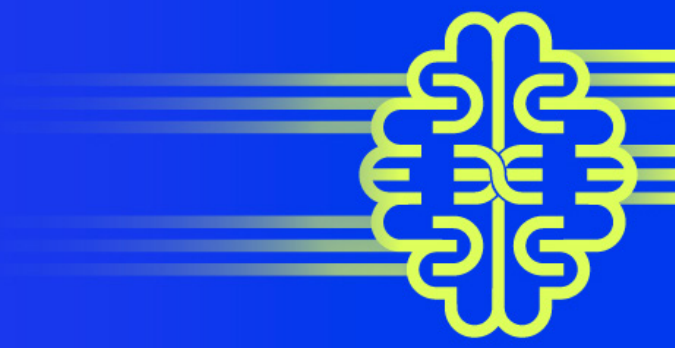
SOLUTION BRIEF

Deep Instinct Prevention Platform



STOP RANSOMWARE
BEFORE IT ENCRYPTS

PREVENTS >99%
KNOWN, UNKNOWN, ZERO-DAY THREATS

GUARANTEES <0.1%*
FALSE POSITIVE RATE

<20MS
MALWARE PREVENTION

There are 350,000 new pieces of malware discovered daily—and this number is growing exponentially. Zero-day, ransomware, filed-based, fileless, supply chain, and adversarial AI attacks continue to morph and evade detection, making it exceedingly difficult to prevent bad actors from infiltrating your hybrid network. An innovative prevention-first approach—made possible by deep learning—is the path forward to take back control.

With work-from-anywhere becoming the new normal combined with the continued evolution of digital transformation and distributed networks, computing has moved closer to the edge. Protecting your endpoints has never been more important.

But it's not just the endpoint. Bad actors can infect systems through files stored in the cloud, files uploaded through applications and downloaded to customers, and files your end users are downloading from the internet. Legacy AV will only prevent known threats. And EDR alone is not enough to stop the unknowns before they are executed on your network.

We must rethink our approach to prevention.

The Deep Instinct Prevention Platform

The Deep Instinct Prevention Platform stops known, unknown, and zero-day threats with the highest accuracy and lowest false-positive rate in the industry. For your organization, this means reduced risk, greater SOC efficiency, and the knowledge that attackers have lost their advantage. With >99% known, unkno wn, and zero-day threat accuracy, a guaranteed <0.1% false positive rate, plus a $3M ransomware warranty backed by Munich Re, the Deep Instinct Prevention Platform meets the promise of true prevention.

Deep Instinct prevents threats prior to execution, unlike detection and response solutions that look for behaviors after the attacker has already installed droppers and artifacts on your network. Deep Instinct's Prevention Platform reduces the risk of a breach by meeting the attackers earlier and stopping threats 750x faster than the fastest known ransomware can begin to encrypt.

Deep Instinct prevents attacks at the endpoint with end-to-end static and multi-layered dynamic analysis. To meet the attacker even earlier, Deep Instinct also prevents malware beyond the endpoint by scanning the in-transit files of your custom applications and workflows, as well as local, private, and public cloud storage and web gateways to prevent the upload or download of malicious files while ensuring the integrity of your environment.

Deep Instinct Powered by Deep Learning

Deep Instinct is the only cybersecurity company leveraging a deep learning-based neural network that autonomously learns and dynamically improves as it's fed more data.

Deep learning is the most advanced form of AI, inspired by the brain's ability to think and learn over time. Our vast neural network has been trained for more than five years on hundreds of millions of files to autonomously prevent threats.

Deep Learning differs from basic machine learning in several critical ways:

Basic machine learning requires a human domain expert, making it slow and prone to error, and is only trained on 2% of available data. Deep learning trains on 100% of available raw data and can make non-linear correlations of the data automatically. With deep learning-based neural networks specifically architected for cybersecurity, decisions are made faster, more accurately, and with much greater efficacy.

A deep learning model is self-sufficient and does not require frequent cloud updates or constant human intervention.

