DEEP LEARNING & CYBERSECURITY

“Just as electricity transformed almost everything 100 years ago, today I actually have a hard time thinking of an industry that I don’t think AI will transform in the next several years.”

- Andrew Ng (Co-Founder of Google Brain)

These words spoken by Andrew Ng, a world leading computer scientist, imply volumes of the potential that AI has in touching every aspect of our increasingly digitized lives. Indeed, AI and its latter incarnations, machine learning and deep learning are revolutionizing the way we conduct business, shop, educate, socialize, and no less protect ourselves from impending threats.

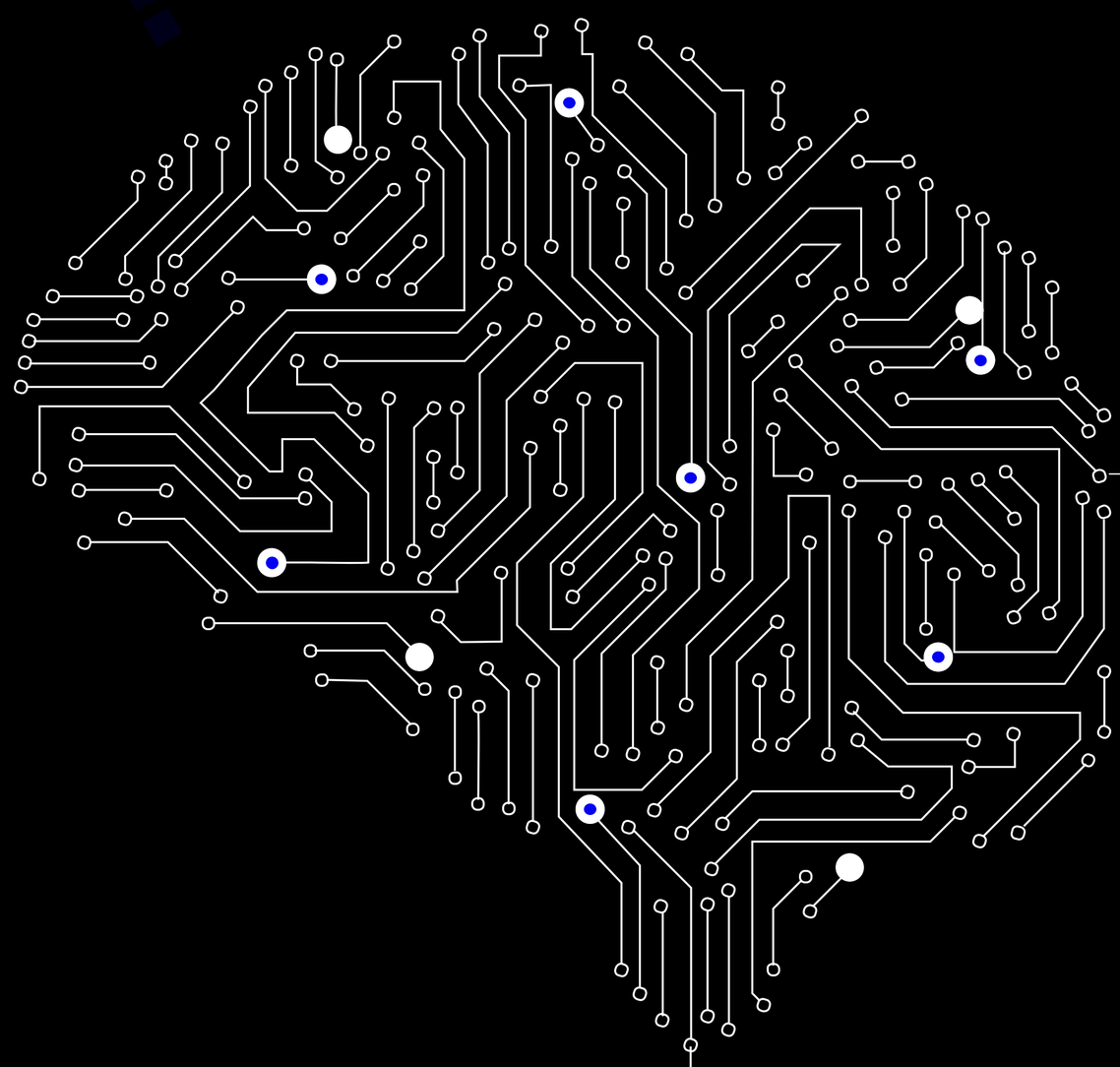
As more aspects of our lives take place on a digital sphere, it will need to be a major priority to keep that sphere safe and free from attack. This increasing digitization will not only make cybersecurity more pertinent than ever before, but the cybersecurity tools we use, will need to employ the most advanced form of AI to ensure that it’s up to the task.

