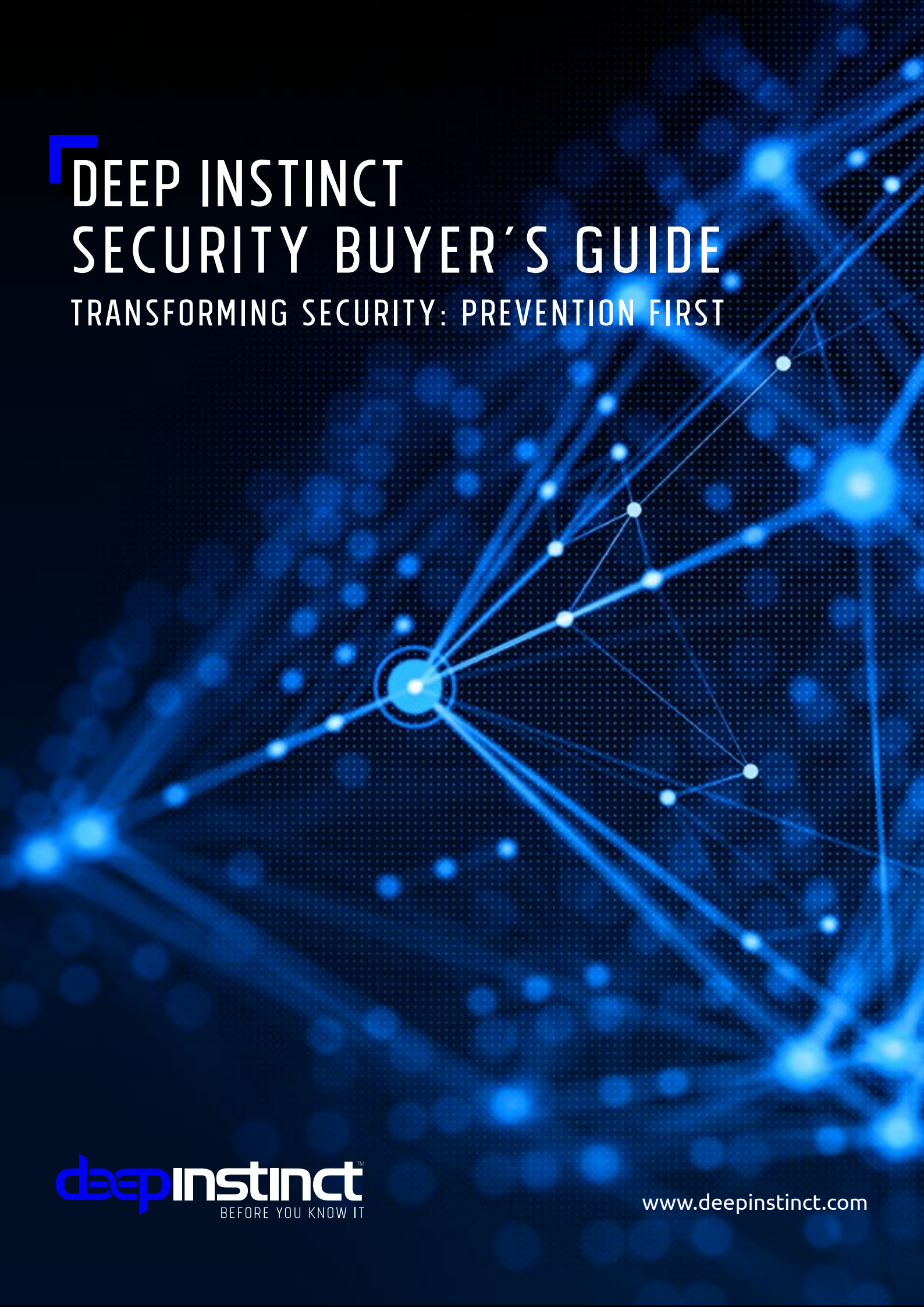
DEEP INSTINCT SECURITY BUYER'S GUIDE

TRANSFORMING SECURITY: PREVENTION FIRST



deepinstinct™
BEFORE YOU KNOW IT

www.deepinstinct.com

TRANSFORMING SECURITY

PREVENTION FIRST.

