UNMATCHED ZERO-DAY & APT PROTECTION

3 Times more attacks on mobile than on desktops

$445B estimated annual cost of cyber crimes[1]

$4.3M Is the average cost of a data breach in the U.S, and worldwide is $3.8M [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]

3rd Ranking - cyber attacks in the list of 2014 global threats[3]

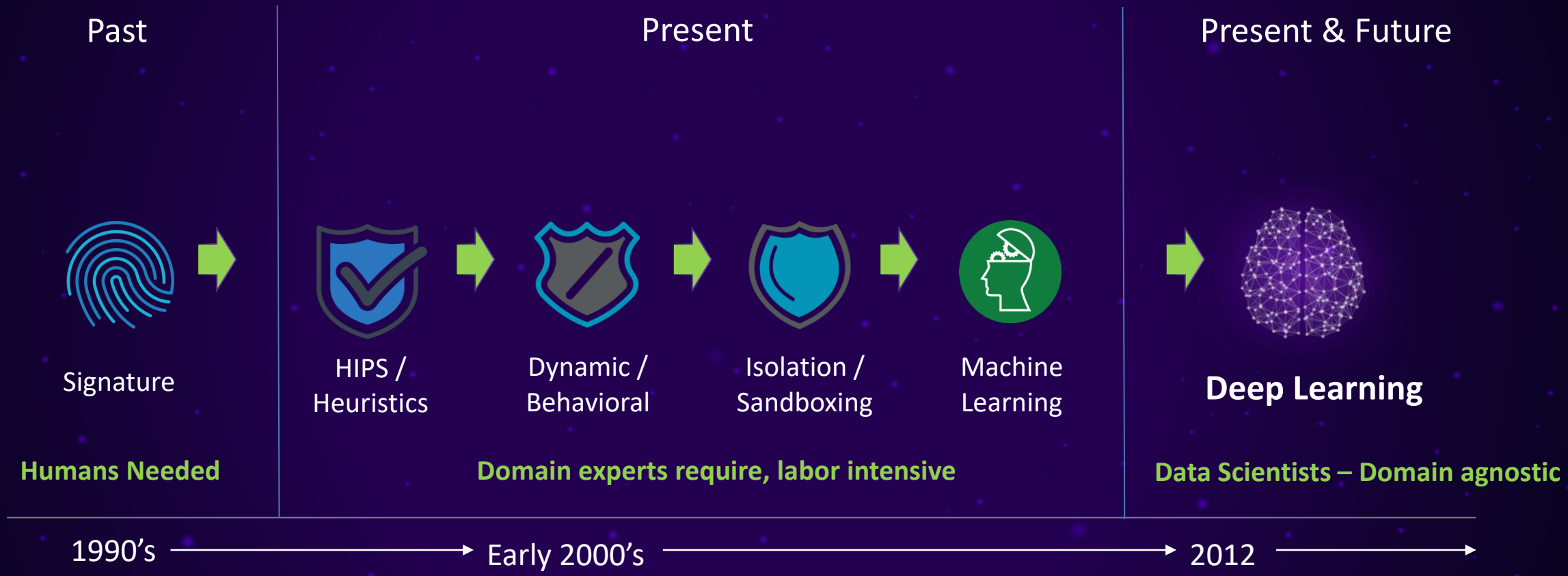
$8.7B The APT protection market is estimated to grow to %8.7 B by 2020[6]

1M new malware created on a daily basis in 2015[5]

+1B Personal data records compromised by cyber attacks in 2014[4]

(1) McAfee (2) MarketsandMarkets (3) Lloyd's (4) Gemalto (5) Symantec (6) Research and Markets (7) Oracle (8) Ponemon Institute

Security Innovation Evolution



Highly autonomous | Predictive | Minimal Human intervention

Detection and Prevention

Endpoints (Laptops, Desktops)

Mobile Devices (Android, IOS)

Servers (Windows)

