# Executive Summary

Prevention Starts with Deep Instinct

The cyber threat landscape is deep, varied, and constantly evolving with new malicious tactics, delivery methods, and known as well as unknown malware. Most security platforms emphasize detection and remediation, focusing on assessing and responding once a breach has occurred and damage has been done. But this is a flawed and outdated approach to cyber defense.

*With more than 350,000 new malware variants discovered each day and ransomware attacks – and their payouts – at an all-time high, it's time to rethink threat detection and response. At Deep Instinct, we **predict** security risks others can't see and we **prevent** threats that others can't stop.*
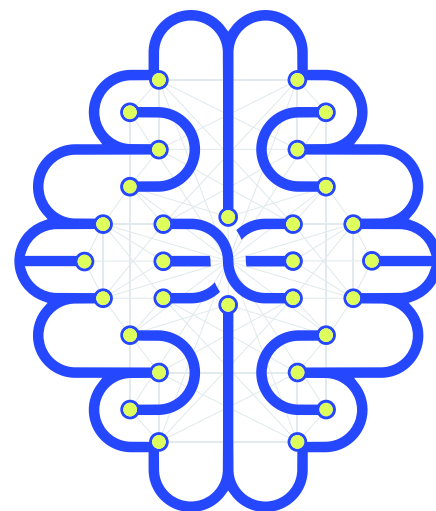
The Deep Instinct Prevention Platform is grounded in the world's first and only purpose-built deep learning cybersecurity framework. Powered by a deep neural network brain that mimics the logic and learning of the human brain, the Deep Instinct Prevention Platform anticipates and prevents attacks with unmatched speed and accuracy. We stop attacks before they happen, identifying malicious files in <20ms and preventing attacks pre-execution.

Our prevention–first approach provides a proactive security posture that protects your organization's hybrid network while maintaining the lowest false positives in the industry. Regardless of your current security posture, you need Deep Instinct too.

We're so confident in our approach that we **promise** to stop 100% of ransomware and back it up with an industry-leading $3M warranty backed by Munich Re. We take our commitment to our customers a step further by also offering a false-positive guarantee of <0.1%.

We prevent malware. Guaranteed.

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 of <0.1%.

The Deep Instinct Advantage

Deep Instinct is the most sophisticated solution for threat prevention on the market today. Our end-to-end prevention ensures that threats never reach the endpoint to execute. Our deep learning deterministic and predictive algorithms detect suspicious and malicious threats with unmatched precision and efficacy.

The Deep Instinct advantage extends beyond just total threat protection.

Many cybersecurity vendors are deploying machine learning (ML)-based solutions that either protect too much—flooding your team with false positives—or lack the power and precision to predict and prevent unknown, zero-day threats. Our vast neural network has been trained for years on hundreds of millions of files to prevent threats autonomously, allowing your highly-skilled, highly-specialized security operators to spend less time responding to and managing false positives, and more time focusing on the security threats that matter. Our technology makes your team smarter, faster, and more agile.

Proactive Prevention

- Fastest response to prevent unknown cyber threats and malware
- Prevent zero-day threats without rules and signatures
- 100% raw data based, non-linear model
- Protect revenue, brand, and business continuity
- Automated actions to delete or quarantine based on policy
- Prevent against adversarial ML attacks

Broad Protection

- Supports the widest variety of file and fileless threat types
- Multi-OS, multi-environment (Endpoint, Mobile, Server, Cloud, Network)
- Wide coverage of attack vectors
- No internet or cloud connection required

No Security Trade-Offs

- Highest efficacy in the industry
- Lowest false positive rate (<0.1%)
- No cloud updates or check-ins required to prevent a threat