If you were to audit a typical organization's security stack, you would find a series of elaborate security controls built to protect specific segments of the environment, types of data, or user behaviors. Whether it is Data Loss Prevention (DLP) attempting to keep sensitive data secure or a Security Incident and Event Management (SIEM) correlating security events to identify potential threats, the security controls in the security stack primarily deal with the results of a successful attack.

The unintended consequence of this approach to security stack architecture is a constant flow of security alerts, all of which must be addressed by an already overburdened security team. Year after year, reluctant CISOs and CIOs renew their licenses for these complex security products even though many are less than satisfied with the results. A recent Ponemon Institute study found that 50% of the over 600 respondents felt their organization makes investments that do not improve overall security posture. The question to ask is, why? Why, after years of investment in best-of-breed security products, do many organizations still feel highly susceptible to widespread compromise?

The answer, unfortunately, is that the security stack you find in most organizations has a built-in bias toward dealing with the after-effects, or triggers, of a successful attack. Most security tools don't tackle the much harder, but more valuable, problem to solve; the root cause for the security challenges faced by the organization causing porous prevention controls.

Deep Instinct is a prevention first security company built on the belief that every organization deserves security solutions that do everything it can to prevent a successful attack first and foremost. If prevention does not occur, Deep Instinct is committed to delivering solutions that make the detection, investigation, and response to the suspected threat as simple as possible. Using a dedicated deep learning framework, Deep Instinct delivers a solution that prevents attacks before they can begin. This preemptive approach dramatically reduces the workload on security teams, while simultaneously improving the security posture, making all the other security controls in the security stack more effective. Deep Instinct customers can see a significant reduction in the cost associated with attacks, up to 90%, enabling security teams to take on more strategic projects without increasing their budget.

THE DEEP INSTINCT ADVANTAGE

Prevention is not a new concept for security practitioners and decision-makers. A few years ago, many organizations took notice of a new set of vendors touting a different approach to prevention. These Next-Gen security providers promoted their use of traditional machine learning to identify threats and many organizations took advantage of next-gen solutions to replace their legacy products. Unfortunately, as time progressed, challenges emerged with many of these new solutions that were not initially evident.

1 First, the machine learning methods used to identify threats rely on human-selected features (or characteristics) of malicious files. Attackers understanding this "feature" approach identified techniques to "trick" the models into determining their malicious files were benign. The ability to bypass the machine learning model coupled with the increasing complexity and sophistication of recent attacks leaves most machine learning solutions struggling to deliver expected results.

2 Further, due to the feature selection approach, these models routinely misidentified benign files as malicious (false positives), resulting in a significant and unnecessary resource drain.

3 Finally, most of the machine learning models in the market only support portable executable (PE) files meaning attacks that use other types of files move freely past the prevention solution.

Vendors facing these challenges began shifting away from prevention innovation and moved towards detection and response solutions. Many early adopters found themselves with a difficult choice; either return to their legacy security providers or continue to build out their security stack with advanced detection and response tools. Many opted for the latter option, so now you see these next-gen players delivering detect, and response products meant to fill the emerging gaps in their prevention capabilities. While neither the legacy nor next-gen providers claimed 100% prevention (which we all know is never possible), organizations are only moderately, if at all, in better shape than they were before Next-Gen providers hit the market.

Deep Instinct is leading the *Third Wave* of security solutions finally delivering on the promises made by the next-gen security vendors. Deep Instinct invested significant development hours and capital resources in 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 posture.

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 machine, making the hard drive a virtual field filled with landmines. Deep Instinct is the only solution delivering zero-time prevention, inspecting every file and process as they appear or move on disk, automatically removing any file/process 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.

