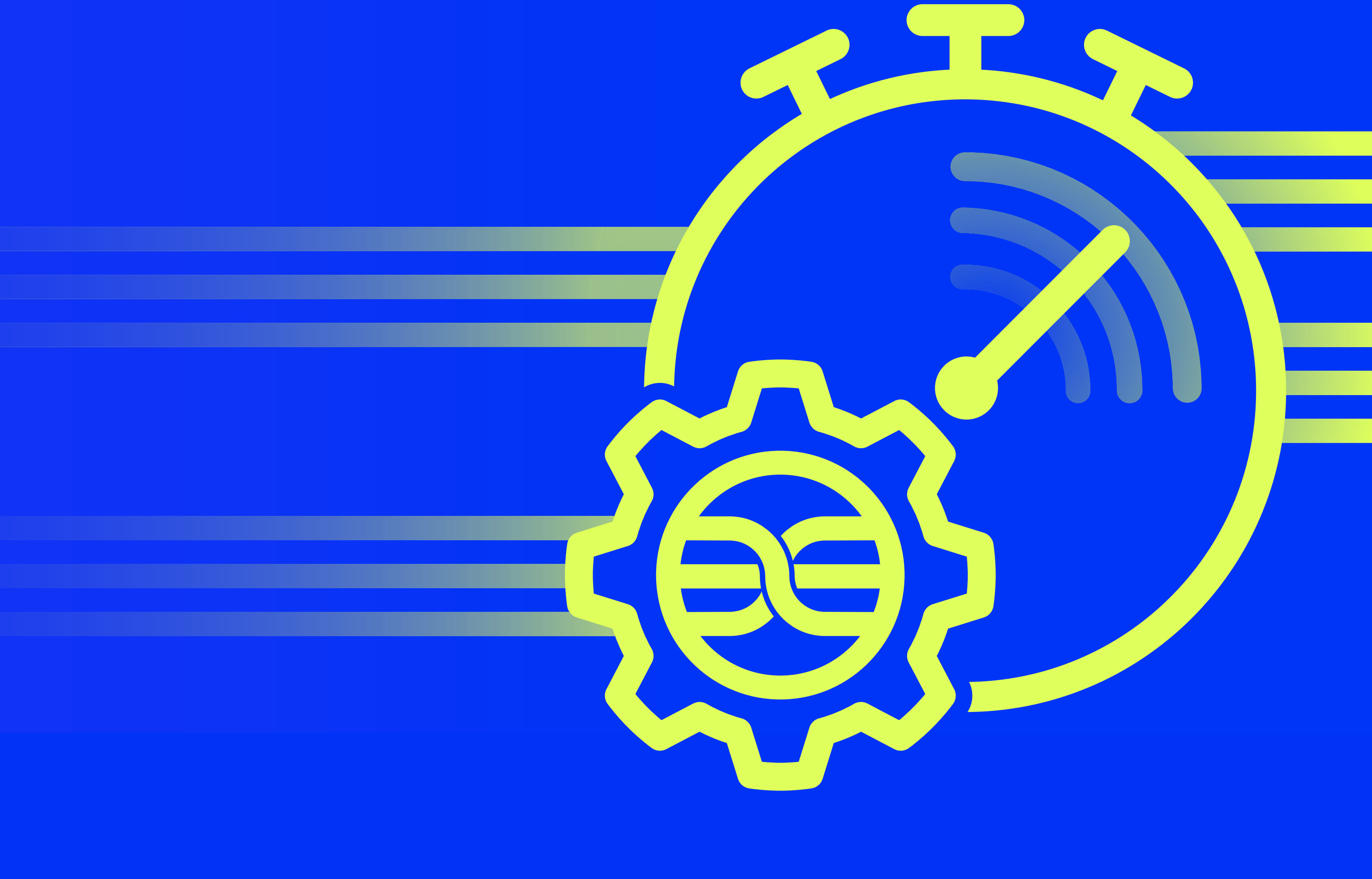
REPORT

Total Threat Protection from the Deep Instinct Prevention Platform

Evaluate Deep Instinct compared to other leading EPP vendors



deep instinct™

www.deepinstinct.com

Challenging the Cybersecurity Status Quo.

Cybercriminals never stop advancing their tools and tactics in a constant war of attrition. With more than 350,000 new malware variants discovered each day, adversarial machine learning becoming a top-level threat, and with SOC teams working tirelessly to stem the tide of alerts—both real and false—the challenges never stop. Unfortunately, established approaches are not stopping ransomware attacks making the headlines every week.

But prevention *is* possible. 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 the world's first and only purpose-built, end-to-end deep learning-based cybersecurity framework. Powered by a deep neural network brain that mimics the logic and learning of the human brain, the Deep Instinct Prevention Platform achieves the following:

- Stops attacks before they happen, pre-execution, by identifying malicious files in <20ms
- Protects against 100% of ransomware attacks, backed by an industry-leading $3M warranty
- Is backed by the world's only low false-positive guarantee of <0.1%

Regardless of your existing security posture, you need Deep Instinct too.

Our threat prevention technology offers an end-to-end cybersecurity solution, protecting network, endpoint, and mobile with zero-time speed and accuracy.

Uniquely Engineered to Stop Unknown Threats Since 2015.

PREDICT

- Self-learning on non-customer data
- No human dependencies
- Trained on massive data sets in hundreds of millions of files

PREVENT

- Instantaneous response
- Threats stopped at pre-execution
- Every file, script, macro checked before anything executes in <20 milliseconds

PROMISE

- Industry's lowest false positive ratio <0.1%, highest ROI
- Ransomware warranty up to $3M
- Peace of mind protection

Broad Protection Against Attack Vectors.