We are entering an era where defeat and victory will be determined by one’s technological advantage. And considering what's invested, it’s a challenge that no one can afford to lose.

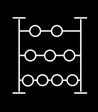
FROM THE BRAIN TO AI

The brain – a mere 3 pounds/1.4 kilos - is the result of eons of evolution, delivering the ability to analyze complex situations and data within less than 150 milliseconds.

The processing infrastructure of the brain, the neural network, consists of at least a hundred billion neurons receiving, processing, and transmitting information via electrical and chemical signals to other neurons via synapse pathways.



HUMANKIND HAS SPENT MILLENNIA TRYING TO REPLICATE THAT PROCESSING POWER.

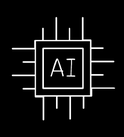


3000 BCE

The first abacus was recorded to have been used in Ancient Mesopotamia between 2700-2300 BCE.

1950

Exploration of AI began in the 1950s using the most primitive computers, taking up full rooms with their machinery and thousands of vacuum tubes.

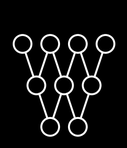


1980'S

AI in its most basic form involves mimicking human logic and its way of thinking. It can be as simple as rule-based decision making, decision trees etc. In the 80’s a new family of AI algorithms emerged called “Machine Learning”.

1997

On May 11, 1997, IBM’s Deep Blue, one of the first artificial intelligence-based computers, beat Garry Kasparov in a six-game chess match.



2010'S

Over the course of the decade, deep learning has achieved 20 to 30 percent improvement in most benchmarks of computer vision, speech recognition, and text understanding. Now, outperforming human beings, it’s the greatest leap in performance in the history of AI and computer science.

THE TERMS ARTIFICIAL INTELLIGENCE AND ITS SUBCATEGORIES OF MACHINE LEARNING AND DEEP LEARNING HAVE BECOME UBIQUITOUS IN MARKETING HYPE. THEREFORE, IT´S ESSENTIAL WE UNDERSTAND THE DIFFERENCES BETWEEN ALL THREE AND THE WAY THEY CAN EACH BE

TRADITIONAL MACHINE LEARNING

ACHIEVEMENTS & DISAPPOINTMENTS

Traditional Machine Learning (ML), which has been available since the 1980's, gives computers the ability to learn on a defined data set, and then based on that learning, to take decisions without being explicitly programmed. It requires the ML processing system to be trained with data samples before it can make decisions on its own.

To prepare the dataset, the domain expert data scientists must first cull the complete data set to carefully select the data samples, performing manual feature engineering to extract relevant attributes to create a vector of features. These samples are used to intelligently train the algorithms to detect and to minimize mistakes, known as 'false positives', and correctly identify data.

TRADITIONAL MACHINE LEARNING

1. RAW DATA
2. MANUAL FEATURE ENGINEERING
3. VECTOR OF FEATURES
4. MACHINE LEARNING

THERE ARE MAJOR LIMITATIONS IN THIS PROCESS INCLUDING:

LIMITED TO HUMAN EXPERTISE

The data features are "selected by humans," so they are vulnerable to misrepresentation, as they are limited to the researcher's knowledge and experience.

