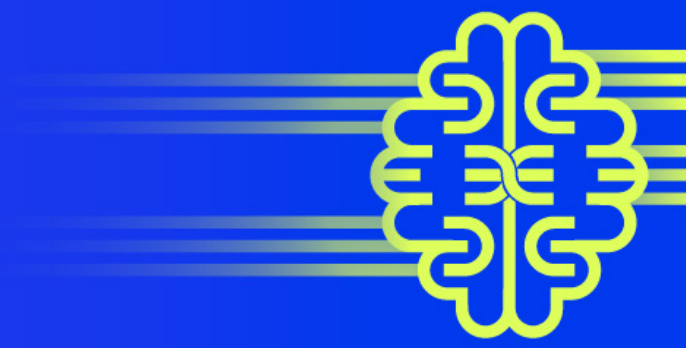
SOLUTION BRIEF

Deep Instinct Prevention Platform



STOP RANSOMWARE
BEFORE IT ENCRYPTS

PREVENT >99%
KNOWN, UNKNOWN, AND ZERO-DAY THREATS

<20MS
MALWARE PREVENTION

It's time to fill the prevention gap in our cybersecurity defenses — the myopic focus on 'assume breach' is simply not enough.

As zero-day, ransomware, filed-based, fileless, supply chain attacks, and new malware variants continue to morph and evade detection, it has become exceedingly difficult to stop bad actors from succeeding once they get inside your hybrid network.

Deep Instinct is reversing this trend to prevent unknown attacks before they can land in your environment through your endpoints, servers, or storage by leveraging the power of deep learning.

- Reduce the risk of unknown threats infiltrating your environment
- Lessen the impact on overworked SOC teams
- Ensure only high fidelity alerts to optimize your current security stack

Deep Instinct meets the attacker earlier and prevents never before seen threats developed by threat actors who are constantly innovating new tactics to evade detection on the endpoint. We also protect your environment against malicious files uploaded through web applications and stored in private and publics clouds, downloaded by your end users from the internet, and transferred into your environment by third party suppliers.

The Deep Instinct Prevention Platform

The Deep Instinct Prevention Platform is the first and only solution based on a unique deep learning framework specifically designed to solve today's cybersecurity challenges — namely preventing threats before they have a chance to execute and land on your environment.

Deep Instinct advantages include the following:

- Provides the fastest threat prevention in under <20ms, pre-execution
- Prevents >99% of unknown, zero day, and ransomware attacks
- Lowers impact on the SOC with a low <0.1% false-positive rate
- Makes malicious vs benign decisions independently, without cloud threat intel
- Protects privacy as only the hash ever leaves your environment
- Ensures lower cost maintenance with only 2-3x updates per year, not daily

For your organization, this means peace of mind with the knowledge that attackers have lost their edge. Your team can focus on the alerts that really matter — not the noise. The rest of your security stack runs more efficiently, and your team's job satisfaction is improved.

Deep Instinct Prevention Platform

Prevention-first approach to stopping unknown threats

Meet the attacker earlier with agentless, on-demand scanning of files in transit

Complement your EDR with dynamic, multi-layered antimalware prevention

At the core of the Deep Instinct Prevention Platform is our industry-leading antimalware static analysis built to take full advantage of the power of deep learning to make faster, more accurate decisions and prevent threats before they can fully execute and land in your environment. Deep Instinct Prevention for Endpoints provides additional layers of prevention with dynamic and behavioral analysis to prevent fileless attacks, like in-memory and code injection, and better protects against ML evasion and poisoning techniques. Deep Instinct Prevention for Applications is focused on preventing malicious files from impacting your network and storage environments.

Deep Instinct Prevention for Applications

Deep Instinct Prevention for Applications is an agentless, on-demand, antimalware solution that scans a high volume of files in transit for malicious content.

Prevent Malicious Files

Deep Instinct meets the attacker earlier to prevent threats hidden in your files by protecting your organization against file uploads through your web applications, user downloads from the internet, and third-party suppliers who transfer files into your environment and leave your organization blind to malicious content traversing your network.

Tailor to your workflows

Easily integrates into your environment with an agentless solution that aligns to existing workflows with a flexible and programmable REST API that is operating system and device agnostic.

Scale to Petabytes

Scan tens of millions of files in transit at enterprise speed and protect any web application or cloud storage from malicious content, without impacting user experience.

Maintain Full Data Privacy

Files never leave your environment. Only the hash is sent to the management console or SIEM for further analysis.

Deep Instinct Prevention for Endpoints

Deep Instinct Prevention for Endpoint complements your existing EDR and SIEM tools with a multi-layered, prevention-first approach.
The moment an attacker attempts to land a malicious payload on their target endpoint, Deep Instinct prevents it – before it can fully execute and infect your network.

Pre-execution Prevention: Static Analysis

Prevent >99% of known and unknown malware, including ransomware, zero-day, filed-based, and script-based attacks with Deep Instinct's deep learning-based static analysis engine.

On-execution Prevention: Dynamic and Behavioral Analysis

Using a multi-layered approach to prevention, Deep Instinct employs additional dynamic analysis layers to detect and automate responses to the most advanced threats, including the following:

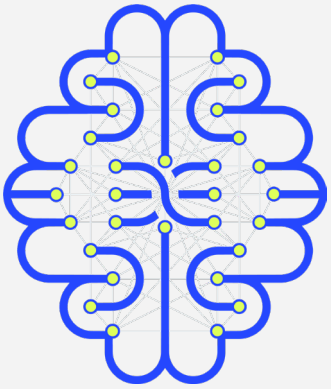
- Fileless attacks like malicious code injection and credential theft
- Advanced scripts, like unknown shellcode
- Multi-stage attacks
- Active Adversarial AI attacks

In addition, Deep Instinct provides additional context to understand the severity and tactics of a threat, including:

- Suspicious events for threat hunting
- MITRE ATT&CK mapping

Automated Analysis and Classification

Deep Instinct provides unique capabilities for threat classification to speed up and improve investigations. All prevented events (hash only) from both solutions are sent to the Deep Instinct console and can be integrated with your SIEM, SOAR, EDR, or other security solutions via REST API, Syslog, or SMTP.



Why is Deep Learning Important?

Deep Learning (DL) provides a unique opportunity to prevent attacks earlier, before threat actors gain entry to your environment. As the most advanced form of AI, DL is inspired by the brain's ability to think and learn over time.

A deep learning-based solution provides the following critical advantages:

- Trains on 100% of available raw data which means it can make non-linear correlations with greater context equaling faster more accurate decisions
- Updates required only 2-3x per year while still catching unknown threats
- Understands the DNA of an attack so it doesn't need to know the entirety of an attack or its intent to know that it is malicious, lowering the need for human-fed feature engineering
- Operates seamlessly without threat intelligence feeds which means it does not have to call out to the cloud to make a decision, speeding up prevention times.
- Avoids the pitfalls of adversarial AI and ML poisoning attacks far greater than other AI

Ultimately, DL-based cybersecurity is what will enable organizations to make prevention a reality, predicting and stopping threats before they execute and keeping the attackers out of your environment.

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.

www.deepinstinct.com | info@deepinstinct.com