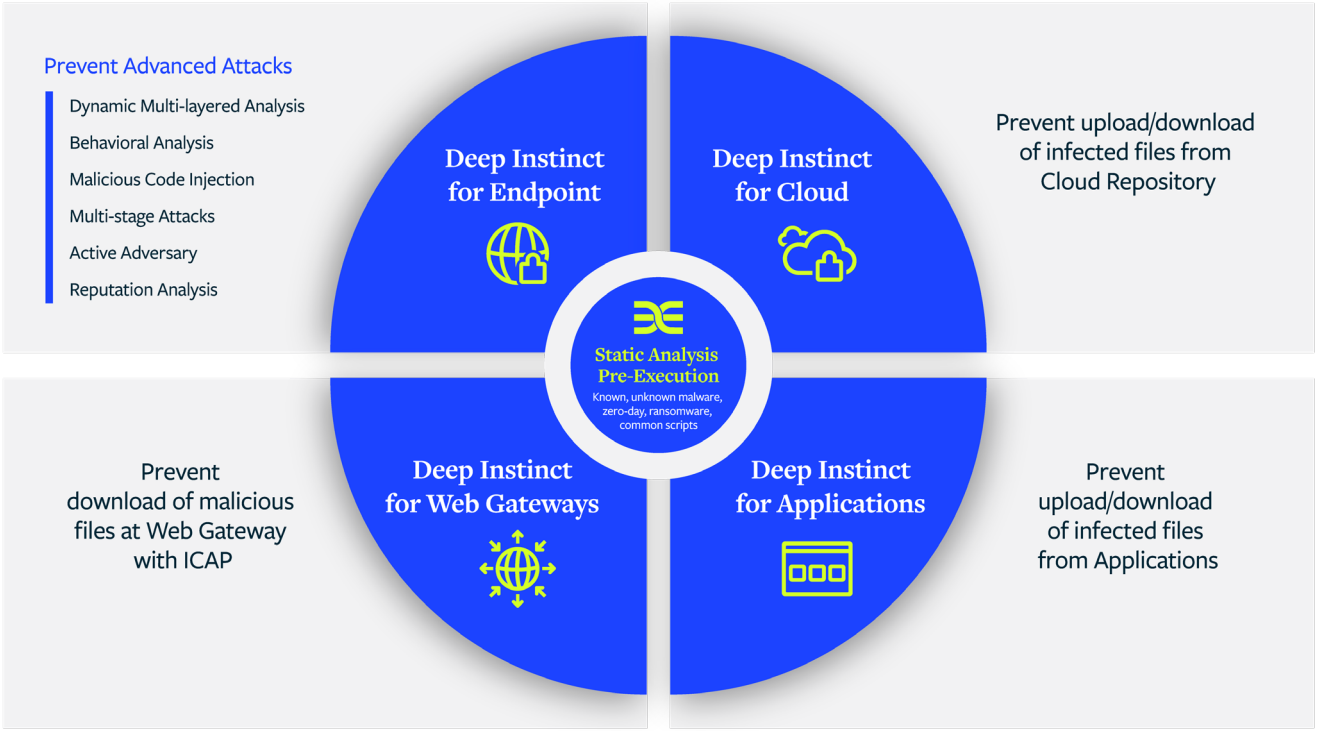
Ultimately, deep learning is what will enable organizations to make prevention a reality, predicting and stopping threats before they execute and compromise your environment.

Product Differentiators

- Integrates with existing security solutions to improve efficiency, effectiveness, and focus on what really matters – stopping attacks.
- Reduces burden on security teams to sift through false positives
- Improves threat hunting capabilities with high-fidelity alerts and suspicious activity rating

**Applies to endpoint only.*

The Deep Instinct Prevention Platform



Deep Instinct for Endpoint

Deep Instinct for Endpoint provides end-to-end, multilayered security. The moment an attacker attempts to land a malicious payload on their target endpoint, Deep Instinct prevents it – before it executes

Pre-execution: Static Analysis

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

- Known malware
- Unknown malware & variants
- File-based attacks
- Zero-Day
- Ransomware
- Common Scripts

On-execution: 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

Post-Execution: Automated Analysis

In the last layer of automated analysis, Deep Instinct can override prevent decisions based on reputation or policy.

All prevented events 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.

Deep Instinct: Beyond the Endpoint

In-transit file scanning

Deep Instinct understands that the endpoint is not your only attack vector. Malicious files can unknowingly be uploaded to your hybrid, distributed environment, or downloaded to your customers.

Deep Instinct prevents malicious files by scanning files in-transit to ensure the integrity of your local, private, and public cloud storage and your custom applications, and prevents malicious file downloads at the web gateway.

Deep Instinct for Cloud

Infected files stored in public or private clouds increase the risk of a breach upon download.

Deep Instinct prevents malicious files from uploading to, or downloading from, your public or private cloud storage.

Deep Instinct for Applications

Your organization is at increased risk from both internal and external file uploads through your custom applications.

Deep Instinct scans in-transit files to ensure that the files uploaded through your custom applications and downloaded to your customers are free of malware.

Deep Instinct for Web Gateways

Legacy AV and ICAP solutions will not stop unknown threats at the web gateway.

If you are currently using a web proxy to filter traffic, Deep Instinct will scan files to prevent users from accessing malicious files from the internet. Deep Instinct connects with the ICAP protocol to become the ICAP server and uses our deep learning static engine to catch >99% of both known and unknown malware.

deep instinct

www.deepinstinct.com | info@deepinstinct.com