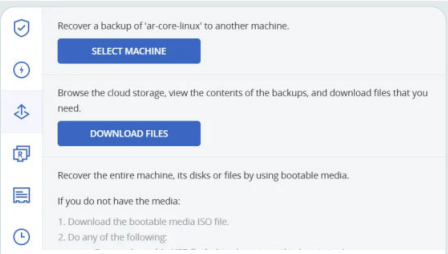
Turn the offer into a repeatable service motion.

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

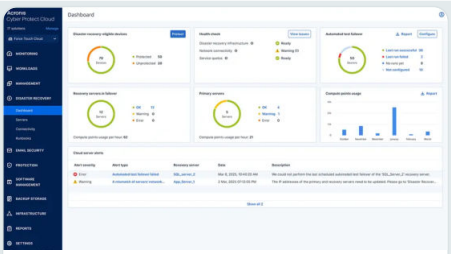
CLASSIFY CRITICAL SERVICES	Rank workloads by business impact, recovery priority, dependency, and acceptable downtime.
VERIFY BACKUP INTEGRITY	Check backup status, retention, immutable or protected storage options, and sample restore outcomes for each priority workload.
DEFINE RESPONSE ACTIONS	Agree when to isolate endpoints, stop services, trigger EDR investigation, recover from backup, fail over, or escalate to specialist response.
MAP COMMUNICATION	Prepare the executive, customer, internal, and technical updates that will be needed while restoration is in progress.
REVIEW AND IMPROVE	Use reports, audit log, and executive summary evidence to close gaps after each test or incident.



Understand incident sequence and affected assets



Confirm clean recovery actions



Track DR readiness for priority workloads

BUYER OUTCOME

Connect prevention, detection, backup, recovery decisions, and stakeholder evidence before a ransomware event forces rushed choices.

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

- Priority workload list
- Restore test results
- EDR or MDR incident evidence
- Failover or recovery decision record
- Post-incident improvement actions

Measures to review

- Critical workloads with tested restore
- Recovery point confidence
- Recovery decision owner assigned
- Containment actions traceable
- Runbook gaps closed

01 **Critical workloads with tested restore**

02 **Recovery point confidence**

03 **Recovery decision owner assigned**

04 **Priority workload list**

05 **Restore test results**

06 **EDR or MDR incident evidence**