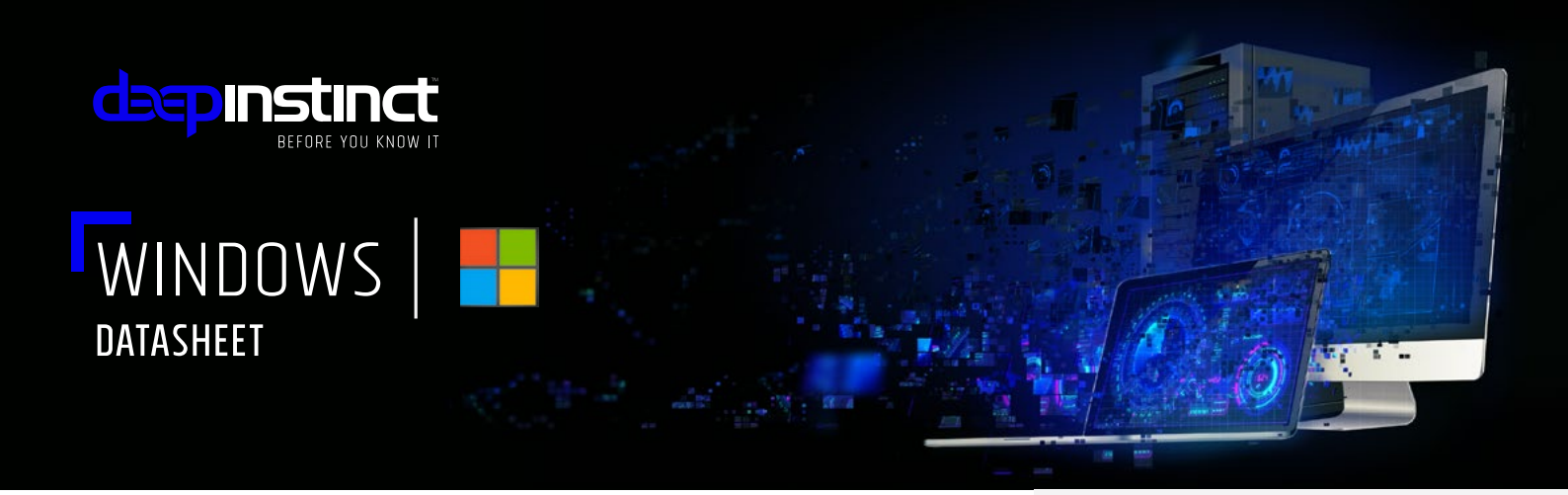
deepinstinct
BEFORE YOU KNOW IT

WINDOWS | DATASHEET



DEEP INSTINCT™ D-CLIENT FOR WINDOWS

Deep Instinct is the first and only company to apply end-to-end deep learning to cybersecurity. Deep learning is inspired by the brain's ability to learn. Once the brain learns to identify an object, its identification becomes second nature. Similarly, as Deep Instinct's artificial brain learns to detect any type of cyber threat, its prediction capabilities become instinctive. As a result, zero-day and APT attacks are detected and prevented in zero-time with unmatched accuracy.

Deep Instinct brings a completely new approach to cybersecurity that is proactive and preventative. The comprehensive defense is designed to protect against the most evasive unknown malware in zero-time, across an organization's endpoints, servers, and mobile devices.

FULL PROTECTION, WITH A PREVENTION FIRST APPROACH

Deep Instinct's solution provides full protection based on multiple layers, including a prediction & prevention first approach, followed by detection & response, against known and unknown cyber threats.

