AI CERTs™

# AI Application Security

# AI Application Security

***A strategic imperative***

Security of AI application is crucial in order to maintain the integrity and consistency of application. Since there is increasingly more reliance on the AI system in all sectors with varying degrees, there is urgent need to focus on the security aspects of AI applications. The second important point is that AI applications interact with various data sources resembling unified sources of information for all the needs. This very nature of AI makes it vulnerable to malicious attacks and cyberattacks.

## LLM and other domain-specific AI applications

LLM is the most common example of GenAI which works on prompt engineering. Apart from this, there are domain-specific AI applications which deal with sensitive data of customers, patients, supply chains, legal structures, taxation, and many others.

## Ignoring security at your own peril

Security aspect of application takes backstage because of emphasis on quicker development cycle and timeline. The focus on development, while important, ignores the crucial aspect of security features of the application. However, with DevOps being the focus of application development, operation is also considered as important.

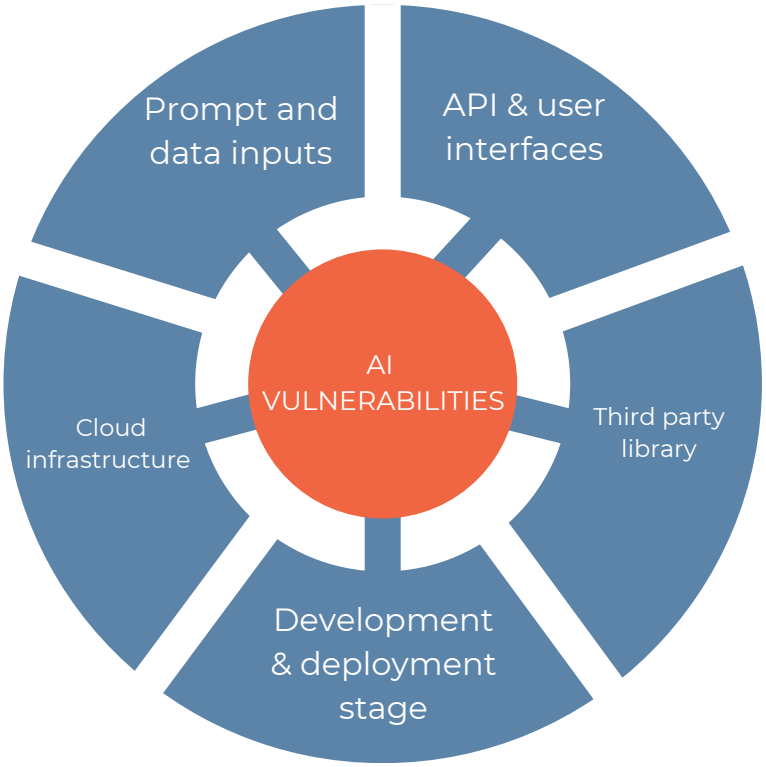
## Security is the key to building a reliable AI application

Development team, project leaders, product managers, and executive leadership must ensure that security is integrated to the development cycle of AI applications. They need to interact with open-source community where security practices are discussed and developed. Integrating security into the AI application development lifecycle is vital to ensure the security of AI system.

## Cyberattacks vulnerabilities

There are various ways cyberattacks can happen but some of the most vulnerable and damaging attacks can happen on the following:

- Prompt and data inputs
- API & user interfaces of AI applications
- AI model, especially in development & deployment
- Third party library
- Cloud infrastructure



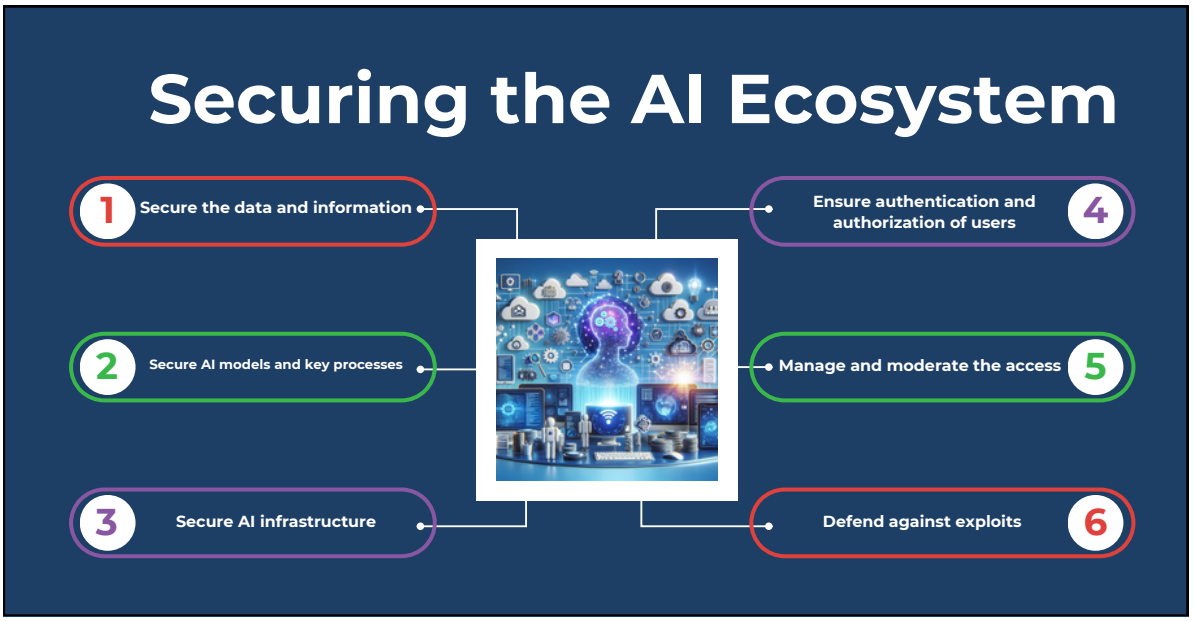

This means we have to secure the entire ecosystem of AI development and deployment including the infrastructure, whether in-house or on the cloud. Considering the importance of various components of AI ecosystem, these three aspects must be defended and secured with utmost importance.

- Data – Data is the key to any AI model. The leakage or attack can cost billions.
- AI models – Any attack on AI model will compromise the integrity of application responses.
- AI infrastructure – Attack on AI infrastructure can shut down and make it ineffective.

## Securing your AI ecosystem

Securing AI applications and infrastructure requires meticulous planning and implementation. Here are quick 6 major ways you can secure and fend off against any attack.

- Secure the data and information
- Secure AI models and key processes
- Secure AI infrastructure
- Ensure authentication and authorization of users
- Manage and moderate the access from time to time
- Defend against exploits on specific time such as development and test period and on the deployment day.



## Conclusion

AI provides immense flexibility and efficiency to the organization. While its integration with the core operational processes is important for an organization to succeed, the security of AI system is vital for protecting secured data, maintaining integrity of information, and ensuring reliability and trust in the system. Fortunately, securing AI is not difficult if organizations make robust security principles an integral part of AI development and implementation.

AI CERTs™

www.aicerts.ai

**Contact**

252 West 37th St., Suite 1200W
New York, NY 10018