DEEP INSTINCT EDUCATION SOLUTION BRIEF

WE PREVENT WHAT OTHERS CAN'T FIND

deepinstinct™
BEFORE YOU KNOW IT

www.deepinstinct.com

Since 2016 over 1,000 school districts, colleges, and universities have experienced a successful cyberattack, and that number is on the rise. With such a diverse user base with varying levels of cybersecurity awareness, IT and security teams need solutions that prevent attacks with little to no human expertise required.

Deep Instinct is uniquely able to meet the needs of security teams in educational institutions. By delivering prevention first, no-hassle products Deep Instinct helps security teams eliminate both the pervasive threats targeting their institutions while lowering the cost and resources required to keep students, teachers, and administrators secure.

Unlike other security products that update continuously, consume significant computing resources, and only work when managed by security experts, Deep Instinct uses deep learning to deliver the widest variety of operating systems and environments security with minimal overhead and resources.

By deploying a lightweight agent to all endpoints and servers, Deep Instinct acts as a 24/7 security analyst watching every asset for any sign of attack. When an attack occurs, Deep Instinct springs into action immediately, thwarting the attack by quarantining files, killing malicious processes, and isolating impacted assets to ensure every student's education is uninterrupted.

> The primary reason that I selected Deep Instinct is due to the benefit of having their agent on every single endpoint, which is like having a cybersecurity analyst sitting there looking over the shoulder of the end user all the time. Another reason is that there is no other product out there on the market that does what it does, the way that it does it, and to the degree that it does it well.
>
> Matthew Frederickson
> Director IT of Council Rock School District

THE DEEP INSTINCT ADVANTAGE

Deep Instinct is leading the Third Wave of security solutions, finally delivering on the promises made by many next-gen security vendors. While hyper-focused on preventing as many attacks as possible and providing all the necessary information needed for analysis and remediation, Deep Instinct invests significant development hours and capital resources developing the first-ever end-to-end cybersecurity deep learning framework. This flexible framework enables Deep Instinct to detect threats on the widest variety of file types across different operating systems, faster and more accurately than previously thought possible. In addition to highly accurate threat prevention, the Deep Instinct approach to security also dramatically decreases Total Cost of Ownership (TCO) and false-positive rates that typically result when attempting to maintain a resilient prevention postures.

With Deep Instinct, you get:

1

Zero-Time Prevention

Many vendors describe their prevention occurring pre-execution or in real-time; however, what they mean is that if a user attempts to run a malicious application, their solution can stop it. At first glance, this sounds reasonable; however, upon further analysis, this approach to prevention means the malicious files are resident on the school's machine, making the hard drive a virtual field filled with landmines. Deep Instinct is the only solution delivering zero-time prevention, inspecting every file as they appear on disk, automatically removing any file deemed to be malicious, ensuring users cannot interact with the files. This approach eliminates the risk associated with leaving idle malware on disk. With Deep Instinct, there is no virtual field of land mines, machines are kept in a continually trusted state, anytime, anywhere.

2

No "Trade-off" Security

It is an accepted fact that increasing detection controls results in a higher rate of false positives. If the goal is to prevent as many threats as possible, it makes sense that as detection thresholds tighten, some mis-categorization can occur. Given this fact, many security teams continuously work to balance their prevention settings with their capacity to investigate false positives; we call this the prevention trade-off dilemma. Deep Instinct uniquely does not inflict this difficult trade-off decision on users. Using Deep Learning, which trains on the entire contents of malicious and benign files, the Deep Instinct solution identifies malware, known and more importantly unknown first seen malware, in milliseconds with high efficacy and unheard-of false-positive rates. This prevention capability ensures security teams do not have to make the problematic trade-off decisions required by other security products that commonly see sharp increases in false positives as they attempt to prevent more threats.

3

Broad Attack Surface Protection

With a wide variety of file types, operating systems, virtual environments, cloud environments, and mobile devices protected against the most common attack vectors (ransomware, malware, fileless attacks, phishing attacks, dual-use, PowerShell, etc.) Deep Instinct delivers consistent security across a diverse attack surface. Substantially driving down the total cost of securing the organization's complete digital workspace.