PRE-EXECUTION

Deep Static Analysis

Uses deep learning, the most advanced AI technology. The Deep Static Analysis provides far greater accuracy than signature and heuristic solutions, and is more accurate than classical machine learning algorithms, which suffer from lower detection rates and higher false positives. The agnostic implementation of deep learning can be applied to any file type and currently supports:

- Windows Portable Executables: PE (such as .exe, .dll, .sys, .scr, .ocx)
- Object Linking and Embedding: OLE (such as .doc, .xls, .ppt, .jdt, .hwp)
- Office Open XML: OOXML (such as .docx, .docm, .xlsx, .xlsm, .pptx, .pptm)
- Embedded Macros (in OLE and OOXML files)
- PDF (Portable Document Format) files: .pdf
- RTF (Rich Text Format) files: .rtf
- Adobe Flash files: .swf
- JAR (Java ARchive) files: .jar
- Image files: .tiff
- Font files: .ttf, .otf
- Archive files: .zip, .rar

D-Client predicts and prevents any malicious file upon the file's initial access on the device, and can also perform a full file scan during the initial installation or on-demand. It can be configured to prevent or detect malicious files, using different thresholds adapted to the organization's needs.

D-Cloud File Reputation (cloud-based)

Additional layer of protection based on file reputation, both for known malicious and benign files.

Script Control

A compliance and policy infrastructure to eliminate the script-based attack surface, including PowerShell, JavaScript, VBScript, Macros, HTML applications and rundll32.

Blacklist

Files can be blacklisted based on hash. The ability to import a list of IoCs based on hashes is also available.

DEEP INSTINCT™ SECURITY ADVANTAGES

- **Superior technology**
  The security solution is uniquely based on deep learning, the most advanced subset of AI technology.
- **Real time is too late**
  Static file analysis is performed pre-execution, ensuring the zero-time prevention of cyber threats.
- **No Trade Offs**
  Provides the highest rate of detection, with the lowest number of false positives.
- **Prevention Unlimited**
  Cross-OS support for Windows, macOS, Android, Chrome OS, iOS and iPadOS. Cross device support for endpoints, mobile devices and servers. Statically scan, pre-execution, the widest variety of files in the industry. Effective against both file-based and fileless attacks and operative with or without connection to the network.

REGULATION COMPLIANCE AND CERTIFICATION

AICPA SOC · ISO · PCI · HIPAA · GDPR · amtso · SE Labs

TECHNOLOGY PARTNERSHIPS

splunk> · MICRO FOCUS · IBM Radar · CITRIX · vmware · amazon web services · DEMISTO · Google Cloud

ON-EXECUTION

Deep Behavioral Analysis

Behavioral analysis capabilities that can detect and stop malicious business logic of threats.

Ransomware Protection

This module detects the behaviors of ransomware during their execution. The encryption techniques and the methods to perform read/write operations to encrypt files, are all known. This module covers them all, with a 100% detection rate and 0% false positive rate. This has been confirmed with over tens of thousands of tests performed by the Deep Instinct research team. This module has been implemented without relying on honeytokens/decoy/canary files, which are well detected by recent ransomware campaigns.

Code Injection Protection

This module detects Remote Code Injection techniques used to move laterally between processes. Code injection is typically implemented to achieve one of the following objectives:

- Evade detection by running malicious code on top of a legitimate
- process (such as explorer.exe).
- Evade detection by using a fileless technique.
- Escalate privileges by injecting to a high privilege process.

Supported code injection techniques:

- Process Hollowing: A legitimate process is executed in a suspended state, and its original code is replaced with malicious code. This technique can also be accomplished by patching the entry point, or by patching the context of the suspended process. An example of a malicious campaign is Duqu, Cobalt Strike.
- Create Remote Thread: A malicious code is executed as a thread created in a remote process.
- Load Library: A DLL is loaded into a remote process and one of its malicious functions is called.
- SetWindowsLong: A window handler is patched to execute malicious code.
- Asynchronous Procedure Call: This is similar to the Create Remote Thread technique, where a malicious code is executed as a threat created in a remote process using APC.
- Setting a Thread Context: The context of a thread is changed, which results in the execution of malicious code.
- IAT Hooking: A function from the Import Address Table (IAT) is hooked to execution malicious code.
- AtomBombing: The Windows Atom table is exploited to write malicious code into a remote process and then executes the malicious code. An example of a malicious campaign is Dridex Banking Trojan.
- PROPagate: This is similar to the SetWindowsLong technique, where a window callback handler is patched to execute malicious code. An example of a malicious campaign is RIG EK.
- Early Bird: A variation of the APC technique with added functionality to bypass detection from security solutions. An example of a malicious campaign is APT33.

