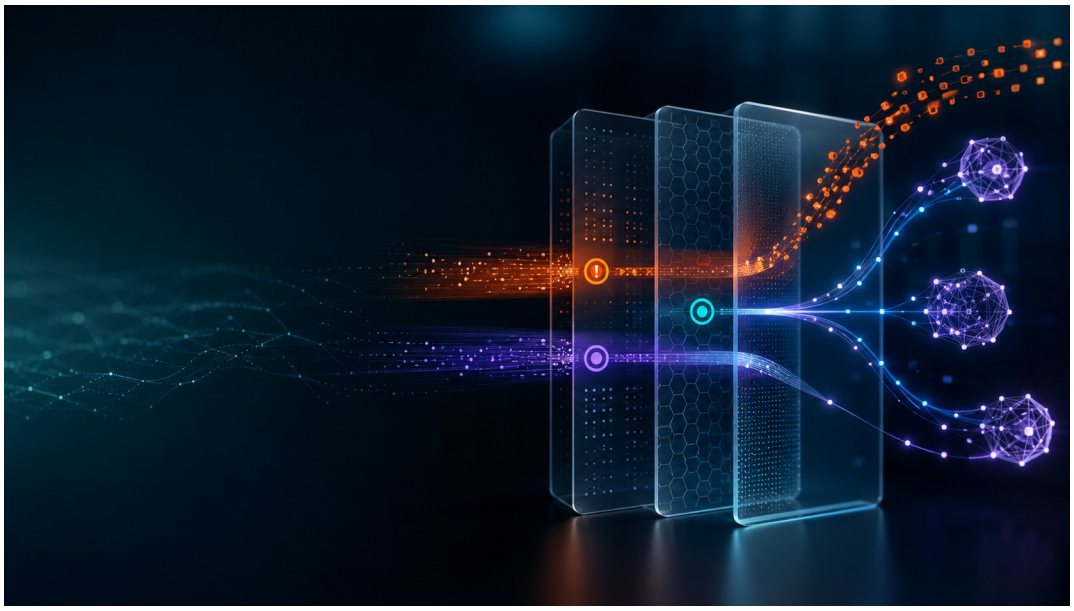
SOTERIA CLOUD SOLUTION BROCHURE

Say yes to AI - with visibility and control

Acronis GenAI Protection helps MSPs and businesses make generative AI safer to adopt, govern and support.



Your users are already experimenting with generative AI. The real choice is whether that adoption remains invisible and unmanaged, or becomes a governed business capability with clear policies, technical controls and evidence.

> **Discover:** See which browser-based GenAI services are being used across the environment.
>
> **Protect:** Stop sensitive data and harmful prompts before they create downstream risk.
>
> **Enable:** Give approved AI use a safe path forward instead of relying on blanket bans.

AI creates value and a new class of unmanaged risk

The productivity benefit is real. So are the governance gaps that appear when users adopt consumer-grade AI tools outside formal IT oversight.

Three risks arrive together

- Shadow AI: the organisation does not know which tools are being used, by whom or for what purpose.
- Data leakage: users may paste personal information, credentials, financial data, source material or confidential business content into external services.
- Prompt abuse: malicious or policy-violating prompts can manipulate AI behaviour, introduce unsafe content or bypass intended controls.

> **The better question:** Do not ask only, 'Can we allow AI?' Ask, 'Which AI services may be used, for which business purposes, with what data, under which controls and with what evidence?'

Why a blanket ban is rarely enough

Blocking every AI service can drive use further into the shadows and deny teams legitimate productivity gains. A managed approach combines discovery, approved-tool decisions, sensitive-data controls, harmful-prompt protection, user education and ongoing reporting.

Govern AI without slowing productive work

Acronis brings visibility, enforcement and reporting into the same multitenant platform used for broader cyber protection.

A practical control stack

- Monitor browser-based GenAI tools and identify adoption trends and anomalies.
- Classify prompt content and prevent unauthorised transfer of sensitive information.
- Detect and block harmful prompts, including prompt-injection techniques.
- Use allow-only or block-only application and domain policies to govern the approved tool set.
- Attribute events to logged-in users and review evidence through central events, widgets and reports.

1. **Observe.** Run detect-only mode and understand actual AI usage.
2. **Decide.** Approve tools, data categories, business purposes and exception owners.
3. **Enforce.** Activate proportionate blocking where the policy and evidence support it.
4. **Improve.** Review events, tune controls, coach teams and extend DLP where broader channels matter.

Turn AI governance into an ongoing managed service

The technology is strongest when it is paired with policy ownership, user enablement and a repeatable review cadence.

A partner-ready service can include

- AI usage discovery and baseline reporting.
- Approved application and domain policy design.
- Sensitive-data and harmful-prompt control configuration.
- Exception handling, incident review and policy tuning.
- Executive service reporting and safe-use enablement.

Make the first 30 days a discovery phase

Soteria Cloud can help you move from unknown AI use to a policy-backed, measurable and supportable service.

Talk to AB - Soteria Cloud Sales

> *Acronis GenAI Protection can support AI governance and data-protection objectives but does not guarantee POPIA compliance or replace legal advice, an information-governance programme, user policy, training or contractual assessment. Capability and application coverage can change by release and service plan.*