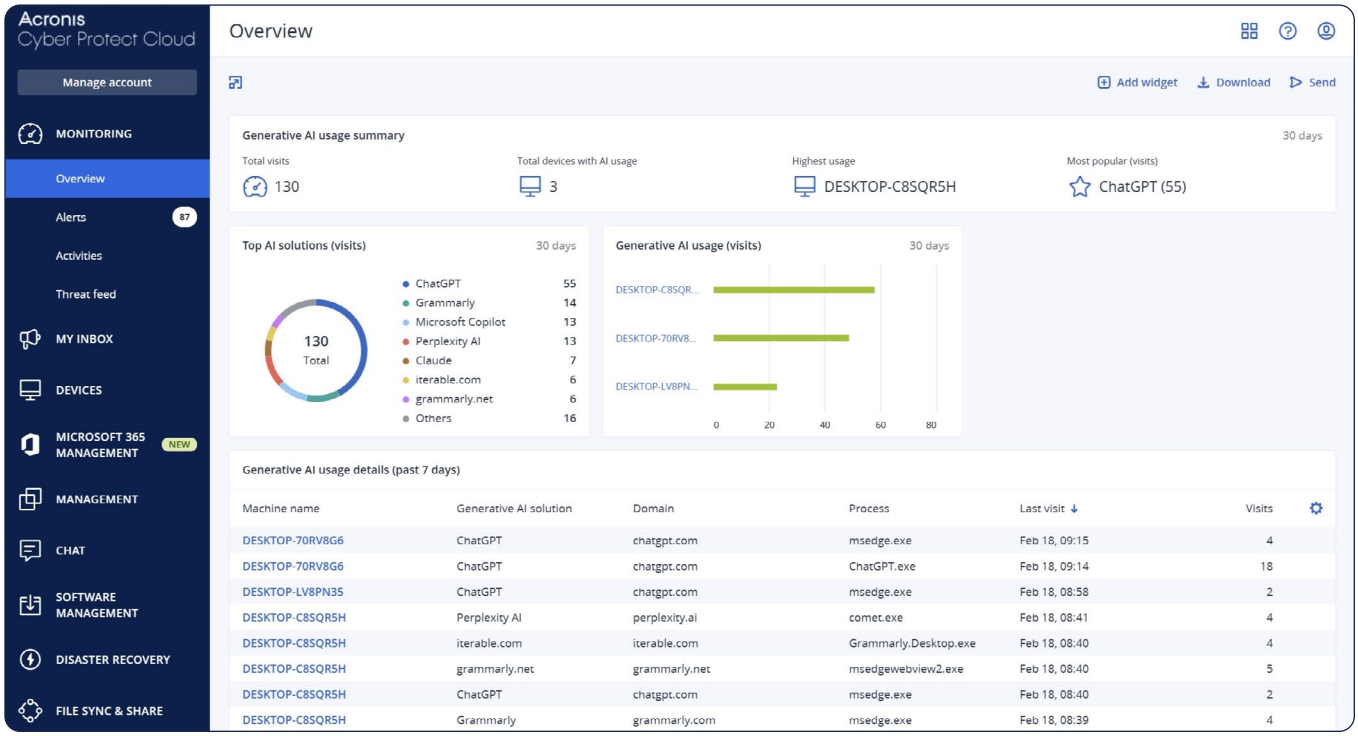
Acronis GenAI Protection

Secure the GenAI era: Expand services and become a trusted advisor in your clients' AI transformation



Generative AI is spreading fast across SMB environments, often through unsanctioned, consumer-grade tools adopted outside IT oversight. While GenAI boosts productivity, it also creates new data leakage risks, compliance exposure, and attack surfaces that clients expect service providers to manage.

Acronis GenAI Protection, built natively into the Acronis platform, gives MSPs of any size a practical, scalable way to govern and secure GenAI usage across client environments without introducing another standalone product, console or operational burden.

Gain full visibility into GenAI usage

Discover which GenAI tools are being used across client environments, by whom and how often. Identify shadow AI, understand adoption trends, and detect anomalous or risky behavior early, before it turns into incidents or compliance issues.

Outcome: Confidently govern AI adoption instead of reacting after data exposure occurs.