LIMITED IN ITS ANALYSIS

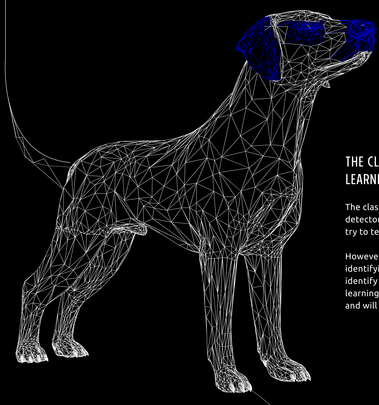
In the manual selection of features, on average, the researcher extracts just a fraction of the available data. As most of the data isn't used or analyzed, the machine can only learn from specific details and cannot analyze the full picture from all characteristics in the data set.

LIMITED SCALABILITY

Although machine learning can scale across diverse datasets, there is an information threshold, which if reached, additional data training doesn't provide any further accuracy.

LIMITED BY RESOURCES

Developing the framework is highly labor intensive, it requires domain experts to constantly fine tune features and their representations.



THE CLASSIC USE CASE OF A TRADITIONAL MACHINE LEARNING CHALLENGE IS IMAGE RECOGNITION

The classic example of a machine learning challenge is the dog detector. We can show the machine thousands of pictures of dogs to try to teach it to identify dogs.

However, what does it do, when it has images of cats that have all the identifying features of images of dogs? The algorithm will incorrectly identify the cat as a dog! The challenge is that in traditional machine learning, identifying dogs is different than separating cats and dogs and will require a completely different set of features.

THE POSSIBILITY FOR ERROR IS ENDLESS

The quality of the data samples used to train the algorithm is critical. It can be difficult to distinguish the samples if they are too similar to each other.

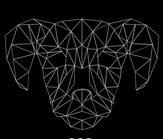
The specific data points the data scientist may select, such as ear, eye, and nose size ratios or fur coloration, may make it easier for the machine to identify that larger dogs are dogs, but for smaller dogs – or animals that look like dogs, such as cats, it can lead to significant confusion.

While we can instantly tell the difference between a Pomeranian dog and a Russian Blue cat, the machine learning algorithm cannot.

The confusion continues when the pictures contain interference, where part of the image is concealed by something else. All these factors lead the algorithm to form a wrong conclusion when it is labeling the sample.

Most of the patterns and correlations in raw data are too complex for any human to specify, no matter how talented. That's why machine learning is limited. We can't teach it what we don't articulate ourselves.

Deep Learning bypasses the entire process of feature engineering and these possibilities for error.



DOG

DOG

DOG

CAT

MAKING THE COMPLEX SIMPLE

The more sophisticated security products tend to use traditional machine learning. Although very accurate at detecting a wide range of known attack vectors, machine learning loses its ground when detecting never seen before attacks, particularly malware that has a unique configuration. This is due to the limitations of the algorithms, where unique and unexpected forms of malware, could slip by undetected.

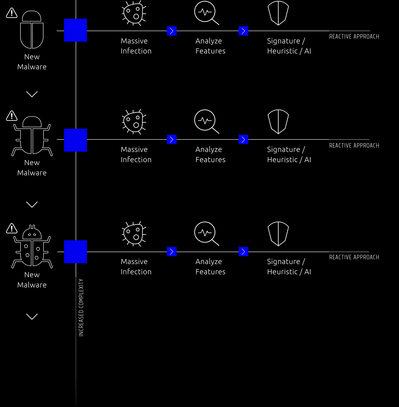
FAILURES OF THE CURRENT APPROACH TO CYBERSECURITY

Every organization has the basics of cybersecurity protection - antivirus software, firewalls, etc. Time and time again, these are proven inadequate against the sophistication and complexity of attacks, like file-less attacks, zero-day attacks, and attacks that don't follow the predefined, "expected" formula of malicious activities.

