**Supporting View:** Data science will assist in breach detection and prevention of cyber fraud. Artificial Intelligence would aid in surpassing the human capacity to detect and mitigate threats. AI allows them to respond to breaches faster by analyzing terabytes of data, detecting the anomalies and predicting the moves of cyber criminals.

The system can check a threat in the existing database, detect similar patterns with smart algorithms, and create a counterattack strategy. With time, such a system gets better at detecting and facing unknown threats, maximizing its speed and efficiency.

Detecting viruses: Artificial Intelligence can analyze terabytes of data in the incredibly short period of time; quickly uncovering suspicious code fragments;

Predicting the moves of cybercriminals: AI solutions can analyze existing threats, security news, and tendencies to forecast possible developments.

Optimizing the functionality: AI can create smart insights that will help businesses improve their software and lower the chances of the next attacks.

Fast detection: Artificial Intelligence analytical and monitoring capacities far exceed human beings. unlike typical processing methods, AI has a smart insight: the technology is capable of facing unknown threats and building response strategies from scratch.

Quick response: AI operates in seconds, quickly going through terabytes of data. With AI and ML security solutions, even big corporations are able to detect threats in seconds

**Opposing View:** Data science doesn’t really help and it can backfire in the hands of hackers. Hackers are embracing the machine learning algorithms behind the technology’s success to create nuanced attacks personalized for specific individuals. Because AI can be “taught” with data sets, hackers can either create their own programs or manipulate existing systems for malicious purposes.

Hackers may also modify enterprise machine learning algorithms by altering inputs to change the way the system recognizes specific elements. This technique can be used to make the system overlook threats and allow hackers to bypass identity and access management controls.

System behaviors are potential targets, as well; with the right modifications, hackers can change the way devices respond or communicate, which may result in dangerous outcomes. Once system information has been changed, it can be very difficult to correct problems and return the network to its original state.

Cyberthreats evolve: Viruses and malware improves all the time, and even AI systems will need constant redesign, improvement, and maintenance.

High adoption barrier: Artificial Intelligence still requires al lot of human resources and computing power, compared to typical antiviruses. You can simply install a ready software rather than spend time and money on building a custom AI solution.

**Supporting View: Data science will assist health care organizations to rollout vaccines for COVID. It can harness machine learning to schedule vaccines, streamline patient communications and even prioritize access.**

**AI enabled digital call centers can help organizations manage the significant level of interest in key vaccine information.**

**There is a chance that reproducing bias or using faulty algorithams can identify who need to get vaccinated incorrectly**