deep instinct
BEFORE YOU KNOW IT

WINDOWS DATASHEET

April 2018 | Version 2.2

DEEP INSTINCT™ D-CLIENT FOR WINDOWS ENDPOINTS AND SERVERS

FILE-BASED

Real-time threat prevention with deep learning artificial brain (D-Brain) – Static file analysis using a lightweight prediction model that autonomously prevents zero-day and APT cyber threats on the devices, without any connection to the network or internet. Supports many file types, including executable files, PDF, Office files, archive files and more.

On-access detection – Detects any file before it is accessed or executed on the endpoint. According to the security policy, the D-Client decides to prevent and quarantine the file, or to allow the file.

File access control – Ability to whitelist files based on hash, certificate and/or path, and to blacklist files based on hash.

D-Cloud services – Provides a fast and scalable reputation infrastructure in the cloud (AWS) that adds a second layer of protection. Files can be re-classified in a second layer of validation using the D-Cloud database of all known threats and benign files and the right verdict is updated in real-time. The service is optional and can be disabled by policy.

FILELESS

Behavioral analysis – Provides an additional layer of protection by monitoring and preventing on-execution malicious behavior, including ransomware and code injection techniques.

Script control – Protects against fileless attacks that are based on scripts, including PowerShell, JavaScript, VBScript, HTML Applications and more.

Macro control – Using the D-Brain, identifies files containing embedded macros and determines whether the macro is malicious or benign.

DEEP INSTINCT™ SECURITY ADVANTAGES

- **Unmatched real-time detection and prevention of unknown malware**
  For file-based and fileless attacks.
- **Most accurate prediction of zero-day threats**
  Lowest false positive rates in the industry.
- **Static and pre-execution analysis**
  Foregoing the need for signatures or sandboxing.
- **Cross-OS support**
  Including Windows endpoints, macOS endpoints, Windows servers, Android and iOS.
- **Autonomous on-device protection**
  Evaluating threats in real- time without requiring any supplemental analysis nor connectivity to the organization's network or even to the Internet.

CERTIFICATIONS

PCI HIPAA By Coalfire

TECHNOLOGY PARTNERSHIPS

splunk> MICRO FOCUS IBM Radar
CITRIX vmware amazon web services

DETECTION, RESPONSE AND REMEDIATION

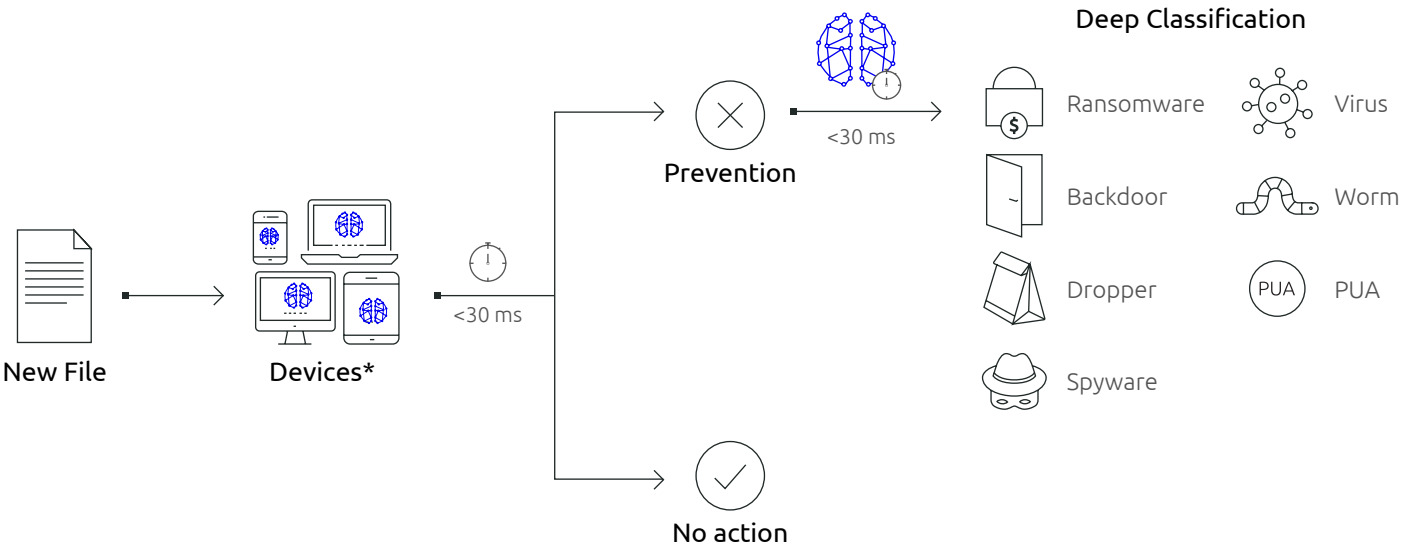
Remediation – Once a problem has been identified, it is resolved using Deep Instinct's response and remediation features, including file quarantine, file restore, file delete, terminate process, infographic of the process chain and more.