THE 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

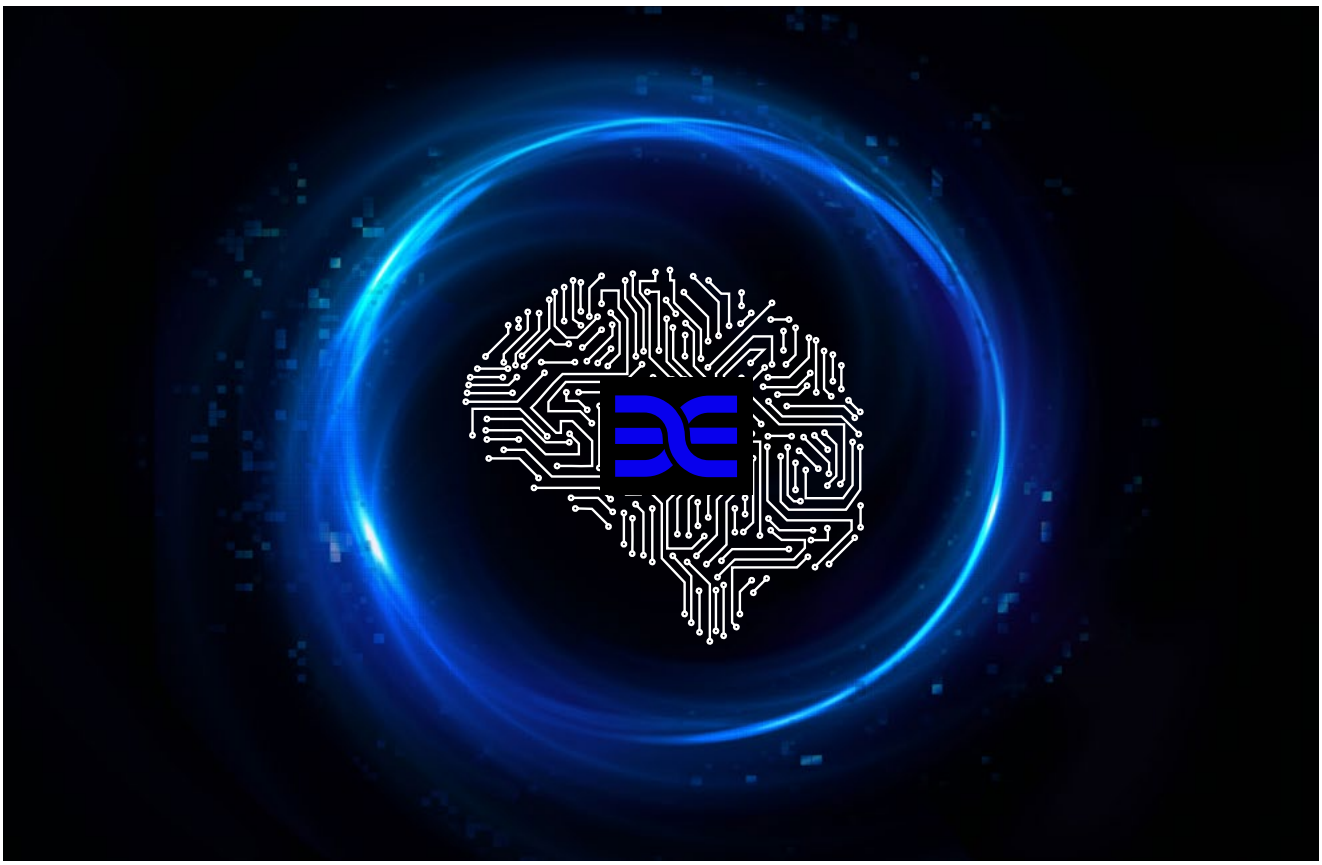
Strive to prevent all known and unknown threats using deep learning

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.

THE DEEP INSTINCT MULTI-LAYERED APPROACH TO SECURITY

The only way to deliver continuous security across a diverse 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

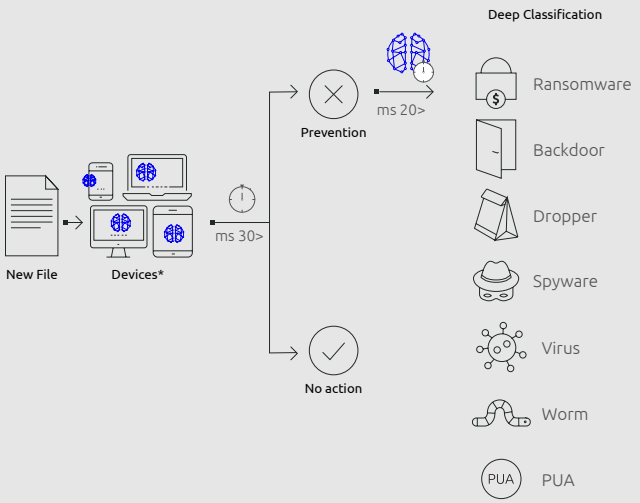
*Next Version

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 organization 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

THREE COMMON SCENARIOS WHERE DEEP INSTINCT CAN TRANSFORM YOUR APPROACH TO SECURITY

Replacing an Existing Antivirus (or Next-Gen AV) Product

For many organizations, the AV represents a checkbox solution needed to meet compliance or regulation requirements. Security teams need to ensure updates to signatures are downloaded and applied as required. They place little effort in providing the product is tuned specifically to relevant use cases.