Known Payloads Protection

This module detects the execution of known payloads during their execution. Protects against shellcodes from many tools, including MSFvenom, Shellter and Veil.

Contextual Script Execution:

This module detects the execution of suspicious scripts, and malicious and suspicious PowerShell commands.

POST-EXECUTION

Deep Instinct provides a set of operational tools to easily manage events and operate the environment:

Automatic Analysis

Deep Classification

Rapid classification of malware (known & unknown) in real-time, with no human involvement, into 7 different malware types and 7 PUA types, by using a unique deep learning malware classification module.

Attack Analysis

Easy understanding of what is going on in the environment during investigations, together with the attack chain.

Advanced Threat Analysis

Malware analysis and insights out-of-the-box for malware found in the organization, by both static and sandboxing analysis.

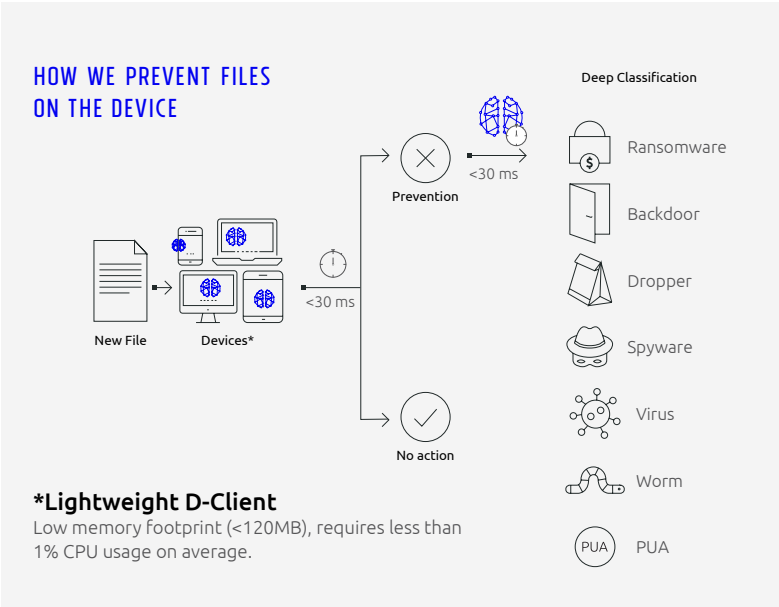
Remediation

Quarantine Files

Quarantine malicious files during their prevention.

Whitelist

Provides the ability to whitelist files detected falsely as malicious based on its hash, certificate and/or path. The ability to import a list of IoCs based on hashes is also available. Hashes that are added will be restored.



***Lightweight D-Client**

Low memory footprint (<120MB), requires less than 1% CPU usage on average.

Delete Files Remotely

Detected files that were not prevented and quarantined can be deleted remotely from the endpoint.

Terminate Running Process

Files that were detected as malicious and processes that were detected as behaving maliciously can be terminated remotely.

Isolate Device From Network

Devices that might create a risk to the organization can be isolated remotely.

ATTACK VECTORS COVERED

Files-Based Malware
Executable and non-executable files are scanned to predict and prevent viruses, worms, backdoors, droppers, wipers, coin-miners, known payloads, PUA and more.

Fileless Malware
Fileless attack vectors are prevented, including script-based attacks, dual-use tools and code injection techniques.

Ransomware
Ransomware is mitigated using a comprehensive protection, by both static and behavioral analysis.

Spyware
Protects against any type of spyware, including banking trojans, keyloggers and credentials dumpers.

Exploits
Protects against any client-side attacks.

