



Acronis

SOTERIA CLOUD DATA SHEET

Acronis GenAI Protection

Visibility, prompt-level data protection and enforceable governance for safer generative-AI adoption.



Acronis GenAI Protection is built into the Acronis platform for service-provider operations. It helps organisations discover browser-based GenAI use, reduce sensitive-data leakage, stop harmful prompts and control which AI applications may be used - without adding another disconnected security console.

See Shadow AI: Monitor which browser-based GenAI tools are used, by whom and how often, with multi-client reporting.

Protect prompt data: Inspect prompts for sensitive content and block unauthorised submission to public or unsanctioned AI services.

Govern AI access: Apply application-level allow or block policies and identify the user associated with GenAI events.

GenAI Protection helps implement technical controls around AI use. It does not by itself establish legal compliance, an approved-use policy or a complete data-governance programme.

From visibility to consistent enforcement

The service can begin in detect-only mode to establish a baseline, then move to block mode after policy, exceptions and business ownership are agreed.



Capability	What it does	Operational value
Shadow AI monitoring	Discovers and reports browser-based GenAI usage across protected environments	Replaces assumptions with evidence for policy and client conversations
Sensitive-data classification	Identifies categories such as PII, PHI, PCI-related data, credentials and confidential content	Reduces the risk of data being pasted into public AI tools
Harmful-prompt protection	Detects and can block prompt injection and other abusive or policy-violating prompts	Protects workflow and output integrity
Application access control	Allows only specified AI applications or blocks specified applications and domains	Aligns tool use to the approved application list
User attribution and reporting	Associates GenAI events with logged-in users and surfaces trends in widgets and reports	Supports investigation, accountability and service review

Important scope boundary

GenAI Protection focuses on browser-based GenAI interactions. Acronis positions its broader DLP capability for more advanced coverage across additional local and network channels, including local GenAI applications. Service design should distinguish the two clearly.

Start with an AI-use discovery period

Soteria Cloud can help define the approved-tool policy, sensitive-data categories, detect-only baseline, exception process and managed reporting cadence.

[Ask AB about GenAI Protection](#)