

SOTERIA CLOUD PERSONAL ENDPOINT PROTECTION

How to protect personal productivity data

Personal-device backup and cyber protection for executives, remote workers, and high-value endpoints.

Individual device protection

Acronis True Image 2026

STARTING POINT

High-value personal and executive devices often hold important data but are not always covered by business backup routines.

For organizations and individuals that need simple protection for Windows and Mac devices outside the standard managed estate.

Acronis Powered by Acronis

Cyber Protection



Endpoint backup and protection service 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 True Image 2026 capability into a practical service outcome.

01 Confirm scope	List servers, endpoints, SaaS data, NAS, hosting workloads, and business owners that need protection.
02 Set recovery targets	Agree retention, recovery point expectations, recovery time expectations, and approval owners.
03 Apply policies	Group workloads, apply backup plans, enable required storage, and check that the first jobs complete.
04 Test recovery	Run file, folder, and system recovery checks before the service is treated as production-ready.
05 Review evidence	Use reports to show coverage, failures, exceptions, and restore-test outcomes.

KEY OUTCOME

Protect personal productivity data. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis True Image 2026

PROTECTION FOCUS

Individual device protection

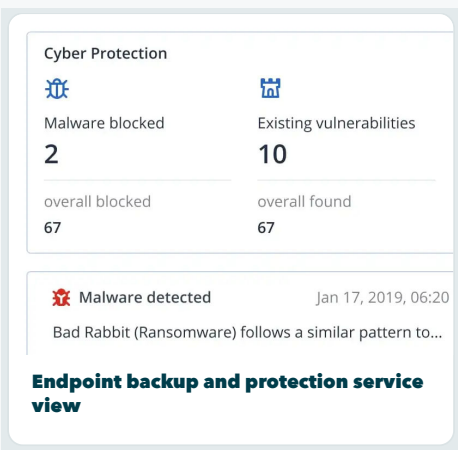
SERVICE OWNER

Soteria Cloud

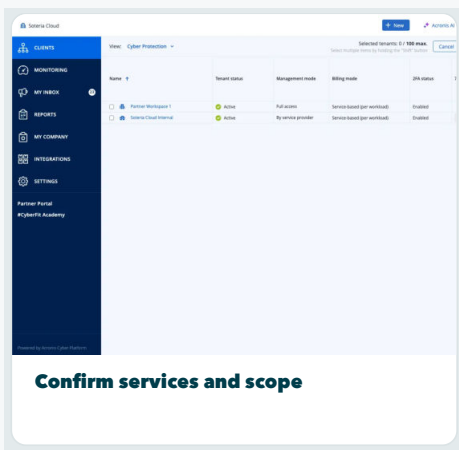
SCREEN CUES

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

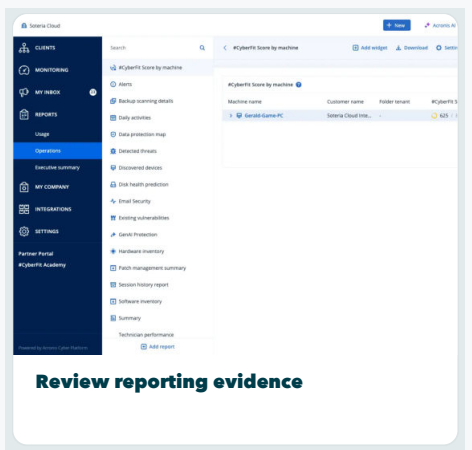
Personal-device backup and cyber protection for executives, remote workers, and high-value endpoints. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Endpoint backup and protection service view



Confirm services and scope



Review reporting evidence

Individual device protection 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

Protect personal productivity data

02

Support Windows and Mac backup needs

03

Create an easy add-on for remote and executive users

Controls to put in place

- Windows device protection
- Mac device protection
- Local and cloud backup options
- Cyber protection features
- File recovery
- User-friendly restore experience

Strong fit scenarios

- Executive laptop protection
- Remote worker device resilience
- Small office endpoint backup

SOTERIA CLOUD

Protection should be operational, not theoretical.

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