

A Global Airline Adopts WitnessAI to Ensure AI Security and Compliance










Introduction

A global airline wanted to ensure safe use of AI by its employees and customers. It tested and purchased WitnessAI as its AI security and compliance solution.




Employee Compliance and Safe Use

The airline handles confidential customer payment and identity information. In addition, the airline develops significant proprietary software and needed to protect its intellectual property. As a global organization, it is subject to a variety of data and user protection regulations in multiple countries. The airline also enforces internal policies regarding aircraft safety and employee AI usage. WitnessAI is used to ensure safe and acceptable AI use by its employees, including:

-  Ensuring customer confidential information is not inadvertently sent to third-party AI applications, such as ChatGPT, DeepSeek, etc.
-  Ensuring that software source code (e.g. for its mobile app) is not inadvertently leaked to third party AI — for example while asking for help optimizing the code.
-  Routing employee prompts to AI models that process for lower costs.
-  Routing aircraft safety guidance prompts to an internal model trained on FAA and airline protocols.
-  Identifying potential malicious insiders who use AI to assist in data or IP theft.
-  Blocking employees from asking AI for aircraft safety guidance.
-  Producing regulatory compliance reports ensuring AI activity controls are in place for GDPR, and other data handling regulations.

Security of Customer-Facing AI Apps

Like many enterprises, the airline is building AI apps to enhance customer support and purchases, driven by large language models trained on internal and customer data. WitnessAI is protecting these AI apps, including:

-  Preventing prompt injection attacks on AI chatbots, to ensure protection of customer data within its LLM.
 -  Preventing jailbreaks, a form of prompt injection intended to bypass model-specific safe use controls.
 -  Preventing unwanted responses, such as recommending a competitor or insulting a customer.
-

Business Value of WitnessAI

The value of WitnessAI for employee compliance and safe use is five-fold: comply with data handling regulations; reduce prompt processing costs by using cost-effective models; reduce chance of data breach and associated costs; protect IP in the form of source code and methods; and ensure protocols are enforced regarding safety advice.

The value of WitnessAI for customer-facing AI app security includes data protection by preventing attacks that would expose customer data; hard-dollar cost savings by preventing prompt-injection attempts from being processed by OpenAI and other model providers. The airline estimated WitnessAI would save approximately \$300,000 per year simply by eliminating OpenAI's 9-cent per prompt processing costs for prompt injection attempts. Finally, the airline protects its brand by using WitnessAI to prevent embarrassing or harmful responses to customers via its chatbot.

About WitnessAI

WitnessAI enables safe and effective adoption of enterprise AI, through security and governance guardrails for public and private LLMs. The WitnessAI Secure AI Enablement Platform provides visibility of employee AI use, control of that use via AI-oriented policy, and protection of that use via data and topic security.

Learn more at witness.ai.

