

ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to govern API clients and service integrations

Make integrations safer by treating API clients, PSA/RMM links, reporting feeds, and automation as governed access points.

Buyer-ready

Operational evidence

Total Data Protection

BEST FIT

MSPs, resellers, IT operations teams, and platform owners integrating Soteria Cloud with service systems.

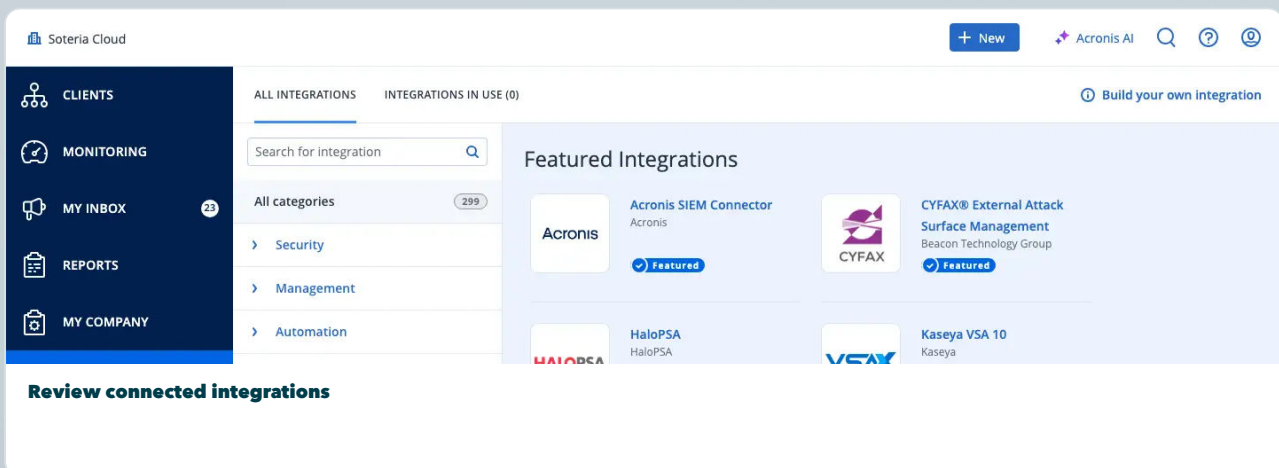
The buyer wants automation and reporting without uncontrolled API credentials, stale integrations, or unknown access paths.

Acronis

Powered by Acronis



Soteria Cloud delivered



BUYER NEED

Make the commercial requirement operational.

Service provider operations increasingly depend on automation, but customers still expect access control, traceability, and clean offboarding.

BUYER TRIGGER

The buyer wants automation and reporting without uncontrolled API credentials, stale integrations, or unknown access paths.

PRODUCTS INVOLVED

Cyber Protect Cloud, RMM, PSA integrations, Workflow Automation, Reporting

CONSOLE SURFACES

Integrations, API clients, Audit log, Roles and permissions, Subscription

01

Every integration should have an owner, purpose, access scope, and retirement path.

02

API credentials are operational assets; review them with the same discipline as admin users.

03

Avoid shared API clients for unrelated automation workflows.

04

Document which integrations influence tickets, billing, reporting, or customer-facing alerts.

05

Use audit evidence when API clients are created, changed, or removed.

06

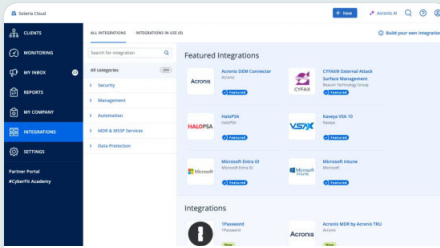
Review integrations before customer offboarding or service tier changes.

PRACTICAL PATH

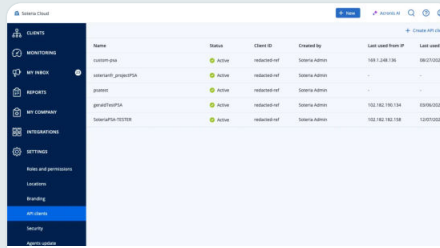
Turn the offer into a repeatable service motion.

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

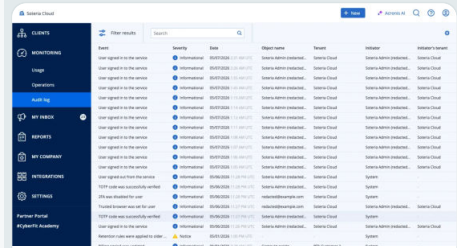
INVENTORY INTEGRATIONS	List PSA, RMM, billing, reporting, automation, and security integrations that connect to Soteria Cloud services.
ASSIGN OWNERSHIP	Give each integration a business owner, technical owner, purpose, data scope, and renewal or review date.
LIMIT ACCESS	Use API clients and roles to reduce credential reach and separate automation by function where practical.
MONITOR CHANGES	Use Audit log to track API client creation, permission changes, integration changes, and unusual activity.
REVIEW LIFECYCLE	Remove unused clients, rotate credentials where required, and update integrations after service changes or customer offboarding.



Review connected integrations



Govern API clients and automation access



Track sensitive integration changes

BUYER OUTCOME

Make integrations safer by treating API clients, PSA/RMM links, reporting feeds, and automation as governed access points.

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

- Integration register
- API client ownership
- Access scope statement
- Audit trail for changes
- Retired or rotated credentials

Measures to review

- Integrations with owners
- Unused clients removed
- Credentials reviewed
- Integration exceptions closed
- Audit events reviewed

01

Integrations with owners

02

Unused clients removed

03

Credentials reviewed

04

Integration register

05

API client ownership

06

Access scope statement

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Acronis-powered protection packaged with Soteria Cloud onboarding, service ownership, reporting, and recurring buyer-ready review.