Other organizations, on the other hand, attempt to squeeze as much capability as they can from their AV, creating complex configurations and "workarounds" to trap as many threats as possible. The good news is that you can easily combine Deep Instinct with the security capabilities available in Microsoft Windows to meet your needs. Whether due to an upcoming renewal event or, worst case, a severe breach, Deep Instinct can replace your aging legacy AV or next-gen AV product, immediately delivering noticeable gains in prevention while lowering the total cost of ownership.

AV Requirements	Legacy AV	Deep Instinct
Anti-Malware	✓ Signature-based: effective against known malware	✓ Deep learning-based; effective against known and unknown
Desktop Firewall	✓	Augment with Microsoft Windows 10
URL Filtering	✓	Roadmap
Scheduled Scans	✓	✓ (optional, not required)
Disk Encryption	✓	Augment with Microsoft Windows 10
On-Demand Malware Cert	✓	✓
Windows Security Center Integration	✓	✓

Augment an Existing AV Suite

Many organizations are using multiple features and products from their AV vendor, which makes replacing the AV suite problematic. In this scenario, Deep Instinct can be deployed as an augmentation to the existing AV product with no conflicts. For example, Deep Instinct's zero-time, run-time, and on-time security capabilities ensure threats do not impact the environment. At the same time, the existing AV suite can handle other tasks such as personal firewalls and encryption.

Augment a New or Existing Endpoint Detection and Response (EDR or XDR) Product

Many organizations in search of better security opted for a product designed to record every action on an endpoint to detect and respond to potential security incidents, perform threat hunting activities to gain better visibility across their environment. This post-execution-focused solution, known as Endpoint Detection and Response (EDR or XDR), continuously runs a series of rules against this repository of endpoint data (and other sources in the case of XDR) data to identify potential threats. When a rule triggers a security incident/alert, the security analyst must then investigate to determine the appropriate response. These tools provide a "backstop" against threats that get past an organization's prevention controls. However, many a security team finds themselves flooded with alerts from their EDR/XDR solution due to the poor performance of their prevention control. Most security teams ultimately opt for their EDR/XDR to be managed by a service provider with appropriate expertise. Here is a perfect situation where Deep Instinct can drive improvement across the security stack. In this scenario, Deep Instinct can be deployed alongside the existing EDR/XDR solution with no issue. With no changes to the current EDR/XDR deployment, security teams will see a dramatic decrease in the volume of alerts. Over time the security team can then audit the rules in their EDR/XDR solution eliminating rules that are no longer required and adding additional rules aimed at rooted out advanced multi-stage attacks.

Measuring Deep Instinct's Performance

Deep Instinct intends to deliver products that do everything possible to prevent attacks from executing. To that end, when measuring the performance of Deep Instinct, you will want to ensure you have a baseline before deploying the solution. In most organizations, the benchmark should include the following metrics:

- Number of skilled people needed to analyze alerts
- Number of successful attacks per week/month
- Number of false positives per week/month
- Time spent maintaining EPP/AV solution completing tasks such as
  - Applying signature updates
  - Whitelisting files
  - Blacklisting files
  - Applying other exceptions
  - Investigating alerts that turned out to be false positives
    - Recovering from false negatives
    - Reimaging machines
    - Restoring machines from backups
    - Locking user accounts
    - Etc.

With this information collected, you can now deploy Deep Instinct across your endpoints, servers, virtual and cloud environments as required.

