DEEP INSTINCT
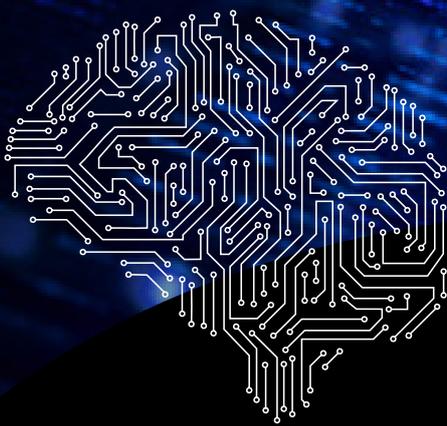# EXECUTIVE SUMMARY

WE PREVENT WHAT OTHERS CAN´T FIND

deepinstinct™
BEFORE YOU KNOW IT

THE DEEP INSTINCT DEEP LEARNING REVOLUTION

Deep Instinct is the first and only company to apply end-to-end deep learning to cybersecurity. Deep learning is inspired by the brain's ability to learn. Once a brain learns to identify an object, its identification becomes second nature. Similarly, as Deep Instinct's artificial deep neural network brain learns to prevent any type of cyber threat, its prediction capabilities become instinctive. As a result, any kind of malware, known and new, first-seen malware, zero-days, ransomware and APT attacks from any kind are predicted and prevented in zero-time with unmatched accuracy and speed anywhere in the enterprise.

Unlike detection and response-based solutions, which wait for the execution of an attack to react, or post-execution which achieves too little too late, our deep learning based prevention approach keeps our customers protected, while dramatically reducing costs.
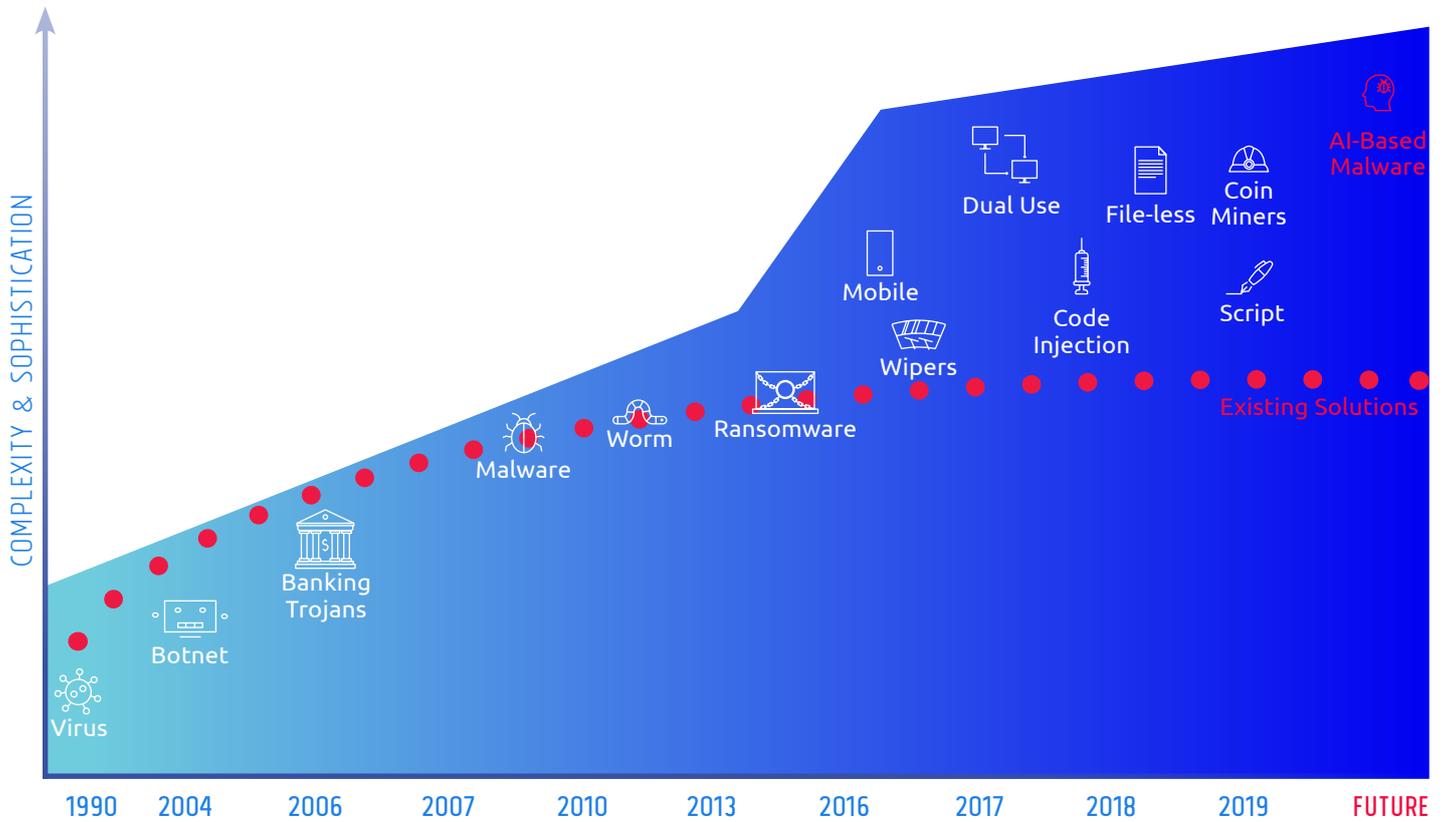