- 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

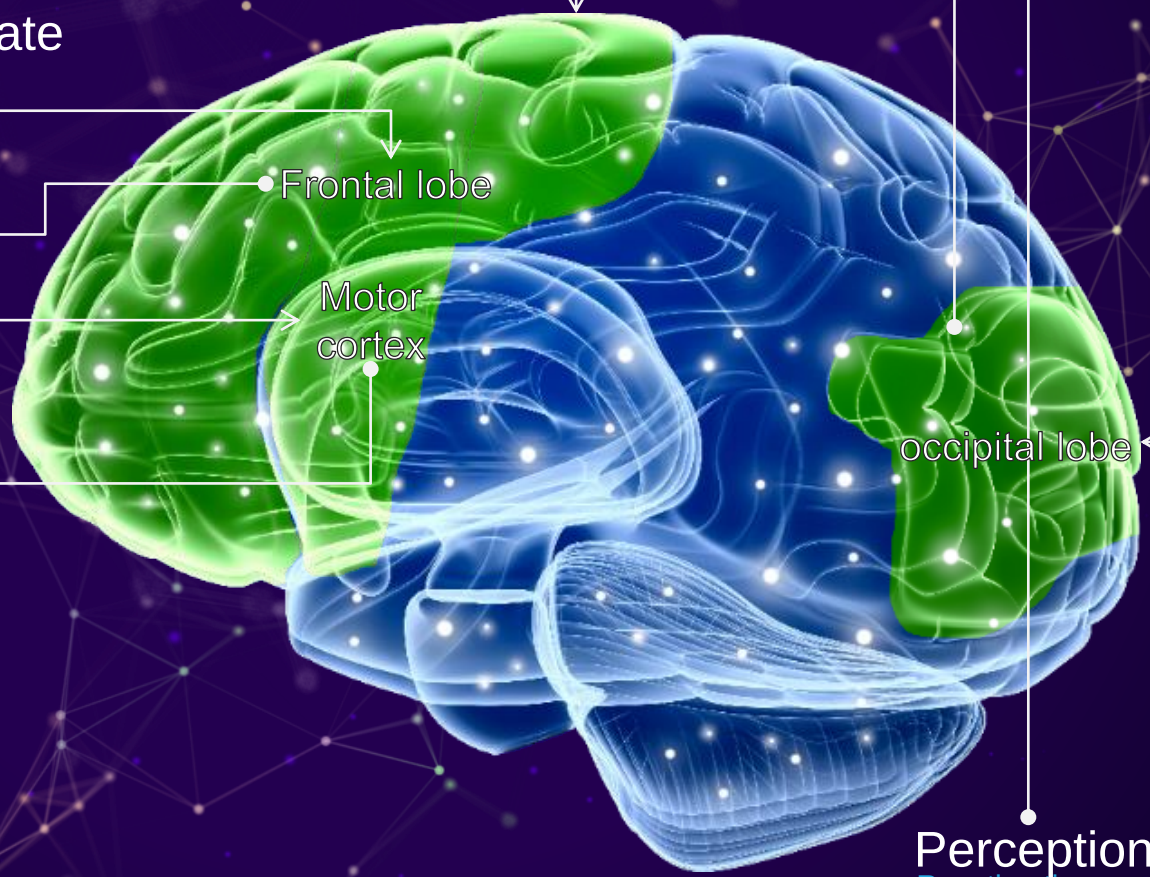
World leading *Deep Learning* research team *(lead by Dr. Eli David)*

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



Machine Learning vs. Deep Learning

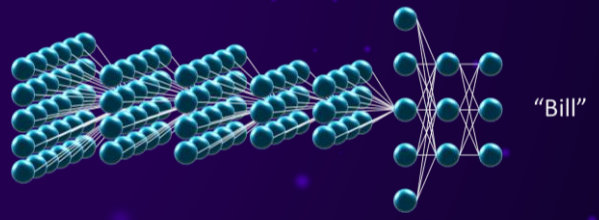
Raw data

Machine Learning

Only 2.5% to 5% of file data
Vector of features

Raw data

100% of Raw File Data



Deep Learning

Deep learning enables to skip the features selection phase, taking into account:

- ALL available features
- Non linear correlations

Malware Mutation Example ML vs. DL

Raw Data

Lego Car = Known Malware – ML & DL

- Mutated Malware
- Same Number of Pieces
- Engine from car is now inside the house

Linear & Non-Linear Mutations

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:

We do not use

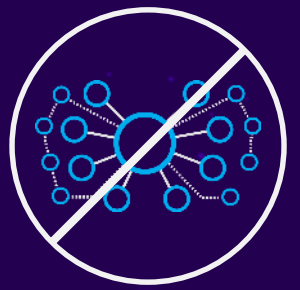
Signatures

Heuristics

Behavioral Analysis

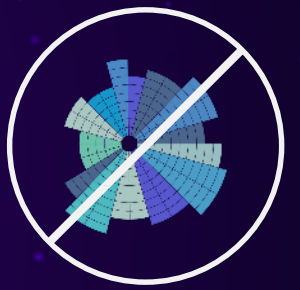
Sandboxing

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)

