Ransomware:

Prevention is Better than the Cure

E-BOOK

deep instinct™

www.deepinstinct.com

VANDIS

www.vandis.com

An Evolving Threat.

Today's greatest cybersecurity challenge?

The spectre of ransomware has moved to the front and center of every major news hub, with organizations such as Colonial Pipeline and the Ireland Health Trust showing the full scope of how severely ransomware can impact business operations and the bottom line.

We saw ransomware increase 435% between 2019 and 2020*. We see several reasons for the significant rise in this type of malware, including the significant fact that attackers have shifted their approach. In the period between 2016 and 2018, the core strategy of ransomware attackers was a volume-centric one that saw the consumer audience targeted on a large scale. The chances of infection were low, and in parallel, many individuals who had their machines and data encrypted were unable or unwilling to pay four or five figure sums to regain access. Few individuals experienced a sense of high urgency to restore all data, and many had back-ups stored in the cloud via their smartphone provider.

A shift in strategy

From 2019 onwards, we witnessed a major shift from attackers to begin targeting large organizations that deliver emergency and life saving services or business critical services that have an outsized role across society or broad business verticals. In the organizations that are targeted, time spent mitigating a ransomware event could have a significant impact not only monetarily, but also on the lives and well-being of many people. Sectors at particular risk include manufacturing, government, energy/utilities, healthcare, financial services, education, and law enforcement.

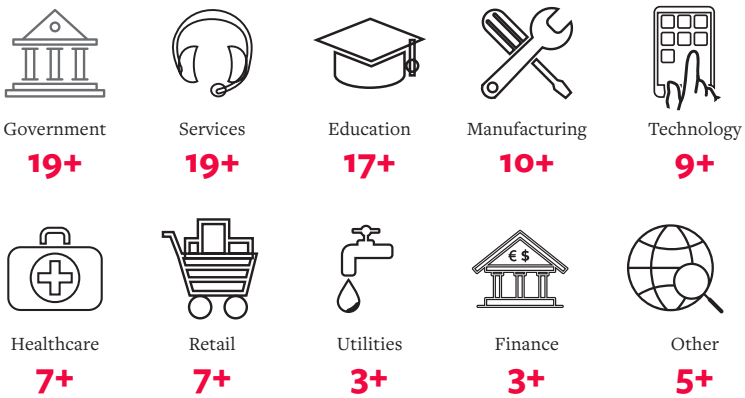
The impact of the Colonial Pipeline hack on millions of homes and businesses is a sobering reminder of the way ransomware can paralyze essential infrastructure. Sadly, this strategy seems to be paying off for some hacking groups, as they see their success in payouts and financial value increasing – with multi-million dollar payouts now the new normal. Many of these at-risk industries have made the decision that ransom payment is the best of a bad set of options available to them.

Ransomware-as-a-Service (RaaS)

Similar to the Software-as-a-Service (SaaS) model, RaaS is a subscription-based model that allows virtually anyone to launch ransomware attacks with little effort. This franchise model features cybercriminals writing code and then selling or renting it to other criminals. Franchisers supply technical guidance on how to start a ransomware attack and if the attack is successful, the ransom is split between the franchiser and the attacker. Much as a franchise model helped fast food chains increase their reach and revenues exponentially, RaaS has facilitated a massive increase in ransomware attacks.

2021 Leading Successful Ransomware Attacks by Industry

Data from January 2021–April 2021**



FACT:
RANSOMWARE ATTACKS

THE AVERAGE RANSOM PAYMENT HAS INCREASED BY *ALMOST 50%* IN 2021.

PAYOUTS AVERAGED $155K AT THE END OF 2020, BUT ROSE TO ALMOST $280K AS OF MAY 2021.

*Source: 2020 Cyber Threat Landscape Report, Deep Instinct
**Source: Blackfog. The State of Ransomware in 2021

Source: Blackfog. The State of Ransomware in 2021

Active Ransomware in 2021.

REvil/Sodin

This ransomware group has been around since early 2019 and really became a prominent and known force in the latter parts of 2019 based on their ability to attack MSPs with great success. The common ransomware dropped is Sodinokibi and follows the standard ransom request process without leveraging the threat of exposing the customer data or selling said data.