Low Maintenance

- Lightweight agent*
- Low CPU usage
- Minimal configuration
- Fully autonomous prevention (no human involvement, no feature engineering)
- Only two updates per year
- Fully trained deep learning brain
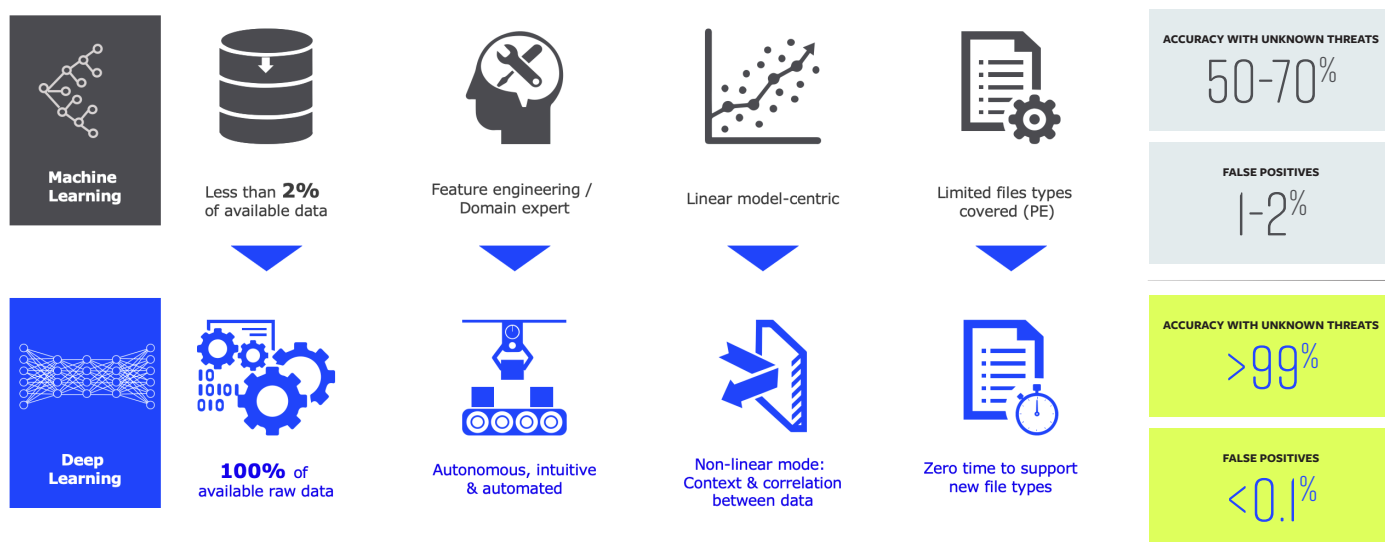
*Agent based solution only

Predict:

Deep Learning is Superior to Machine Learning

Machine Learning algorithms are subject to human fallibility and suffer from low detection rates and high false positives, while also suffering from accuracy issues 50%–70% of the time. According to researchers, ML algorithms may help you some of the time, but they are dependent on human training to stay up to date. If the training data is paired to the wrong set of features, the resulting model can be highly unreliable[1]. ML-based security tools are also being increasingly targeted by bad actors to bypass controls and exfiltrate data undetected or alter the inferences and poison the data.

Deep Instinct's multi-layered approach begins with our Deep Neural Network that provides 99% accuracy with less than <0.1% of false positives. Deep learning self-learns as it ingests data, providing improved performance over time – detecting and preventing more hard-to-detect threats with a high degree of accuracy. Not dependent on manual engineering, deep learning does not require frequent updating to maintain prevention efficacy.

Deep Learning vs. Machine Learning

Machine Learning	Less than **2%** of available data	Feature engineering / Domain expert	Linear model-centric	Limited files types covered (PE)	ACCURACY WITH UNKNOWN THREATS 50-70%
					FALSE POSITIVES 1-2%
Deep Learning	**100%** of available raw data	Autonomous, intuitive & automated	Non-linear mode: Context & correlation between data	Zero time to support new file types	ACCURACY WITH UNKNOWN THREATS >99%
					FALSE POSITIVES <0.1%

https://www.frontiersin.org/articles/10.3389/fcomp.2020.00036/full

Prevent:

Real Time is Too Late

Time is not on your side: an unknown ransomware dropper in your email or from a website can spread quickly. In less than a few seconds after your employee has clicked on an email or clicked a malicious file the ransomware has deployed and is spreading via worms or elevated privileges. The ransomware has access and is permeating your organization's internal protected networks and every system it touches will help spread it faster. Organizations then typically face a two-pronged threat: first, they face a ransom demand to decrypt their systems and return stolen data; second, they are extorted for a second payment to prevent sensitive company and customer data from being made public on the dark web.

