UNMATCHED ZERO-DAY & APT PROTECTION
$445B estimated annual cost of cyber crimes\(^{(1)}\)

$170B The cyber Security market is estimated to grow from $71.1B in 2014 to $170B by 2020 \(^{(2)}\)

$4.3M Is the average cost of a data breach in the U.S. and worldwide is $3.8M \(^{(8)}\)

80% By 2020, 80% of access to the enterprise will be via mobile devices, up from 5% today. \(^{(7)}\)

$8.7B The APT protection market is estimated to grow to $8.7B by 2020 \(^{(6)}\)

1M new malware created on a daily basis in 2015 \(^{(5)}\)

3rd Ranking - cyber attacks in the list of 2014 global threats \(^{(3)}\)

3 Times more attacks on mobile than on desktops

+1B Personal data records compromised by cyber attacks in 2014 \(^{(8)}\)

$170B The cyber Security market is estimated to grow from $71.1B in 2014 to $170B by 2020 \(^{(2)}\)

80% By 2020, 80% of access to the enterprise will be via mobile devices, up from 5% today. \(^{(7)}\)

$8.7B The APT protection market is estimated to grow to $8.7B by 2020 \(^{(6)}\)

1M new malware created on a daily basis in 2015 \(^{(5)}\)

3rd Ranking - cyber attacks in the list of 2014 global threats \(^{(3)}\)

+1B Personal data records compromised by cyber attacks in 2014 \(^{(8)}\)

$170B The cyber Security market is estimated to grow from $71.1B in 2014 to $170B by 2020 \(^{(2)}\)

80% By 2020, 80% of access to the enterprise will be via mobile devices, up from 5% today. \(^{(7)}\)

$8.7B The APT protection market is estimated to grow to $8.7B by 2020 \(^{(6)}\)

1M new malware created on a daily basis in 2015 \(^{(5)}\)

3rd Ranking - cyber attacks in the list of 2014 global threats \(^{(3)}\)

+1B Personal data records compromised by cyber attacks in 2014 \(^{(8)}\)
**Security Innovation Evolution**

**Past**
- Signature
- Humans Needed
- Signature Needed
- Domain experts require, labor intensive
- 1990’s

**Present**
- HIPS / Heuristics
- Dynamic / Behavioral
- Isolation / Sandboxing
- Machine Learning
- Data Scientists – Domain agnostic
- Early 2000’s

**Present & Future**
- Deep Learning
- 2012

Highly autonomous | Predictive | Minimal Human intervention
Detection and Prevention

- **Endpoints** (Laptops, Desktops)
  - Deep Learning prediction for APT and Zero-day malware
  - Static File Analysis prevents malware pre-execution
  - Augment existing endpoint solution
  - On-Device Protection (connected or disconnected)
  - Seamless deployment – SCCM, GPO, BigFix etc

- **Mobile Devices** (Android, iOS)

- **Servers** (Windows)

World leading **Deep Learning research team** *(lead by Dr. Eli David)*

33 Published Whitepapers on AI

World leading **Security Research Team** *(Israeli Intel Community)*
What We Are Doing Differently – Deep Learning Artificial Brain

Reaction time + Action time = Response time

- Analyze and Evaluate
  - Reaction time

- Plan
  - Reaction time

- Initiate Action
  - Action time

Perception
  - Reaction time
**Machine Learning vs. Deep Learning**

- **Raw data**
  - Machine Learning: Only 2.5% to 5% of file data
  - Deep Learning: 100% of Raw File Data

**Deep learning** enables to skip the features selection phase, taking into account:
- ALL available features
- Non linear correlations
Malware Mutation Example ML vs. DL

Machine Learning
- Trained on Car – Now Known
- Trains on Linear Patterns only – 2.5% - 5% of (file)
- Detection of Car >98% rate
- Unknown Malware (House) – Non-Linear Mutation
- Unknown Malware (House) – Undetected
- **Unknown Malware NOT Blocked**

Deep Learning
- Trained on Car – Now Known
- Trained on Linear & Non-Linear Patterns (100% of File)
- Detection of Car >98%
- Unknown Malware (House) – Non-Linear Mutation
- Unknown Malware (House) – Detected >98%
- **Unknown Malware BLOCKED**
**We Do NOT:**

- Signatures
- Heuristics
- Behavioral Analysis
- Sandboxing

**We do not use**

**We do not require**

- Threat intelligence feeds
- Connectivity
- Manual analysis for classification
- Wait for execution of attack
- Frequent updates
**Malware, Prediction Differences ML vs. DL**

3rd Party & Customer Testing / Internal Testing

**ML Brain (Agent)**

- Machine Learning
- Prediction Model

- >98% Detection of Known Malware
- <62.5% Detection Rate Unknown Malware
- 2.5% - 5% False Positive Rate

**DL Brain (Agent)**

- Prediction Model

- >99% Detection of Known Malware
- >98% Detection Rate of Unknown Malware
- <0.013% False Positive Rate
A Two-Step Approach – Training and Prediction

**Training in Deep Instinct Premises**
Hours/Days process

**Installation of the trained module through a dedicated client**

**On-device Prediction**
Real-time
The value of the Deep Instinct prediction model (D-Brain)

- Spora Ransomware (link)

Deep Instinct prevents zero-day malware attacks
It covers the gap of 45 days (at least) between the unknown to known
It protects even if the D-Brain has been last updated 10 months prior to the attack
Deep Instinct and latest zero-day ransomware campaigns

- **WannaCry (May/17)**
  - Infected more than 230,000 computers in over 150 countries. Parts of the United Kingdom's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.

- **NOT Petya (June/17)**
  - A spin-off of Petya was used for a major global cyberattack, which utilizes the EternalBlue vulnerability previously used by WannaCry. Ukrainian Govt. and firms, Maersk, DLA Piper, Rosneft, and many others companies

- **Spora (Jan/17)**
  - Distributed via spam emails pretend to be invoices. These emails come with attachments in the form of ZIP files that contain HTA files which upon run extracts a Javascript file which further extracts an executable and runs it.
Deep Instinct Awarded as Technology Pioneer by World Economic Forum 2017

2017 Technology Innovation Award

Deep Instinct on the list of “Top 13 companies that use deep learning”

Deep Instinct received “Best in Show” award in Nvidia’s deep learning conference
THANK YOU

www.deepinstinct.com

@DeepInstinctSec
Product Demonstration
QUESTIONS?