Ryuk/Conti

This group has been causing damage since 2018 – so it's by no means new – but it is still a formidable threat. As of March 2021, there was a shift in how this operates by adding wormlike capabilities which enable machine to machine transfer and removing the necessity to drop the payload to each machine by external means.

Egregor

This ransomware was typical in how it operated, but has been used less frequently as members of the organization have been arrested en masse. In 2020, one of the largest (and most successful) was the MAZE ransomware group which operated as a RaaS company. In November 2020 many MAZE members wishing to continue their work went to Egregor.

Netwalker

A very advanced ransom group which has had limited use post January 2021 due to seizure and arrests. Prior to this, Netwalker heavily leveraged Emotet and Trickbot as trojans to ensure access to networks and facilitate their propagation through environments they desired to ransom.

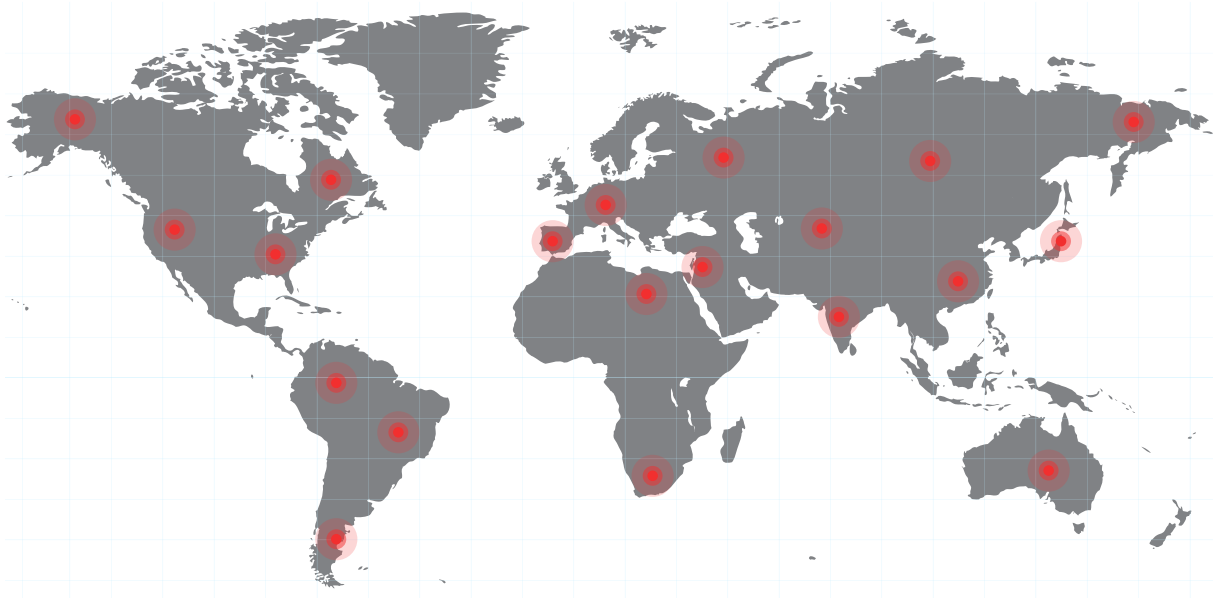
DoppelPaymer

This made the news in February 2021 as Kia Motors of America experienced an "outage" which was later confirmed to be ransomware, specifically DoppelPaymer. The intent was to impact Hyundai, but the attackers only managed to impact Kia with the attack. Unfortunately, this was a name and shame attack and Kia was threatened with leaks of "massive amounts of data" unless they paid the ransom.

Darkside

This was ransomware as a company/ransomware as a service provider from mid-2020 through mid-2021. This group first came to attention in August 2020 and portrayed themselves as the "good bad guys" who were performing a Robinhood function of taking from the "greedy corporations" and giving the proceeds of the attacks to charity.

It's also important to note this ransomware enterprise had a mission statement which prohibited attacks on educational institutions, non-profit organizations, medical facilities, or anything which could be considered "politically motivated."



Why Ransomware Attacks Succeed?