[1] The Challenges of Leveraging Threat Intelligence to Stop Data Breaches. *Frontiers in Computer Science*, August 2020.

Why Speed Matters: The Chronology of a Ransomware Attack

Deep Instinct detects and prevents malware pre-execution in <20 milliseconds, 10 times faster than real time. Prevention is possible with the right partner. Our customers recognize that preventing breaches saves time, money, and reputation.
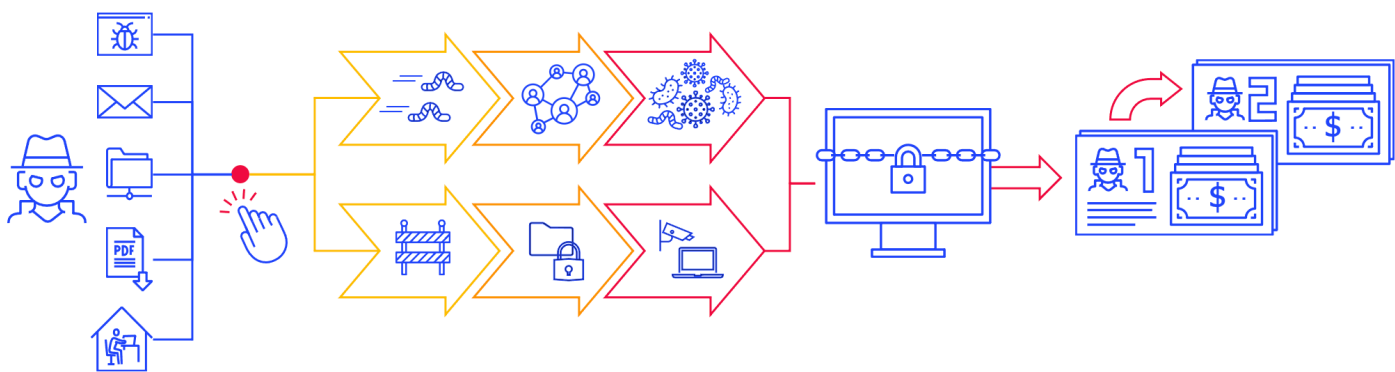
Promise:

Two Unique Customer Commitments

Customer peace of mind is always our priority. That's why we have worked with one of the world's largest reinsurers, Munich Re, to offer two industry-leading warranties. Available as part of the Premium Subscription package, they provide additional reassurance in two key areas:

1. Ransomware warranty – *the world's highest*

Payments vary according to the number of customer endpoints as shown below.

	10K –20K Endpoints	>20K Endpoints
Per Infected Device	US $1,250	US $1,000
Max Per Year	US $2M	US $3M