Prevent sensitive data exposure

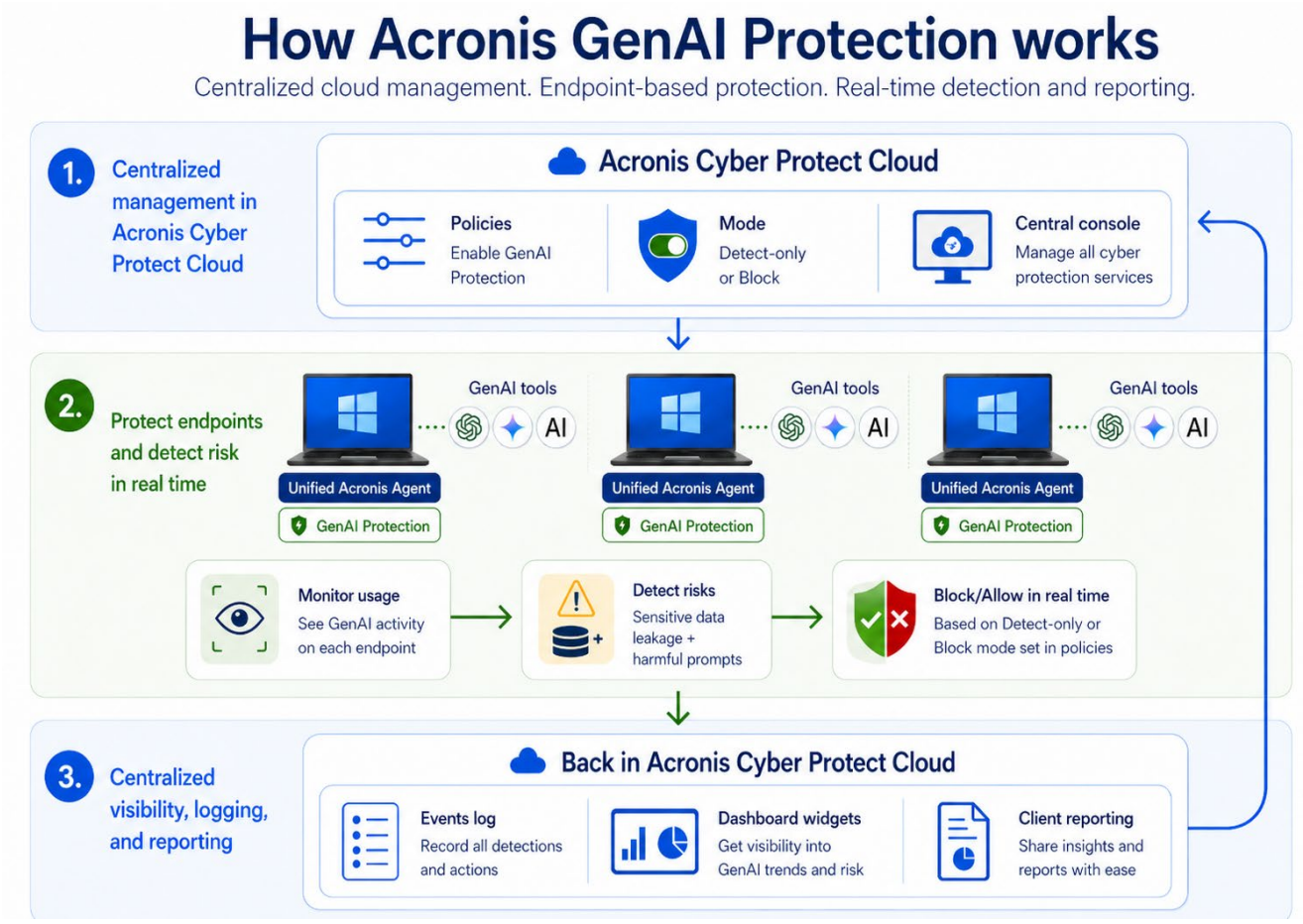
Inspect GenAI prompts for regulated and sensitive data such as PII, PHI, PCI-related data, credentials and confidential information. Block unauthorized submissions to public or unsanctioned AI tools to reduce data leakage and regulatory risk.

Outcome: Protect client data and reduce compliance exposure without stopping productivity.

Stop harmful prompts and AI abuse

Detect and block malicious or policy-violating prompts, including prompt injection attempts and other techniques designed to manipulate AI behavior or bypass controls.

Outcome: Reduce AI-driven attack exposure while protecting workflows and output integrity.



All the functionalities you need, built for MSP operations

Shadow AI monitoring and reporting

Monitor GenAI tool usage across customer environments, including which tools are accessed, by whom and how often. Use reporting and dashboard insights to uncover shadow AI, detect anomalies and support policy decisions.

Sensitive data classification

Inspect prompts for regulated and business-sensitive content, including PII, PHI, PCI-DSS-related data and data marked “Confidential.” Strengthen control over what users can share with external AI services.

Data loss prevention (DLP) for GenAI interactions

Apply data loss prevention controls to GenAI interactions by detecting and blocking unauthorized submissions of sensitive content to public or unsanctioned AI tools.

Harmful prompt detection

Identify harmful prompts and prompt injection attempts designed to manipulate AI behavior, introduce unsafe content or bypass policy controls.

Detect-only mode

Run in alert-only mode to observe AI usage, surface policy violations and build behavioral baselines before enabling enforcement.

Block mode

Activate enforcement mode to automatically stop policy-violating or malicious AI interactions and apply protection consistently across environments.

Centralized events log

Review GenAI-related detections, violations and actions in a centralized event log to support investigation, auditing and policy refinement.

Information-rich widgets

Use dashboard widgets to track GenAI activity, understand usage trends and make more informed policy and enforcement decisions.

Why Acronis

Unlike enterprise-focused AI security tools that add cost, complexity and separate consoles, Acronis GenAI Protection is built for MSPs and integrated into a unified, multitenant platform. It gives service providers a practical way to monitor AI usage, reduce risk and expand security offerings without introducing more tool sprawl.

Turn GenAI risk into a managed service opportunity

With Acronis GenAI Protection, you can:

- Address a fast-growing client concern.
- Differentiate your security offering.
- Enable safe GenAI adoption instead of blocking it.
- Expand revenue without adding operational overhead.

Get 1:1 Demo

Acronis

Learn more at
acronis.com