Every Second Counts

Current approaches to ransomware center around detection and response. In the case of Endpoint Detection and Response (EDR) most require a threat to be executed before detection. EDR is specifically designed to detect suspicious activity that has successfully entered an environment (post execution). If a user clicks on a malicious file, it executes, and the endpoint can be compromised in less than .016 seconds! An advanced EDR solution can help victims:

- Identify the threats
- Track and record the threats
- Quarantine and contain some threats
- Remove some of the identified threats

An EDR solution comes into play based on the detections and kick off post detection, triage responses. EDR actions may include the following:

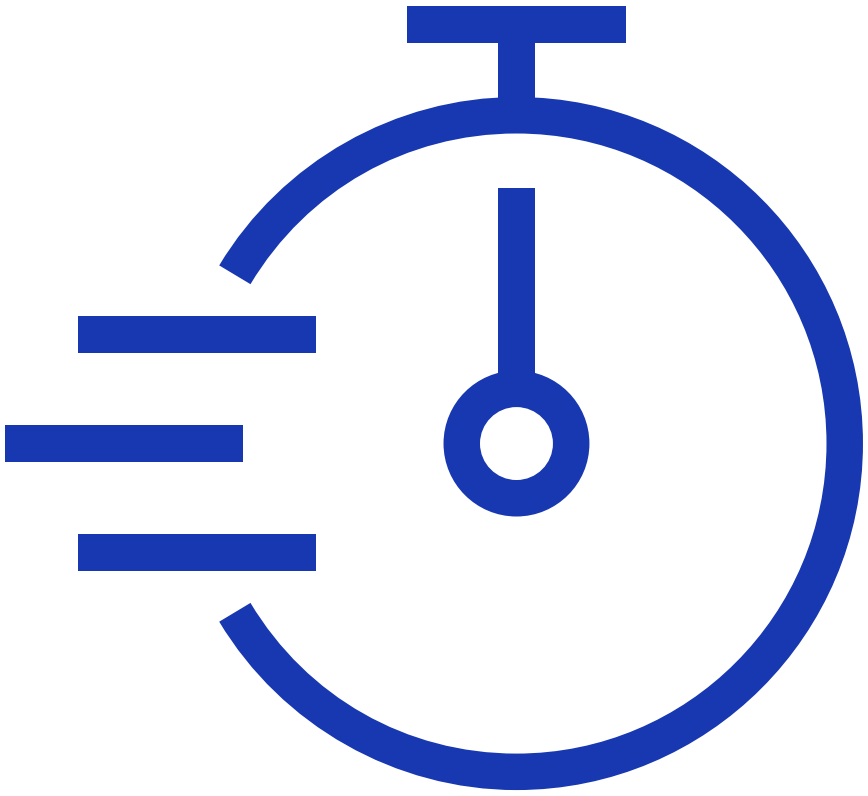
- Isolating the compromised host on the network
- Tracking and recoding of endpoint activities
- Reviewing the timeline and activities of events
- Collecting and documenting additional threat indicators
- Possible quarantine and removal of threat

The major challenge for organizations in this scenario is Dwell Time – that time between endpoint compromise and detection and response. A higher dwell time increases the chance for a malicious executable/file to run, spread, and drop more payloads, and attempt to obfuscate to avoid detection before an investigation can start.

63%

SAY **TIME IT TAKES TO IDENTIFY** AN ATTACK IS BIGGEST CYBER-ATTACK PREVENTION BARRIER

Source: The Third Annual Study on the State of Endpoint Security Risk. Ponemon Institute LLC, 2020.



The Future of Preventing Ransomware.

The world's only end-to-end deep learning cybersecurity framework

Deep learning has been around for some time time and has been applied to innovating some of the most advanced industries in the world – from car manufacturers to improve autonomous vehicles, to streaming services improving their recommendation engines, to search engine leaders driving improvements in voice recognition technology.

