

The MSP playbook for GenAI Security

Secure the path forward for clients — make GenAI adoption safe

Generative AI is spreading rapidly across SMB environments, often outside formal IT oversight. That creates new risks around Shadow AI, sensitive data leakage, and harmful prompts that MSPs are increasingly expected to manage. Acronis GenAI Protection helps MSPs bring GenAI usage under control without adding another standalone point solution.

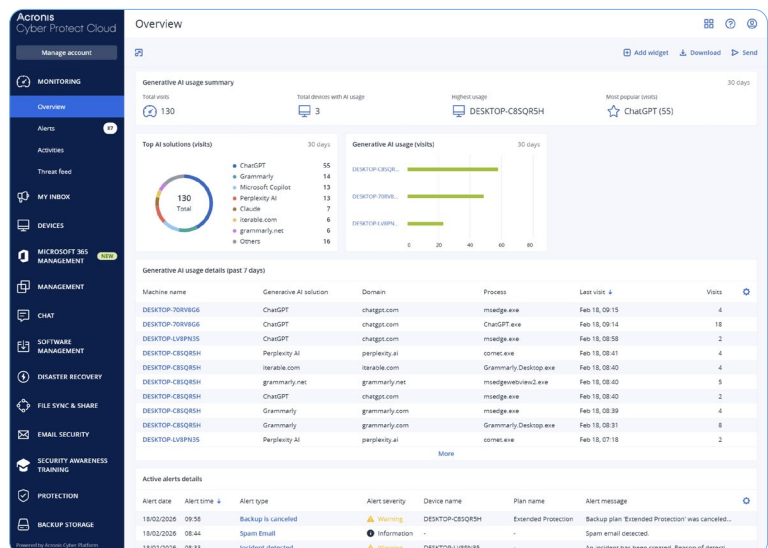
For MSPs with no security focus, this is also a practical way to launch AI-security services, strengthen trusted-advisor value, and expand service offerings without building a specialized security practice and team from scratch.

Top use cases

Bring Shadow AI under control

[SEE DEMO](#)

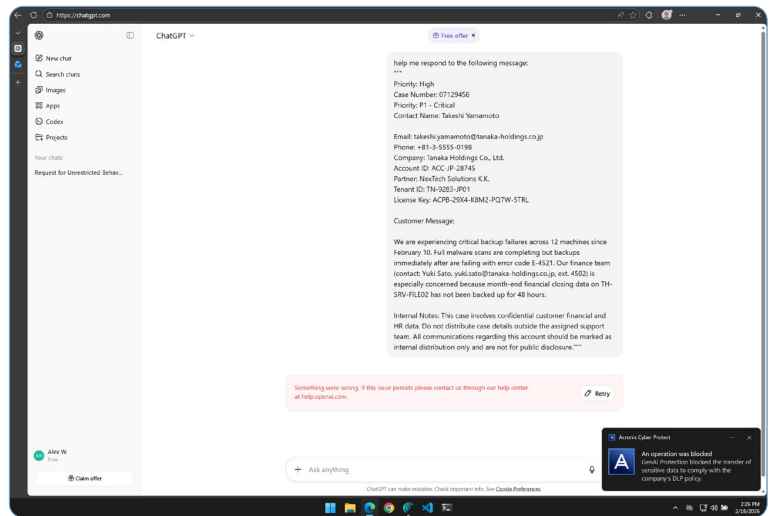
SMBs are adopting browser-based GenAI tools quickly, often without centralized approval, policy, or visibility. Acronis GenAI Protection helps MSPs discover and monitor which GenAI tools are being used across client environments, identify risky or unsanctioned usage, and enforce policy before unmanaged adoption turns into a larger security or business issue.



Protect sensitive data from leaking into public AI tools

[SEE DEMO](#)