2. Efficiency (low false positive) warranty – *the world's only*
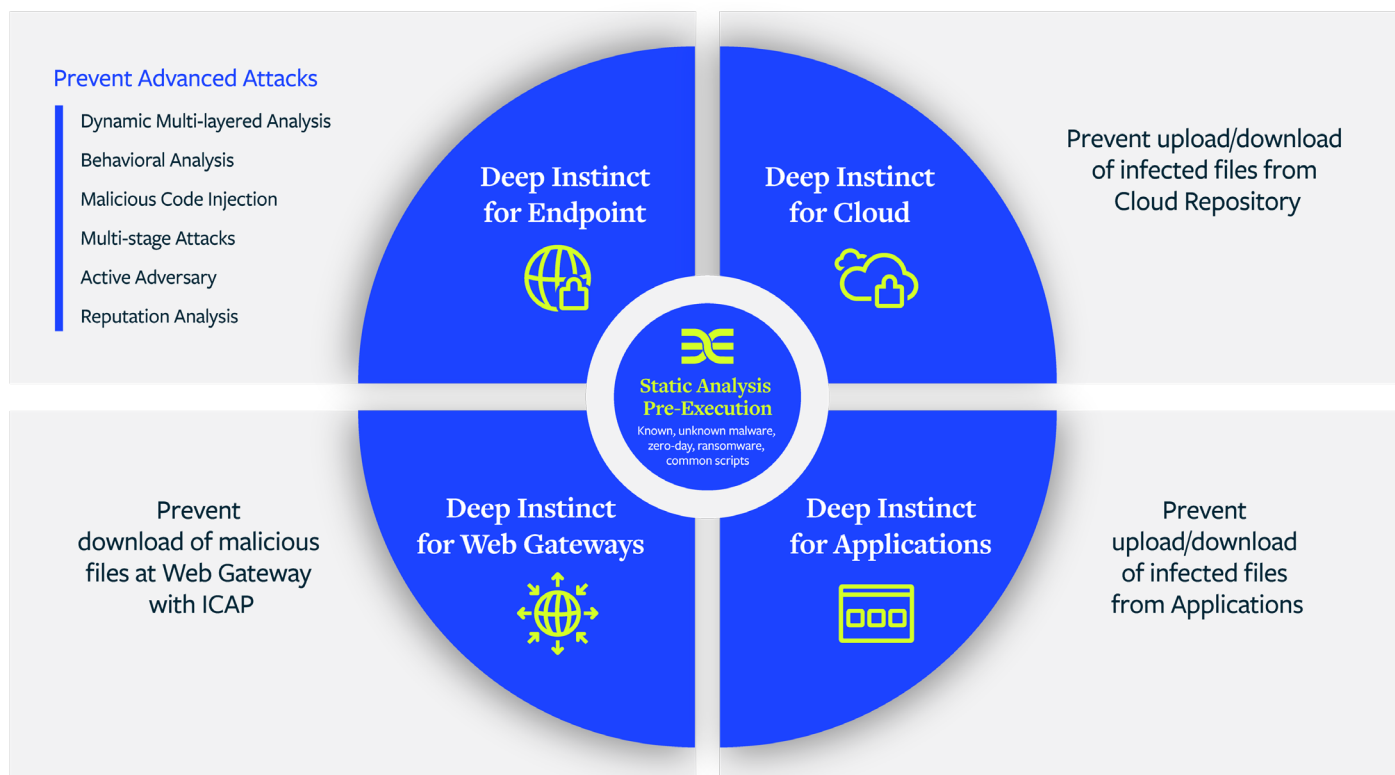
High false positive ratios massively reduce the efficiency and effectiveness of SecOps teams, creating unnecessary administrative work at the expense of more strategic activities. We commit to <0.1% False Positive Events per device over a two-quarter period, with 50% of the annual subscription paid out if this threshold is exceeded. No other cybersecurity vendor offers this form of performance commitment.

Warranties validated via extensive due diligence

Customers can rest assured that Munich Re specialists conducted a wide and intensive examination of Deep Instinct's Prevention Platform. Munich Re AI experts looked at our feedback loops in production, decision processes, and how we update models, plus core static and dynamic capabilities against ransomware and other ransomware-related attack vectors. Offering these new warranties was an entirely new venture for Munich Re, whose own data scientists thoroughly examined every aspect of the Deep Instinct solution before they were sufficiently satisfied to underwrite the guarantees with us.

The Deep Instinct Prevention Platform

Deep Instinct both prevents threats at the endpoint and extends prevention without requiring an agent to ensure file integrity of your cloud storage and custom applications, while protecting your network by eliminating threats at your web gateway. Deep Instinct for Endpoint: Prevention-first approach to stop more threats, faster.