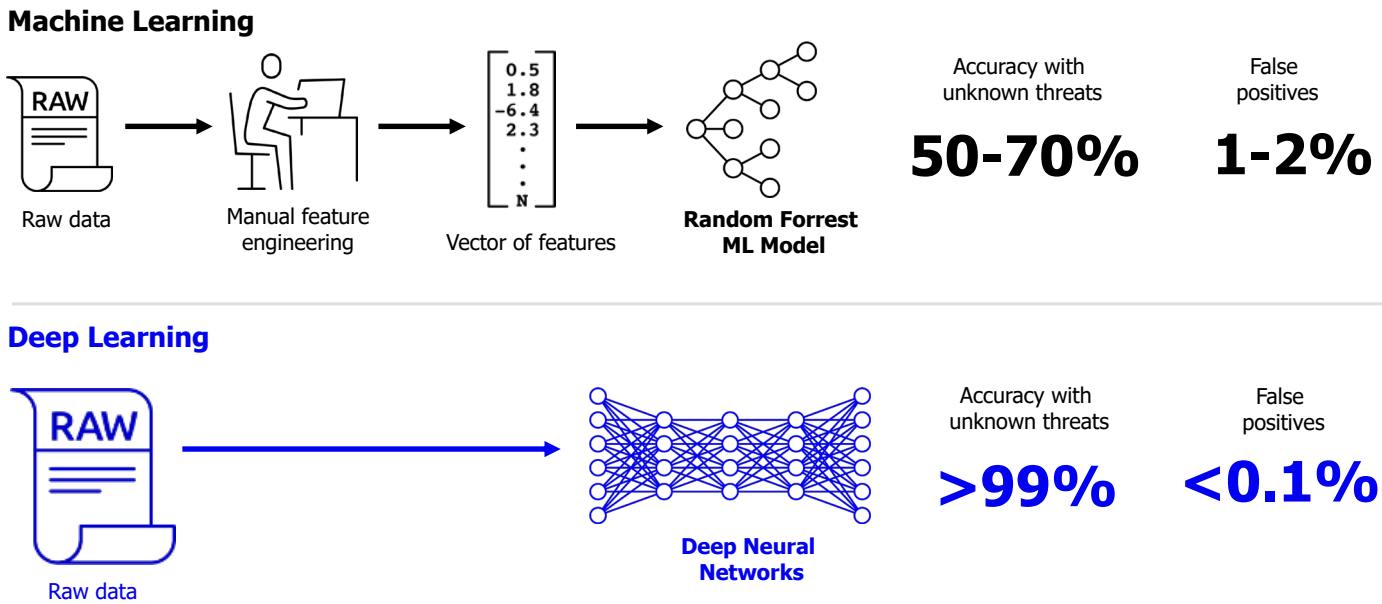
Historically, the barrier to entry to deep learning is high – it involves elite data scientists, requires vast computing power using GPUs (graphics processing unit), and works on huge volumes of raw data. Deep Instinct has risen to the challenge of harnessing deep learning tools to vastly improve cybersecurity detection and prevention and continuously enhanced the only purpose-built, end-to-end deep learning cybersecurity solution in the world. Our mission is to support organizations with the highest level of prediction and prevention available anywhere.

The limitations of Machine Learning (ML)

So how are we able to predict with such efficacy and speed? Deep learning features rich neural networks that have unique capabilities to solve tasks that machine learning models can't. Machine learning (ML) requires a human domain expert to define and engineer features for conducting classification. These features can be reverse engineered by bad actors, as was witnessed by the Cylance workaround.

On multiple occasions, our "brain" has detected major ransomware such as Ryuk even though it had not been updated for 12 or 18 months. We can predict threats that are not yet visible.

Quite simply, deep learning is far more accurate than machine learning based approaches. Perhaps best of all, there is no feature engineering, so it's far harder for bad actors to improve or create malware that understands how we work in order to breach our detection and response.



Source: The Challenges of Leveraging Threat Intelligence to Stop Data Breaches, Front. Comput. Sci., 28 August 2020

Prevent at Pre-Execution Phase.

One major differentiator customers notice is our ability to prevent at pre-execution phase. Our focus is on ensuring the threat never makes an impact, rather than working to limit or curtail damage after the fact.

Decisions taken more than 10x faster than real-time

Deep Instinct scans, predicts, and prevents any never before seen malicious malware or files, like ransomware, and stops the threat before it executes. This means that ransomware does not have the opportunity to enter the network and organizations will not have to worry about having their files encrypted or exfiltrated.

Deep Instinct performs these scans in less than 20 milliseconds, which means pre-execution decisions are made 10 times faster. Most current solutions are focused on post-execution detection which means the attack has already been executed and there is a higher chance of a successful ransomware campaign.

No need for cloud delays

The journey to the cloud and back to make a decision takes time, which can mean the difference between a ransomware threat taking hold or not. Deep Instinct can make a malicious vs benign determination without needing to send data to the cloud first.

