SAFEBASE

Eleven Questions to Answer About Your AI Security Posture

The consumerization of artificial intelligence has turned the business world upside down. As technology providers of every stripe scramble to enhance their product offerings with AI, cybersecurity, GRC, and legal teams are working together to develop company-wide AI security guidelines to keep their data and employees safe.

> **As your company begins to offer AI-enabled capabilities, it's critical that you can effectively communicate how your products are optimized to reduce AI security risks.**

In this guide, we have the top eleven questions your organization should be prepared to answer to demonstrate the safety of your AI products, as well as best practices for communicating your artificial intelligence security posture now and in the future.

Top eleven AI security questions to answer

Buyers of your AI-enabled products, like buyers of any enterprise technology in this day and age, are likely to conduct a thorough third-party risk assessment. They may include a security questionnaire as part of that process, seeking insight into the security controls your company has in place.

When it comes to AI security, buyer questions will likely cover the use of customer data in your training models, internal policies and training on AI, and ongoing safety monitoring. It will be in your team's best interest to proactively develop answers to these questions, saving your team time while demonstrating your commitment to proactivity – a key driver of customer trust.

Based on our experience working with hundreds of trust-minded organizations, we've compiled a list of the top eleven questions around artificial intelligence and cyber security your company needs to be prepared to answer:

1. **Do the organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements?**
2. **Will customer data be used to train artificial intelligence, machine learning, automation, or deep learning?**
3. **Does the organization have an AI Development and Management Policy?**
4. **Does the organization have policies and procedures in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems?**
5. **Who is the third-party AI technology behind your product/service?**
6. **Has the third-party AI processor been appropriately vetted for risk? If so, what certifications have they obtained?**

Take time to document thorough responses to each of these questions and house them in a place that is easily accessible to customer-facing team members.

If you've already created a Trust Center, you can publish the responses to these questions in your private or public Knowledge Base for easy access.

7 **Does the organization implement post-deployment AI system monitoring, including mechanisms for capturing and evaluating user input and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management?**

8 **Does the organization communicate incidents and errors to relevant AI actors and affected communities and follow documented processes for tracking, responding to, and recovering from incidents and errors?**

9 **Does your company engage with generative AI/AGI tools internally or throughout your company's product line?**

10 **If generative AI/AGI is incorporated into the product, please describe any governance policies or procedures.**

11 **Describe the controls in place to ensure our data is transmitted securely and is logically and/or physically segmented from those of other customers.**

Communicating AI security for maximum effectiveness

When it comes to sharing your AI security stance with buyers and customers, responding to these questions is only the first step. You also need to consider how you communicate your responses, taking an intentional approach to inspire customer trust.

Default to openness with your buyers and customers

Given the ever-uncertain nature of AI and its impact on cyber security, transparency has never been so important. In an environment such as this, a lack of transparency will be a major red flag for your buyers and customers.

Approach buyer and customer conversations about your product's AI safety with as much openness as possible. Make it easy to find and understand your responses to their questions, aggregating information in one central location and providing information and documentation in clear terms.

To make transparency achievable, some organizations find it helpful to establish clear guidelines for what information must remain restricted to particular audiences and why. Any documentation that doesn't meet that criteria remains open to all audiences by default.

Share your responses about AI security proactively

The organizations best poised to build and maintain customer trust in the age of AI will be the ones that don't wait to be asked about their AI security. Instead, they make documentation and information regarding security available to buyers and customers proactively. Often, this takes the form of sharing security documentation before an official buyer security review has been requested.

When communicating about your artificial intelligence security, an orientation toward proactivity will send buyers and customers a signal about the strength of your security posture. Consider passing along a link to your top eleven question responses during the early stages of the sales cycle. This effort will inspire confidence in your product security from the get-go and, as an added bonus, may mitigate the need to respond to a security questionnaire.

Empower your internal stakeholders with AI security information

Building and maintaining customer trust in the age of AI is a team effort. Ensure that all customer-facing touchpoints, including sales, customer success, and even marketing, have access to your responses around AI security risks and are equipped to leverage them should questions arise.

Take the time to educate them on your AI security stance and empower them to be stewards of your company's security posture in their ongoing conversations with buyers and customers.

Maintain the integrity of your responses in real time

As artificial intelligence cyber security guidelines evolve, the details of your AI security stance may change on a dime. Make sure you're prepared to keep them up to date by building systems and leveraging security review technology that will allow you to easily make changes to your responses and add new questions and responses to your database as they come up.

Also critical will be the ability to push out new or updated content proactively to internal stakeholders, buyers, and customers. Ensure you have the systems in place to regularly communicate updates to your policies and protocols to all those who need to be in-the-know.

Gather feedback to optimize customer trust

Finally, you'll want to create mechanisms for internal and external feedback. Are your responses to the top questions useful and clear? Are you or your team members routinely receiving pushback or follow up questions to the information you share? Ensure that you have channels or dashboards set up to help you understand the impact of your efforts and guide your strategy.

Building customer trust in the age of AI

The business world's understanding of the impact of artificial intelligence and cyber security is just beginning to form. As AI changes rapidly, documenting your responses to these eleven questions is just the first step in an ongoing effort to build and maintain customer trust.

Expect to add to, edit, and communicate your evolving AI security stance to buyers and customers as time goes on. An intentional effort to create transparency and proactivity around your AI-enabled product and features will go a long way towards creating solid, meaningful customer relationships in the age of AI.

SafeBase is the leading Trust Center Platform designed for friction-free security reviews. With an enterprise-grade Trust Center, SafeBase automates the security review process and transforms how companies communicate their security and trust posture.

If you want to see how fast-growing companies like LinkedIn, Asana, and Jamf take back the time their teams spend on security questionnaires, create better buying experiences, and position security as the revenue-driver it is, schedule a demo.

SAFEBASE