DEEP INSTINCT DEEP LEARNING PLATFORM

LEARN ▪ PREDICT ▪ PREVENT

ANY WHERE

- Network Perimeter
- Endpoint
- Mobile
- Data center
- Cloud

ANY THREAT

- Malware
  (Ransomware, Spyware, trojans etc.)
- Active adversaries
- Insider threats

ANY ENVIRONMENT

- Online / Offline
- VDI
- Cloud / On-Premise
- Multi-Tenancy
- Air Gapped

ANY OS

- Windows
- macOS
- iOS
- Android
- Chrome OS

THE CYBERSECURITY CHALLENGE

CYBER THREAT SOPHISTICATION & COMPLEXITY ARE ADVANCING, CURRENT CYBER SOLUTIONS
IN THE MARKET ARE NOT KEEPING UP

COMPLEXITY & SOPHISTICATION

AI-Based Malware

Dual Use   File-less   Coin Miners

Mobile   Code Injection   Script

Wipers

Ransomware

Worm

Malware

Banking Trojans

Botnet

Virus

Existing Solutions

| 1990 | 2004 | 2006 | 2007 | 2010 | 2013 | 2016 | 2017 | 2018 | 2019 | FUTURE |

FREQUENCY AND COMPLEXITY OF ATTACKS ARE ACCELERATING
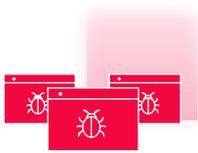
Over **350K** new machine-generated malware are created every day

Source: AV test, 2018

Zero-day attacks are **FOUR TIMES** more likely to compromise organizations

Source: Ponemon Institute 2018

THE COLLATERAL DAMAGE

Nearly **TWO-THIRDS** of enterprises have been **COMPROMISED** in the past 12 months

Source: Ponemon Institute 2018

A BIG BREACH Is averaged to cost an enterprise between **$40M-$350M**

Source: IBM 2018

It took organizations **196 DAYS**, on average, to **DETECT A BREACH**
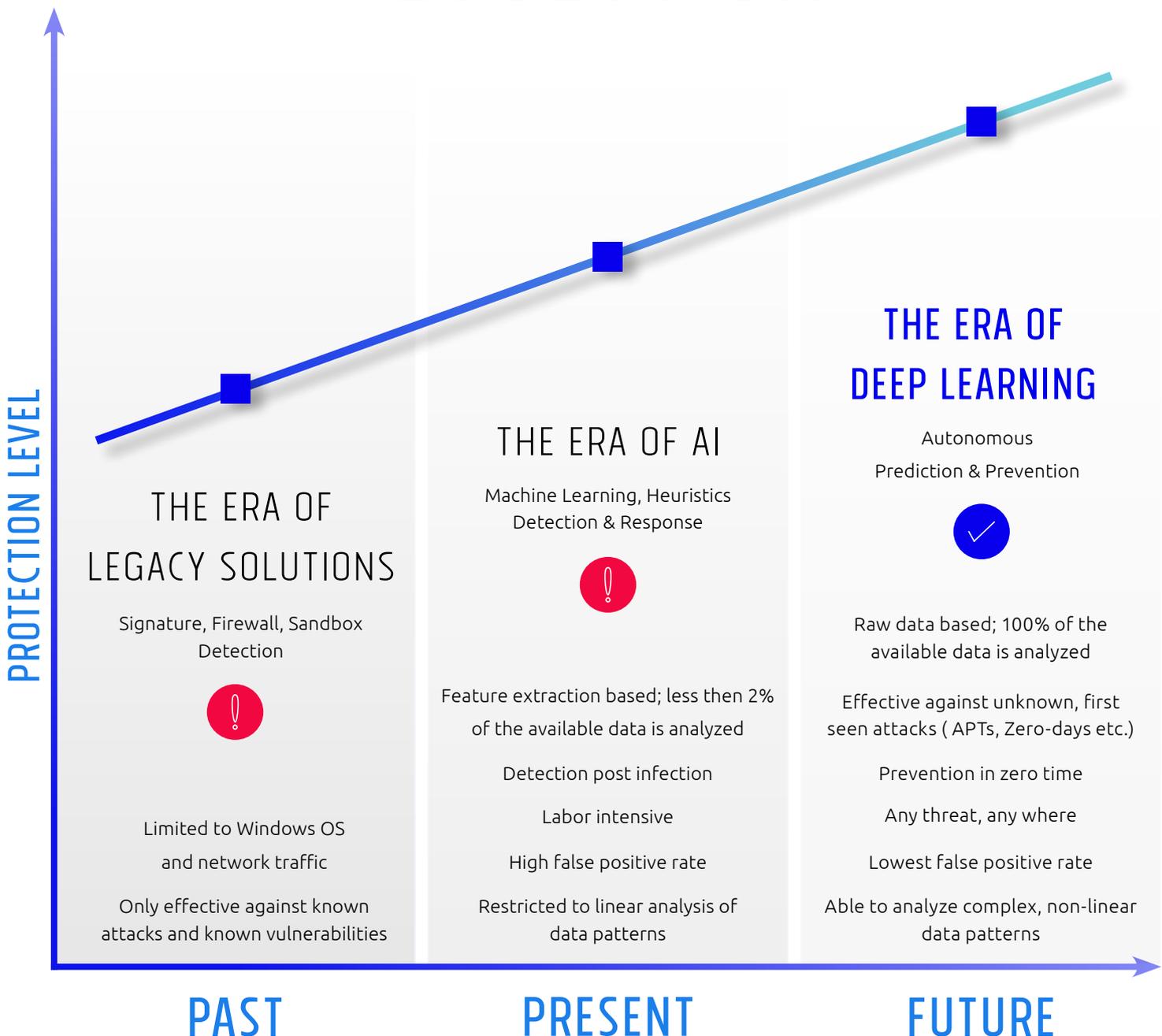
Source: Ponemon Institute

