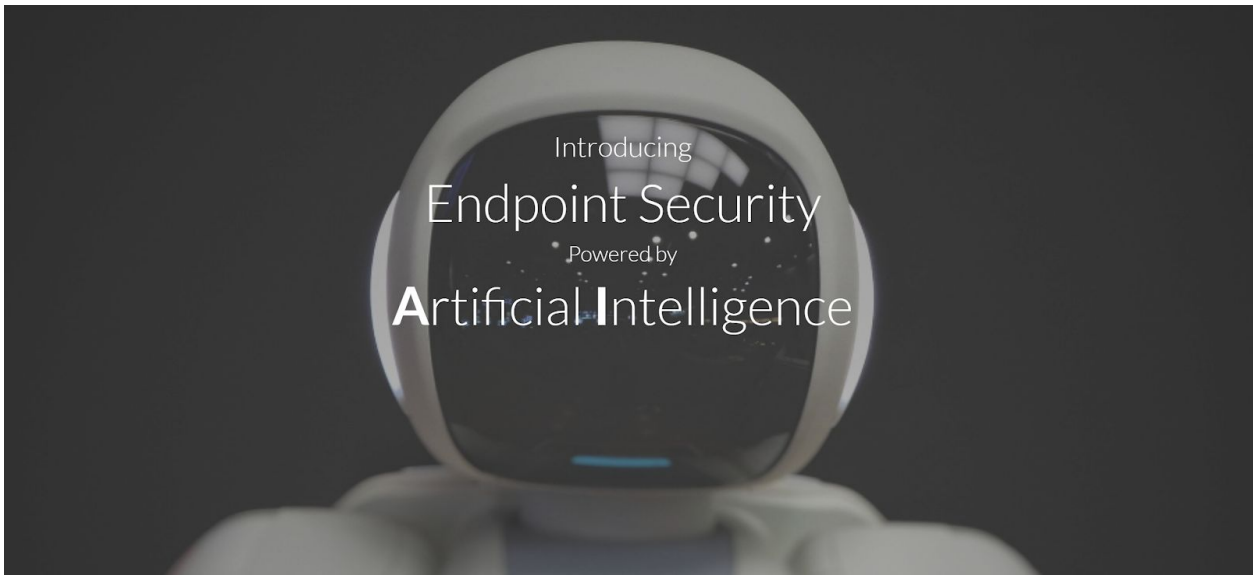
The power of Artificial Intelligence in IT



Artificial Intelligence is the latest buzzword in the world of technology. Experts believe that many aspects of our lives are already affected by Artificial Intelligence (AI) and Machine Learning (ML). So far, Machine Learning has been known for its power to enable robots with logic required to mimic and perform tasks traditionally done by human. An example of these robots could be automated teller machines that are widely used across the world. Programmers use AI to identify repetitive and routine work (performed by human) in order to create such logic. Once patterns and workflows are clearly defined, work can be completely delegated to a robot. Any changes to the logic will then require a simple code change.

The use of Artificial Intelligence, however, can not be limited to workflow automation. As businesses become more dependent on technology, the need to safeguard information that flows within the business operation arises. Cybersecurity professionals have begun to use AI and ML to protect business IT infrastructures from malicious attacks. Companies of all sizes are now the target of cyber attacks. Many large corporations and even government entities have been the victims of such attacks. Unfortunately, the number of attacks, financial losses resulted from them, and the volume of ransom

payments made to retrieve stolen information have all kept rising in the past decade.

Aside from financial data, many companies nowadays are concerned with the safety of their intellectual properties and trade secrets. Obviously, the risk of cyber attacks goes up as the number of devices and users connected to a company network increases. Responding to a company email on a personal mobile device is a norm and many companies don't even understand the risks associated with such behavior. Basic cyber security training is either missing from employee manuals or limited to a couple of sentences on the use of social media channels at work. This is all when the frequency and severity of cyber attacks continue to increase. Moreover, Cybercriminals constantly look for new and creative ways to sneak in and steal information, executing highly sophisticated attacks that leave no trace.

As much as we like to believe in human ingenuity, many of the threats against computer systems simply cannot be controlled or prevented by human. Today, companies rely on many web applications, connected networks, and remote workforce to get work done. Managing all users and applications at all times is a time-consuming and expensive task which cannot be performed by one or two people or a set of traditional security equipment or hardware.

This is where Artificial Intelligence (AI) shines. Machine Learning (ML) can be applied to not only monitor networks but to also identify and isolate abnormal behavior as potential risk, even if there's no record of it anywhere ever before. The next generation of cyber security products use the power of AI to detect threats and stop suspicious files from accessing the company network. This allows cyber security professionals to evaluate files that are quarantined by the software, determine the risks associated with them, and make informed decisions.

The biggest advantage of an AI enabled cyber security solution is in its core ability to find patterns in malicious behaviors recorded by the machines. The

advanced learning ability can then be used to prevent attacks that share certain characteristics found by the machine in the past or in other networks. This alone can save companies a lot of time and money currently spent on purchasing new technologies just to safeguard against unknown threats as the newer and more aggressive attacks are designed and deployed. Unfortunately, AI is also used by cyber criminals to find vulnerabilities and spread the threat faster. Pentagon released a report on the use of AI as well as investments made by countries such as China and Russia in machine learning in order to raise awareness about this topic. While this is a national security concern for Pentagon, we believe that it's time for the business community to pay attention the risks and evaluate the costs and other implications of not building proper defense mechanism to prevent even more sophisticated attacks powered by AI.