For the past several years, organizations have discovered that their prevention was far too porous, forcing them to shift their focus to an "assumed breach" approach, where the imperative is to hunt after the attack after it's penetrated the perimeter.

Therefore, most enterprises have installed traditional machine learning-based systems to find the attacks that are already operating within their system; the average time it takes to detect these attacks ranges from minutes to months and occasionally, years. But, even during the shortest period of attack, significant damage is being done.

THE EVOLUTION OF MALWARE



DEEP LEARNING INFRASTRUCTURE

DEVELOPING AN ARTIFICIAL BRAIN

Similar to the human brain, the basis for deep learning, which has been increasingly adopted since 2010's, is the neural network. A deep learning neural network consists of hundreds of thousands of artificially constructed neuron-synapse combinations. Like the human brain, this neural network is not linear. All the neurons in each layer are connected directly to all the neurons in the subsequent layers, allowing for simultaneous parallel processing.

The multilayered neural networks of the human mind analyze not only what someone is saying based on their speech, but also simultaneously (parallel) process the tone of voice, body language, and facial expressions to get the full interpretation of what those words mean. A neural network derives meaning by looking at the whole – parallel processing; sequential processing would simply analyze the words, without getting to a complex understanding. Just as humans process data from multiple senses, the neural network processes all the available data that is inputted.

HUMANS BRAIN

Billions of neurons are connected to each other through synapses.
The neurons are electrically excitable cells that receive, process and transmit information via chemical signals.
The width of the synapse represents the connection strength between neurons.

VS

ARTIFICIAL BRAIN

Hundreds of thousands of similar type "neurons" are connected to each other.
The connection strength between "neurons" is represented by weights.

HOW DO HUMANS LEARN?

- We hold preconceived premises, facts and theories about a given situation
- We anticipate the outcome of the situation
- The result might be different than we expected
- We adjust our expectations to the result in reality change our future prediction based on the newly learn information

THE HOLISTIC VALUE OF DEEP LEARNING

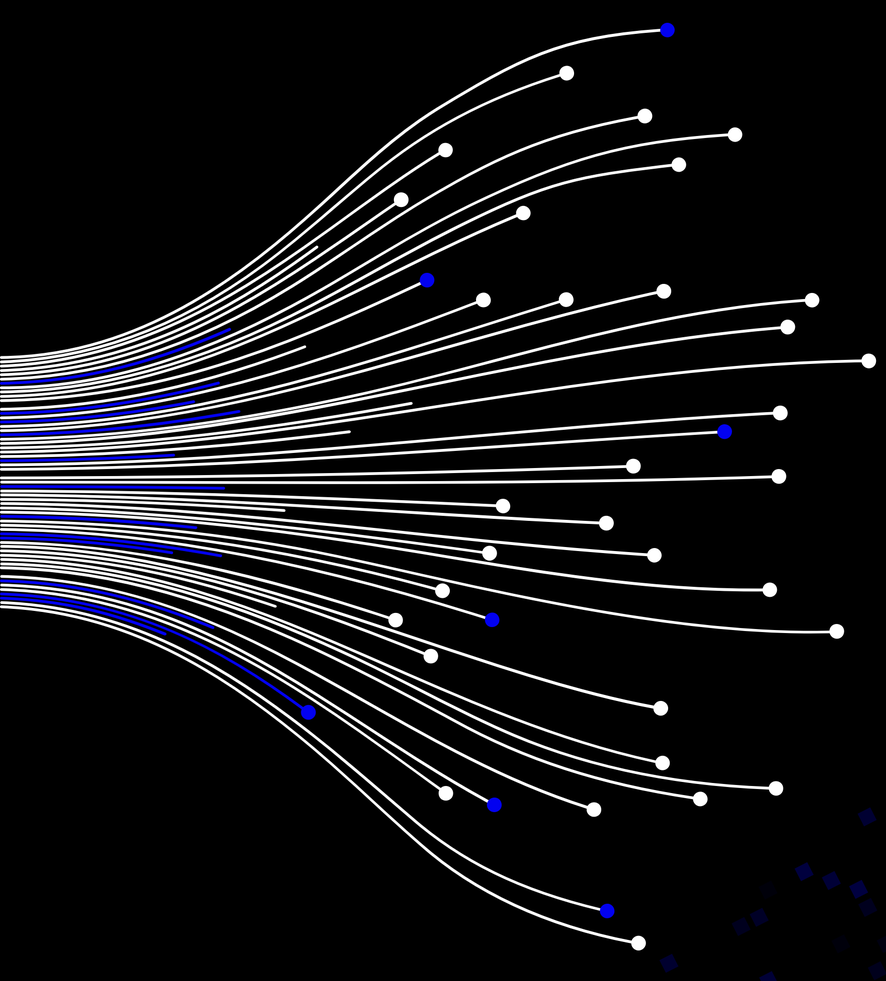
Deep neural networks create pathways that go directly from raw data to comprehensive insights. Deep learning uses its neural networks and perceptions, to create its non-linear data patterns that it can apply to new data sets, as directed by specialized deep-neural algorithms.