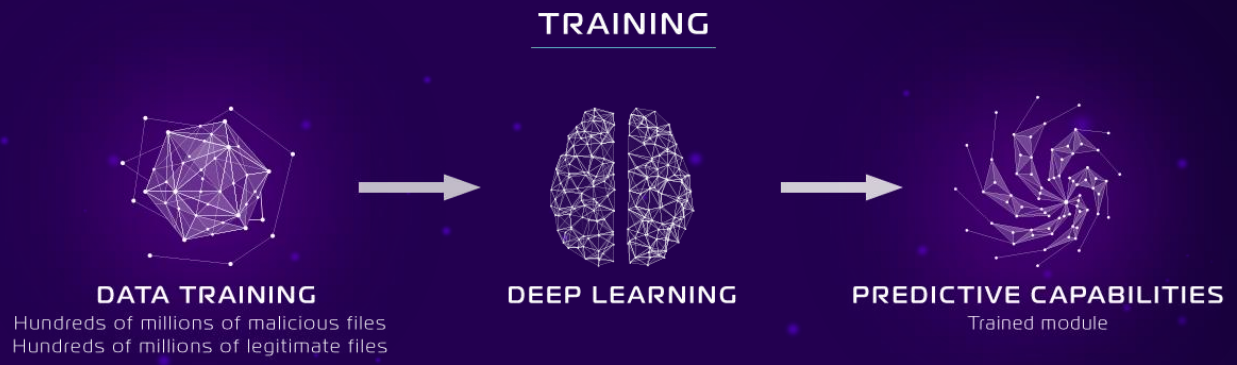
deepinstinct™

Prediction Model

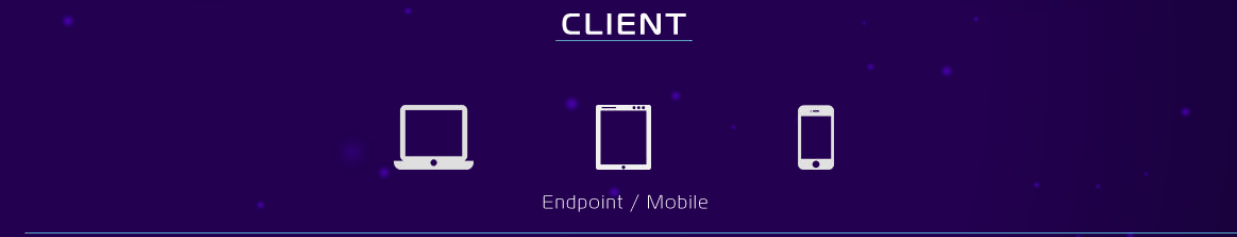
>99% Detection of Known Malware
>98% Detection Rate of **Unknown Malware**
< .013% False Positive Rate

A Two - Step Approach – Training and Prediction

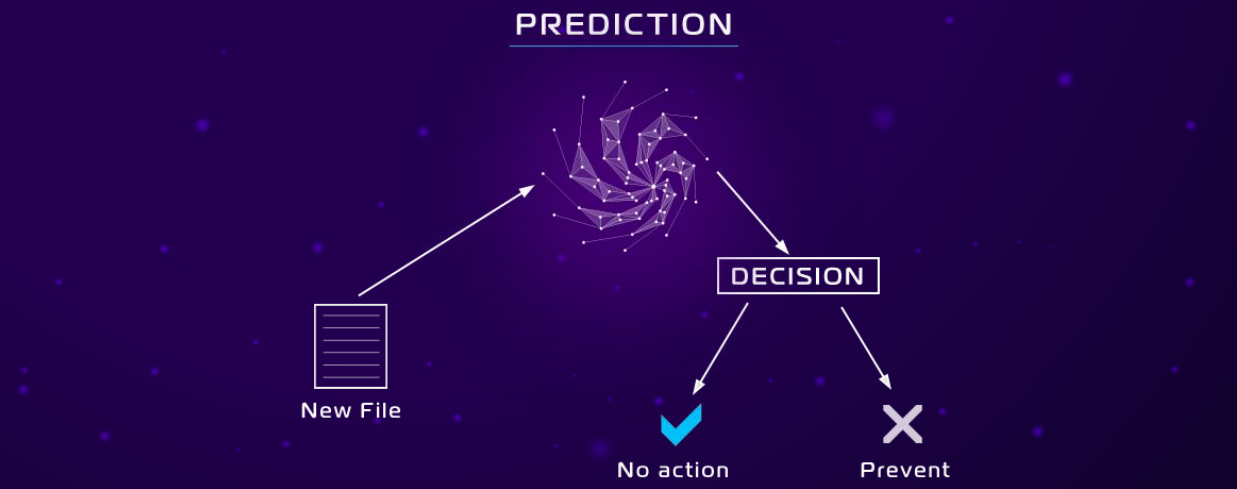
Training in Deep Instinct Premises
Hours/Days process



