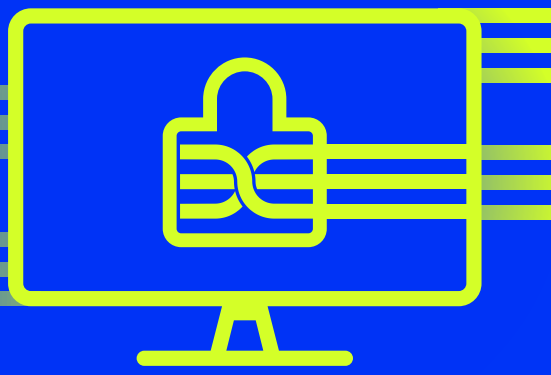
DATASHEET

Deep Instinct for Endpoint



WORLD'S ONLY
DEEP LEARNING
BASED CYBERSECURITY SOLUTION

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

PREVENTS THREATS IN
<20MS

ONLY
1-2 UPDATES
NEEDED PER YEAR

Preventing Unknown Attacks in <20ms

Today's adversaries have time on their side—you don't.

From the moment malware executes on the endpoint, it's a race against time to stop it. Traditional security solutions struggle to detect and respond quickly to unknown threats, taking minutes, hours, or even days—during which time the malware has succeeded, and your environment has been breached. Legacy AV, signature, rule, and heuristics-based tools can prevent known attacks but are largely ineffective against unknown and zero-day threats.

Deep Instinct prevents ransomware and other known, unknown, zero-day threats in <20ms – before an attack can execute on the endpoint.

With a lightweight, agent-based solution, Deep Instinct for Endpoint prevents >99% of known and unknown malware, dramatically reducing false positives, improving the effectiveness of your existing security solutions, and lowering your organization's overall risk. Your security teams will spend less time responding to benign alerts and more time focusing on higher-value priorities like threat hunting, patching, and hardening your defenses.

The Deep Instinct Difference: Deep Learning vs Machine Learning

Endpoint Detection and Response (EDR) solutions rely on basic machine learning. This approach requires the attack to begin executing before it can be detected. Ransomware, for example, begins to encrypt in 15 seconds, but the average EDR solution can take minutes or hours to detect —too long to prevent a breach. By the time EDR tools detect an attack, droppers and artifacts have already installed on your network endpoints.

With multiple deep learning engines, Deep Instinct's multi-layered approach to prevention provides the highest efficacy and the fastest detection and prevention. This applies to both known and never-before-seen malware, as well as fileless, in-memory, and script-based attacks. Deep Instinct can also detect suspicious behavior to improve your threat hunting, investigation, and root-cause analysis.

Product Benefits

- Prevents known, unknown, and zero-day threats in <20ms
- Saves security teams time by dramatically reducing false positives to <0.1%
- Ensures malware does not execute on your endpoint
- Stops multi-stage, complex ransomware attacks
- Enacts layered prevention against the most complex attacks
- Protects against adversarial AI
- Does not require cloud lookup

Deep Instinct for Endpoint

The moment an attacker attempts to land a malicious payload on their target endpoint, Deep Instinct for Endpoint prevents it—before it executes.

Deep Instinct has pioneered the use of deep learning in cybersecurity to prevent known and unknown malware, zero-day exploits, ransomware, and common script-based attacks for the broadest range of file types, faster and with fewer false positives versus security tools that rely on signatures, heuristics, or basic machine learning.

Predict and Prevent: Pre-execution Static Analysis

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

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

Static Analysis File Types

- PE
- PDF
- Office
- Macro
- RTF
- SWF
- JAR
- TIFF
- Fonts
- Mach-O
- ELF
- APK
- JTD
- HWP
- LNK

Script Control Coverage

- PowerShell
- JavaScript
- VBScript
- Macros
- HTML applications (HTA files)
- rundll32

On-Execution: Dynamic and Behavioral Analysis

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

- Fileless attacks
- Remote Code Injection (Reflective .NET, Reflective DLL)
- Known, Unknown Shellcode
- Credential Theft
- Anti-AMSI Bypass
- Credential Dumping
- Spyware, including banking trojans, keyloggers, and droppers
- Advanced scripts like unknown shellcode
- Multi-stage attacks
- Active Adversarial AI attacks