ONLY

12%

ARE DEALING WITH RANSOMWARE ATTACKS AT THE PREVENTION STAGE

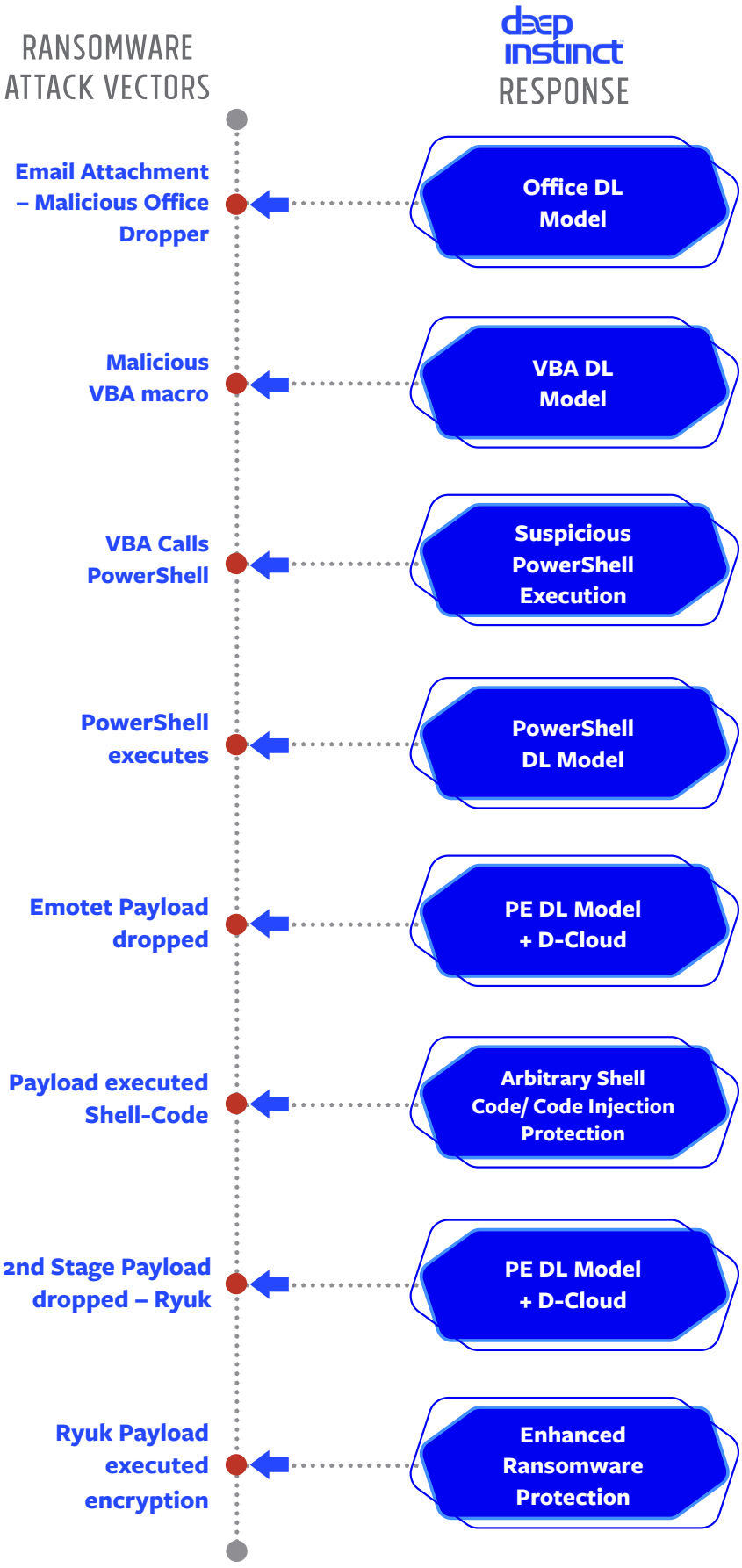
Source: The Third Annual Study on the State of Endpoint Security Risk. Ponemon Institute LLC, 2020.

FACT:

THE AVERAGE TOTAL COST OF A RANSOMWARE ATTACK IS $440,750, YET ONLY 10% OF THIS TOTAL COST HAS BEEN SPENT ON PREVENTING THIS TYPE OF ATTACK.

Source: 2020 Cyber Threat Landscape Report, Deep Instinct

More than "One Swing at the Ball."



Deep Instinct uses a multiple layered security approach, giving organizations many opportunities to prevent a ransomware attack.

