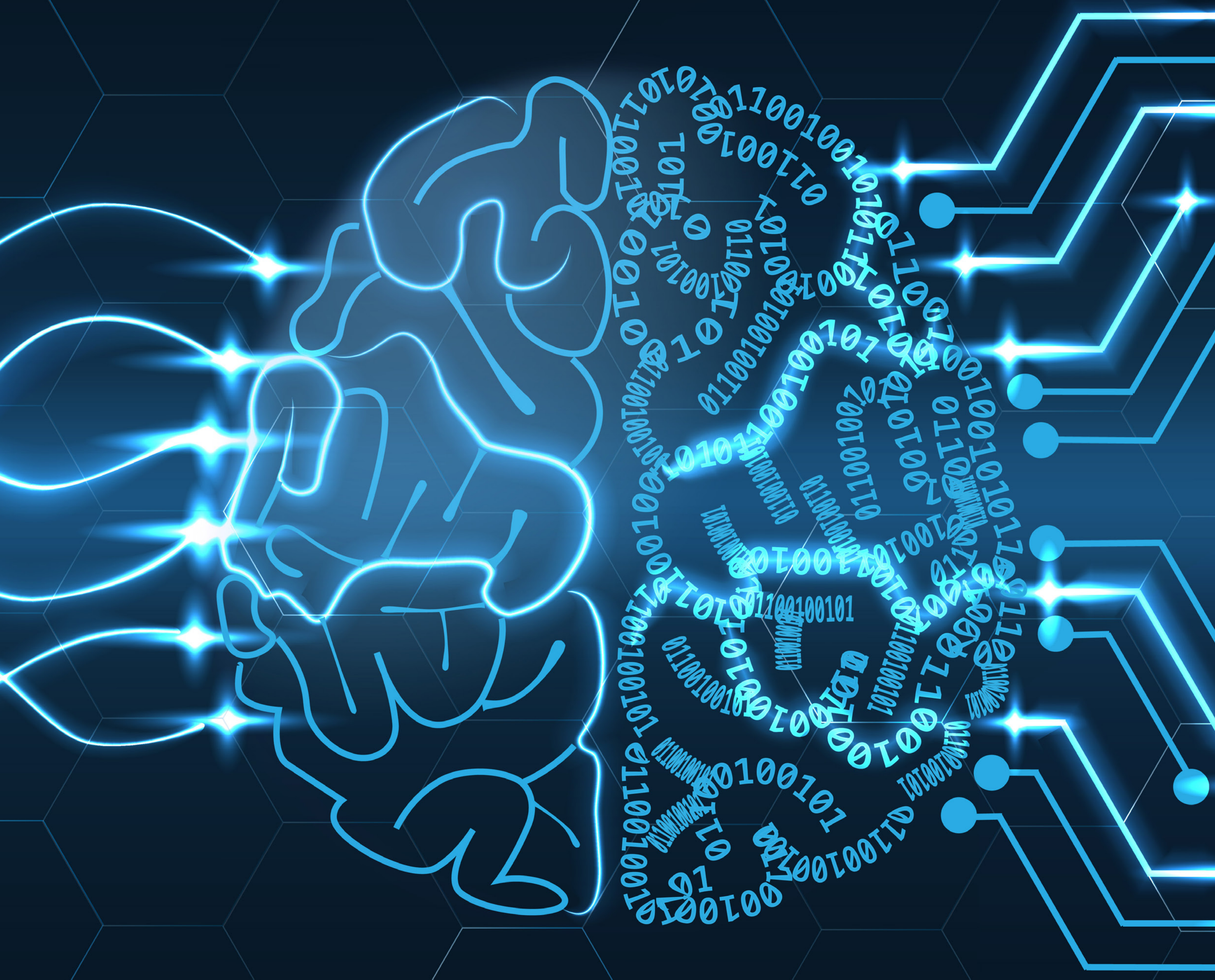
# Deep Instinct™ Overview

Prevent What Others Can't Find



www.deepinstinct.com

deepinstinct™

SAFE. IN THE DEEP SENSE.

# The Deep Instinct Revolution

Harnessing the power of **deep learning**, Deep Instinct is revolutionizing cyber security - Unleashing game-changing threat **detection and prevention technology**.

