

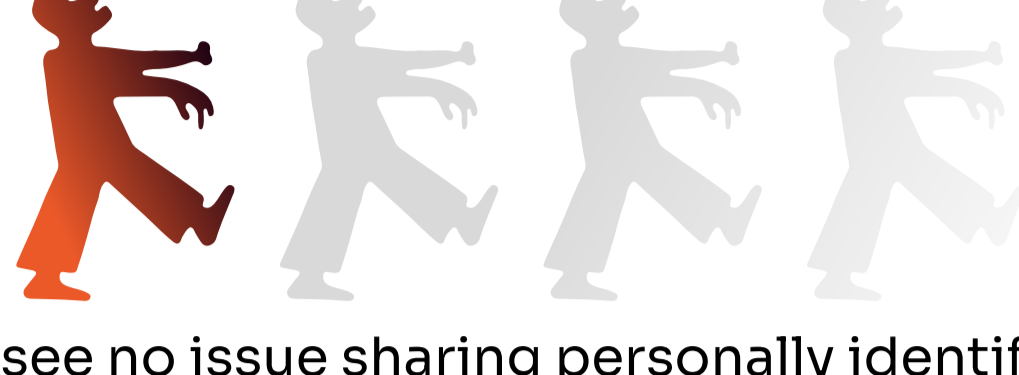
SECURITY IN AI-POWERED CX

Haunted by security nightmares?

The major threats for organizations working with LLMs. If you're using LLMs not vetted for security or thinking of trying to train your own LLMs, read this first.



Employees putting customer information into AI



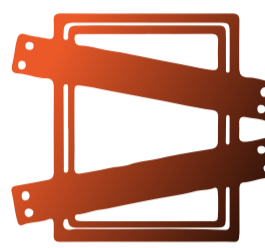
1 in 4 employees see no issue sharing personally identifiable information such as names, email addresses and phone numbers with AI solutions.

Set up guardrails to prevent AI from sharing confidential information outside the organization.



Misinformation

More than 75% of consumers



are worried about misinformation from AI.

AI that's trained on all kinds of data, regardless of accuracy, will spew inaccurate information.



Ethical and Environmental considerations

2 in 5 consumers



are concerned about AI ethics.

AI models consume significant amounts of energy. Ensure any AI solutions you work with follow ethical practices to offset such consumption.



Hallucinations

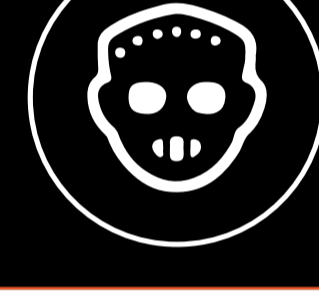
COME HERE



Grok AI from Twitter famously made defamatory statements against NBA star Klay Thompson, accusing him of throwing bricks through windows of multiple houses in Sacramento, CA.

The reason? It "misunderstood" the phrase "shooting bricks."

Language is hard — for humans and AI. Safeguard your customers by rigorously testing the AI.



Lack of Domain Adaptation

Train your AI on domain- and industry-specific language, including your brand-related terminology, so it's aware of the context and nuances.

You

How do I update my WOW TV account?

ChatGPT

If you're referring to your World of Warcraft (WOW) subscription or account management, you typically don't update it in the same way as you would update a game client. However, if you need to make changes to your subscription or account details, you can do so through the Battle.net account management system. Here's how:

1. Visit the **Battle.net Website**: Open your web browser and go to the Battle.net website.
2. **Log In**: Click on the "Log In" button in the top-right corner of the page and enter your Battle.net account credentials (email address and password) associated with your WOW account.



Biases

Eliminate discriminatory biases to make all your customers feel welcome and included.

Customer data you should protect

What customer data should you protect? **Short answer: All. Of. It.**

Personally Identifiable Information

Personally Identifiable Information (PII) is any data that can directly identify or be traced back to an individual.

- Names
- Contact information like addresses, email and phone numbers
- Digital and online identity like social media usernames and IP addresses
- Government-issued identifiers like driver's license or passport numbers
- Physical attributes
- Personal history like property ownership records
- Educational records like student ID or transcripts
- Employment information like employee ID or salary information

Financial information

Any sensitive information related to a person or entity's monetary transactions or other financial activities, like credit card numbers or bank account details.

Personal health information (PHI)

Any personal data related to an individual's physical or mental health condition, healthcare services received, or payment for those services.

Behavioral data

Any information about customer online activities and preferences, like browsing history, purchases and content interactions.

Is your AI compliant?

Your AI should be compliant with one or more of the well known security standards. 98% of organizations prioritize showing their commitment to security through affiliations to external privacy organizations.



The ISO 27001 standard provides companies with guidance for establishing, implementing, maintaining and continually improving an information security management system. **Fun fact: Language I/O is the only translation platform certified against the latest 2022 version of ISO 27001.**



SOC 2 is a security framework that specifies how organizations should protect customer data from unauthorized access, security incidents, and other vulnerabilities.



Comprehensive data privacy laws like GDPR and CCPA govern how organizations can collect, store, and use personal data of individuals.



The U.S. Health Insurance Portability and Accountability Act (HIPAA) requires the companies that work with protected health information (PHI) to implement and follow physical, network, and process security measures.



PCI DSS (Payment Card Industry Data Security Standard) is a set of rules and guidelines designed to help organizations that handle credit card information keep that information safe and secure.