Prevent Advanced Attacks

- Dynamic Multi-layered Analysis
- Behavioral Analysis
- Malicious Code Injection
- Multi-stage Attacks
- Active Adversary
- Reputation Analysis

Deep Instinct for Endpoint

Deep Instinct for Cloud

Prevent upload/download of infected files from Cloud Repository

Static Analysis Pre-Execution
Known, unknown malware, zero-day, ransomware, common scripts

Prevent download of malicious files at Web Gateway with ICAP

Deep Instinct for Web Gateways

Deep Instinct for Applications

Prevent upload/download of infected files from Applications

Deep Instinct for Endpoint

Prevention-first approach to stop more threats, faster.

- Prevent malware in near real time with higher efficacy
- Increase the efficiency of your current investments
- Lightweight agent

Deep Instinct for Cloud

Ensure your files stored in the cloud do not contain malware.

- Ensure the integrity of your files stored in the cloud
- Gain cloud agility benefits with peace of mind
- No agent required

Deep Instinct for Web Gateways

Stop your users from unknowingly downloading malicious files from the web.

- Stop malware at the web gateway
- Increase efficacy to prevent more threats
- No agent required

Deep Instinct for Applications

Custom applications with a high volume of file uploads and downloads present a security challenge.

- Ensure the integrity of your applications
- Maintain essential document sharing whilst securing it
- No agent required

Rapid Delivery of New Insights

The Deep Instinct Prevention Platform integrates seamlessly with your current stack including EDR, SIEM, SOAR and ITSM environments. For example, high fidelity alerts from Deep Instinct can be sent to your SIEM to correlate events and coordinate actions across multiple domains.

Existing Security Stack **SIEM Environments** **SOAR and ITSM**
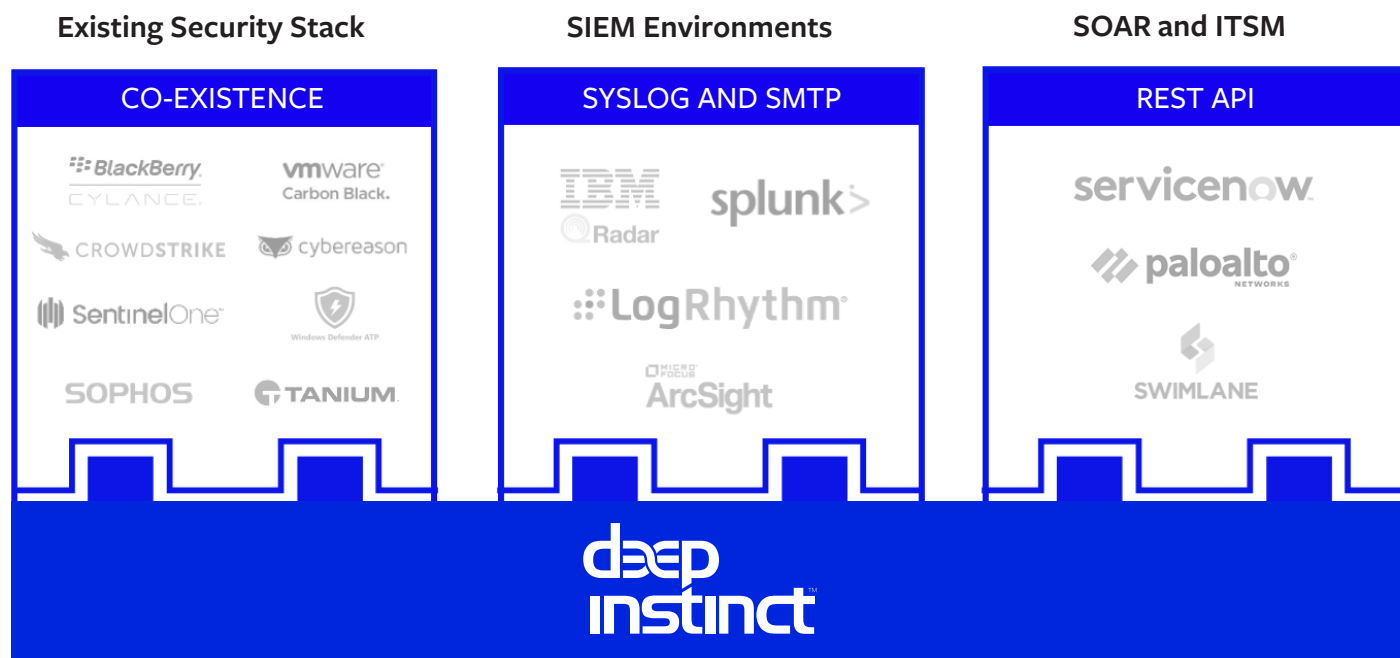
Augmenting Your Existing Security Investments