- The **first** company to apply **deep learning to cybersecurity**.
- **Any threat. Anywhere. Anytime. :** the only **omni-cybersecurity** platform with the predictive ability to prevent, detect and respond to any threat – known and unknown – protecting any device type, with any OS, against any file-based or file-less attack.
- Real-time **pre-execution prevention**, **detection** & **response** of unknown and known malware, including advanced persistent threats (APT), zero-day, and ransomware.
- Unique **unknown malware classification** to identify malware types **without human involvement**.
- **No tradeoffs:** Highest Detection rates, lowest false positive rates.

## 2017: THE YEAR OF CYBERCRIME EPIDEMIC

New kind of cyberattacks; dramatic increase in volumes; much greater impact

**Inarguably, the need for a cybersecurity paradigm shift has never been greater. The spread and impact of unknown and new types of attacks has reached epidemic proportions:**

Over **100 unknown malware attacks** hit an organization every hour

There are **360K new malicious files** appearing daily

**5 new malware variants** are discovered every second

Ransomware hits businesses **every 40 seconds**

It takes most business **˜197 days** to detect a breach

A new ransomware family appears **every 9 days**

And, the attacks are causing damages in great scale.

### NSA and CIA Leaks

- Wikileaks releases Vault7 - a trove of CIA crafted tools, exploits and techniques.
- ShadowBrokers releases the NSA equivalent containing EternalBlue and other invaluable exploits.
- The leaks give hackers a huge leap forward.

### Data Breaches

- Equifax: personal data of 145M people.
- Yahoo: every one of Yahoo's 3B accounts was hacked.
- Uber: hackers stole the data of 57M customers.
- Deloitte: confidential data, including client emails compromised.

### WannaCry Ransomware

- Numerous industries, including health care, shipping and automotive had > 300K machines hit.
- Shutdowns in UK's NHS and German Rails.

### NotPetya Wiper

- Overall > $1.2B in losses.
- FedEx: $30M loss.
- The Danish shipping firm Maersk: $300M loss.
- Merck: $310M loss.

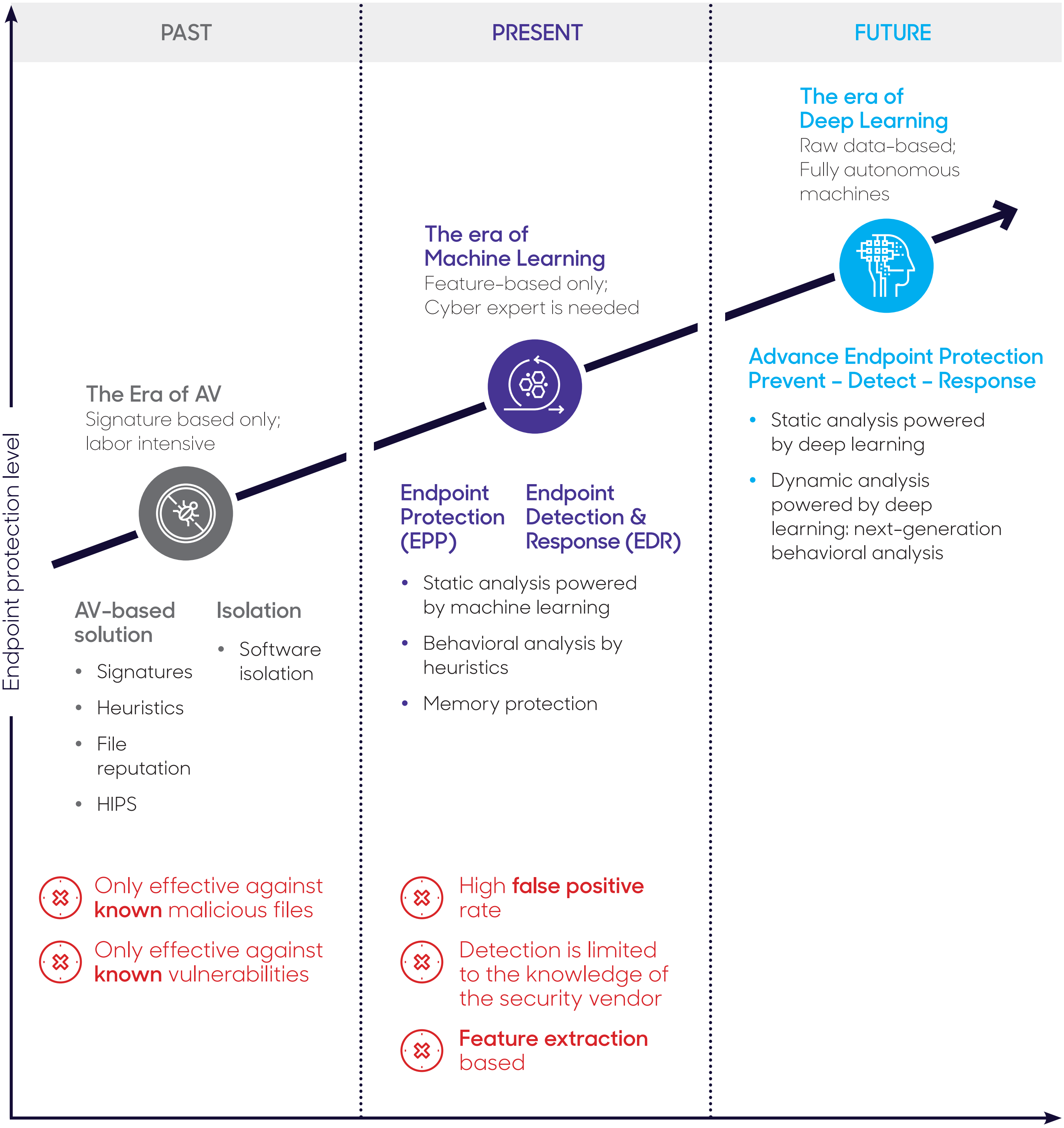
## Deep Learning: Changing the Rules of the Game

