STOP CYBER THREATS WITH THE DEEP INSTINCT PREVENTION PLATFORM

DATASHEET

PREVENTION STARTS WITH DEEP INSTINCT

Deep Instinct is the only cybersecurity company leveraging a deep learning-based neural network that learns and improves dynamically as it's fed more data.

Deep learning is inspired by the brain's ability to think and learn over time. Deep Instinct's deep neural network brain detects cyber threats and learns to stop them instinctively. As a result, Deep Instinct prevents zero-day attacks from Advanced Persistent Threats (APT) in near zero-time with unmatched speed and accuracy.

Protection from cyber threats begins with predicting and stopping them pre-execution. Deep Instinct's solution provides full protection in multiple layers, detecting and preventing both known and unknown threats, and eliminating them before they can do damage.

Any Attack Vector
Organizations can experience intrusions from any point across their environment. Threat actors can compromise accounts through phishing, social engineering, or brute-force attacks. They use exploits against web browsers, services, or applications to get into the victim's system. The Deep Instinct Prevention Platform detects and prevents breaches on any network endpoint.

Deep Instinct's protection is effective against virtually any attack vector. The moment an attacker attempts to land a malicious payload on their target, D-Client identifies and prevents it.

ADVANCED THREAT PROTECTION

Ransomware
Ransomware is prevented using comprehensive protection leveraging both static and behavioral analysis.

File-Based Malware
Malware is prevented by scanning executable and non-executable files to predict and prevent viruses, worms, backdoors, droppers, wipers, coin-miners, known payloads, PUA, and more.

Fileless and Memory Injection Attacks
Fileless attacks, including script-based attacks, shellcode, dual-use tools, and code injection techniques are prevented through a combination of deep learning and behavior analysis.

Spyware, Droppers, and Viruses
Spyware, including banking trojans, keyloggers, and credential dumpers are prevented using dedicated engines to identify malicious code and user actions.

Adversarial AI Threats (Adversarial Machine Learning)
Adversarial machine learning (ML), one of the most challenging trends in cybersecurity, is prevented via our purpose-built deep learning-based solution.

DEEP INSTINCT™ SECURITY ADVANTAGES

- **Superior Technology**
  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.
- **Real time is Too Late**
  Detect and prevent malware pre-execution. Deep Instinct stops threats in <20 milliseconds, 10 times faster than real time.
- **No Tradeoffs**
  With the industry's highest detection rate and the lowest number of false positives (< 0.1%), Deep Instinct delivers peace of mind while reducing workloads on security teams.
- **Cross-Platform Support**
  Deep Instinct provides protection across multiple platforms, from workstations and servers to mobile devices such as phones and tablets. D-Client supports Windows, MacOS, Android, Chrome OS, iOS, iPadOS, and Linux.[i]

REGULATION COMPLIANCE AND CERTIFICATION

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

TECHNOLOGY PARTNERSHIP AND INTEGRATIONS

splunk> · MICRO FOCUS · IBM Radar · citrix · vmware · aws · CORTEX · Google Cloud

ADVANCED THREAT CAPABILITIES

Microsoft Office and PDF File Protections
Deep Instinct provides advanced protection for MS Office and PDF files.

- Embedded DDE (OLE, OOXML) object in Microsoft Office document
- Macro protection

In-Memory Protection
Memory and shellcode injection attacks, also known as fileless-based attacks, are one of the fastest growing threats in the world. Advanced protection is required to keep your environments safe.

- Arbitrary Shellcode protection
- Remote Code Injection protection
- Net Reflection protection
- Credential Dumping protection
- Known Payload Execution protection

Script Control
PowerShell has become a favorite tool of cyber criminals. It is a trusted tool already in place and allows bad actors to leverage the "living-off-the-land" attack tactic. PowerShell also provides easy access to the Windows API, allowing criminals to perform administrative tasks without the risk of being blocked by existing security tools.

- Macro execution protection
- PowerShell execution/command protection
- HTML applications (HTA files) and JavaScript via rundll32 executions protection
- ActiveScript infrastructure protection
- ActiveScript execution (JavaScript & VBScript) protection

Suspicious Activity Monitoring – Threat Hunting
Understanding and responding to unusual activity in your environment is the key to effective detection and response.

