safetica

AI Protection

Protect sensitive data while enabling productive AI use

Generative AI is transforming how employees work while creating new, risky paths for sensitive data exposure. As approved and shadow AI use grows, security teams need visibility beyond which tools are being used. They must understand who is using AI, what sensitive data is shared, and where additional protection is needed without restricting the productivity benefits AI provides.

Gain control without blocking AI Tool Access

Safetica AI Protection delivers visibility into AI activity and sensitive data sharing, with granular controls that protect data while enabling employees to use AI productively.

With Safetica, security teams can:

Discover approved and shadow AI use

across your organization to understand which applications employees are using.

See sensitive data in context

including who is sharing it, where it is going, and how it is being used.

Protect data before it reaches AI

with DLP policies by controlling sensitive files, pasted content, prompts, and risky user actions.

Apply granular controls

based on AI application, data sensitivity, employee, department, and activity.

Investigate AI risk with greater context

and determine the appropriate response instead of blocking AI access entirely.

safetica

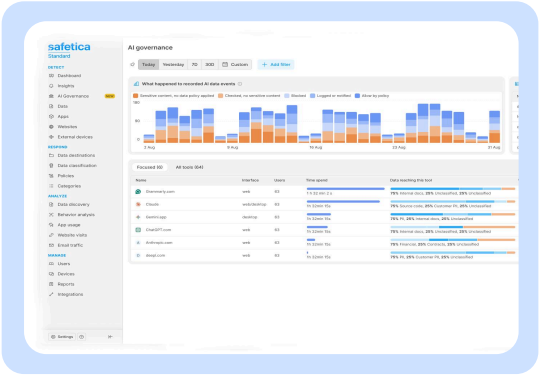
Govern AI use. Protect sensitive data.

Safetica provides layered AI Protection combining visibility into organizational AI use with the controls security teams need to protect sensitive data from exposure and manage risk without impacting productive AI adoption.

AI Governance

Gain visibility and control as employees increase AI activity

Safetica AI Governance helps security teams understand and govern approved and shadow AI use by providing visibility into the applications employees use, the data they share, and where to apply controls. You can:

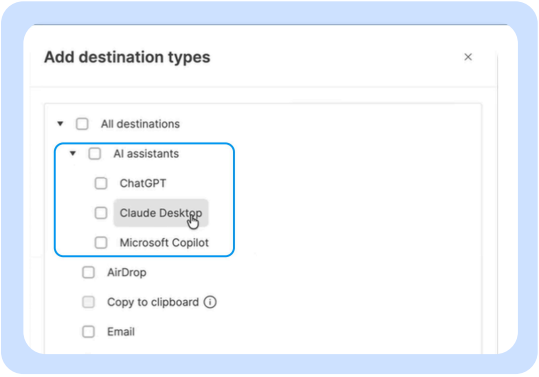


- **Discover your AI environment**. Maintain a centralized view of approved and shadow AI applications across the organization.
- **Understand AI activity**. See who uses AI, how frequently applications are accessed, what data and files are shared, and the current protection in place
- **Turn visibility into control**. Monitor activity, restrict sensitive data sharing, limit access for specific users or groups, or block risky tools entirely.
- **Investigate with context**. Use embedded, AI-guided prompts to explore usage and risk, summarize findings, and identify actions that can strengthen protection.

Data Policies for AI Assistants

Protect sensitive data before it reaches AI

Safetica extends DLP protection to commonly used AI assistants, helping security teams control sensitive information shared through file attachments, copied and pasted content, and prompts while enabling appropriate AI use. Security teams can:



- **Protect sensitive data before it reaches AI tools.** Apply DLP policies to monitor and control sensitive file attachments, pasted text, prompts, and other data shared with ChatGPT, Claude, and Microsoft Copilot.
- **Apply controls based on context.** Define policies according to data sensitivity, AI tool, employee, department, and specific user action, rather than completely blocking AI access.
- **Protect data across application and browser use.** Maintain protection across supported desktop applications and Chromium-based browser experiences on macOS and Windows.
- **Allow productive AI use to continue.** Restrict risky data-sharing actions without unnecessarily blocking productive access to approved AI tools.

With Safetica you get the visibility needed to understand AI use, the context to identify real risks, and the control to protect sensitive data.

SAFETICA INC
99 S ALMADEN BOULEVARD #600
SAN JOSE, CA 95113

+1 (408) 668 1241
INFO@SAFETICA.COM
SAFETICA.COM