The core of the product is Deep Static Analysis, or the D-Brain. The D-Brain uses deep learning, which provides far greater accuracy than signature, heuristic, and classical machine learning solutions. The Deep Static Analysis is broken down into multiple layers or models within the Deep Static Analysis.

These layers include the PE DL Model, Office DL, VBA DL, and PowerShell DL models. They all have their own role to play in protecting a system running the Deep Instinct platform. For example, the Office Model looks at Office Object Linking and Embedding: OLE, Office Open XML: OOXML, Embedded Macros (in OLE and OOXML files), Embedded DDE objects, or PDF (Portable Document Format) files.

Deep Instinct's Behavioral Analysis components include Enhanced Ransomware Behavior protections, In-Memory Protection, Remote Code Injection, Arbitrary Shell Code protection, Known Payload Execution, and Suspicious PowerShell Execution.

Lastly Deep Instinct's D-Cloud services provides an instantaneous lookup of the reported malicious file and categorize the type of threat being detected using a secondary DL model for classification.

Augmenting and optimizing existing security investments.

If we look at the typical cybersecurity landscape, many of the technologies below will be present. Deep Instinct complements all of these – for example, we help optimize EDR with actionable intelligence, cover offline assets with higher efficacy and remove cloud dependency vulnerabilities. Our deep classification lets SOC teams know exactly what they are dealing with.

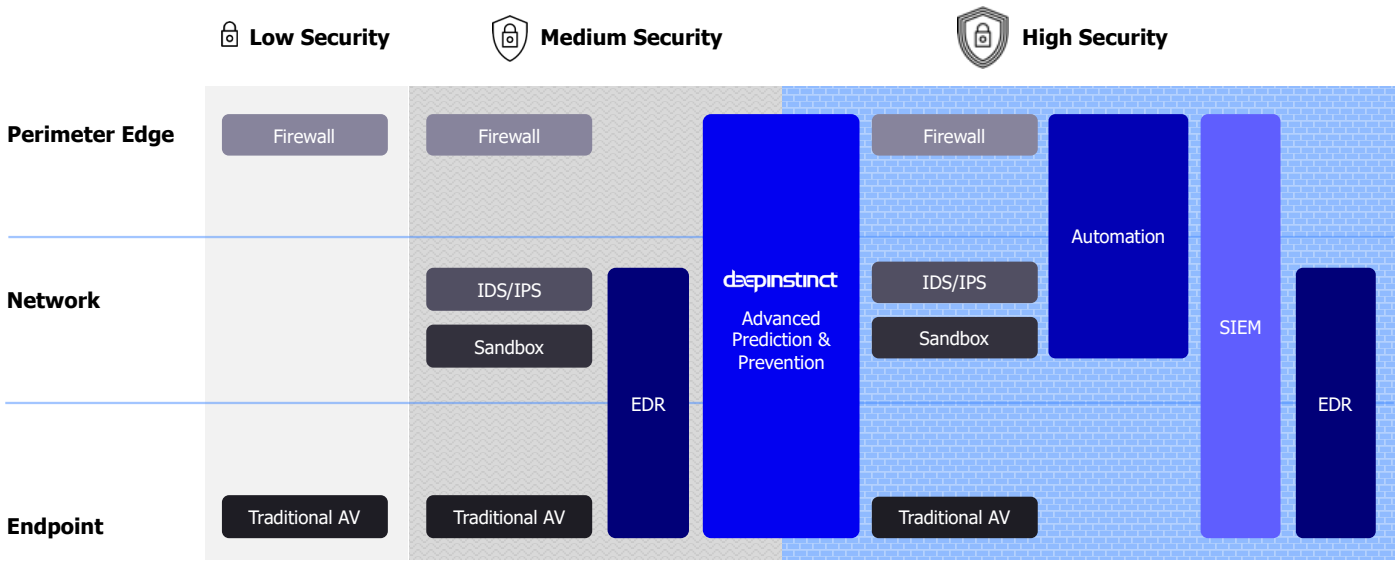
Most importantly, we support a key shift in threat posture philosophy – moving from reactive clean ups, to predicting and preventing at never seen before levels, yet still allowing EDR technologies to perform key roles, such as investigating security incidents.

Thousands of new highly advanced threats are developed and deployed daily. Today, organizations need a multi-layered approach of integrated solutions that work together to improve your security posture.

