# How to Fortify Your Defense Perimeter with Artificial Intelligence

The world as we know it today is prone to just about any kind or type of Cyber Security threat or risk.

In order to combat this, there are many mechanisms in place which a business or a corporation can use. These range all the way from software to hardware based solutions.

Although all of the above mentioned are effective counter measures, there is one flaw to them: They can only prevent security breaches to a certain as they are happening. But how about having the ability to predict security breaches ***before they even occur***? This is where the role of Artificial Intelligence (also known as "AI") can come into play.

What is it exactly? It is defined as: "The development of computer systems which are able to perform tasks that normally require human intelligence, such as that of visual perception and decision making".

So, for example, a specifically designed Artificial Intelligence package can examine the underlying software code of a piece of Malware or a Spyware (such as that of a Trojan Horse). It can proactively discover and analyze the unique characteristics of the code, and from there, build a "Threat Vector Profile". The end resultant is a huge repository of these profiles.

Once all of this information and data is "learned" by the Artificial Intelligence package, it can then be deployed on the front lines of defense to help thwart off the Malware and the Spyware. One of the strongest advantages of Artificial Intelligence is that it can use various modeling techniques to even predict what future Cyber-attacks could potentially look like.

From this, a business or corporation can then determine the exact security technologies that they need in a logical fashion.

Other advantages of using Artificial Intelligence in Cybersecurity include the following:

1) It can detect and/or predict a Cyber threat in just less than 100 milliseconds.
2) It can detect Cyber threats which can affect any critical component of the IT Infrastructure, ranging from the hardware to the software applications to the memory systems and the databases.
3) It is constantly learning about the unique characteristics of Cyber threats and risks in real time, 24 X 7 X 365.
4) It offers a ***proactive*** stance to combatting Cyber threats, rather than a ***reactive*** one. This simply means that a business or a corporation can avoid the damage before it actually happens.
5) It utilizes a concept known as "Machine Learning"-meaning, it has the ability to change its learning techniques as it is being exposed to newer Cyber threat data.
6) It encompasses the concepts which are used in Data Warehousing. It can discover the most hidden trends in a large data set (which no human could possibly find) and make it relevant/useful to the situation at hand.
7) It can distinguish between intentional and unintentional risks. From here, the appropriate alarm bells can be set off (legacy security technologies do not possess this capability, so in this situation, even an unintentional action would still set off the alarm bells, wasting the critical time and resources of the IT Security staff).

In conclusion, the use of Artificial Intelligence will be probably the best form of security that a business entity can implement. The level of sophistication of these tools is occurring on a daily basis. But best of all, Artificial Intelligence Tools are very affordable to procure and implement-even the smallest of the SMBs can afford them.