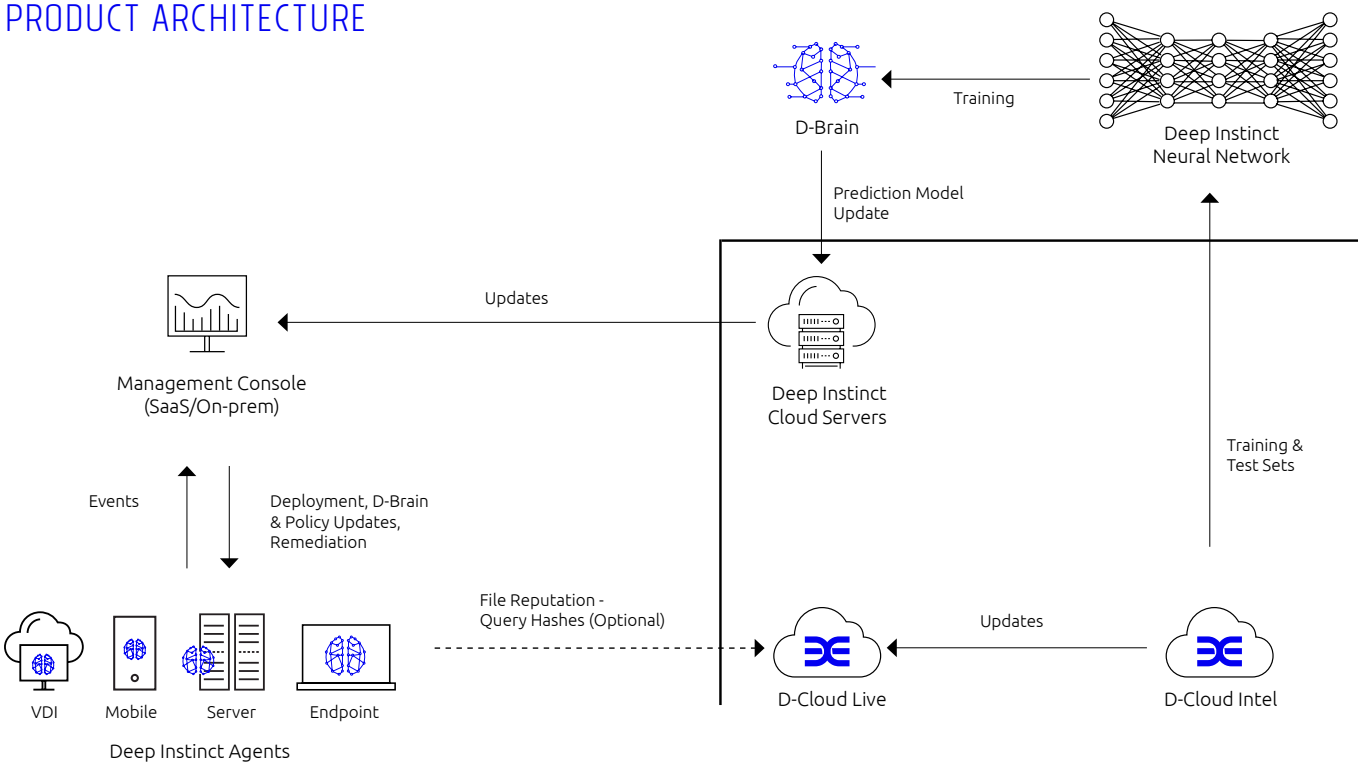
SYSTEM REQUIREMENTS

Operating System	Windows 7 SP1, 8, 8.1, 10 Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016, 2019
.NET Framework	Version 3.5 or higher
CPU	Dual-core CPU or higher
RAM	2 GB or higher (recommended 4 GB)
Disk Space	500 MB free disk space

SUPPORTED VIRTUAL ENVIRONMENTS

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

PRODUCT ARCHITECTURE



BECOME ONE OF THE LEARNED FEW

www.deepinstinct.com info@deepinstinct.com