- Suspicious activity detection and reporting
- Suspicious PowerShell command execution protection
- Automatic MITRE ATT&CK mapping and reporting

PRE-EXECUTION

Deep Instinct stops attacks before they happen by identifying malicious files in <20ms and preventing execution instantly. Speed and accuracy are critical to detecting, preventing, and quarantining threats.

Deep Static Analysis
Our Deep Static Analysis engine identifies threats faster and with fewer false positives than tools that rely on signatures, heuristics, or machine-learning frameworks, and prevents threats in a broad range of file types[ii].

- Windows Portable Executables: PE (e.g. .exe, .dll, .sys, .scr, .ocx)
- macOS Executable file: Mach-O (e.g. .macho)
- Linux binaries: (elf executables)
- Android packages: (apk files)
- RTF (Rich Text Format) files: .rtf
- Object Linking and Embedding: OLE (e.g. .doc, .xls, .ppt, .jdt, .hwp)
- Adobe Flash files: .swf
- Office Open XML: OOXML (e.g. .docx, .docm, .xlsx, .xlsm, .pptx, .pptm)
- JAR (Java ARchive) files: .jar
- Font files: .ttf, .otf
- Archive files: .zip, .rar
- Embedded Macros: (in OLE and OOXML files)
- Image files: .tiff
- PDF (Portable Document Format) files: .pdf

Deep Instinct's data science team is constantly researching new file types to add broader coverage.

D-Cloud File Reputation (cloud-based)
D-Cloud adds another layer of protection based on file reputation of known malicious and benign files.

Script Control[iii]
Deep Instinct reduces or eliminates script-based attacks including PowerShell and ActiveScript.

Contextual Script Execution
Deep Instinct detects the attempted execution of suspicious scripts and malicious or suspicious PowerShell commands.

ON-EXECUTION

Deep Instinct provides layers of defense that activate when an attack tries to execute.

Behavioral Analysis
Behavioral analysis capabilities detect and prevent malicious actions before they happen.

Ransomware Protection
Deep Instinct's behavioral analysis detects ransomware during execution without relying on common techniques that recent ransomware strains avoid.

Code Injection Protection
Deep Instinct reliably detects malware before it can execute despite developers using code injection to evade detection or escalate privileges. This includes Shellcode and LSAAS Dumping protections.

Known Payloads Protection
Deep Instinct detects known payloads during execution, delivering protection against many malicious tools.

POST-EXECUTION

Deep Instinct combines a prevention-first approach with features that help combat active adversaries.

Automatic Attack Analysis
Easily understand what is happening in the environment during investigation, along with the attack chain.

Deep Classification
Deep Instinct uses deep learning to rapidly classify malware, both known and unknown, in real-time and with no human involvement into seven different malware types and seven PUA types.

MITRE ATT&CK Mapping
Deep Instinct maps events directly to the MITRE ATT&CK framework, giving security operations the insight needed to respond to the event and investigate and respond to other threats.

Advanced Threat Analysis
Static and sandbox analysis delivers insights on any malware found in the environment.

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 is tailored to the specialized needs of Security and SOC teams. The dashboard and widget customization allows each authorized end-user to customize their own view.

Built-In Reporting
Ad hoc or scheduling of threat or trend reporting is easy with our built-in tools.

True Multi-Tenancy
Providing Partners, MSPs, and MSSPs with the capabilities to manage all entities from the same security instances and management console keeps all data safe and isolated from cross-contamination. Our solution allows security and SOC teams to administer multiple environments from one, centralized console including fixable pool-based licensing administration.

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.

Monitoring Integration
Seamless integration with security monitoring, alerting, log aggregation, and orchestration solutions by providing hooks, configuration, and customizable outputs for Syslogs, SMTP, SIEM, and REST API solutions.

Incident Response
If system isolation becomes necessary, our network isolation feature allows for simple system lockdown whether the system is in-network or remote. This action can also be done via the REST API.