DEEP LEARNING, NOT JUST AI

Deep learning, also known as "deep neural networks" is the most advanced subset of artificial intelligence.

It's the first and only AI method capable of training directly on raw data and does not require feature engineering by a human expert. Deep learning is the only method that analyzes 100% of the raw data and can scale well to hundreds of millions of training samples. It continuously improves as the training data set becomes larger, and back propagation of values is tweaked to ensure greater predictive accuracy.

Among all other solutions to combat cyber threats, deep learning is proven to be most effective, resulting in unmatched detection rates and lowest false positives.

CYBERSECURITY
EVOLUTION

PROTECTION LEVEL

THE ERA OF
LEGACY SOLUTIONS

Signature, Firewall, Sandbox
Detection

Limited to Windows OS
and network traffic

Only effective against known
attacks and known vulnerabilities

THE ERA OF AI

Machine Learning, Heuristics
Detection & Response

Feature extraction based; less then 2%
of the available data is analyzed

Detection post infection

Labor intensive

High false positive rate

Restricted to linear analysis of
data patterns

THE ERA OF
DEEP LEARNING

Autonomous
Prediction & Prevention

Raw data based; 100% of the
available data is analyzed

Effective against unknown, first
seen attacks (APTs, Zero-days etc.)

Prevention in zero time

Any threat, any where

Lowest false positive rate

Able to analyze complex, non-linear
data patterns

PAST   **PRESENT**   **FUTURE**

OUR OFFERING

PREVENTION UNLIMITED

Using a proprietary deep learning framework, Deep Instinct offers a zero-time threat prevention platform with multilayer protection for any security need, against any known or unknown threat. It can be applied anywhere in the enterprise, be it network perimeter, endpoints, mobile, servers and VDIs.
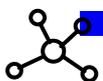
Network
- Gateway-based solution
- API-based solution integrates seamlessly with network solutions through REST-APIs, ICAP or SCAP
- Provides a numerical verdict of the malicious status to support remediation response
- Files can be transferred over gateways (web, email or network FW), storage devices or cloud drives

Endpoint
- Agent-based autonomous solution
- Services multiple operating systems
  - Windows
  - macOS
  - Chrome OS
- Supports VDI environment
- Online or offline protection
- Lightweight model with low memory consumption

Mobile
- Agent-based autonomous solution
- Services both iOS and Android
- Lightweight model with low memory consumption

REAL-TIME IS TOO LATE

Pre-Execution
Predict & Prevent

- **Deep Static Analysis:**
  On broad range of files types preventing the attack before the files are accessed or any process is executed.
- **File reputation service (D-cloud):**
  Both for known malicious files and benign files.
- **Script control:**
  A compliance and policy infrastructure eliminates the script based attack surface.
- **Blacklisting:**
  Blacklist files based on hashes, based on IoCs, and based on import IoC lists.