4

No Operational Headaches

Since the Deep Instinct deep learning brain is pre-trained, there is no need for constant security updates, continuous Internet connectivity, or burdensome maintenance to keep pace with threats. With only 1 to 2 updates a year, security teams have more time to work on other vital projects, effectively increasing the size and capacity of the security staff without adding resources or swelling budgets.

DEEP INSTINCT´S DRIVING PRINCIPLES

When selecting a cybersecurity vendor to partner with towards protecting your users and environment from harm, it is essential to understand the vendors' philosophy. At Deep Instinct, we operate under the following three driving principles in all that we do:

1

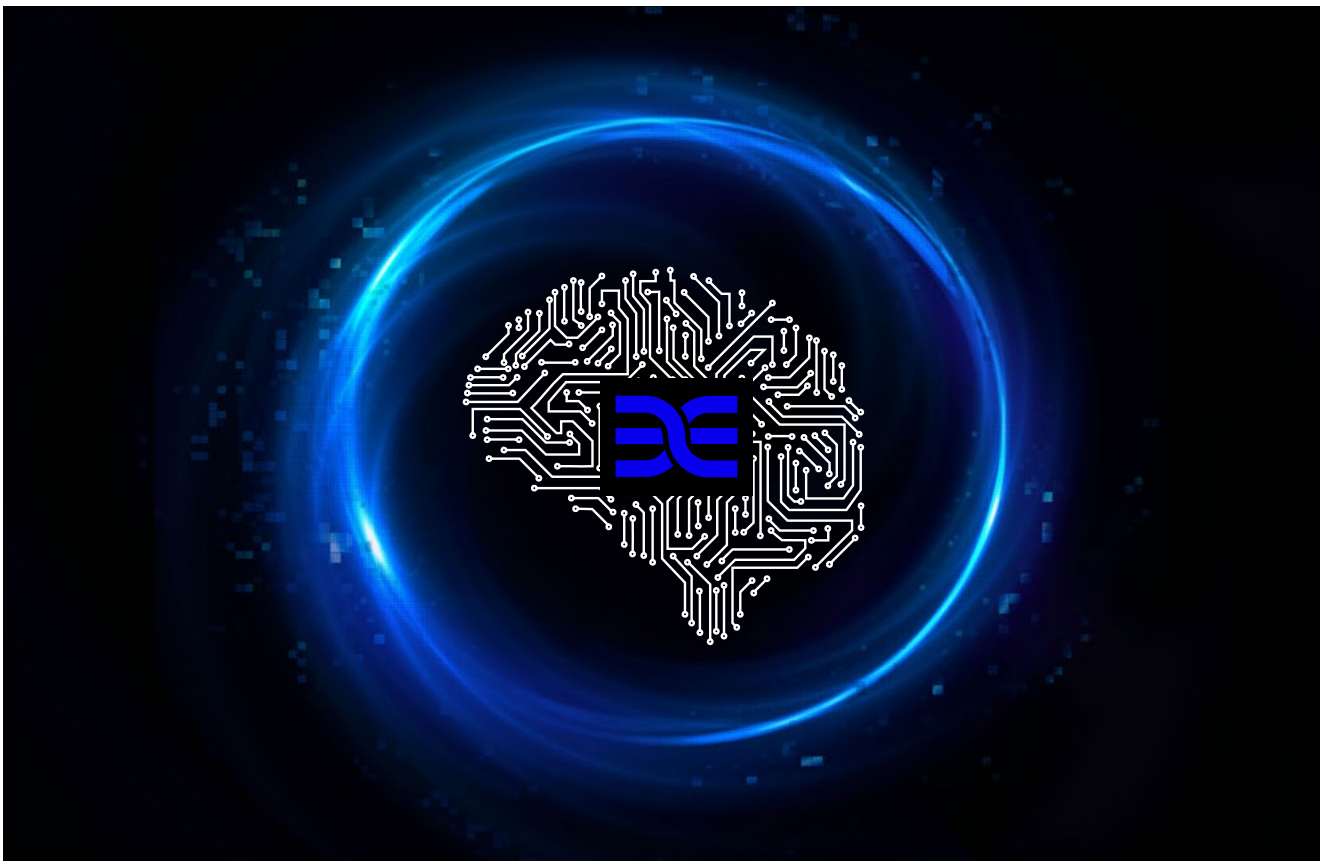
Strive to prevent all known and unknown threats using deep learning

