deepinstinct™
BEFORE YOU KNOW IT

ENDPOINT & MOBILE PROTECTION SOLUTIONS

Competitive Comparison

WHY DEEP INSTINCT?

Deep Instinct is the first and only company to apply deep learning to cybersecurity. By using deep learning's predictive capabilities, any kind of threat is prevented in zero-time.

Unlike other endpoint and mobile protection solutions, Deep Instinct applies full deep learning on raw data, and not machine learning on hand-craft engineered features. That gives many advantages, where other solutions fail.

This comparison will showcase many of the advantages and differentiators of Deep Instinct's product over and above that of our competitors.

Deep Instinct is the only cybersecurity company that has deep learning-based, zero-time threat prevention platform, to protect:

- Any type of device, from any location: endpoint, mobile, server, tablet or network
- Multiple OS: Windows, macOS, Android, Chrome OS, iOS, iPadOS
- Against any file- or fileless-based attacks
- Achieving industry low levels of false positives

While providing:

- Lower TCO (total cost of ownership)
- Required EDR capabilities

Deep Instinct does not require any of the following:

- Signatures
- Online connectivity (for threat detection)
- Sandboxing (for threat detection)
- Traditional machine learning algorithms
- Experts for feature engineering
- AI training on-site
- Frequent updates
- Waiting for execution of the attack
- Skilled and expensive SOC team

Deep Instinct vs. Traditional Antivirus Endpoint Protection Solutions

		deepinstinct	Symantec	McAfee	SOPHOS	TREND MICRO	KASPERSKY	WEBROOT Smarter Cybersecurity	Microsoft
Static analysis algorithm		Deep learning (raw data) 🟢	Machine learning Signatures 🟠	Machine learning Signatures 🟠	Deep learning (hand-craft engineered features) Signatures 🟡	Machine learning Signatures 🟠	Machine learning (Decision Tree) Signatures 🟠	Machine learning (in the cloud only) Signatures 🔴	Machine learning (simple; better in the cloud) Signatures 🟠
Detection rate		🟢	🟠	🔴	🟠	🟠	🟠	🔴	🟠
False positive rate		🟢	🔴	🟠	🟠	🔴	🟢	🟠	🔴
Static analysis: Supported file types		Deep learning: Any 🟢	ML: PE, Mach-O Signatures: any 🔴	ML: PE Signatures: any 🔴	ML: PE Signatures: any 🔴	ML: PE Signatures: any 🔴	ML: PE Signatures: any 🔴	Signatures: any 🔴	Signatures: any 🔴
Behavioral analysis		Ransomware Code injection Shellcodes Contextual scripts 🟢	SONAR 🔴	Anti-exploitation Reducing attack surface 🔴	Ransomware Code injection Known shellcodes Credentials dumping 🟢	Ransomware Machine learning 🔴	Ransomware Anti-exploitation 🟠	🟠	🔴
Malware classification		Deep Classification (any threat) 🟢	Signatures (known threats only) 🟠	Signatures (known threats only) 🟠	Signatures (known threats only) 🟠	Signatures (known threats only) 🟠	Signatures (known threats only) 🟠	Signatures (known threats only) 🟠	Signatures (known threats only) 🟠
OS support: Endpoints		Windows macOS Chrome OS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux Chrome OS 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS 🟢	Windows macOS Linux 🟢
OS support: Mobile		Android iOS, iPadOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android 🟢	Android iOS 🟢
Management server deployment		Cloud On-premises 🟢	On-premises Cloud (partial) 🟡	On-premises Cloud (partial) 🟡	Cloud On-premises (partial) 🟡	Cloud On-premises 🟢	On-premises Cloud (up to 1K devices) 🟡	Cloud only 🟠	Cloud for monitoring (ATP) On-Premises for management (GPO) 🟠
Management console		One 🟢	Several 🟠	One 🟢	One 🟢	One 🟢	One 🟢	One 🟢	Several 🟠
Agent footprint	# of agents	One 🟢	One 🟢	One 🟢	Several 🟠	One 🟢	Several 🟠	One 🟢	One 🟢
	CPU	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢
	Disk space	150MB 🟢	>1.7GB 🔴	>600MB 🟠	>220MB 🟠	>550MB 🟠	>500MB 🟠		>400MB 🟠
Fileless attacks	Scripts	Contextual analysis Macro static analysis Script control (PowerShell, JScript, VBScript, Macro, HTA, rundll32) 🟢	Script Control (VBScript) Signatures 🟠	Signatures 🟠	🔴	🔴	🟠	🔴	🟠
	Dual-use	🟢	🟢	🔴	🟢		🟠	🔴	🟠
	Code injection	🟢	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Remediation	Kill process	🟢	🔴	🔴	🔴	🟢	🟢	🔴	🔴
	Network isolation	🟢	🟢	🔴	🟢	🟢	🔴	🔴	🟢
	Rollback	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🔴

Legend: 🟢 Very high / full support 🟡 High / partial support 🟠 Medium / limited support 🔴 Low / no support