Deep Classification – Determines the malware family type of PE (Portable Executable) files. After a PE file is scanned by the D-Brain and detected as malicious, the file is scanned again by the Deep Classification brain providing results in milliseconds. Our classification model categorizes the malware into 7 different types: Ransomware, Backdoor, Dropper, Virus, Worm, Spyware and PUA.

Scanning – Performs a full file scan during the initial installation to identify pre-existing malware and new threats on the device. Scheduled periodic scans can be implemented, as defined by the administrator.

HOW WE PREVENT FILES ON THE DEVICE

Real-time process



***Lightweight D-Client**

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

DEEP LEARNING FACTS

- **20%-30% higher accuracy**
  During the past 2-3 years, deep learning has resulted in 20%-30% higher accuracy in benchmarks of computer vision, speech recognition, and text understanding. This is the greatest leap in performance in the history of computer science and AI.
- **Operates directly on raw data**
  While deep learning is a sub-field of machine learning, in contrast to traditional machine learning methods, deep learning can operate directly on raw data, without any need for human experts manually selecting a limited list of features.
- **Very deep neural networks**
  Nowadays, we can train very deep neural networks, with many tens of layers and billions of synapses.
- **Widely available infrastructures**
  Academic deep learning infrastructures are widely available. While they are great for research, their applicability in real-world high performance solutions is limited.
- **Deep Instinct applies deep learning**
  Only a handful of companies in the world have developed their own deep learning infrastructures, Deep Instinct being one of them.

DEEP INSTINCT™ MANAGEMENT
(ON-PREMISES OR IN THE CLOUD)

The management system uses a central cross-platform management and monitoring server, hosted on-premises at the organization's data center or in the cloud, for all endpoints (desktop, server and mobile devices).

Monitoring
Easy monitoring of the organization's security and deployment status.

Policy
Provides tools for configuring the organization's security policy. Manages different policies for groups or individual devices. Groups can be imported from the Active Directory tree, or pre-defined according to device name, OS version, D-Client version, IP range, tag, Tenant ID and more.

Intelligence
Provides an Advanced Threat Analysis feature that performs additional threat analysis for any malware file identified. Produces reports with a wide range of information for further analysis.