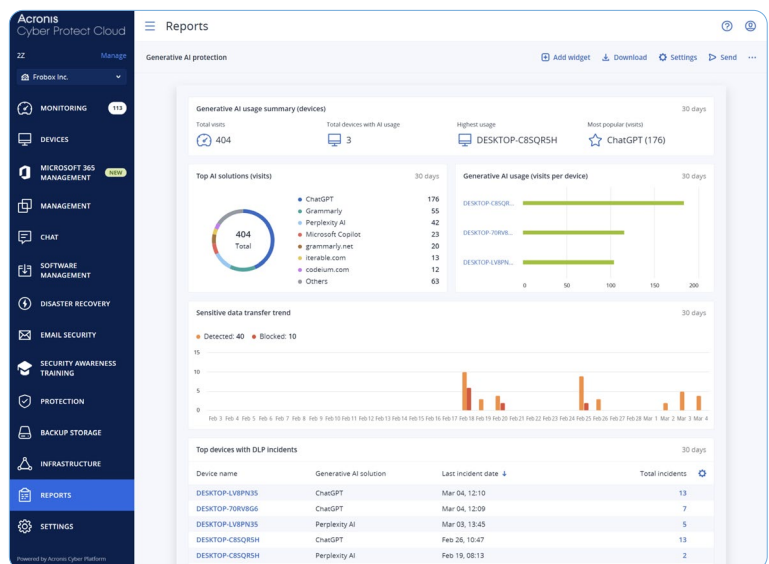
Users routinely paste business information into prompts to accelerate daily work. That creates exposure for PII, PHI, credentials, financial data, and other confidential information. Acronis GenAI Protection helps MSPs inspect prompts for sensitive content and prevent unauthorized submission to public or unsanctioned AI tools — turning “safe AI use” from a policy statement into an enforceable managed service.



Reduce AI-driven attack exposure with harmful prompt protection

[SEE DEMO](#)

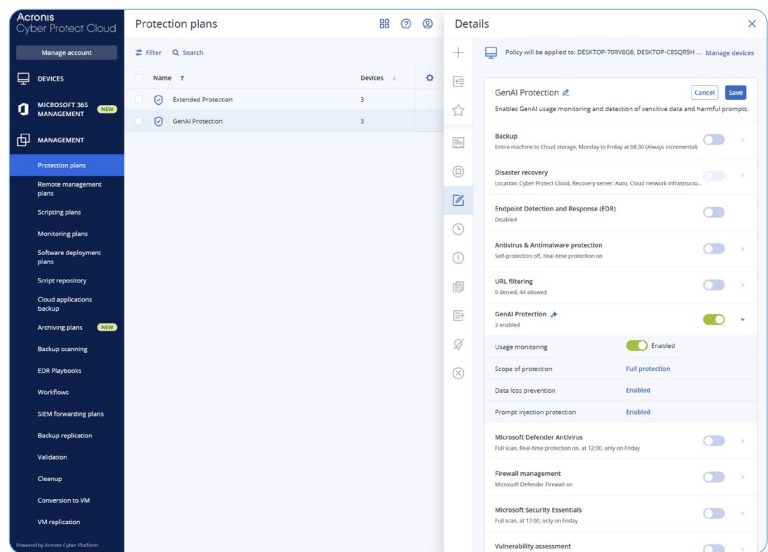
Prompt injection and other harmful prompt techniques are emerging as practical attack vectors. Left unchecked, they can manipulate AI behavior, degrade output integrity, and create downstream security and compliance risk. Acronis GenAI Protection helps MSPs detect and block harmful prompts before they disrupt workflows or introduce avoidable exposure for clients.



Launch AI-security services without enterprise-grade complexity

SEE DEMO

Many AI security offerings are built for large enterprises and delivered as standalone tools with extra consoles, licensing, and integration overhead. Acronis GenAI Protection is built for MSPs and integrated into the broader Acronis platform, giving generalist partners a low-barrier way to add AI-related protection without building a specialized security practice from scratch.



Strengthen trusted-advisor value with practical AI governance

Many SMB clients know AI is valuable, but they do not fully understand the risks or how to govern its use. That creates an opening for MSPs to lead with guidance, visibility, and practical controls. Acronis GenAI Protection helps partners move from reactive support into a more strategic advisory role by helping clients adopt AI more safely and confidently.

Expand service value and stay competitive

GenAI security is not only a new risk area — it is also a new business opportunity. Acronis' partner messaging and enablement materials position GenAI Protection as a way for generalist MSPs to create new revenue streams, remain competitive, and expand security-led service value with accessible pricing and a unified delivery model.

Support safer AI transformation for clients

Clients want the productivity upside of GenAI, but they need a safer path forward. Acronis GenAI Protection helps MSPs support AI adoption without forcing clients to choose between innovation and control. By combining usage visibility, sensitive data protection, and harmful prompt prevention, it gives MSPs a practical foundation for helping clients move toward AI-enabled workflows with greater confidence.

Why Acronis

Acronis GenAI Protection is designed specifically for MSP delivery. It is simple, integrated, and built to fit naturally into the broader Acronis Cyber Protect platform, rather than adding another standalone tool to manage. For MSPs struggling with cost and complexity, that means faster time to value, easier service introduction, and a more practical path to securing GenAI usage across customers.

[LEARN MORE](#)[TRY NOW](#)