Deep Instinct vs. Endpoint Detection & Response Solutions

		deepinstinct	BlackBerry CYLANCE	CROWDSTRIKE	SentinelOne	Carbon Black.	cybereason	elastic	paloalto
Static analysis algorithm		Deep learning (raw data) 🟢	Machine learning (Random Forest) 🟠	Machine learning (Logistic Regression) 🟠	Machine learning (Random Forest) 🟠	Signatures (OEM with Avira) 🔴	Signatures (OEM with Bitdefender) 🔴	Machine learning (GBDT) 🟠	Machine learning (SVM) 🟠
Detection rate		🟢	🟢	🟠	🟠	🔴	🔴	🟢	🟠
False positive rate		🟢	🔴	🔴	🔴	🟠	🟠	🔴	🔴
Static analysis: Supported file types		Deep learning: Any 🟢	ML: PE, Mach-O 🔴	ML: PE 🔴	ML: PE, Office, PDF 🟠	Signatures: PE 🔴	Signatures: PE 🔴	ML: PE, Office, Macros, PDF, Mach-O 🟡	ML: PE 🔴
Behavioral analysis		Ransomware Code injection Shellcodes Contextual scripts Credentials dumping 🟢	Code injection Anti-exploitation Known shellcodes Credentials dumping RAM scraping 🟡	Ransomware (partial) Anti-exploitation Known Shellcodes Credentials dumping 🟡	Ransomware Code injection Known shellcodes Keyloggers Credentials dumping ML 🟢	Code injection (partial) Ransomware (partial) Known shellcodes Credentials dumping 🔴	🔴	Ransomware Code Injection Credentials dumping 🟠	Ransomware Code injection Anti-exploitations 🟠
Malware classification		Deep Classification (any threat) 🟢	Cloud reputation (known threats only) 🟠	🔴	Cloud reputation (known threats only) 🟠	🔴	🔴	🔴	🔴
OS support: Endpoints		Windows macOS Chrome OS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢	Windows macOS Linux 🟢
OS support: Mobile		Android iOS, iPadOS 🟢	Android iOS 🟢	Android iOS 🟢	🔴	🔴	Android iOS 🟢	🔴	Android 🟠
Management server deployment		Cloud On-premises 🟢	Cloud On-premises 🟢	Cloud only 🟠	Cloud On-premises 🟢	Cloud On-premises 🟢	Cloud On-premises 🟢	Cloud On-premises 🟢	Cloud On-premises 🟢
Management console		One 🟢	One 🟢	One 🟢	One 🟢	Several 🟠	One 🟢	One 🟢	One 🟢
Agent footprint	# of agents	One 🟢	Several 🟠	One 🟢	One 🟢	Several 🟠	One 🟢	One 🟢	One 🟢
	CPU	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢	<1% 🟢	<5% 🟠	<1% 🟢	<1% 🟢
	Disk space	150MB 🟢	140MB 🟢			>170MB 🟢			
Fileless attacks	Scripts	Contextual analysis Macro static analysis Script control (PowerShell, JScript, VBScript, Macro, HTA, rundll32) 🟢	Script Control (PowerShell, JScript, VBScript, Macro) PowerShell analysis 🟡	Suspicious PowerShell, rundll32, regsrv32 🟡	🟢	🟢	🟠	🟢	🟠
	Dual-use	🟢	🟢	🟢	🟢	🔴	🟠	🟢	🟠
	Code injection	🟢	🟢	🔴	🟢	🟢	🟠	🟢	🟢
Remediation	Kill process	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
	Network isolation	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢
	Rollback	🔵	🔴	🔴	🟢	🔴	🔴	🔴	🔴

Legend: 🟢 Very high / full support 🟡 High / partial support 🟠 Medium / limited support 🔴 Low / no support

🔵 NeuShield add-on

Deep Instinct vs. Mobile Threat Defense Solutions

	deepinstinct	Check Point SOFTWARE TECHNOLOGIES LTD	Lookout	Symantec	wandera	ZIMPERIUM ADVANCED MOBILE SECURITY	CROWDSTRIKE	BlackBerry CYLANCE
Static analysis algorithm	Deep learning (raw data) 🟢	Machine learning (in the cloud only) 🔴	Signatures Machine learning (in the cloud only) 🔴	Machine learning 🟠	Machine learning 🟠	Machine learning 🟠	N/A (Application Shielding) 🔴	Machine learning 🟠
Detection rate	🟢	🟠	🟠	🟠	🟠	🟠	N/A 🔴	🟠
False positive rate	🟢	🟠	🟢	🟠	🟠	🟠	N/A 🔴	🟠
Prevention / Remediation	Prevention Remediation 🟢	Remediation 🟠	Remediation 🟠	Remediation 🟠	Remediation 🟠	Remediation 🟠	N/A 🔴	Remediation 🟠
Device-level detections	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Network-level detections	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴
OS support: Endpoints	Windows macOS Chrome OS 🟢	🔴	🔴	Windows macOS Linux 🟢	🔴	🔴	Windows macOS Linux 🟢	Windows macOS Linux 🟢
OS support: Mobile	Android iOS, iPadOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢	Android iOS 🟢
Management server deployment	Cloud On-premises 🟢	Cloud On-premises 🟢	Cloud only 🟠	Cloud only 🟠	On-premises only 🟠	Cloud only 🟠	Cloud only 🟠	Cloud On-premises 🟢

Legend: 🟢 Very high / full support 🟡 High / partial support 🟠 Medium / limited support 🔴 Low / no support

Glossary

TERM	DESCRIPTION
Static analysis algorithm	The algorithm that analyze files to determine whether it is malicious, without executing the files. Can be signature-, machine learning- or deep learning-based.
Detection rate	The percentage of identified malware correctly, out of the total number of malware analyzed.
False positive rate	The percentage of falsely identified non-malicious files as malicious, out of the total number of non-malicious files analyzed.
Supported file types	The only file types that are checked and analyzed using the static analysis algorithm.
Behavioral analysis	The mechanism that analyze processes to determine whether it is behaving maliciously.
Malware classification	The classification of a malware that determine to which type of malware it belongs. This provides a better understand of the malware's capabilities and potential threat.
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.
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 attack vectors including scripts, abusing legitimate files (dual-use) and code injection loaded into memory.
Remediation	The process to reverse or stop threats caused by malware. This can be implemented using one or more methods.