

THE DEEP INSTINCT 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 the brain learns to identify an object, its identification becomes second nature. Similarly, as Deep Instinct's artificial brain learns to detect any type of cyber threat, its prediction capabilities become instinctive. As a result, zero-day and APT attacks are detected and prevented in zero-time with unmatched accuracy.

Deep Instinct brings a completely new approach to cybersecurity that is proactive and preventative. The comprehensive defense is designed to prevent the most evasive, unknown malware in zero-time, across an organization's endpoints, servers, and mobile devices.

PARTNERSHIP ECOSYSTEM & CERTIFICATIONS

INDEPENDENT 3RD PARTY TESTS COMPLIANCE & REGULATION



TECHNOLOGY PARTNERSHIP



CERTIFICATION



STRATEGIC INVESTORS



INDUSTRY RECOGNITION



GLOBAL LOCATIONS

**NEW YORK
HEADQUARTERS**
501 Madison Ave
Suite 1202
New York City, NY
USA, 10022
+1-212-981-2703

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

SYDNEY
Level 3 100 Harris Street
Pyrmont NSW
Sydney 2009
Australia
+61-1800-355015

TOKYO
Asgent Inc 6-4
Akashicho, Chuo-ku
Tokyo, 104-0044
Japan
+81-3-6853-7401






CONTACT US

info@deepinstinct.com

deepinstinct
BEFORE YOU KNOW IT

DEEP INSTINCT DEEP LEARNING PLATFORM

ANYWHERE

-  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

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**



“...Because these deep learning 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**



“...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.”

**Declan Hogan | Group CIO
AirAsia**



5 BENEFITS OF APPLYING DEEP LEARNING TO CYBERSECURITY

1

Raw Data Training – Deep learning is the only AI method capable of training directly on raw data. It therefore achieves better resilience and can be trained for extreme scenarios.

2

Independent of Human Intervention – Due to deep learning’s ability to achieve industry highest prevention rates and lowest levels of False Positives, it minimizes the need for human intervention.

3

Analyze Any Type of Data – Deep learning analyzes any and all types of data, irrespective of the file type or the OS.

4

Non-linear Correlations – Deep learning achieves the highest detection rate and the lowest false positives due to its ability to analyze multiple levels of non-linear correlations and complex data patterns.

5

Unlimited Training Samples – As the only method that can scale to hundreds of millions of training samples, the deep learning algorithm continually improves as the training dataset grows.

To prevent the most sophisticated, evasive and unknown malware, learn more about deep learning’s application to cybersecurity.