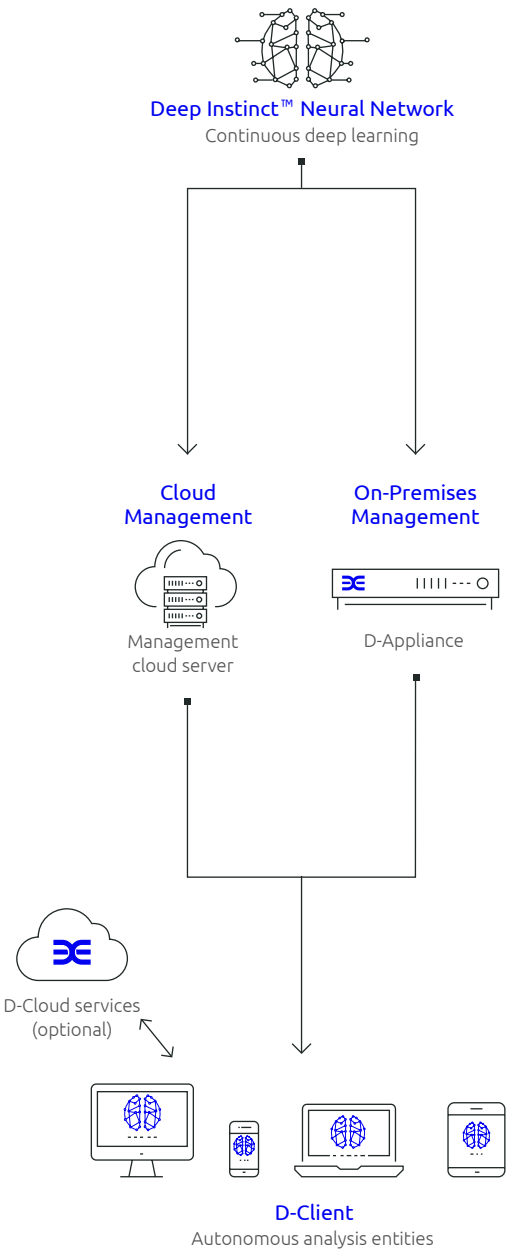
Logs and Reports
Provides advanced logging and reporting capabilities for security, deployment and threat analysis events. Integrates with lead SIEM products and SMTP servers for log forwarding.

RBAC
Ability to set different user roles to groups or individual users in the organization.

Deployment
Integrates with Windows deployment tools, such as SCCM or GPO. Upgrades directly from the management console. Does not require rebooting after installation or upgrade.

Multi-Tenancy
Provides enterprises servicing multiple MSP customers, individual MSPs and large enterprises with the capabilities to manage all entities from the same instance and management console. It includes features to allow administrators and SOC teams to manage multi-MSP and multi-tenant environments.

PRODUCT ARCHITECTURE



D-CLIENT SYSTEM REQUIREMENTS

Windows Operating Systems
Windows 7 SP1 (32-bit, 64-bit)
Windows 8 (32-bit, 64-bit)
Windows 8.1 (32-bit, 64-bit)
Windows 10 (32-bit, 64-bit)
Windows Server 2008 R2 SP1 (64-bit)
Windows Server 2012 (64-bit)
Windows Server 2012 R2 (64-bit)
Windows Server 2016 (64-bit)

Virtual Environments, VDI and DaaS*
Citrix Systems XenServer, XenDesktop and XenApp
VMware ESX and Horizon
Amazon Workspaces
Microsoft Hyper-V
Oracle VirtualBox

Hardware Requirements	
CPU	Dual-core CPU or higher
RAM	▪ 2 GB or higher (recommended 4 GB) ▪ Must meet OS minimum requirements
Disk	500 MB free disk space

* Contact Deep Instinct team for supported versions

ABOUT DEEP INSTINCT™

Deep Instinct is the first company to apply deep learning to cybersecurity, and the only cybersecurity solution based on a proprietary deep learning framework. Deep Instinct's on-device, proactive solution protects against zero-day threats, APT and ransomware attacks with unmatched accuracy. Deep Instinct's omni-cybersecurity platform provides comprehensive prevention, detection-and-response against the most evasive known and unknown malware in real-time. This is available for all major operating systems, across all endpoints, servers, and mobile devices.

TO GET STARTED WITH THE CYBERSECURITY REVOLUTION

ISRAEL
23 Menachem Begin Rd
28th Floor
Tel Aviv
Israel, 6618356

NEW YORK
501 Madison Ave
Suite 1202
New York City, NY
USA, 10022

SINGAPORE
The Working Capitol
140 Robinson Rd #04-00
Singapore
068907

+972 (3) 545-6600 www.deepinstinct.com contact@deepisntinct.com

deepinstinct
BEFORE YOU KNOW IT