ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to turn DLP into a governance workflow

Position Soteria Cloud DLP around discovery, policy tuning, exceptions, user behavior, and evidence for sensitive data control.

Buyer-ready | Operational evidence | Total Data Protection

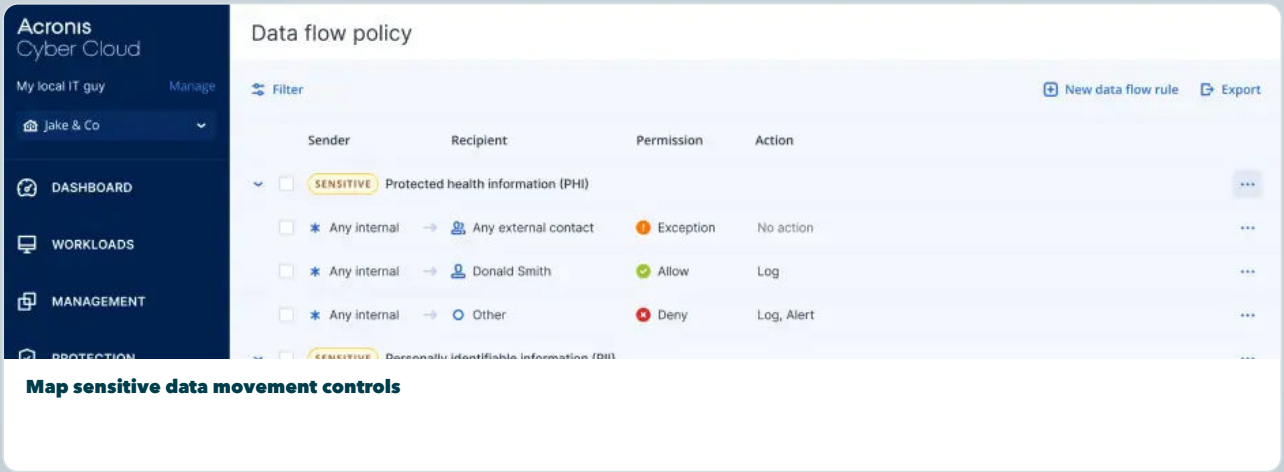
BEST FIT

Compliance owners, MSPs, IT leaders, legal teams, healthcare, finance, professional services, and regulated customers.

The buyer needs to reduce sensitive data leakage risk without blocking legitimate business workflows.

Powered by Acronis

Soteria Cloud delivered



Map sensitive data movement controls

BUYER NEED

Make the commercial requirement operational.

DLP buying decisions are driven by sensitive data exposure, regulatory pressure, insider risk, and the need for practical governance evidence.

BUYER TRIGGER

The buyer needs to reduce sensitive data leakage risk without blocking legitimate business workflows.

PRODUCTS INVOLVED

Advanced DLP, DeviceLock DLP Discovery, Cyber Protect Cloud, Reporting

CONSOLE SURFACES

DLP workflow, Audit log, Reports, Users, Roles and permissions

01

Start DLP with observed data flows before moving to strict enforcement.

02

Separate accidental leakage, risky behavior, and malicious intent in the review conversation.

03

Treat exceptions as governed business decisions with owners and expiry dates.

04

Map DLP policies to departments and data types, not only devices.

05

Use audit trails to show policy changes and exception handling.

06

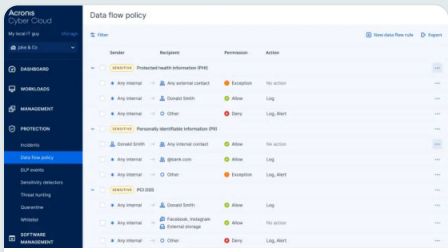
DLP success is lower leakage risk with fewer disruptive false positives.

PRACTICAL PATH

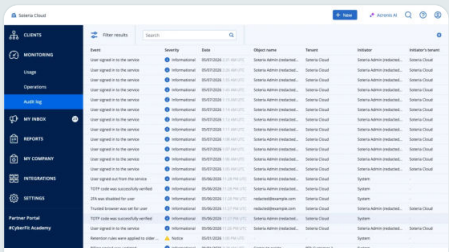
Turn the offer into a repeatable service motion.

Soteria Cloud positions Acronis technology around buyer outcomes, support ownership, recurring review, and evidence that can be explained without product jargon.

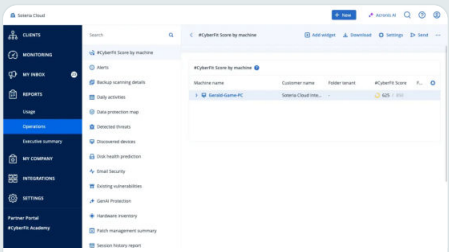
DEFINE SENSITIVE DATA	Identify PII, PHI, PCI, confidential files, customer data, contracts, financial data, and internal IP that need control.
OBSERVE DATA MOVEMENT	Use discovery and monitoring to understand where sensitive data lives and how it moves across users, devices, and channels.
DESIGN PRACTICAL POLICIES	Create monitoring, warning, blocking, and exception rules that match real business processes.
GOVERN EXCEPTIONS	Assign owners, approval reasons, review dates, and evidence for any allowed sensitive data movement outside the baseline.
REPORT RISK REDUCTION	Show data flows discovered, events reduced, exceptions governed, and policies improved over time.



Map sensitive data movement controls



Track policy and exception activity



Show governance evidence

BUYER OUTCOME

Position Soteria Cloud DLP around discovery, policy tuning, exceptions, user behavior, and evidence for sensitive data control.

EVIDENCE

Show the proof buyers expect to see.

Soteria Cloud service reviews give buyers visible status, known exceptions, agreed actions, and a reviewable record of protection activity.

Evidence to keep

- Sensitive data categories
- Observed data flow summary
- DLP policy decisions
- Exception register
- Audit trail and trend report

Measures to review

- Sensitive flows mapped
- Policy events reviewed
- False positives reduced
- Exceptions with owners
- High-risk channels controlled

01 **Sensitive flows mapped**

02 **Policy events reviewed**

03 **False positives reduced**

04 **Sensitive data categories**

05 **Observed data flow summary**

06 **DLP policy decisions**