SOTERIA CLOUD ADVANCED DATA LOSS PREVENTION

How to reduce sensitive data leakage from endpoints

Control everyday data movement across removable media, local files, endpoint channels, and sensitive information workflows.

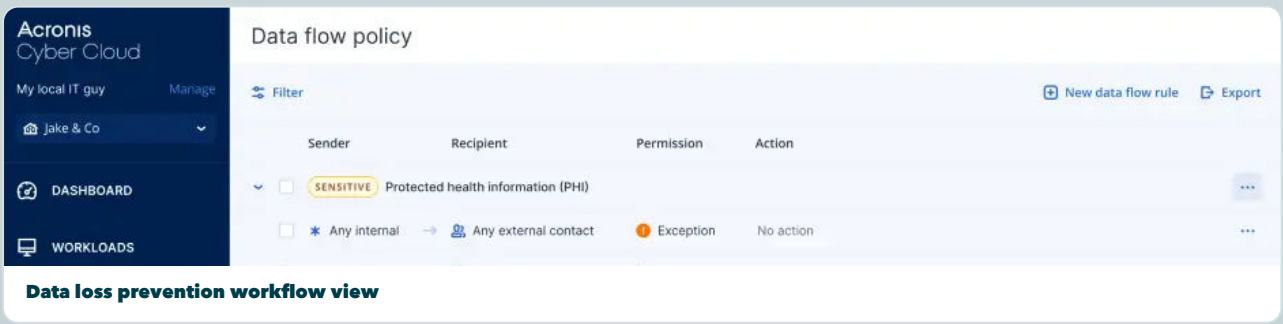
Data protection and compliance | Acronis Advanced DLP and DeviceLock | Total Data Protection

BEST FIT

Organizations with regulated data, employee data, customer records, financial files, or intellectual property on endpoints.

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

Acronis Powered by Acronis



Data loss prevention 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 data types need stronger handling controls

02
Which device channels create unacceptable risk

03
Where monitoring is enough and blocking is required

04
How exceptions are approved and reviewed

05
Which roles need different data movement rules

06
What evidence supports compliance conversations

Readiness checklist

- Identify sensitive data categories and user groups
- Map removable media, printing, transfer, and local copy risk
- Start with monitoring for high-uncertainty areas
- Move to blocking where risk is clear
- Review incidents and exception patterns monthly

Gaps to close

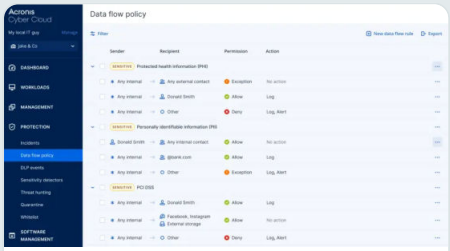
- USB and endpoint channels left outside governance
- Sensitive files discovered only after an incident
- One policy applied to roles with different needs
- No approval trail for exceptions

PRACTICAL PATH

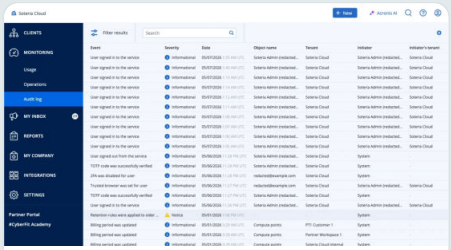
Turn the requirement into an operating model.

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

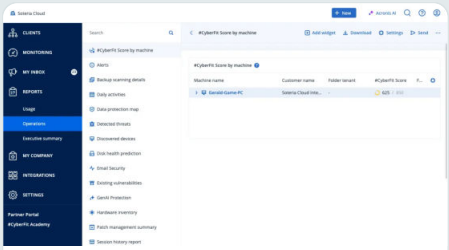
CLASSIFY DATA RISK	Define the sensitive data and roles where leakage creates legal, financial, or operational exposure.
MAP CHANNELS	Review removable media, device ports, local storage, transfer tools, printing, and endpoint activity.
SET POLICIES	Apply monitoring, warning, or blocking policies according to risk and business need.
HANDLE EXCEPTIONS	Create a review path for approved transfers, temporary needs, and role-based exceptions.
PROVE CONTROL	Report activity, blocked movement, exceptions, and policy changes through Soteria Cloud reviews.



Map sensitive data movement controls



Track policy and exception activity



Show governance evidence

SOTERIA CLOUD OFFER

Soteria Cloud Advanced Data Loss Prevention

POWERED BY

Acronis Advanced DLP and DeviceLock

SERVICE FIT

Best for buyers that need endpoint data control with practical governance and visible evidence.

OUTCOME

Reduce unauthorized data movement. 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 data locations identified**

02 **Controlled device channels**

03 **Policy exceptions reviewed**

04 **Blocked risky transfers**

05 **Compliance evidence available**

Business outcomes

- Reduce unauthorized data movement
- Improve visibility into sensitive data handling
- Support governance and compliance programs

Strong fit scenarios

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

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Control where sensitive data goes before leakage becomes a business problem. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.