DATASHEET

Deep Instinct
Prevention for Applications

Meet the attacker earlier to prevent malicious files from entering your environment

SCANS TENS OF MILLIONS
FILES PER DAY

PREVENTS >99%
UNKNOWN THREATS EFFICACY

<0.1%
FALSE POSITIVE RATE

<20MS*
MALWARE PREVENTION

An Underserved Attack Vector: Malicious files

Unknown malware and zero-day attacks are successfully infiltrating everywhere in your environment, not only on the endpoint. Yet as an industry, we have underserved an important threat vector — files in motion, files uploaded or downloaded, and files stored. Organizations must look for new ways to stop the attack as far away from your sensitive applications and infrastructure as possible.

Enterprises have millions of files flowing from internal and external sources without a fast, effective, and cost-efficient way to scan them for malicious content — leaving a large gap in your defenses as attackers continue to find new ways to get inside. Malicious actors are patient and will wait for malware infected files — that have slipped through and are hidden in your storage — to be opened and provide them with access.

User downloads from the internet or web application file uploads to your public and private clouds are either not being scanned or your existing solution or methodology is too slow and unable to detect unknown threats before they are stored. Once an infected file is executed you are at the mercy of your existing cybersecurity solutions like detection and response to stop the threat before a breach occurs.

Deep Instinct Prevention for Applications

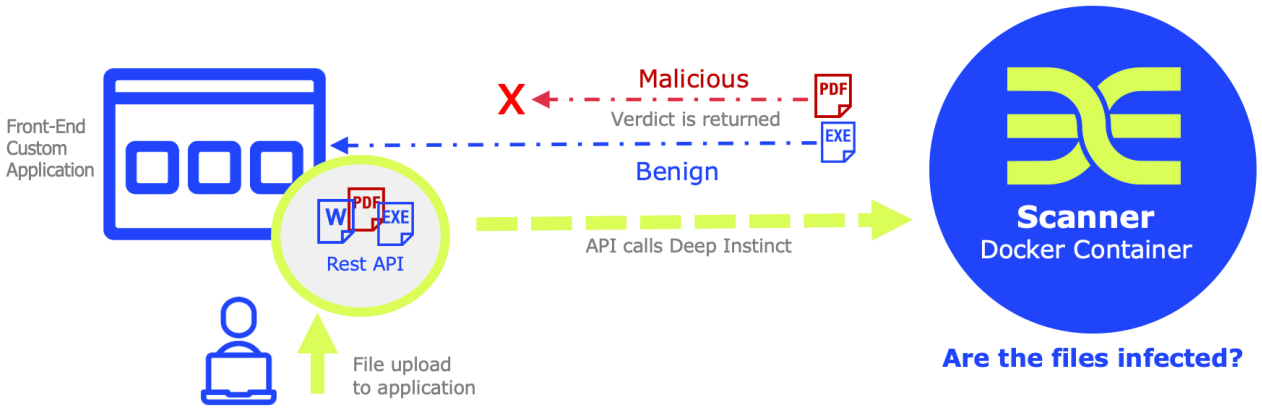
Deep Instinct Prevention for Applications is an agentless, on-demand, antimalware solution for the enterprise that is device and system agnostic. With our unique, industry-leading deep learning approach, your organization can prevent ransomware, zero-day, and unknown malware infected files before they reach your endpoint, server, or storage. Deep Instinct scans the entire content of a file to provide fast and extremely accurate malicious vs benign decisions in <20ms with <0.1% false positives and an extremely low footprint.

No matter the industry, whether you are a large banking institution, online retailer, healthcare, or government organization, your files are a risk. Customer uploads, user downloads, and third-party suppliers transferring files into your environment leave your organization blind to the content traversing your network.

Deep Instinct Value

- Protect custom web applications by preventing >99% of unknown threats
- Scale to scan tens of millions of files per day with very low latency
- Maintain full privacy as only the file hash that ever leaves the enterprise
- Align workflows with a flexible and programmable API that is operating system and device agnostic
- Integrate with and lower infrastructure costs
- Reduce risk and easily meet compliance with a prevention-first approach

**20ms scan based on 2MB file, results may vary with larger files*



ONE EXAMPLE: An end user uploads a file through a custom web application.
*The file is sent to Deep Instinct to be scanned and a verdict is returned in <20ms.**

Deep Instinct Prevention for Applications has revolutionized threat protection beyond the endpoint with flexible, deploy-anywhere, in-transit file scanning at enterprise speed and protects any web application or cloud storage from malicious content without impacting user experience. Deep Instinct stops the unwitting spread of malware from within your organization or back to your customers and partners.