2

Make detection and response automated, fast and effective for any threat that cannot be prevented

3

Deliver effective, intuitive security solutions that anyone can use



As you learn more about Deep Instinct, you will see these driving principles represented in how we deliver the capabilities security teams need to stay a step ahead of attackers. Nowhere are these principles more visible than in the Deep Instinct multi-layered approach to security.

DEEP INSTINCT MULTI-LAYERED APPROACH TO SECURITY

The only way to deliver continuous security across a diverse educational environment is to take a multi-layer approach to security. The Deep Instinct approach ensures no matter when or where an attack occurs, the solution can act fast to neutralize the threat and the damage that could follow.

ZERO-TIME
PREDICT & PREVENT

- Static File Analysis
- Instant File Reputation
- Script Threat Prevention
- Blacklist Threat Prevention

RUN-TIME
DETECT & DEFEND

- Dynamic Behavioral Analysis
- Automated Threat Hunting*

ON-TIME
REVIEW & REMEDIATE

- Root Cause Analysis
- Auto-Threat Classification
- Advanced Threat Analysis
- Targeted Response

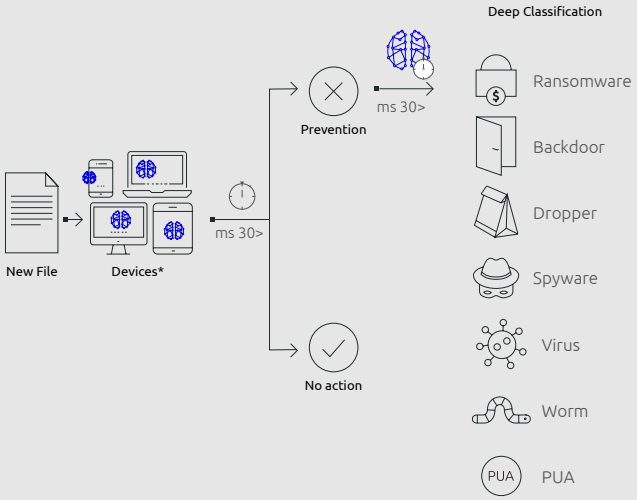
*Next Version

First, Deep Instinct's **Zero Time Predict and Prevent** layer uses deep learning to identify malicious files to thwart attacks before they can ever begin. As new files or processes are identified, Deep Instinct scans the file/process and determines intent in less than 20 milliseconds. In an instant, malicious items are prevented from running. With additional capabilities such as instant file reputation, blacklists, and dynamic script control, users of Deep Instinct can see dramatic results, from lower false positives to high output across the entire security team.

Deep Instinct's **Run-Time Detect and Defend** layer builds upon the Zero-Time capabilities by delivering dynamic behavior analysis designed to uncover suspicious behavior fast. With native anti-ransomware, remote code injection, known shellcodes and PowerShell command or script execution, Deep Instinct delivers a security solution able to detect and prevent advanced attacks before they cause harm.

Lastly, Deep Instinct's **On-Time Review and Remediate** layer provides visibility into the attackers targeting your educational institution and facilitates the ability to take decisive actions fast. Auto-threat classification and advanced threat analysis give security teams the information they need to understand how an attack occurred and what the attackers were attempting to achieve. With a variety of targeted response options built-in, any security analyst can ensure the attackers' current efforts are terminated and guard against future attacks.

HOW WE PREVENT FILES ON THE DEVICE



Lightweight D-Client*
Low memory footprint (<120MB), requires less than .1% CPU usage on average

DEEP INSTINCT BROAD PROTECTION AGAINST THREATS TYPES

No other security solution on the market delivers the breadth of attack coverage of Deep Instinct while ensuring the solution is intuitive enough for any security analyst to use.

