

SOTERIA CLOUD ADVANCED DATA LOSS PREVENTION

How to reduce unauthorized data movement

Control where sensitive data goes before leakage becomes a business problem.

Data protection and compliance

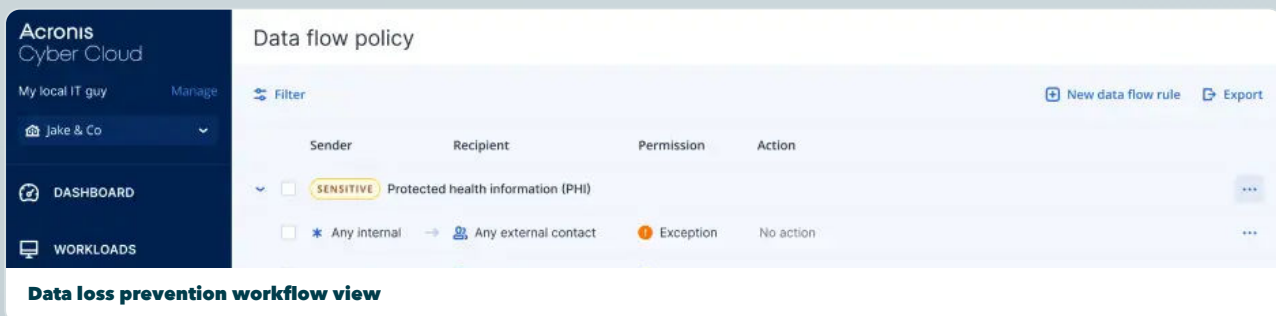
Acronis Advanced DLP and DeviceLock

STARTING POINT

Data loss often happens through everyday channels: USB devices, unmanaged transfers, local copies, and accidental disclosure.

For organizations that need stronger oversight of endpoint data movement, removable media, and sensitive information handling.

Acronis Powered by Acronis



The screenshot shows the 'Data flow policy' configuration page in the Acronis Cyber Cloud console. On the left is a sidebar with navigation links: 'My local IT guy', 'Manage', 'Jake & Co', 'DASHBOARD', and 'WORKLOADS'. The main content area is titled 'Data flow policy' and includes a 'Filter' button, a '+ New data flow rule' button, and an 'Export' button. Below these is a table with columns: 'Sender', 'Recipient', 'Permission', and 'Action'. The table contains two rows: 1) A row with a 'SENSITIVE' label, 'Protected health information (PHI)' in the Recipient column, and an ellipsis in the Action column. 2) A row with 'Any internal' in the Sender column, 'Any external contact' in the Recipient column, 'Exception' in the Permission column, and 'No action' in the Action column. Below the table, the text 'Data loss prevention workflow view' is displayed.

Sender	Recipient	Permission	Action
	Protected health information (PHI)		...
Any internal	Any external contact	Exception	No action

Data loss prevention 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 Advanced DLP and DeviceLock 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

Reduce unauthorized data movement. The service is shaped around the workloads, users, data, and risk profile that matter most.

TECHNOLOGY FOUNDATION

Acronis Advanced DLP and DeviceLock

PROTECTION FOCUS

Data protection and compliance

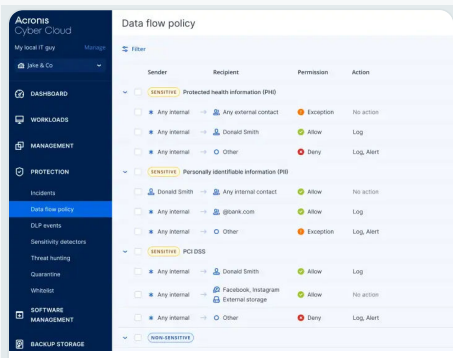
SERVICE OWNER

Soteria Cloud

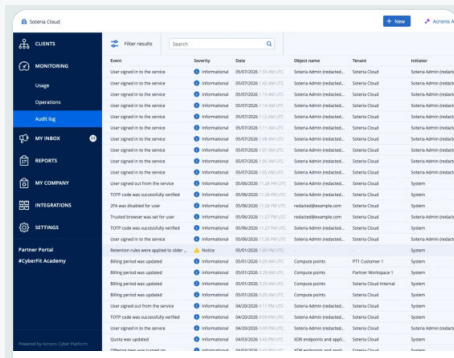
SCREEN CUES

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

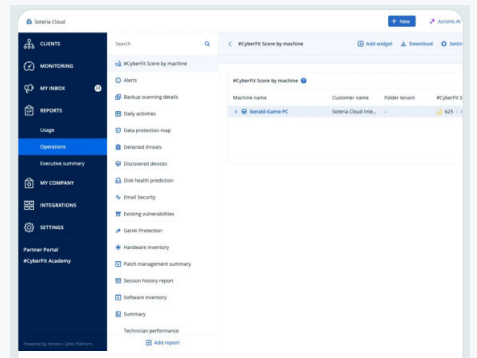
Control where sensitive data goes before leakage becomes a business problem. The screens below help buyers understand where scope, controls, and reporting evidence come from.



Map sensitive data movement controls



Track policy and exception activity



Show governance evidence

Data protection and compliance 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

Reduce unauthorized data movement

02

Improve visibility into sensitive data handling

03

Support governance and compliance programs

Controls to put in place

- Device and port controls
- Content-aware data controls
- Endpoint DLP policy
- Discovery of sensitive data
- Activity logging
- Compliance-oriented reporting

Strong fit scenarios

- Protect regulated data
- Control removable media risk
- Support cyber insurance and audit conversations

SOTERIA CLOUD

Protection should be operational, not theoretical.

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