HOW-TO

SOTERIA CLOUD DEVICELOCK DLP & DISCOVERY

How to find sensitive data on endpoints

Discover and control sensitive data movement at the endpoint.

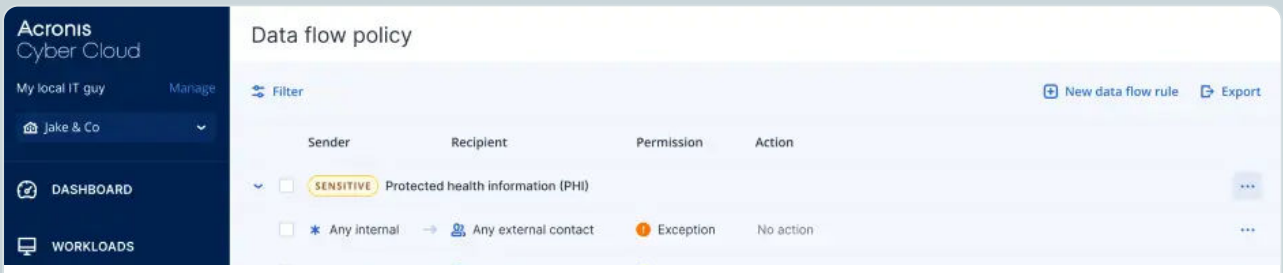
Endpoint data control **Acronis DeviceLock DLP and Discovery**

STARTING POINT

Sensitive data can leave through endpoints before central systems ever see the risk.

For organizations that need endpoint-level control over data leakage, removable media, and sensitive file exposure.

Acronis **Powered by Acronis**



Device and data control workflow 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 DeviceLock DLP and Discovery capability into a practical service outcome.

01 Identify sensitive data	Map where regulated, customer, finance, HR, and intellectual property data is handled.
02 Choose controls	Set device, port, transfer, content, and exception policies by role and risk.
03 Pilot carefully	Start with monitoring, review findings, and then move higher-risk groups into enforcement.
04 Manage exceptions	Approve business exceptions with expiry dates and traceable ownership.
05 Show governance	Use reports and audit evidence to support compliance, insurance, and leadership reviews.

KEY OUTCOME

Find sensitive data on endpoints. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis DeviceLock DLP and Discovery

PROTECTION FOCUS

Endpoint data control

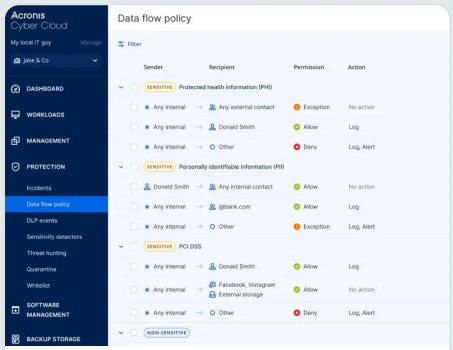
SERVICE OWNER

Soteria Cloud

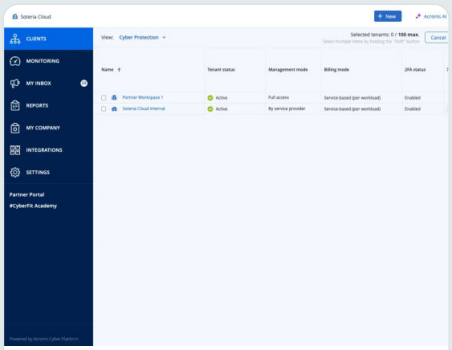
SCREEN CUES

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

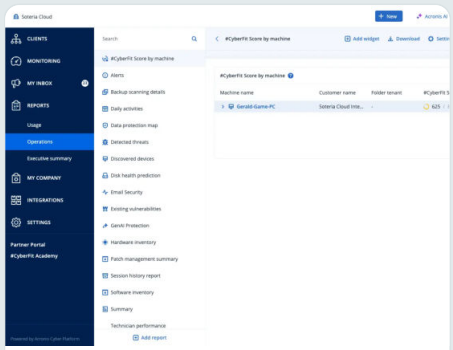
Discover and control sensitive data movement at the endpoint. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Device and data control workflow view



Confirm services and scope



Review reporting evidence

Endpoint data control 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

Find sensitive data on endpoints

02

Control risky device and channel usage

03

Support compliance with practical endpoint evidence

Controls to put in place

- Endpoint DLP controls
- Device and port control
- Content discovery
- Policy enforcement
- Activity logging
- Compliance reporting

Strong fit scenarios

- Removable media control
- Sensitive data discovery
- Regulated endpoint governance

SOTERIA CLOUD

Protection should be operational, not theoretical.

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