Installation of the trained module through a dedicated client

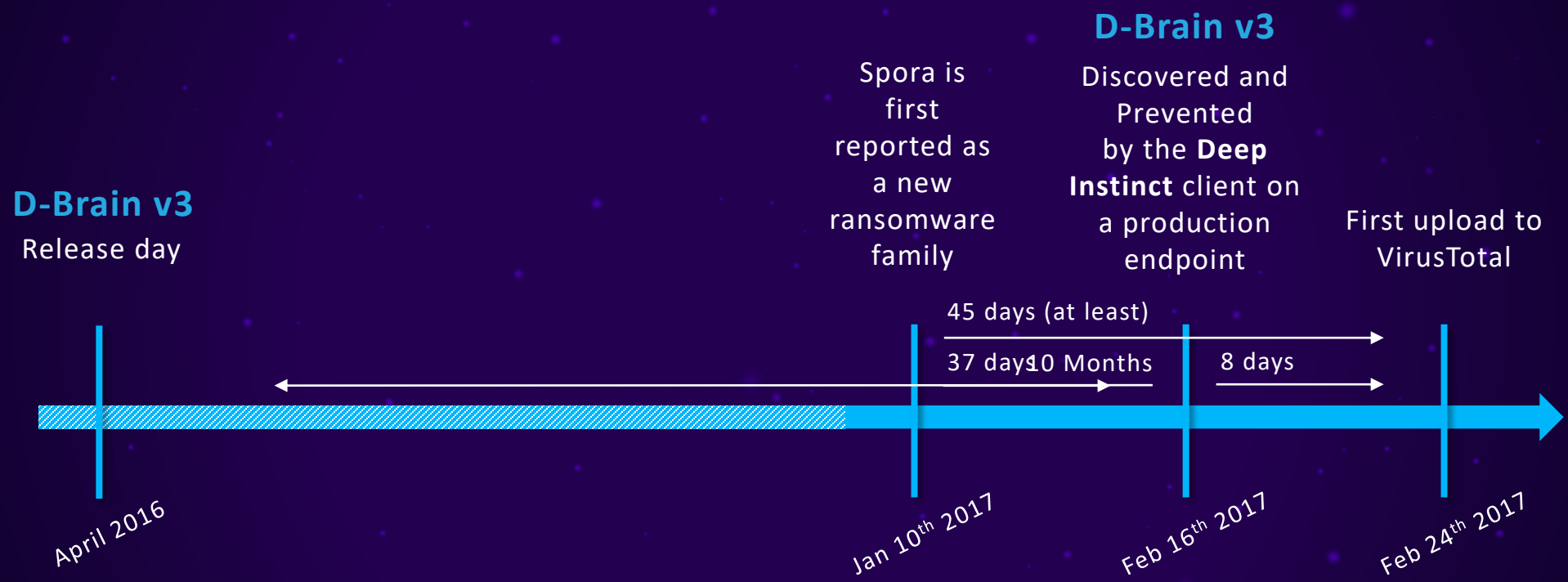


On-device Prediction
Real-time



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

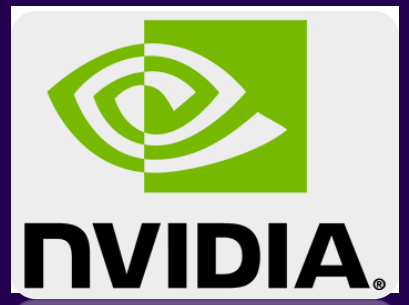
It protects even if the D-Brain has been last updated 10 months prior to the attack

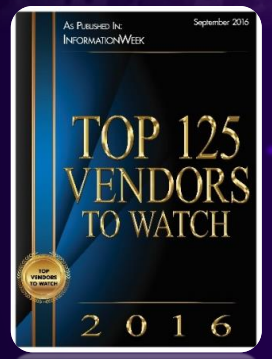
Deep Instinct and latest zero-day ransomware campaigns

- 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. Ukraianian 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.