While organizations today are using a number of different approaches in their attempt to detect cyber threats, these approaches are all limited in one way or another. Even, the great hope for machine learning as a means for fighting cybercrime comes up short.

Clearly, this kind of compromise is not an option.

> *“Malware has proven increasingly difficult to detect via signature or heuristic-based methods, which means most Antivirus (AV) programs are woefully ineffective against mutating malware, and especially ineffective against APT attacks (Advanced Persistent Threats).”*
>
> tom's HARDWARE

## FROM AV TO DEEP LEARNING: ENDPOINT AND MOBILE SECURITY EVOLUTION



### PAST

**The Era of AV**
Signature based only; labor intensive

**AV-based solution**

- Signatures
- Heuristics
- File reputation
- HIPS

**Isolation**

- Software isolation

☒ Only effective against **known** malicious files

☒ Only effective against **known** vulnerabilities

### PRESENT

**The era of Machine Learning**
Feature-based only; Cyber expert is needed

**Endpoint Protection (EPP)**

**Endpoint Detection & Response (EDR)**

- Static analysis powered by machine learning
- Behavioral analysis by heuristics
- Memory protection

☒ High **false positive** rate

☒ Detection is limited to the knowledge of the security vendor

☒ **Feature extraction** based

### FUTURE

**The era of Deep Learning**
Raw data-based; Fully autonomous machines

**Advance Endpoint Protection Prevent – Detect – Response**

- Static analysis powered by deep learning
- Dynamic analysis powered by deep learning: next-generation behavioral analysis

In fact, there is only one approach that has the power to bring on a real revolution in predicting unknowns, and preventing and detecting-and—responding to threats, with unprecedented speed and accuracy.

This is **deep learning.**

> *Unfortunately, machine learning will never be a silver bullet for cybersecurity...*
>
> Forbes

Deep learning is the most advanced subset of artificial intelligence. Also known as "deep neural networks," it takes inspiration from how the human brain works. Namely, the more data that is fed to the machine the better it is at intuitively understanding the meaning of new data – and, therefore, does not require the interface of a (human) expert to help it understand the significance of each new input.

