OBSERVE·AI

The Generative AI and GPT Security Cheat Sheet for Contact Centers

Contact centers handle a variety of sensitive customer data, including credit card numbers, personal information, and (for highly-regulated industries) a host of potential health or financial details.

We've assembled an extensive list of security questions to ask when identifying a Generative AI solution for your contact center:

---

01 Data Privacy and Storage:

- ☐ Where is the data stored?
- ☐ What privacy laws govern the stored data?
- ☐ Does the AI provider comply with GDPR, CCPA, and other relevant data protection regulations?
- ☐ What controls are in place to ensure data is not used beyond its original purpose?
- ☐ How long is the data retained and how is it securely disposed of when no longer needed?

02 Data Access:

- ☐ Who has access to the data and under what conditions?
- ☐ Are there strong access controls and authentication processes in place?
- ☐ How does the provider ensure that data isn't misused by those who have access?

03 Data Transmission:

- ☐ How is data protected during transmission?
- ☐ Does the provider use encryption protocols like Transport Layer Security (TLS) to protect data in transit?

04 Training Data

- ☐ What data was used to train the AI?
- ☐ How was the data anonymized and is there any risk of de-anonymization?
- ☐ How is the proprietary data protected during AI model training?

05 Security Certifications:

- ☐ Does the provider have third-party security certifications (like ISO 27001, SOC2, etc.) that verify their security posture?
- ☐ How regularly are these certifications reviewed and renewed?

06 Security Incident Response:

- ☐ How does the provider respond to security incidents or breaches?
- ☐ Is there a robust incident response plan in place?

07 AI Ethics and Bias

- ☐ How does the provider handle ethical issues like AI bias?
- ☐ What measures are in place to ensure the AI's outputs are fair and unbiased?

08 Vulnerability Management:

- ☐ How does the provider protect against vulnerabilities in the AI, including adversarial attacks?
- ☐ What is the patch management policy and how quickly are vulnerabilities resolved?

09 Predictability and Transparency:

- ☐ How transparent is the AI system's decision-making process?
- ☐ Is there a possibility of the AI making uncontrolled, unsupervised decisions that could impact security?

10 Future-Proof Security:

- ☐ How does the provider plan to keep up with evolving security threats and trends?
- ☐ How is the system designed to handle emerging security issues in the AI landscape?
