

ENDPOINT DATA CONTROL

Soteria Cloud DeviceLock DLP & Discovery

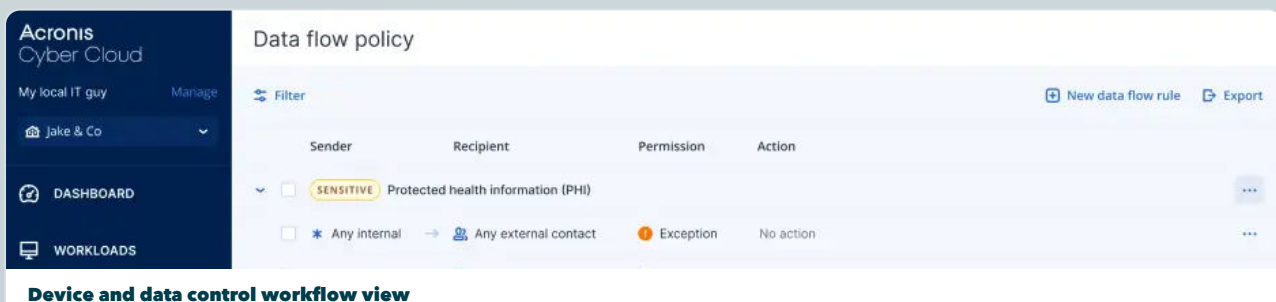
Discover and control sensitive data movement at the endpoint.

AT A GLANCE

Acronis DeviceLock DLP and Discovery

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

Acronis Powered by Acronis



The screenshot displays the Acronis Cyber Cloud interface. On the left is a dark blue sidebar with the 'Acronis Cyber Cloud' logo, a user profile 'My local IT guy' with a 'Manage' link, and a dropdown menu for 'Jake & Co'. Below this are links for '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. A table lists data flow rules with columns for Sender, Recipient, Permission, and Action. The first rule is labeled 'SENSITIVE' and 'Protected health information (PHI)'. The second rule shows a flow from 'Any internal' to 'Any external contact' with an 'Exception' permission and 'No action'.

Sender	Recipient	Permission	Action
☐ SENSITIVE	Protected health information (PHI)		...
☐ * Any internal	→ ☐ Any external contact	☒ Exception	No action

Device and data control workflow view



SPECIFICATIONS

Capabilities, fit, and service coverage.

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

OFFER

Soteria Cloud DeviceLock DLP & Discovery

TECHNOLOGY

Acronis DeviceLock DLP and Discovery

CATEGORY

Endpoint data control

PRIMARY FIT

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

PROTECTION PROMISE

Discover and control sensitive data movement at the endpoint.

SERVICE MODEL

Soteria Cloud onboarding, support, reporting, and review

Included capabilities

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

Business outcomes

- Find sensitive data on endpoints
- Control risky device and channel usage
- Support compliance with practical endpoint evidence

COMMON USE CASES

Removable media control; Sensitive data discovery; Regulated endpoint governance

SERVICE COMPONENTS

Endpoint data risk review; Discovery scan planning; DLP policy rollout; Ongoing governance reporting

SOTERIA CLOUD VALUE

Protection delivered with practical implementation, operational visibility, and support ownership.

PROOF POINTS

Endpoint DLP and discovery capability; Soteria Cloud implementation and support; Complements Advanced DLP packages

TOTAL DATA PROTECTION

Zero Downtime. Zero Data Loss.

Soteria Cloud helps protect the workloads, identities, users, and services that keep the business moving.