On-Execution
Detect & Automatically Respond

- **Deep Behavioral Analysis:**
  Detect and remediate enhanced ransomware threats, code injection techniques, known payloads etc.
- **Automatic Threat Hunting & Response*:**
  Detect and remediate active adversaries operating inside the organizational network.

*Upcoming version

Post-Execution
Automatically Analyze & Remediate

- **Deep Classification:**
  Rapid classification of malware (known & unknown) in zero-time, with no human involvement.
- **Attack Chain:**
  Root Cause Analysis to describe the process chain that led to the event.
- **Advanced Threat Analysis:**
  A set of tools that perform advanced analysis on threats found within the organization.
- **Remediation:**
  Mitigation and operation of existing threats identified in the environment. This includes: quarantine file and restore, file deletion, terminate running process, isolate device network and whitelisting files based on hashes, certificates and/or paths.

No Trade-Offs
- Highest prevention rates
- No false positives

Low TCO
- Minimal human intervention
- User friendly with an easy management console

Zero Risk
- Fast & easy deployment
- Not dependent on Internet or Network connection

High Efficiency
- 1 to 2 updates required annually
- No business interference

CUSTOMER TESTIMONIALS

"By teaming up with Deep Instinct on the development of HP Sure Sense, we are providing end users with a powerful solution that confidently predicts and prevents security threats both today and in the future."

**Andy Rhodes | Global Head Commercial
Personal Systems**
HP Inc

"We've tried other sources of cybersecurity in the past, but they weren't enough to protect against the level of sophistication that we're seeing in these malware and bot attacks today. With deep learning AI protection from Deep Instinct, not only are we able to stay ahead of the threats with the company's prevention-first approach, we can stop them before they ever become an issue. For a large airline like ours, serving over 90 million passengers a year across the Asia-Pacific region, it's essential to our business."

Declan Hogan | Group CIO
AirAsia

"We believe AI-based deep learning tools are the next wave in advanced cyber protection. Because these tools are autonomous and constantly learning, not only do they require fewer updates— but unlike typical machine learning tools, they also require no additional human intervention and feature engineering, which helps lower support and management costs. Providing options like Deep Instinct to our customers allows them to be on the cutting edge of security, while enabling them to concentrate on growing their businesses."

Alex Ryals | Vice President of Security Solutions, Americas
Tech Data

"Deep Instinct checked all the right boxes and proved itself as the only technology capable of adapting to our unique environment, without disrupting our everyday business operations. The deep machine learning has surpassed our expectations, ensuring our customers remain safe and helped mitigate risks for attacks we might not even be aware of. We would recommend every retailer to work with a deep learning AI-based model for cybersecurity if they want to protect their customers and safeguard their assets against attack."

Bruno Mariano | Director Of Technical Support
Kings Food Markets

COMPLIANCE, CERTIFICATION & PARTNERSHIPS

INDEPENDENT 3RD PARTY TESTS

> " SE Labs' tests are renowned for being technically challenging and in depth.
> It's **RARE TO ACHIEVE 100 PERCENT RATINGS**, which is **PRECISELY WHAT DEEP INSTINCT HAS DONE** with
> its D-Client solution. It's impressive that the company's technology was capable not
> only of blocking all of the advanced threats, but to do so with **ZERO FALSE POSITIVES.** "
>
> Simon Edwards, CEO of SE Labs and chairman of the board of the Anti-Malware Testing
> Standards Organization (AMTSO)

COMPLIANCE & REGULATION

CERTIFICATION

TECHNOLOGY PARTNERSHIPS

STRATEGIC INVESTORS

INDUSTRY RECOGNITION

Cool Vendor for Digital Workplace Security

Awarded as Technology Pioneer

Rewarded the Infosec award for Artificial Intelligence and Machine Learning by Cyber Defense Magazine

Artificial Intelligence-Infused Security Solutions

Global excellence award from Infosecurity Products Guide

Most Disruptive Startup at Nvidia Inception Awards

Ranked by Forbes among the "Top deep learning companies in the world"

Fortress Cyber Security Award winner in the category of Software and Apps

Most Innovative Startup in the best of Black Hat Awards Program by Dark Reading editors.

ABOUT THE TEAM

Deep Instinct is leading the fight against global cyberthreats with a team of highly experienced cybersecurity and deep learning professionals who have proven success records.

Our cybersecurity team includes veterans of the Israel Defense Force's cyber units, National Intelligence units and executives from top global cybersecurity companies.

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.

BECOME ONE OF THE LEARNED FEW

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

+1-212-981-2703

www.deepinstinct.com

TEL AVIV
23 Menachem Begin Rd
28th Floor
Tel Aviv
Israel, 6618356

+972-03-545-6600

info@deepinstinct.com

SYDNEY
Level 3 100 Harris Street
Pyrmont NSW
Sydney 2009
Australia

+61-1800-355015

deepinstinct
BEFORE YOU KNOW IT