Detected and Prevented by Deep Instinct

Awards 2016 & 2017





WORLD ECONOMIC FORUM — Deep Instinct Awarded as Technology Pioneer by World Economic Forum 2017

FROST & SULLIVAN — 2017 Technology Innovation Award

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

NVIDIA — Deep Instinct received “Best in Show” award in Nvidia’s deep learning conference

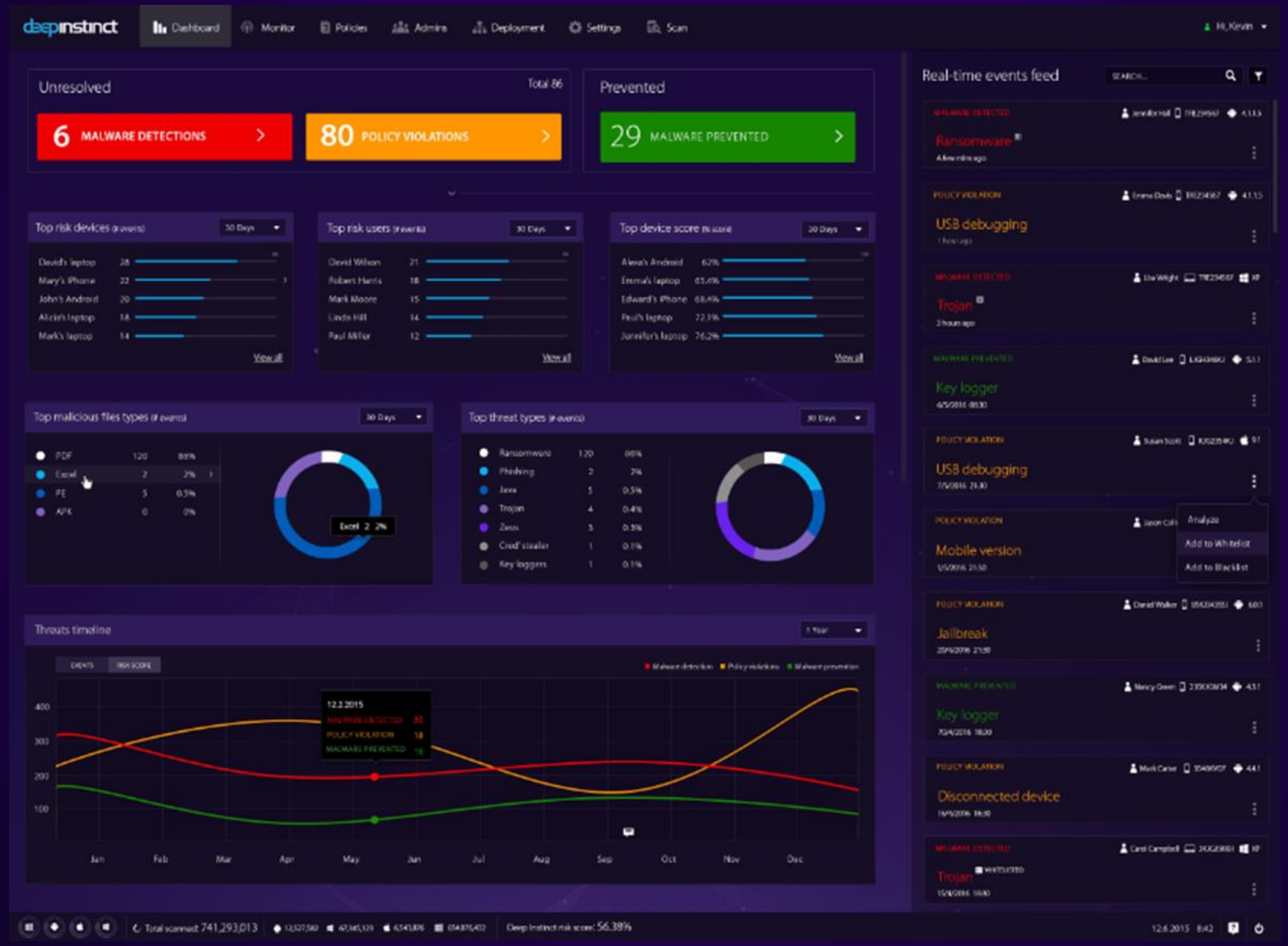
THANK YOU

www.deepinstinct.com

@DeepInstinctSec

deepinstinct

Product Demonstration



QUESTIONS?