The advantages of deep learning are many:

### Independent learning
with predictive capabilities that are intuitive and automatic.

### Any and all data
using millions to billions of pieces of raw data for analysis, without being limited to 'feature extraction' (i.e. partial data) or specific file types (i.e. PE), as with machine learning.

### Unknown files expertise
with the highest detection and prevention rates and unmatched low rates of false positives.

Accordingly, this combination of capabilities endows deep learning with unprecedented accuracy and efficacy in its decision making.

## The Deep Instinct Paradigm Shift

Deep Instinct is proud to introduce the first and only cybersecurity solution that is based on a proprietary deep learning framework that was specifically designed for cybersecurity.

Our solution provides end-point and mobile prevention and detection-and-response, against any file-based or file-less attack, for every operating system, on any device, in one unified platform, delivering unmatched accuracy and efficacy.

The unique deep learning algorithms and modeling methods that we have developed ensure immediate response with only a millisecond for prevention and detection.

The result is unparalleled cybersecurity prowess in blocking and preventing even the most evasive unknown, first-seen malware, including persistent threats (APT), zero-day attacks, and ransomware.

## DEEP LEARNING IS THE GREAT LEAP IN THE PERFORMANCE OF AI IN HISTORY

In recent years, deep learning is so effective that it has reached a 20%-30% improvement across most benchmarks in computer vision, speech recognition, and text understanding. This represents the greatest leap in the performance of artificial intelligence in history.

With its effectiveness and high levels of accuracy, the adoption of deep learning is accelerating, and we see it already promoted for many commercial applications:

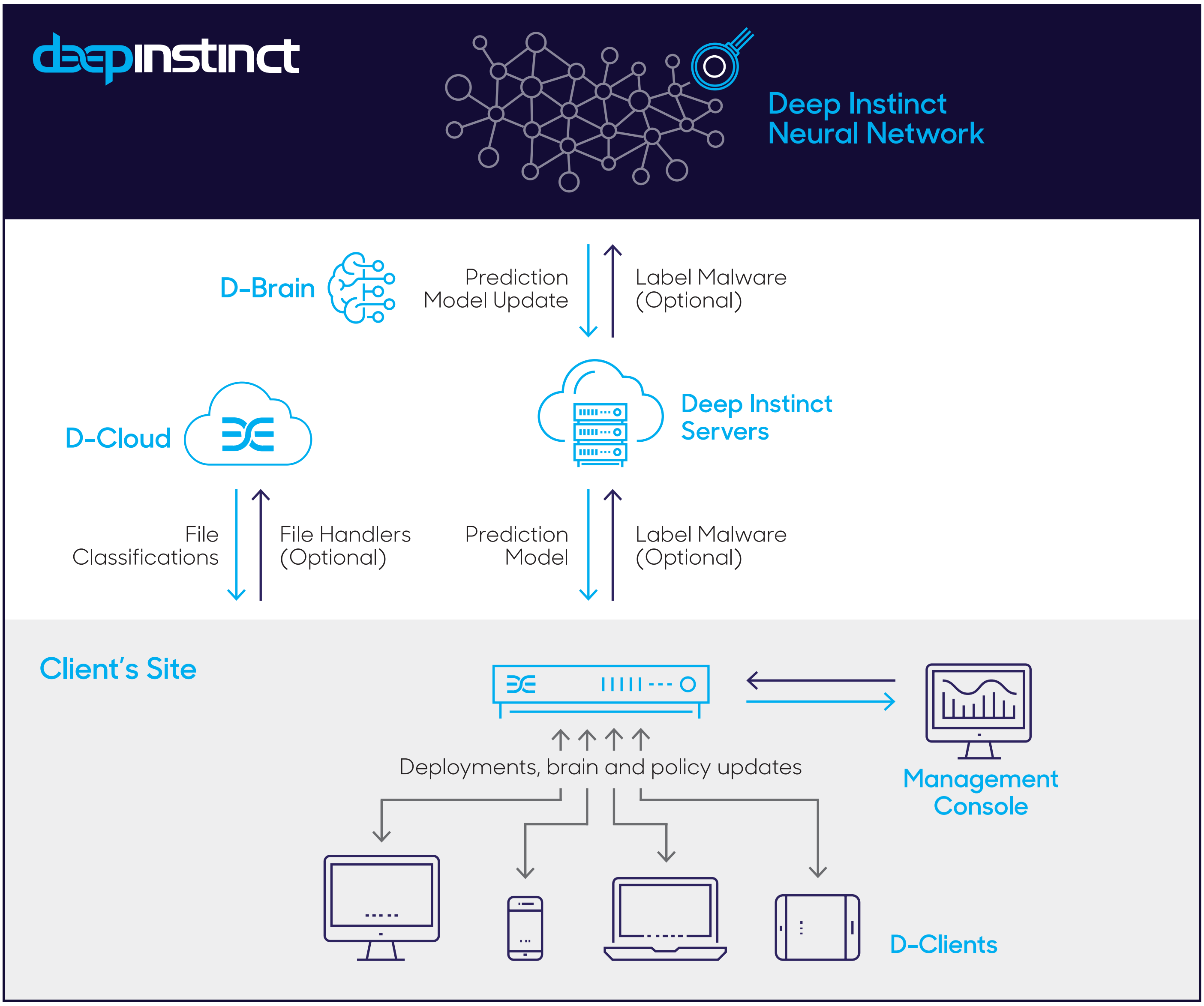
### Personal video recommendations (youtube)
monitoring and recording users viewing habits, studying and learning everything about viewers' habits and preferences, and working out what would keep them engaged

