

SOTERIA CLOUD CLOUD SECURITY

# How to improve cloud workload security posture

Make cloud exposure, configuration risk, and network control easier to see and act on.

Cloud workload protection

Acronis Cloud Security and Smart Firewall

Total Data Protection

BEST FIT

## Azure and cloud infrastructure buyers that need practical governance without slowing delivery.

Cloud environments move quickly. Misconfiguration, weak visibility, and unmanaged network exposure create avoidable risk.

Acronis Powered by Acronis



Soteria Cloud

+ New

Acronis AI

Q

?

ⓘ

CLIENTS

MONITORING

MY INBOX 23

REPORTS

View: Cyber Protection

Selected tenants: 0 / 100 max.  
Select multiple items by holding the "Shift" button

Cancel

Next

⚙

| Name ↑                                       | Tenant status | Management mode | Billing mode                 | 2FA status | 7-day history |
|----------------------------------------------|---------------|-----------------|------------------------------|------------|---------------|
| <input type="checkbox"/> Partner Workspace 1 | Active        | Full access     | Service-based (per workload) | Enabled    |               |

Cloud security service configuration 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 cloud workloads are in scope**

**02**

**Which exposures create unacceptable business risk**

**03**

**How firewall and network rules are governed**

**04**

**Who owns remediation actions**

**05**

**How security posture is reviewed over time**

**06**

**Which cloud changes require extra approval**

## Readiness checklist

- Inventory cloud workloads, networks, and ownership
- Review exposure, configuration, and access risk
- Prioritize controls for business-critical workloads
- Set firewall and remediation responsibilities
- Track posture improvements in recurring reviews

## Gaps to close

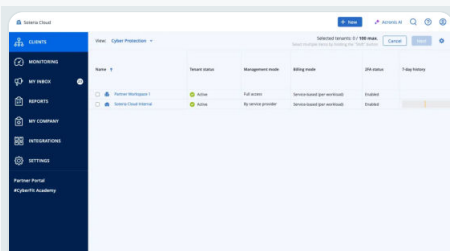
- Cloud assets created faster than governance can see them
- Firewall changes without business-level review
- Configuration issues treated as low-priority noise
- No single view of open cloud security actions

**PRACTICAL PATH**

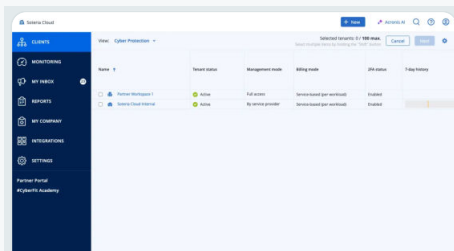
# Turn the requirement into an operating model.

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

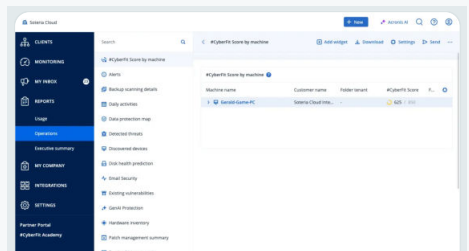
|                        |                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------|
| <b>DISCOVER ASSETS</b> | Identify cloud workloads, networks, public exposure, ownership, and business importance.          |
| <b>ASSESS POSTURE</b>  | Review configuration, access, firewall, and workload security signals through Soteria Cloud.      |
| <b>PRIORITIZE RISK</b> | Focus remediation on exposed services, critical workloads, and repeat configuration patterns.     |
| <b>APPLY CONTROLS</b>  | Improve firewall policy, access control, and workload configuration without slowing valid change. |
| <b>SHOW PROGRESS</b>   | Report open risks, closed actions, exceptions, and posture trends.                                |



**Cloud security service configuration view**



**Confirm services and scope**



**Review reporting evidence**

**SOTERIA CLOUD OFFER**  
**Soteria Cloud Cloud Security**

**POWERED BY**  
**Acronis Cloud Security and Smart Firewall**

**SERVICE FIT**  
**Best for buyers that want visible cloud security governance tied to practical remediation.**

**OUTCOME**

**Improve cloud security posture. 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**

**Cloud assets reviewed**

**02**

**High-risk exposures reduced**

**03**

**Firewall changes controlled**

**04**

**Remediation actions closed**

**05**

**Posture trend improved**

## **Business outcomes**

- Improve cloud security posture
- Control network exposure with clearer policy
- Support cloud governance without slowing delivery

## **Strong fit scenarios**

- Azure security baseline
- Cloud firewall and exposure review
- Governed cloud workload onboarding

**SOTERIA CLOUD**

## **All your data. One strategy. Zero compromise.**

Visibility and control for cloud workloads, networks, and security posture. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.