Deep Instinct Prevention for Applications integrates with your existing infrastructure to meet the attacker earlier and prevent malware from wherever it attempts to gain access into your environment. Deployment flexibility, via REST API or ICAP, allows for simple integration with existing workflows and processes, and customized responses.

A step beyond traditional AV, security web gateway, and sandbox solutions

The cybersecurity landscape has lacked a solution with the efficacy, speed, and scale required by an enterprise to prevent unknown threats. It's not enough to have a solution that checks file extensions and allows or blocks based on file type because attackers or insiders can hide scripts by modifying them.

Web applications often require script files to be uploaded without any assurance that those scripts don't contain a threat. In these cases, a file scanner must be able to identify file types based on the content, rather than extension alone. End users are constantly attempting to download from the internet from untrusted sources providing another source of trouble.

Organizations using AV and sandbox solutions face challenges because of the following:

- Signature-based solutions are only useful if the attack is known but will not stop the unknowns.
- Sandbox solutions are resource intensive, slow to respond, cannot scale to the needs of the enterprise, are costly, and result in poor user experiences.
- Sandbox solutions are also easily evaded by attackers who have built their malware to bypass controls and not detonate if a sandbox environment is detected.
- Proxy solutions using the ICAP protocol offer scanning, but the scans are too slow, miss unknown threats, lack efficacy, and experience high latency, negatively impacting user experiences.

**20ms scan based on 2MB file, results may vary with larger files*

Imagine the Possibilities

Deep Instinct meets the attacker earlier to prevent more threats — known, unknown, ransomware, or zero day — before they hit the endpoint, server, or enter storage. We reduce risk and provide greater protection to predict and prevent the next big threat while protecting your privacy as files never leave your enterprise. BYOD, remote work, and the increasing sophistication of attacks requires a shift to a prevention-first mindset no matter where the threat originates.

Scale to Enterprise with Low TCO

- Scales to scan tens of millions of files per day and protects data privacy
- Tailors to your IT and application workflows, not vice versa
- Reduces infrastructure costs through efficient use of resources

Stop malware file infections without latency

- Scans files at speed with near zero latency
- Returns malicious vs benign verdict in <20ms*
- Does not rely on the cloud to provide a verdict

Lower burden on SOC operations

- Provides <0.1% false positive rate to improve SOC productivity
- Updates infrequently required with an average of 3x per year
- Lowers maintenance burden to save SOC time

Prevent unknown malware with the highest efficacy

- Stops attacks with >99% unknown threat efficacy
- Prevents ransomware, zero-day, file, and script-based attacks
- Maintains the same prevention efficacy even without internet connectivity

Technical Specifications

Deep Instinct Prevention for Applications is implemented via REST API or ICAP

Scan files via REST API before they reach the endpoint, server, or storage
Scan in-transit files (attempted file downloads from internet) via ICAP (integrating with web gateways, firewalls & CASB)

- Flexible Docker Container Deployment
- Expansive list of file types scanned
  - File Format, Common file extensions/types
  - Portable Executable (PE32, PE64), .exe, .dll, .sys, .scr, .ocx
  - macOS Executable, Macho32, Macho64, MachoFAT
  - Object Linking and Embedding, .doc, .xls, .ppt, .jdt, .hwp
  - Office Open XML, .docx, .docm, .xlsx, .xlsm, .pptx, .pptm
  - Portable Document Format, .pdf
  - Rich Text Format, .rtf
  - Adobe Flash, .swf
  - Java Archive, .jar
  - Tag Image File Format, .tiff
  - Font, .ttf, .otf
  - Apple Disk Image, .dmg
  - Archives, .zip, .rar, .7z, .tar, .tar.z, .tar.gz, .tar.bz2, .xar, .gzip
  - Macros and scripts, Embedded in document files
- Classification of malware via optional D-Cloud reputation engine
- Platform, OS, and device agnostic
- Integrates with SIEM and SOAR

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.

www.deepinstinct.com | info@deepinstinct.com