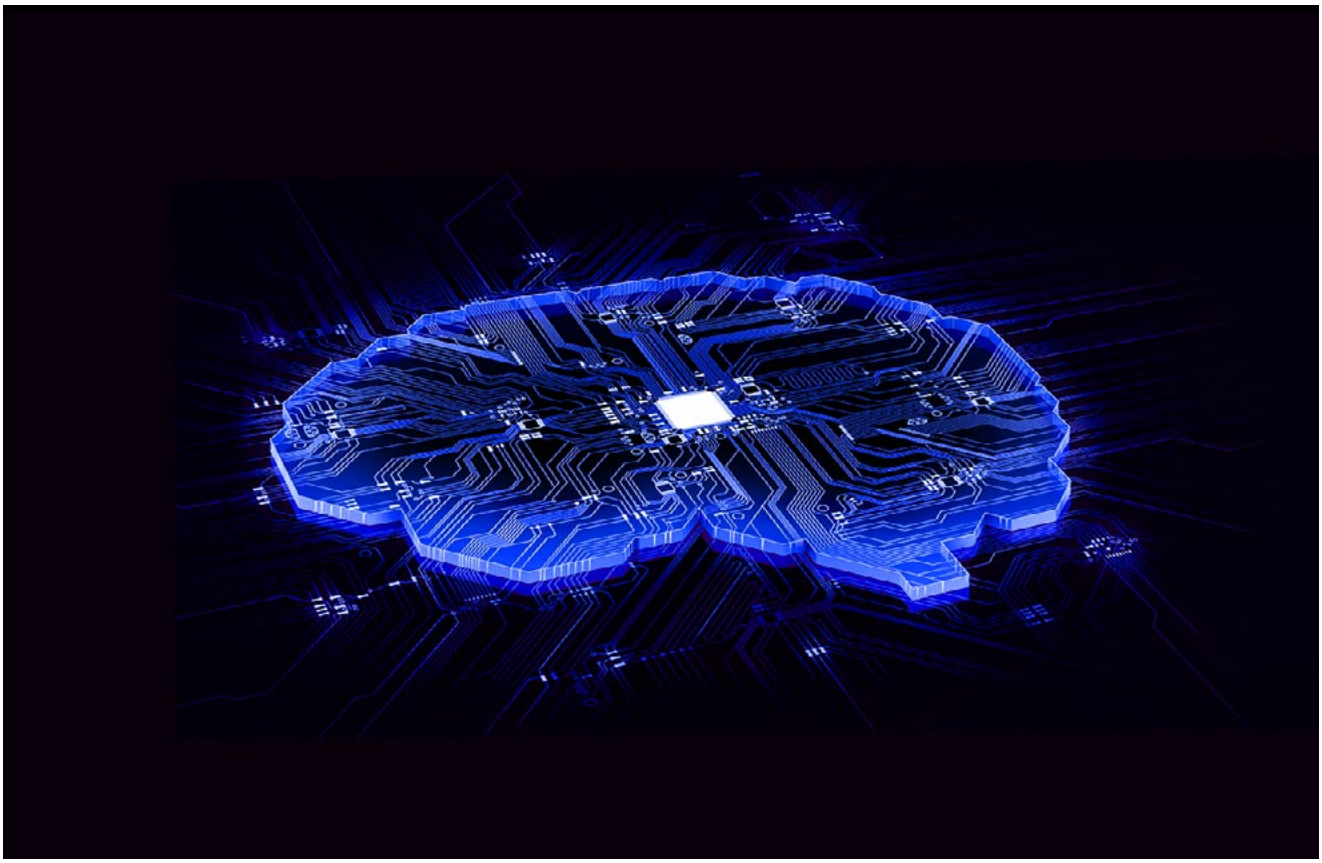
Deploying Deep Instinct

With Deep Instinct, there are no regular updates required or additional model training required, so the product will begin to deliver value immediately. As part of the initial deployment, Deep Instinct will complete a comprehensive scan of the asset. This scan will identify known and unknown threats lying dormant on the machine as well as potentially unwanted programs, such as toolbars, adware, or dual-use tools that drive down the performance of the device.

Once this initial scan is complete, no other scan is required (unless deemed necessary to meet regulatory or compliance requirements). Now, each time a user attempts to download or move a file to the machine, Deep Instinct Static Analysis will scan the file as it moves onto disk. If the engine determines the file to be malicious, the file is blocked and sent to quarantine. This ability delivers the only zero-time prevention capability in the market.

If a malicious file does pass this static analysis phase, Deep Instinct includes behavior analysis capabilities purpose-built to root out activity commonly associated with malicious intent and terminate processes automatically. For instance, the ransomware protection triggers when any encryption action is detected while code injection and known payload protection provide additional capabilities to thwart an attacker's advances.