Ransomware

- Protection against any type of ransomware

Spyware

- Banking trojans
- Keyloggers
- Credential dumping
- Botnet

File-based Malware

- **Executables** – Virus, Worm, Backdoor, Dropper, PUA, Wiper, Coin-miner
- **Non-executables** – Documents (Office, PDF, RTF), Images, Fonts, Flash, Macros
- **Known shellcodes**

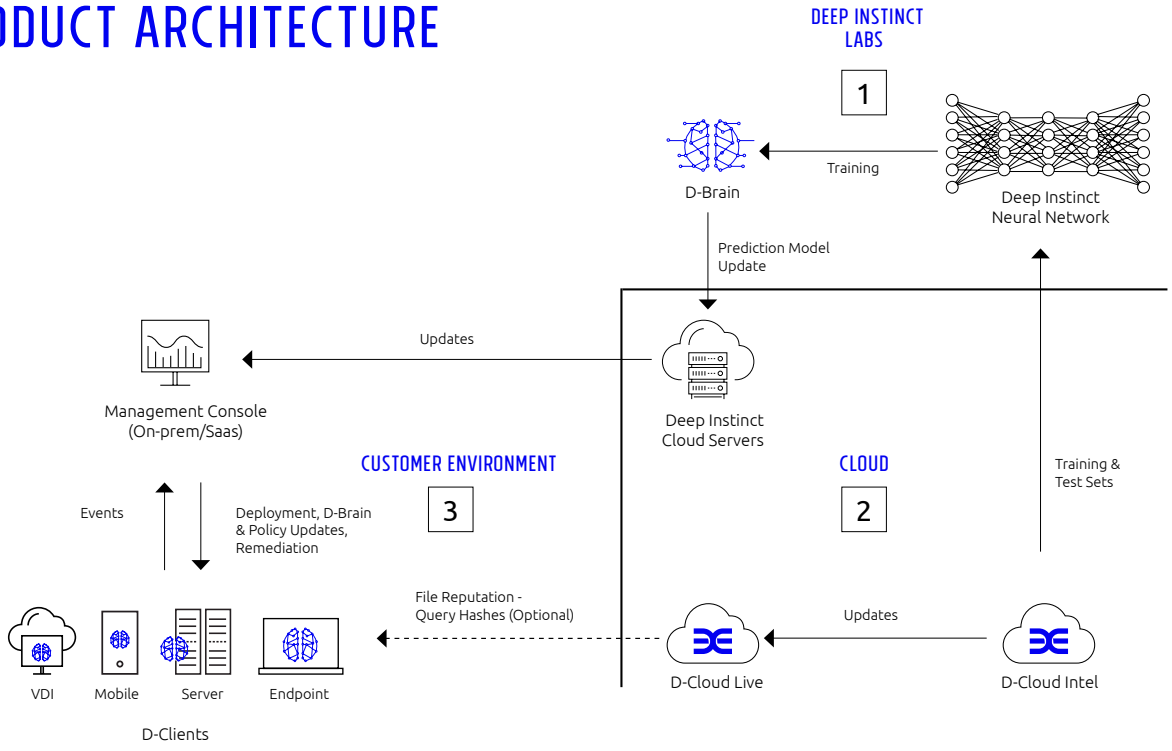
File-less Malware

- **Scripts** – PowerShell, VBScript, JavaScript
- **Code Injection**
- **Dual-use tools**

Exploits

- Documents
- Flash files
- Images
- Fonts

PRODUCT ARCHITECTURE



SYSTEM REQUIREMENTS

Operating System	Windows 7 SP1, 8, 8.1, 10 Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016
.NET Framework	Version 3.5 or higher
CPU	Dual-core CPU or higher
RAM	2 GB or higher (recommended 4 GB)
Disk Space	500 MB free disk space

SUPPORTED VIRTUAL ENVIRONMENTS

Amazon Workspaces
Citrix Systems XenServer, XenDesktop and XenApp
VMware ESX and Horizon
Microsoft Hyper-V
Oracle VirtualBox

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

UNITED KINGDOM
5 Ribbon Pond Drive
Newark on Trent
Nottinghamshire
NG24 3WW

+44 7810 553692

deepinstinct
BEFORE YOU KNOW IT