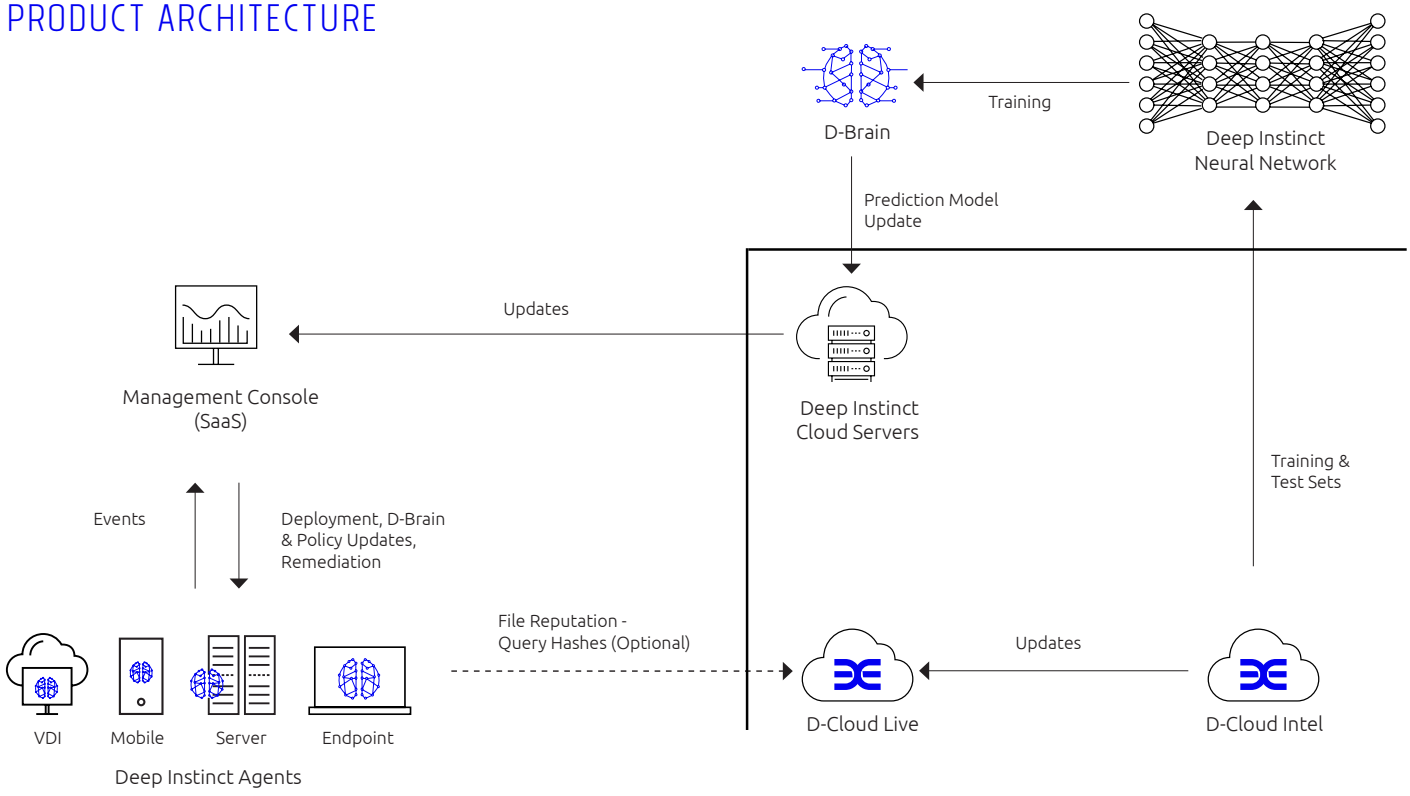
SUPPORTED SYSTEMS

Windows
macOS
Android
Chrome OS
iOS
Linux

SUPPORTED VIRTUAL ENVIRONMENTS

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

PRODUCT ARCHITECTURE



[i] Features vary by supported platform. See supporting documentation for details.
[ii] Specific file types vary by supported OS.
[iii] Specific script control capabilities vary by supported OS.

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 prevent threats pre-execution, before any damage is done, and have >99% unknown threat accuracy and a <0.1% false positive rate. The Deep Instinct Prevention Platform extends and enhances existing security stacks to provide complete protection against malware and other cyber threats anywhere in the enterprise — network, endpoint, and mobile.

0721V1