### Healthcare & genomics
to predict the outcomes of genome alterations and provide a more precise understanding of diseases

### Agriculture
to predict crop yields based on the analysis of masses of satellite images

### Image recognition
sorting and classifying millions of uploaded images for more accurate search results

### Personal (virtual) assistants
for speech recognition to better understand spoken commands and questions, and predicting user needs and preferences.



Deep Instinct Neural Network

D-Brain

Prediction Model Update

Label Malware (Optional)

D-Cloud

Deep Instinct Servers

File Classifications

File Handlers (Optional)

Prediction Model

Label Malware (Optional)

Client's Site

Deployments, brain and policy updates

Management Console

D-Clients

## HOW WE DO IT

**Our offering is comprised of the following components:**

### The Deep Instinct Neural Network

The proprietary deep learning computing infrastructure and algorithms for detecting and preventing cyber threats, developed by the company's data scientists and mathematicians together with our cyber research team.

### D-Brain

The prediction model that is the output of the Deep Instinct Neural Network, and which is included in the following components that are installed by the organization.

### D-Client

Includes D-Brain and is deployed on the organization's endpoints, mobile devices, and servers.

### D-Appliance

A management and monitoring server that also includes D-Brain and comes with a Management Console.

### D-Cloud

A cloud-based infrastructure for adding reputation based classification.

## The Deep Instinct Advantage

### Immediate instinct. Unmatched accuracy

- Immediate response with only a millisecond for detection and prevention.
- Unmatched accuracy with intuitive detection of zero-day, APT, and ransomware, even for the most evasive unknown threats, while maintaining the lowest rates of false positives.

### Transcending the evolution of threats

- Fully autonomous learning, from millions to billions of files (malicious and benign) from different sources (3rd party, publicly available sources, darknet, malware mutations, and our own "home grown" malwares).
- Harnesses the power of Nvidia GPUs, for training that is 100x faster.
- Learns from raw data, not just feature extraction.

### Omni-cyber platform

- Real-time pre-execution prevention of any device with any OS (Windows, iOS, MacOS, Android).
- Enables an augmentation approach to enhance existing AV suites.
- Flexible deployment, either as cloud-native by design or on-premise.

## About The Team

Our advanced deep learning algorithms and prediction models are developed by an interdisciplinary team of experienced mathematicians, data scientists, and deep learning experts who hold PhDs and/or MScs and have a domain expertise in operational cybersecurity.

Our team includes veterans of the special cyber units in the Israel Defense Forces (IDF), and leadership that brings extensive executive experience from top global cybersecurity companies.