The deep learning algorithms transform decision-making, removing the need to define attributes and enabling analysis of the big picture by using 100 percent of the available data. They look at every single aspect of the data; the file type, the contents, etc.

This combination makes its results consistently more accurate and intuitive. It can tell the difference between a Pomeranian and a Russian Blue due to the massive number of characteristics from the raw data that it processes to reach a decision – like our own neural networks.

HOW DO MACHINES LEARN?

- The data scientist prepares data samples for training
- The model is trained by feeding it with millions of samples of labeled data.
- Throughout the training process, the brain learns how to instinctively detect and identify data.
- The brain reaches prediction level, where it makes reasonably accurate predictions.
- Confirmations of predictions help to refine the model's knowledge.



THE BENEFIT OF APPLYING DEEP LEARNING TO CYBERSECURITY

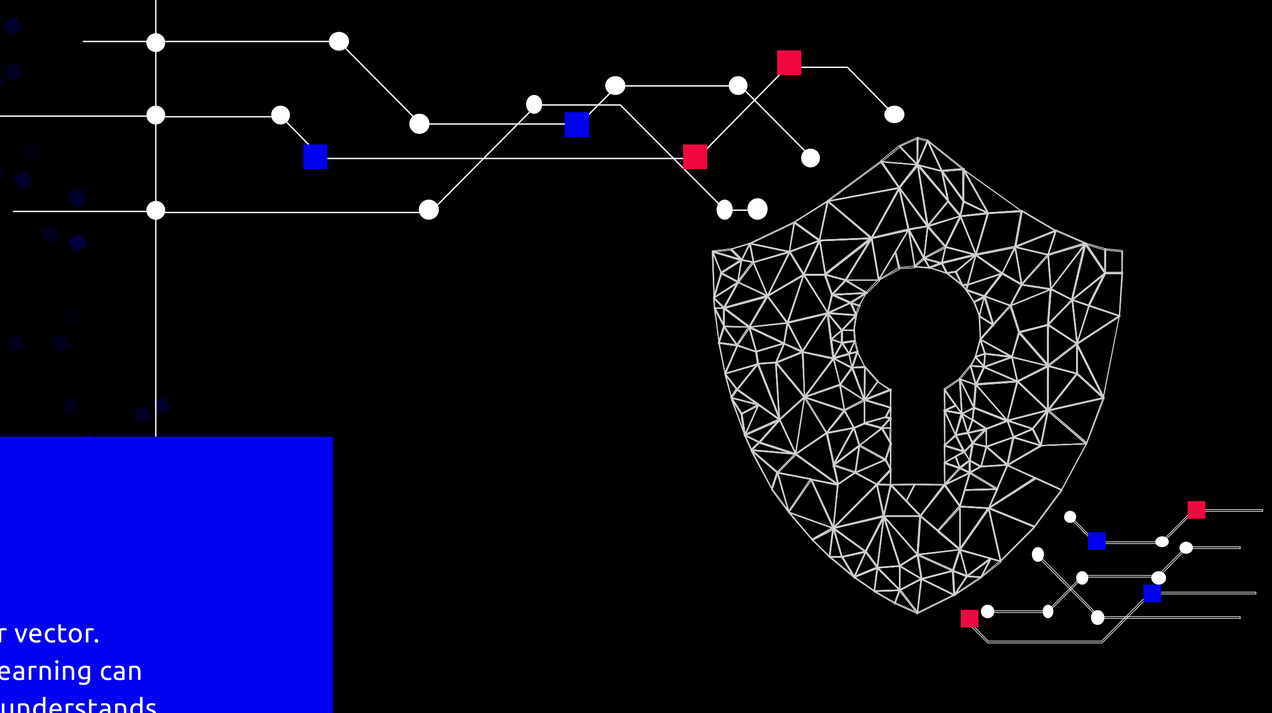
RAW DATA TRAINING.
Capable of training directly from raw data, it is able to detect a new sample with greater levels of accuracy.

