EMA Vendor to Watch: Deep Instinct

About Deep Instinct

Deep Instinct provides an on-device, anti-APT/zero-day malware solution. Deep Instinct is currently unique in the marketplace. It is the only commercially available cyber defense solution that uses a cutting-edge technology called "deep learning." Deep learning is the next generation of artificial intelligence that uses the concept of brain synapses in its design and operation to mimic the function of the human brain for learning and decision-making. Founded in 2014, Deep Instinct Israel is headquartered in Tel Aviv. Deep Instinct USA is headquartered in San Francisco, CA.

VENDOR TO WATCH

Deep Instinct – October 2015
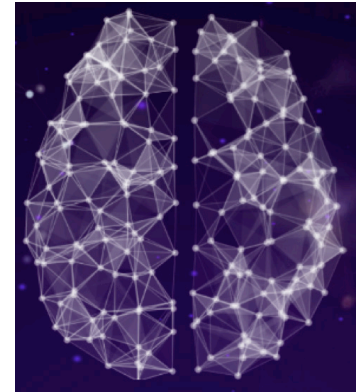
Figure 1. Proprietary state-of-the-art algorithms learn to identify malicious objects in real time.

What Deep Instinct Does

Deep Instinct's solution brings deep learning to cybersecurity for the first time. Usually within the purview of research labs, deep learning has most often been applied to language translation, voice and image recognition, and other cognitive fields. Deep Instinct uses deep learning's ability to process data from any source—PCs and mobile devices—to provide complete protection on any platforms and operating system.

Using deep learning, data is broken into its smallest parts—what the deep learning experts call "fragments." These fragments are processed by the artificial synapses to learn to evaluate whether the data from the file (e.g., app, pdf file, audio file, etc.) is malicious or benign. This prediction process occurs in milliseconds on the device itself and requires very few system memory and processing resources, operating behind the scenes without hindering user performance. Furthermore, this process can take place even when the device is not connected to the Internet (e.g., when a device is in airplane mode).

Though on the surface this technology appears to be much like machine learning, which is the current tech buzz, according to experts in the field, deep learning's underlying structure renders more accurate decisions faster. Deep Instinct's solution continuously learns from the ongoing analysis of both malicious and benign files in both structured and unstructured data sets. Just like a real brain, each evaluation more finely hones its deterministic capabilities. The more training, the more accurate its decisions. Thus, Deep Instinct's solution provides effective protection for endpoints and mobile devices against zero-day malware and APT attacks that require instant identification.

EMA Perspective

This solution is compelling, particularly as attackers constantly create new malware variants that cannot be detected by signature- or heuristic-based solutions and cannot be detected and prevented in real time using sandboxing solutions. This type of proactive learning solution can achieve detection, prediction, and prevention for advanced, persistent cyber threats, whether known or unknown. Real-time identification, utilizing a deep learning prediction model, prevents known and unknown malware from harming the system. This ongoing, proactive protection should be appealing to enterprises to protect their assets against constantly evolving cyber threats.

Deep Instinct uses a new approach of comprehensive, proactive protection. As for the technology, there is not much competition in the deep learning space at this time, as the few other pockets of technologists and academics that understand deep learning and have any sort of operational technology have been acquired by big vendors like IBM, Apple, Google, Facebook, and Baidu.

In a time when cyber-attacks are rampant and personnel resources are few, technology, such as that offered by Deep Instinct, can take a large part of human effort out of endpoint and mobile device's protection and remediation by replacing human detection with intelligent systems needed for automation and scale. We will be seeing more of this technology.