SOTERIA CLOUD DEVICELOCK DLP & DISCOVERY

How to discover and control endpoint data movement

Find sensitive data on endpoints and reduce leakage risk through practical controls and governance evidence.

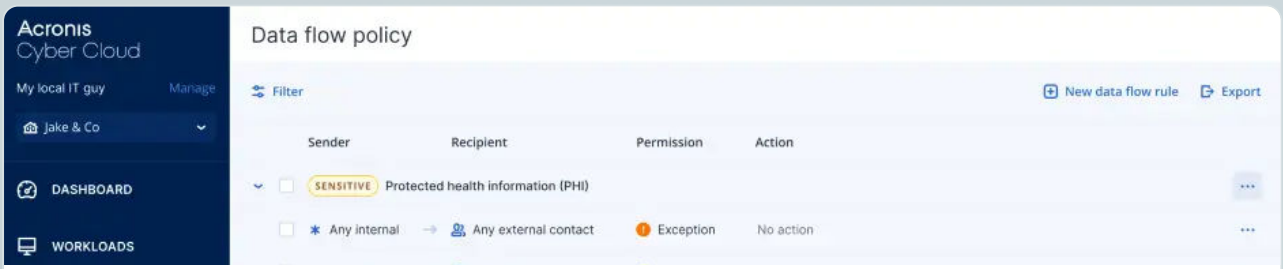
Endpoint data control | Acronis DeviceLock DLP and Discovery | Total Data Protection

BEST FIT

Compliance, IT, and security buyers that need endpoint data discovery and data movement control.

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

Acronis **Powered by Acronis**



Device and data control workflow view

DECIDE FIRST

Make the business choices clear before rollout.

Useful protection starts with the workloads, users, data, recovery targets, and risk decisions that shape the service.

01
Which sensitive data needs discovery

02
Where endpoint data movement creates risk

03
Which channels require monitoring or blocking

04
How discovery results become policy action

05
Who reviews events and exceptions

06
What evidence supports audits and governance

Readiness checklist

- Define sensitive data types and endpoint groups
- Run discovery where exposure is most likely
- Review removable media and endpoint channels
- Apply policies based on discovered risk
- Track exceptions, incidents, and changes

Gaps to close

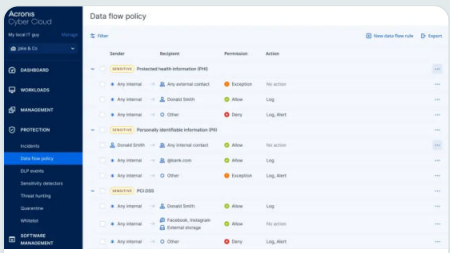
- Endpoint data unknown until a leakage event
- Discovery findings not converted into controls
- Device policies too broad for real work patterns
- Compliance evidence spread across manual notes

PRACTICAL PATH

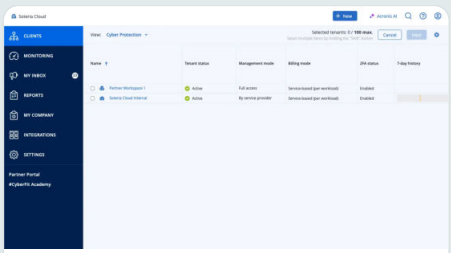
Turn the requirement into an operating model.

Soteria Cloud surrounds Acronis technology with assessment, policy design, onboarding, review, and support ownership.

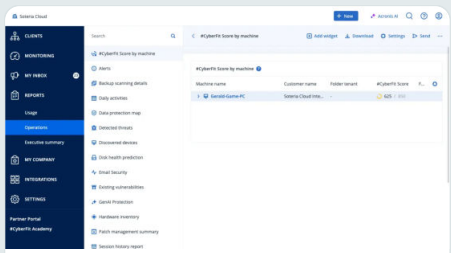
DEFINE DISCOVERY SCOPE	Identify endpoint groups, sensitive data types, departments, and storage locations for review.
FIND EXPOSURE	Use discovery to locate sensitive files and understand where risky data sits.
MAP MOVEMENT	Review USB, device, transfer, and local endpoint channels that can move data.
APPLY CONTROLS	Turn findings into monitoring, warning, blocking, and exception rules.
REPORT EVIDENCE	Show discovered risk, controlled channels, events, exceptions, and closed actions.



Device and data control workflow view



Confirm services and scope



Review reporting evidence

SOTERIA CLOUD OFFER

Soteria Cloud DeviceLock DLP & Discovery

POWERED BY

Acronis DeviceLock DLP and Discovery

SERVICE FIT

Best for buyers that need endpoint discovery and DLP control with clear compliance evidence.

OUTCOME

Find sensitive data on endpoints. The plan is stronger when controls, recovery expectations, and reporting evidence are connected from the start.

EVIDENCE

Measure the things that prove protection is working.

Good cyber resilience is visible. Buyers need coverage, exceptions, recovery confidence, and service actions they can understand.

01 **Sensitive files discovered**

02 **Risky channels controlled**

03 **Policy actions applied**

04 **Exceptions reviewed**

05 **Governance evidence available**

Business outcomes

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

Strong fit scenarios

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

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Discover and control sensitive data movement at the endpoint. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.