Deep Instinct enhances the security tools you might already own, like EDR, to improve their effectiveness, drastically reduce false positives, and limit the burden on your SOC team – allowing you to get more from your existing security. 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.

Some of our customers decide that Deep Instinct can replace some of their more traditional AV solutions or complement them to provide even higher levels of protection.
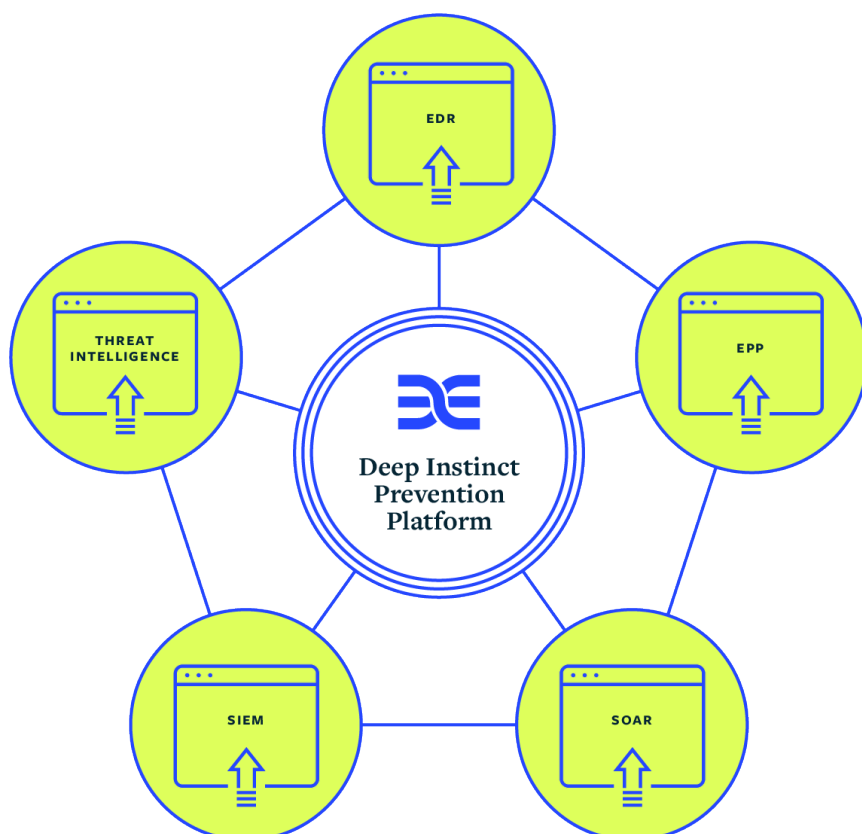
Why They Trust Us

Prevention is possible with the right partner. Our customers recognize that preventing breaches saves time, treasure, and reputation.

T··Systems·

"The functionality that Deep Instinct provides is best-in-class, leveraging deep learning to achieve unmatched accuracy and speed anywhere in an enterprise ecosystem, with multi-layered protection across all endpoints, networks, mobile devices, and operating systems."

