



ENDPOINT DATA CONTROL

Soteria Cloud DeviceLock DLP & Discovery

Discover and control sensitive data movement at the endpoint.

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

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

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

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

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

SOTERIA CLOUD POSITION

Discover and control sensitive data movement at the endpoint. Soteria Cloud packages the capability around business outcomes, operational ownership, and a clearer path from decision to adoption.

BEST FIT

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

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

Find sensitive data on endpoints

02

Control risky device and channel usage

03

Support compliance with practical endpoint evidence

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

Endpoint DLP controls

Device and port control

Content discovery

Policy enforcement

PROOF POINTS

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

Book a Soteria Cloud executive review.