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

Ransomware

- Ransomware protection against encryption and extortion-based threats

Spyware

- Banking trojans
- Keyloggers
- Credentials dumping
- Botnet

Exploits

- Documents
- Flash files
- Images
- Fonts

Mobile

- Applications
- Network attacks (MitM, SSL MitM)
- Compliance

Deep Instinct *vs* Traditional Antivirus Endpoint Protection Solutions.

	deep instinct	Microsoft	TREND MICRO	Symantec	McAfee by Intel	CROWDSTRIKE	SentinelOne	BlackBerry CYLANCE
Analysis Technology	Deep Learning ●	Machine Learning, Signatures ◔	Machine Learning, Signatures ◔	Machine Learning, Signatures ◔	Machine Learning, Signatures ◔	Machine Learning ◔	Machine Learning ◔	Machine Learning ◔
Adversarial AI / Adversarial ML protection	●	○	○	○	○	○	○	○
Detection Rate	●	◔	◔	◔	○	◔	◔	●
Low False Positive Rate	●	○	○	○	◔	○	○	○
Behavioral Analysis	Ransomware Code Injection Shellcode Contextual Scripts ●	○	Ransomware Machine Learning ○	SONAR ○	Anti-Exploitation Reduced Attack Surface ○	Ransomware (partial) Anti- exploitation Known Shellcodes Credentials dumping ◑	Ransomware Code injection Known shellcodes Keyloggers Credentials dumping ◑	Code injection Anti- exploitation Known shellcodes Credentials dumping RAM scraping ◑
Malware Classification	Deep Classification (any threat) ●	Signatures (known threats) ◔	Signatures (known threats) ◔	Signatures (known threats) ◔	Signatures (known threats) ◔	○	Cloud Reputation (known threats) ◔	Cloud Reputation (known threats) ◔
Supported Platforms	Windows macOS ChromeOS Linux Android iOS iPadOS ●	Windows macOS Linux Android iOS ●	Windows macOS Linux Android iOS ●	Windows macOS Linux Android iOS ●	Windows macOS Linux Android iOS ●	Windows macOS Linux Android iOS ●	Windows macOS Linux ◑	Windows macOS Linux Android iOS ●
Agent Footprint	One Agent <1% CPU 150M on Disk ●	One Agent <1% CPU >400M on Disk ◔	One Agent <1% CPU >550M on Disk ◔	One Agent <1% CPU >1.7G on Disk ○	One Agent <1% CPU >600M on Disk ◔	One Agent <1% CPU 20M on Disk ●	One Agent <1% CPU 200M on Disk ◕	One Agent <1% CPU 140M on Disk ●
Fileless Attack: Script	Contextual Analysis Macro Static Analysis Script Control (PowerShell, Jscript, VBScript, Macro, HTA, rundll32) ●	◔	○	Script Control (VBScript) Signatures ◔	Signatures ◔	Suspicious PowerShell, rundll32, regsrv32 ◑	●	Script Control (PowerShell, JScript, VBScript, Macro) PowerShell analysis ◑

CONTINUED ON NEXT PAGE ▶

Key: ● Full support ◕ Very High support ◑ Partial support ◔ Limited support ○ No support

CONTINUED FROM PREVIOUS PAGE ▶

Deep Instinct *vs* Traditional Antivirus Endpoint Protection Solutions.

	deep instinct	Microsoft	TREND MICRO	Symantec	McAfee by Intel	CROWDSTRIKE	SentinelOne	BlackBerry CYLANCE
Fileless Attack: Dual-Use	●	◔	○	●	○	●	●	●
Fileless Attack: Code Injection	●	○	○	◔	○	○	●	○
Remdiation: Kill Process	●	○	●	○	○	●	●	●
Remediation: Network Isolation	●	●	●	●	○	●	●	●
Remediation: Rollback	○	○	●	○	○	○	●	○
MITRE ATT&CK Integration	●	◑	○	◔	◑	●	●	●
Native Suspicious / Malicious Behavior detection to drive Threat Hunting	●	◔	◔	◔	◔	●	●	●
Native Shellcode / Memory Injection detection	●	◑	○	●	○	◑	◑	●
Native Credential Theft protection (LSASS Cache Dump)	●	◑	○	○	○	◔	◔	○

Key: ● Full support ◕ Very High support ◑ Partial support ◔ Limited support ○ No support

Glossary.

Term	Description
Agent Footprint	The resources that the agent software requires from the device to run. The footprint typically includes the CPU, memory, and disk space usage to run, but it does not include the space usage of the data on which it operates.
Detection Rate	The percentage of detected malware threats, compared to the total number of malware threats.
Behavioral Analysis	The algorithm that analyzes files to determine whether it is malicious by monitoring the behavior of the files while it is running.
False Positive Rate	The percentage of falsely detected non-malicious files as malicious compared to the total number of non-malicious files analyzed.
Fileless Attacks	An attack during which no portable executable (PE) file is written to and executed from disk. Fileless attacks can be implemented using various methods including attacks using scripts, macros, existing legitimate files (dual-use), and code injection loaded into memory.
Malware Classification	The classification of a malware that determines to which type of malware it belongs. This provides a better understanding of the malware's capabilities, and potential threat.
Remediation	The process to reverse or stop threats caused by malware. This can be implemented using one or more methods.
Static Analysis Algorithm	The algorithm that analyzes files to determine whether it is malicious, without executing the files.
Supported File Types	The type of files that are analyzed using the static analysis algorithm. Only supported file types are statically checked by cybersecurity solutions.

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.