



DATA PROTECTION AND COMPLIANCE

Soteria Cloud Advanced Data Loss Prevention

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

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

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

- 01 Reduce unauthorized data movement**
- 02 Improve visibility into sensitive data handling**
- 03 Support governance and compliance programs**

EXECUTIVE BRIEF

Acronis
Cyber Protect Cloud

Complete cyber protection.
Simplified.

Dashboard

- OVERVIEW: 2,835 Protected workloads
- PROTECTION STATUS: All protected (No issues)
- ACTIVITY: No active alerts
- WORKLOADS: Servers (1,320), Workstations (1,275), Mobile devices (240)
- STORAGE: 2.4 TB Total storage, Securely stored in the cloud

Risk
Identify and prioritize what matters most.

Control
Apply proven protection across your environment.

Outcome
Ensure business continuity and drive better results.

Secure. Compliant. Always Protected.
Back up, protect, and recover everything from a single cloud-native platform.

- Complete Data Protection
- Built-in Cybersecurity
- Easy to Manage and Automate
- Scalable for Any Business



EXECUTIVE CONTEXT

The business reason this matters.

The brief frames the operational pressure, the commercial reason to act, and the outcomes leadership should expect from the Soteria Cloud approach.

BUSINESS ISSUE

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

SOTERIA CLOUD POSITION

Control where sensitive data goes before leakage becomes a business problem. Soteria Cloud packages the capability around business outcomes, operational ownership, and a clearer path from decision to adoption.

BEST FIT

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

Sender	Recipient	Permission	Action
SENSITIVE Protected health information (PHI)			
Any Internal	Any external contact	Exception	No action
Any Internal	Donald Smith	Allow	Log
Any Internal	Other	Deny	Log, Alert
SENSITIVE Personally identifiable information (PII)			
Donald Smith	Any internal contact	Allow	No action
Any Internal	@bank.com	Allow	Log
Any Internal	Other	Exception	Log, Alert
SENSITIVE PCI DSS			
Any Internal	Donald Smith	Allow	Log
Any Internal	Facebook, Instagram	Allow	No action
Any Internal	External storage	Deny	Log, Alert
NON-SENSITIVE			

From operational pressure to board-ready confidence.

Visual evidence and structured service packaging help buyers understand the path from risk to outcome.

01

Reduce unauthorized data movement

02

Improve visibility into sensitive data handling

03

Support governance and compliance programs

DECISION PATH

How the offer becomes an executive outcome.

Soteria Cloud positions the capability as a managed operating model, not a disconnected tool purchase.



DECISION DRIVERS

Device and port controls

Content-aware data controls

Endpoint DLP policy

Discovery of sensitive data

PROOF POINTS

- Acronis and DeviceLock-backed capability
- Soteria Cloud implementation support
- Fits security and compliance bundles

Book a Soteria Cloud executive review.