Stefan Stefaniak
Cyber Security Advisory, Team Leader

T-Systems Poland

SEIKO

"With the increase in remote work, we knew that our existing endpoint security would not be enough to deal with zero-day attacks and unknown malware threats. Based on our past experience, we believe that Deep Instinct is the most promising next-generation anti-virus solution."

Masakatsu Nemoto
General Manager, IT Planning Division

Seiko Holdings Group

NVIDIA.

"Deep Instinct's unique approach in applying true deep learning to cybersecurity is yielding revolutionary breakthroughs that are being embraced by a growing market."

Jeff Herbst
Vice President of Business Development

NVIDIA

KINGS
WHERE INSPIRATION STRIKES

"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 learning company has surpassed our expectations, ensuring our customers remain safe and helped mitigate risks for attacks we might not even be aware of."

Bruno Mariano
Director of Technical Support and Services

Kings Food Markets

THE 20

"The security landscape needed to change, to somehow achieve greater innovation, speed, and agility than the attack vectors. Deep learning cybersecurity is the shake-up the industry needed, and for us, our partners, and customers it's an exciting new development and not a moment too soon."

Jonathan Blakey
CIO

The 20

The Benefits of Resilient Prevention

Gartner peerinsights™

Reduced False Positives — 5 out of 5 ⭐

"With the surge in malware attacks targeting vulnerable endpoints, the need for a solution that provides autonomous prevention with minimal false positives is critical."

Director of IT in the Healthcare Industry

Zero-Time Prevention — 5 out of 5 ⭐

"What I like most about Deep Instinct is its ability to stop a piece of malicious software from even downloading to the hard disk, whereas most I've dealt with require the malicious software to land on the disk for it to act upon it."

CEO in the Services Industry

Broad Attack Surface Protection — 4.9 out of 5 ⭐

"Threats are rapidly outpacing traditional AV solutions ability to protect and respond. Next generation solutions have significant management requirements associated with them. Evolving threats and an extremely competitive job market required us to simplify our endpoint security management while not sacrificing the endpoint protection, and for that reason we chose Deep Instinct."

CISO in the Financial Industry

No Operational Headaches and at a Reduced Cost — 4.9 out of 5 ⭐

"What I like most about Deep Instinct is that it does exactly what a product in this space should do: protect against next-gen and traditional threats, and do it reliably. It presents clear and concise information to...quickly deal with actionable items, respect endpoint resources, and do it all at a reasonable price point."

Director of IT at K-12 School District

Forrester Total Economic Impact (TEI) Study

Forrester Research conducted an ROI analysis on the cost savings and business benefits enabled by the Deep Instinct Prevention Platform.

FORRESTER

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

ROI
446%

Reduction in number of alerts due to false positive elimination
99%

Payback
<3 months

Net Present Value (NVP)
$2,816,678

Present Value (PV)
$3,455,824

Deep Instinct

FOUNDED IN 2015
GLOBAL CUSTOMER BASE
3,000 END CUSTOMERS

HEADQUARTERED IN NYC AND TLV
OFFICES IN LONDON AND TOKYO

DEEP LEARNING FRAMEWORK
PROTECTED BY 5 GRANTED PATENTS

Strategic and Financial Investors

BlackRock.

chrysalis investments

MILLENNIUM

Unbound

COATUE

untitled. INVESTMENTS

RPM

hp

NVIDIA.

LG

SAMSUNG
SAMSUNG VENTURE INVESTMENT

Industry Recognition

WIRED
The 10 Hottest Startups in Tel Aviv 2019

Forbes
Ranked among the "Top 13 Companies that uses Deep Learning in the World"

THE CHANNEL CO.
CRN MOBILE 100 2020
CRN 2020 Mobile 100 List

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021
Endpoint Protection

2021 FORTRESS CYBER SECURITY AWARD
Endpoint Detection

SE Labs AAA APR-JUN 2021 ENTERPRISE ENDPOINT PROTECTION
Endpoint Protection

---

deep instinct™

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.