INDEPENDENT OF HUMAN INTERVENTION.
Does not rely on human intervention to perform feature engineering and data manipulation to detect even new and unknown samples.

ANALYZE ANY TYPE OF DATA.
The input agnostic development of the algorithm means that Deep Learning can handle any and all types of data.

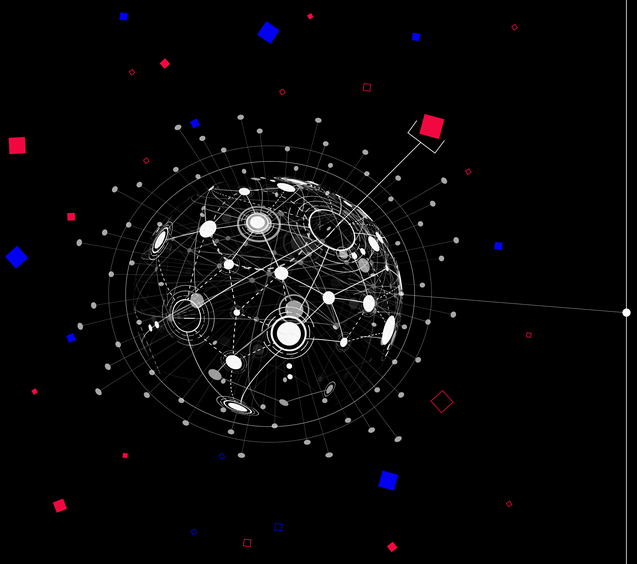
NON-LINEAR CORRELATIONS.
Not limited to simple linear correlations, it can analyze multiple levels of complex data patterns.

UNLIMITED TRAINING SAMPLES.
Deep learning continually improves as the training data set constantly grows, it is the only method that can scale into hundreds of millions of training samples.



GETTING TO THE BIG PICTURE

Deep learning uses raw data, to scan and analyze every aspect of a file or vector. By the nature of this ability to determine patterns from raw data, deep learning can detect malicious anomalies and predict unknown attacks. The algorithm understands and defines by itself what is relevant – or not, allowing it to find complex non-linear correlations, which are hard to define, significantly improving accuracy.



AN INNOVATIVE APPROACH TO SECURITY

Deep Instinct is transforming the industry with its technological innovation, transforming security to a model of prevention. Its deep learning-based cybersecurity solution prevents attacks from entering the enterprise in the first place.

Unlike detection and response-based solutions, which wait for the attack to run before reacting, deep learning can operate preemptively where files and vectors are automatically analyzed prior to execution. By taking this preventative approach customers are kept protected in zero time. This is critical in a threat landscape, where real time is too late.

