

SOTERIA CLOUD ADVANCED BACKUP

# How to protect critical systems from deletion, corruption, and ransomware impact

Reliable backup that is designed around restore outcomes, not just retained copies.

Backup and recovery

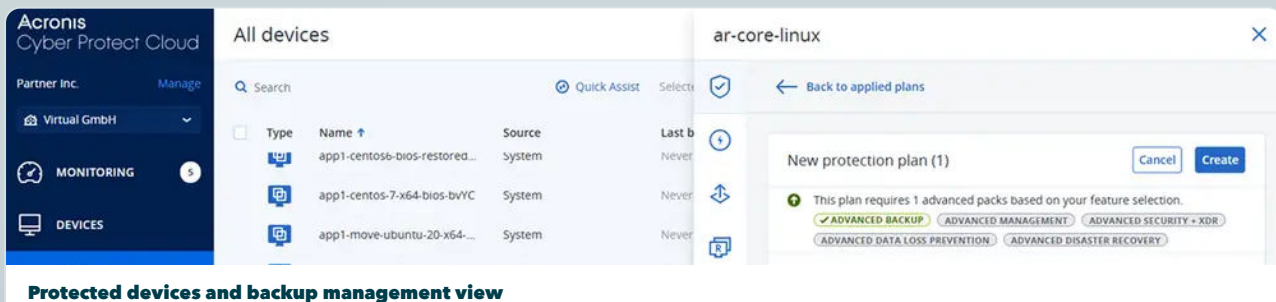
Acronis Advanced Backup

STARTING POINT

**Backups only matter when they can be restored quickly, cleanly, and at the right level of granularity.**

For organizations that need dependable protection for servers, workstations, virtual machines, NAS, and core business data.

Acronis Powered by Acronis



The screenshot displays the Acronis Cyber Protect Cloud management console. On the left, a sidebar shows navigation options: 'MONITORING' and 'DEVICES'. The main area is titled 'All devices' and contains a table of protected devices. A modal window titled 'New protection plan (1)' is open on the right, showing a list of advanced packs: 'ADVANCED BACKUP', 'ADVANCED MANAGEMENT', 'ADVANCED SECURITY + XDR', 'ADVANCED DATA LOSS PREVENTION', and 'ADVANCED DISASTER RECOVERY'. The 'ADVANCED BACKUP' pack is selected.

| Type            | Name                          | Source | Last backup |
|-----------------|-------------------------------|--------|-------------|
| Virtual Machine | app1-centos6-bios-restored... | System | Never       |
| Virtual Machine | app1-centos-7-x64-bios-bvYC   | System | Never       |
| Virtual Machine | app1-move-ubuntu-20-x64...    | System | Never       |

**Protected devices and backup management 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 Advanced Backup capability into a practical service outcome.

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

**KEY OUTCOME**

**Protect critical systems from deletion, corruption, and ransomware impact. The service is shaped around the workloads, users, data, and risk profile that matter most.**

**TECHNOLOGY FOUNDATION**

**Acronis Advanced Backup**

**PROTECTION FOCUS**

**Backup and recovery**

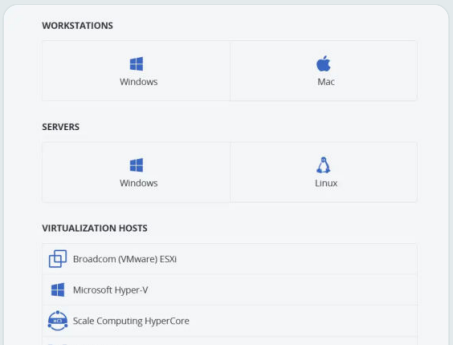
**SERVICE OWNER**

**Soteria Cloud**

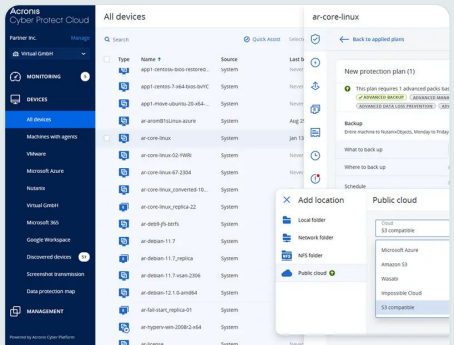
SCREEN CUES

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

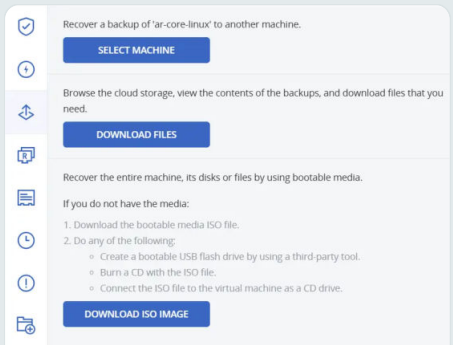
Reliable backup that is designed around restore outcomes, not just retained copies. The screens below help buyers understand where scope, controls, and reporting evidence come from.



**Identify workloads that need protection**



**Apply backup policies and monitor status**



**Confirm recovery actions before sign-off**

**Backup and recovery 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 critical systems from deletion, corruption, and ransomware impact**

02

**Recover files, systems, and workloads with practical restore options**

03

**Build predictable recovery into the managed service model**

## Controls to put in place

- Image-based backup
- File and folder recovery
- Physical and virtual workload support
- NAS backup options
- Policy-based retention
- Cloud storage aligned to Soteria Cloud protection plans

## Strong fit scenarios

- Endpoint and server backup modernization
- Protection for branch offices and remote teams
- Backup standardization across multiple customers

SOTERIA CLOUD

# Protection should be operational, not theoretical.

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