AI Risks in Customer Support Operations

Introduction

AI has revolutionized customer support, but using public or insecure AI tools can expose your business to significant risks. Protect your customers and operations by understanding these threats.

1. Data Breaches

- ⚠ Customer data may be transmitted and stored insecurely, increasing exposure to cyberattacks.
- ⚠ Public AI tools often lack compliance with industry-specific data security standards.

2. Lack of Customization

- ⚠ Public AI doesn't align with your business's unique needs, leading to generic and inaccurate responses.
- ⚠ Poor customer experiences can damage your brand reputation.

3. Regulatory Compliance Risks

- ⚠ Using non-compliant AI tools could lead to hefty fines under laws like GDPR, CCPA, or HIPAA.
- ⚠ Public AI models may not guarantee safe handling of Personally Identifiable Information (PII).

4. Operational Downtime

- ⚠ Public AI tools are not built for mission-critical applications.
- ⚠ Limited support and unreliable performance can disrupt your operations during peak times.

5. No Control Over Data Usage

- ⚠ Many public AI providers use customer interactions for training their models, exposing your business secrets.
- ⚠ Sensitive information may end up in the wrong hands without your consent.

Why Choose Secure AI Solutions?

- ✓ **Data Privacy First:** End-to-end encryption with no storage of sensitive data.
- ✓ **Customized for You:** Tailored to your industry, ensuring accuracy and relevance.
- ✓ **Compliant by Design:** Built to meet global regulatory standards.
- ✓ **Robust Support:** Guaranteed uptime with dedicated customer assistance.
- ✓ **Your Data, Your Control:** Zero usage of your data for external training purposes.

GDPR

SOC 2 Type II

ISO 27001

HIPAA

Auralis AI has built in trust layers with enterprise guardrails and best in class certifications

Protect your business with secure, compliant AI solutions.
Speak to an expert to get started!

Schedule a Consult →

AURALIS