With a deep learning-based solution, businesses don't have to play cat and mouse, chasing after potential threats to detect and remediate them; no sandboxes or filtering system are necessary. Businesses can continue as normal, without any operational delays. Files can be accessed immediately as the deep learning algorithms have already determined they are safe.

THE BENEFIT: DEEP LEARNING FOR DEEP DEFENSE

Deep Instinct uses deep learning as the basis of its cybersecurity solution. Its D-Brain platform uses deep learning algorithms that have been specifically designed for cybersecurity with multiple benefits to be gained.

PREDICTION OF UNKNOWN THREATS

With its ability to detect any type of anomaly that distinguishes a file from being benign, the deep learning algorithms let's us predict and prevent any kind of threat, known and unknown.

ZERO-TIME DETECTION AND PREVENTION

The pre-execution approach to threat prevention, followed by detection and response and then analysis and remediation, ensures that attacks are identified and blocked before any damage can be caused.

ZERO-TIME CLASSIFICATION

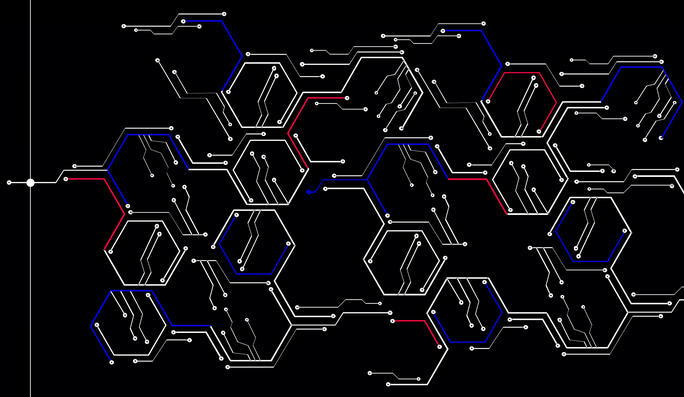
Analysis of enormous amounts of data automatically detects any type of anomaly, classifying malware in zero time with unparalleled accuracy.

ANY DEVICE, ANY OPERATING SYSTEM, ANY FILE

The algorithm's system agnostic design means that every endpoint, server, mobile device, network and operating system is protected against any type of attack, be it fileless or file based.

CONNECTIONLESS EDGE DEPLOYMENT

The deep learning prediction model can be deployed on edge devices as efficient, lightweight client software.



THE CLICHÉ IS TRUE – AN OUNCE OF PREVENTION BEATS A POUND OF CURE.

Stopping threats before they become an issue literally saves millions in operational downtime, lost business, mitigation effort, fines and customer defection.

CONCLUSION

The deep learning neural network autonomously applies its predictive determination to prevent threats from entering the enterprise. Through the application of deep learning, Deep Instinct has shown that it is not only possible to prevent threats, but do so, with unparalleled efficacy.

The are many benefits in applying deep learning to cybersecurity, but principally it saves the enterprise considerable costs and resources from no longer having to contend with the collateral damages of an attack. The highly accurate and automated solution reduces the pressure on the SOC team, lowering personnel demands and removing alert fatigue. Time and computing resources are not sacrificed to the disastrous fallout of a breach. And business continuity is blissfully assured.

ABOUT DEEP INSTINCT

Founded in 2015, Deep Instinct provides comprehensive protection against the most evasive known and unknown malware in zero-time, across an organization's endpoints, servers and mobile devices. Beyond protecting consumers, small business and Fortune 500 companies, Deep Instinct utilizes its deep learning capabilities to offer innovative ways to protect and prevent even the largest systems against attack. With new partnerships expanding every day, Deep Instinct is the first vendor with a patented deep learning cybersecurity framework to block malware attacks from entering the enterprise.

Deep Instinct is led by a highly experienced and interdisciplinary team of deep-learning scientists and Ex-IDF intelligence cyber units. This combined force is revolutionizing the way deep learning is applied to cybersecurity.

FOR MORE INFORMATION: www.deepinstinct.com info@deepinstinct.com