## INDUSTRY RECOGNITION

Gartner 2016 CoolVendor

Cool Vendor for **Digital Workplace Security 2016**

Best of black hat Awards

Most Innovative Startup in the Best of Black Hat Awards program, Dark Reading editors, **Black Hat 2016**

NVIDIA INCEPTION AWARDS

Most Disruptive Startup at **Nvidia Inception Awards 2017**

WORLD ECONOMIC FORUM

Awarded as Technology Pioneer at **World Economic Forum 2017**

Forbes

Ranked by Forbes Among the **"Thirteen companies that use Deep Learning to produce actionable results"**

## Strategic Investors

coatue

ColumbusNova
Technology Partners

NVIDIA

## Partnership Ecosystem & Certifications

### Industry Certifications

PCI

HIPAA
Health Insurance Portability & Accountability Act

SE Labs

### Official Member & Partner

MEMBER amtso
Anti-Malware Testing Standards Organization

WORLD ECONOMIC FORUM

### Technology Partnerships

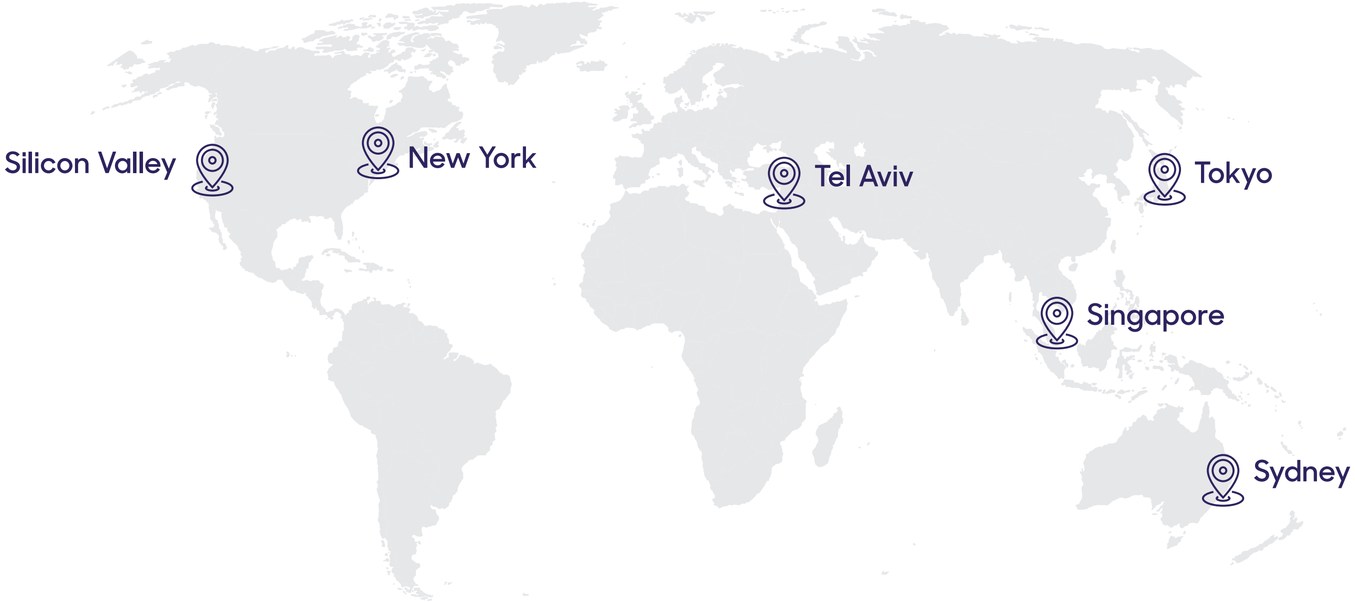
splunk>

IBM Radar

citrix Ready

MICRO FOCUS

## Global Locations



**To get started with the cybersecurity revolution contact us at:**
**contact@deepinstinct.com**

ISRAEL
23 Menachem Begin Rd.,
28th Floor, Tel Aviv,
Israel, 6618356
+972 (3) 545-6600

NEW YORK
501 Madison Ave.,
Suite 1202
New York City, NY,
USA, 10022

SINGAPORE
The Working Capitol
140 Robinson Rd., #04-00
Singapore
068907

@DeepInstinctSec

deepinstinct
www.deepinstinct.com