Threat actors know where to look for the vulnerabilities, weakness, and gaps in an organization's environment, network, or security posture. Our global dependencies on technology makes for a target rich environment that they can circumvent and easily bypass traditional antivirus software. The threat actors of 2021 employ highly developed tools to target vulnerabilities that leverage:

- Memory-based attacks
- PowerShell scripting language Remote logins
- Macro-based attacks
- And many others

Organizations need to review and reassess their basic cyber hygiene steps to improve their security posture. This reassessment includes examining the core role of each security solution. EDR can deliver a wealth of insights, but in parallel, the highest level of prevention is also required.



Frictionless implementation and immediate.

Fast and easy start

Some of our customers first tell us they already have several solutions in place and ask how Deep Instinct can complement your existing security stack and improve your efficacy, lower your false-positives and stop more threats.

Deep Instinct has a proven track record of fast and efficient deployments, with zero production impact. The D-Agents can be easily deployed, configured, and integrated into any deployment software and asset tracking solution via our REST API and standard deployment options.

Minimally invasive

With any new technology, security teams have questions around the resultant maintenance and admin that will be involved. Deep Instinct requires just several updates a year, yet remains highly effective even if an update is delayed. Compare and contrast this with existing "legacy technologies," which can involve monthly patches. Despite Deep Instinct's huge computing power, its footprint is actually tiny – less than 1% CPU consumption. This light footprint also means installation on endpoints typically takes less than 60 seconds.

Additional peace-of-mind

We have worked with one of the world's largest re-insurers, Munich Re, to offer two industry-leading warranties*. Available as part of the Premium Subscription package, they provide additional reassurance in two key areas:

Ransomware warranty of up to $3M

In the highly unlikely event of a successful ransomware attack, we will cover the operational costs of re-imaging, troubleshooting, and so forth. Per OFAC guidance, we do not condone paying the actual ransomware and this policy will not be used to pay or refund if the customer chooses to do that.

The industry's only false positive warranty

High false positive ratios massively reduce the efficiency and effectiveness of SecOps teams, creating unnecessary admin at the expense of more strategic activities. With dramatically lower levels of false positive alerts, security teams can be much more efficient, lowering total cost of ownership (TCO). We commit no more than 0.1 False Positive Events. In the event that a customer experiences more False Positive Events for two consecutive quarters, they will be reimbursed by us. No other cybersecurity vendor offers this form of performance commitment.

**Available when purchasing or renewing a two-year Premium Subscription package for 10k+ endpoints.*

"Post-proof-of-value, it took us about two weeks to have everything rolled out with just one IT employee overseeing the process."

Director, Information Technology, Education

Source: Forrester Research, "The Total Economic Impact Of Deep Instinct Advanced Endpoint Security Solution" The Cost Savings And Business Benefits Enabled By Deep Instinct Advanced Endpoint Security Solution NOVEMBER 2020

Elevating your current ransomware defense stance

Whatever your existing security investments (AV, MTD, EDR or others), Deep Instinct can help make these more effective. Deep Instinct is different.

Predict.

Using our unique deep learning deterministic and predictive algorithms, Deep Instinct can detect and prevent suspicious vs malicious threats with unmatched speed and efficacy even in today's ever increasing threat landscape.

Prevent.

By stopping threats at pre-execution, more than 10x faster than real-time, ransomware attacks have far fewer chances of being successful.

Promise.

Reflecting our confidence in our solution and commitment to customers, we offer:

- A ransomware warranty: providing of peace of mind, with coverage up to $3M.
- An efficiency warranty: a low false positive rate commitment.

VANDIS

Vandis, a Deep Instinct partner, provides Managed Services and IT Solutions to optimize the security and performance of network infrastructures, on-premise and in the cloud. We design IT solutions to meet each organization's unique needs and goals. From SMB to enterprise clients, Vandis delivers comprehensive strategies for secure IT infrastructures. www.vandis.com

Request a demo at www.vandis.com/contact-us

deep instinct

www.deepinstinct.com | info@deepinstinct.com

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack—providing complete, multi-layered protection against threats across hybrid environments.

© Deep Instinct Ltd. This document contains proprietary information. Unauthorized use, duplication, disclosure or modification of this document in whole or in part without written consent of Deep Instinct Ltd. is strictly prohibited.