Once Deep Instinct has been operational for 30 days, take your first set of metrics for comparison against the baseline. For most customers, the difference in the first 30 days is dramatic, with a sharp decrease in successful attacks and a near-zero false-positive result. This result, in turn, means security teams spend virtually no time recovering from successful attacks and can focus their efforts on other strategic projects. Pull these same stats at 60- and 90-days post-deployment, comparing to the benchmark every month. Based on our experience with customers, after 90 days, the security team's productivity increases dramatically as well as the overall morale of the group as the deployment of the Deep Instinct solution expands. This information makes the business case for continued use of Deep Instinct straightforward.

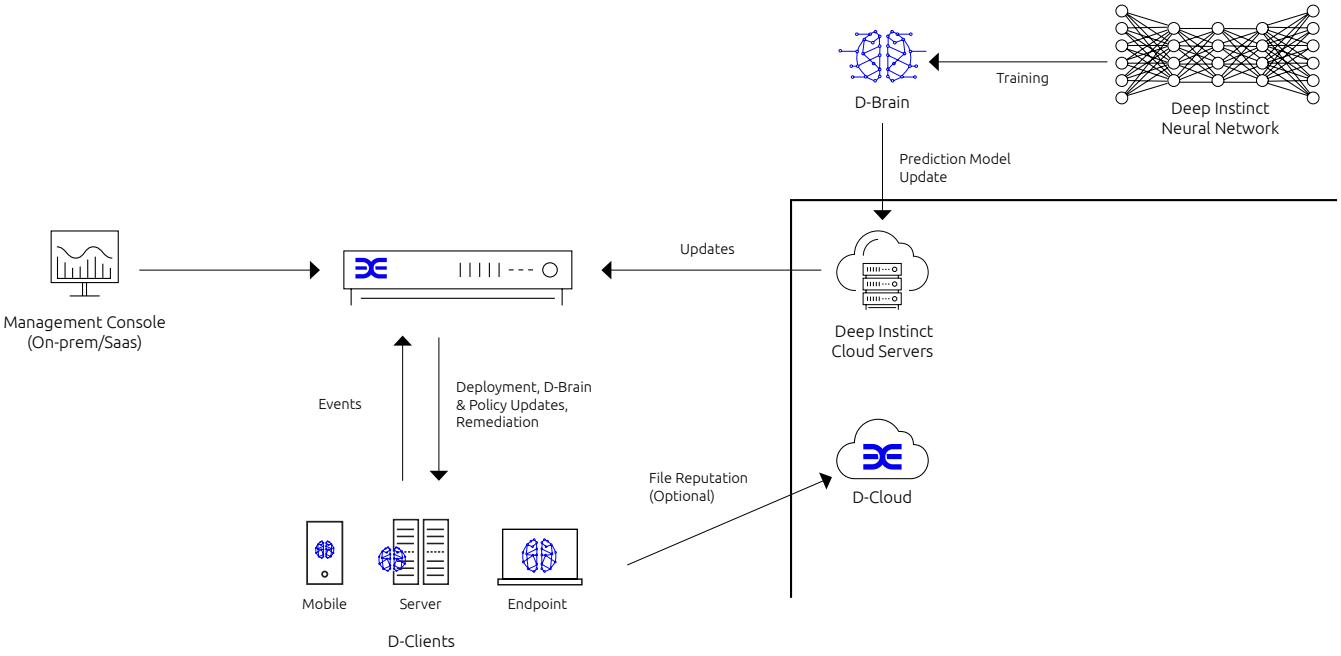


CONCLUSION

As the buyer of security products, we understand you have heard all these claims before from dozens of security vendors, so it is understandable that you need “to see it to believe it”. We take pride in our ability to prevent attacks and encourage potential customers to bring in our solution and test. Our team of security experts will work with your teams to determine the types of threats you are regularly facing and, in a controlled environment, show you how Deep Instinct performs. While anyone who claims 100% prevention or even detection is showing their lack of knowledge about the reality of cybersecurity, we are confident the results from the Deep Instinct solution will be compelling.

Better prevention. Fewer false positives. More time to work on other projects. Now is the time to take charge of your security.

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