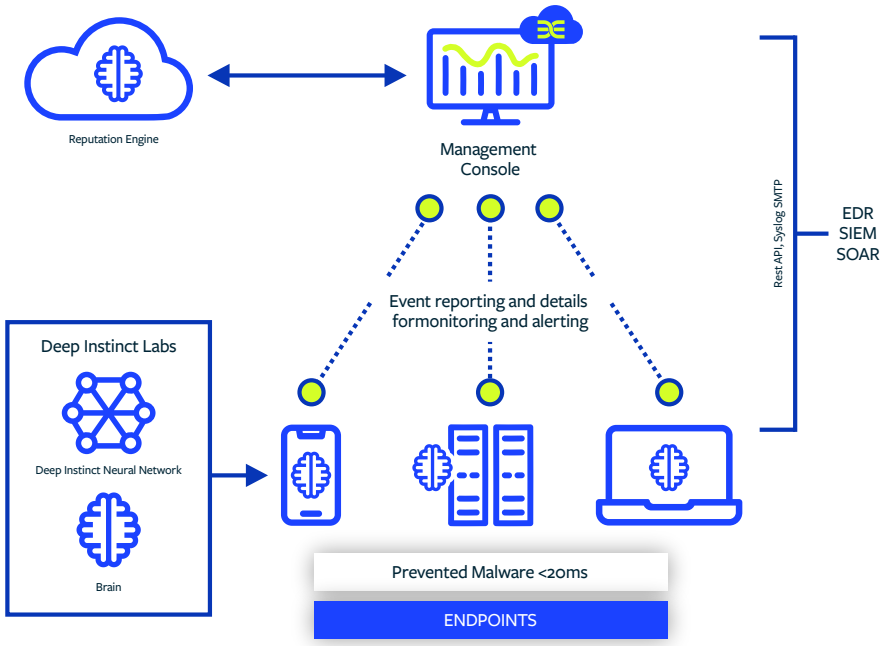
In addition, Deep Instinct provides context to understand the severity and tactics of a threat:

- Alerting on suspicious events for threat hunting
- Mapping to MITRE ATT&CK for threat context
- Conducting reputational analysis

Post-Execution: Automated Analysis

Deep Instinct includes optional automated and reputational analysis which can override decisions based on policy and imported allow lists.

Product Architecture



Automate Responses and Integrate with SIEM, EDR, SOAR

All prevented events are sent to the Deep Instinct Console and malware is instantly classified to provide context into the attempted attack. Organizations can enact a manual or automated response to achieve the following:

- Isolate the machine
- Quarantine/Delete/Restore
- Update policy: allow and restore (Hash, Certificate, Folder, Script, Process)
- Terminate the process
- Clean the registry to remove persistence
- Send prevented events to a sandbox for further analysis

Deep Instinct integrates with your SIEM, SOAR, EDR or other existing security tools via REST API, Syslog, and SMTP to improve investigation, remediation, and threat hunting.

Additional Features

Deep Instinct combines our leading cyber-prevention capabilities with intuitive feature sets that help our customers save time and work smarter.

Professional UI and Dashboard
Our easy-to-navigate and highly intuitive management console can be customized to present what is most important to the authorized end user.

Built-In Reporting
Automated and ad hoc threat and trend reporting.

True Multi-Tenancy
Native multi-tenant solution for Partners, MSPs, and MSSPs keeps all data safe and isolated from cross-contamination and administers multiple environments from one, centralized console.

Enhanced Security
Full audit logging/recording of all admin actions, role-based access control, 2FA, and SAML integration.

Group-Based Policy
Configuration of security policies based on a variety of manual or automated criteria, including naming convention, IP, AD, OU, and more.

Supported Virtual Environments

- Amazon Workspaces
- Citrix Hypervisor and XenDesktop
- VMware ESX and Horizon
- Microsoft Hyper-V

Supported Systems

- Windows
- macOs
- Android
- Chrome OS
- Linux

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.