DATA SHEET

Deep Instinct
Prevention for Applications

Stop malware before it enters your data repositories or reaches your servers or endpoints.

PREVENTS
>99%
UNKNOWN THREATS

<0.1%
FALSE POSITIVE RATE

SCANS TENS OF MILLIONS
FILES PER DAY

<20MS*
DECISION TIME

Files are the lifeblood of your business. They're created, shared, distributed, and stored everywhere, which puts your critical data at risk. More often than not, the files uploaded from customers and end users either aren't scanned, or are scanned with inadequate solutions like NGAV, CDR, or Sandbox. These approaches can't scale to meet the volume and velocity of threats, are too slow, and have not evolved to stop unknown malware. Plus, third-party files traversing your network leave your organization blind to malicious content. Enter Deep Instinct.

Protect Your Data by Keeping Malware Out

Deep Instinct is leading the charge toward better data security with flexible, deploy-anywhere, in-transit file scanning that meets the demands of the enterprise. Deep Instinct prevents ransomware, zero-day, and other unknown malware before they reach your applications and data repositories, all without impacting user experience. We stop the unwitting spread of malware within your organization to better protect your sensitive data and reduce the burden on your SOC.

Agentless, On-Demand File Scanning to Prevent Unknown Threats

Deep Instinct Prevention for Applications (DPA) is an agentless, on-demand, anti-malware solution that is device- and system-agnostic. DPA seamlessly connects to your existing infrastructure to quickly scan files and provide a malicious-vs-benign verdict before the file is allowed into your application or storage repository. Our containerized deployment, connected via REST API or ICAP, allows for simple DevOps integration with existing workflows and processes, as well as customized responses.

DPA quickly scans all file content to provide fast and accurate decisions with high throughput, limitless scalability, low false positives, and an extremely light footprint.

Predictive Prevention with Deep Learning

Deep Instinct Prevention for Applications has been architected from the ground up on a purpose-built deep learning framework dedicated to cybersecurity. Deep learning is the most advanced form of AI, which means you can anticipate an attacker's next move by understanding the distinct characteristics of malware and preventing it before it lands inside your environment.

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

Benefits

Predictive Prevention
Protect your data with the highest efficacy against zero-day, ransomware, and unknown threats – powered by Deep Learning.

Deployment Flexibility
Deploy anywhere, with a containerized architecture and a programmable REST API or ICAP integration that easily aligns with AppDev and DevOps workflows.

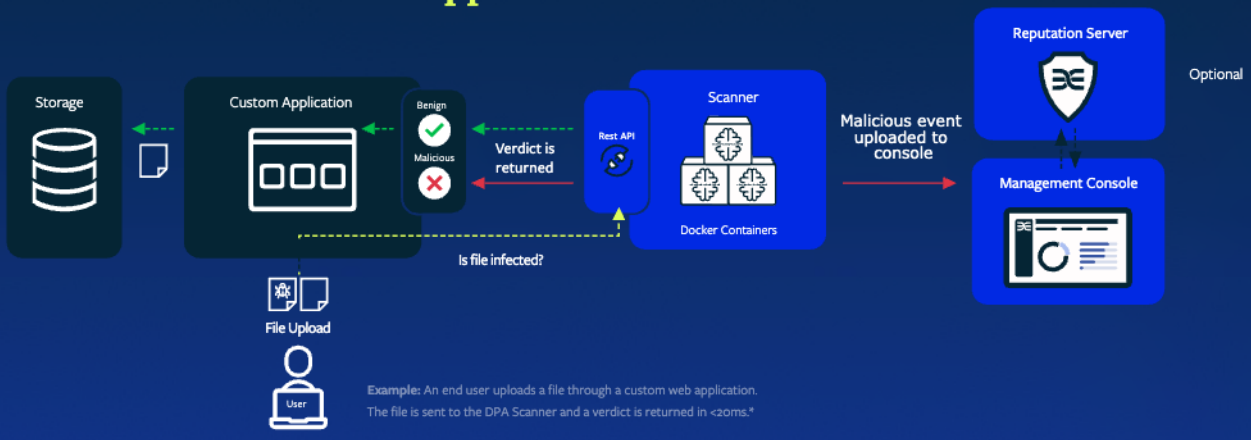
Near-Zero Latency
No discernable impact on customer and end-user experiences.

Low TCO
Low TCO with minimal infrastructure requirements, small footprint, and high throughput.

Autonomous
Does not rely on rules or signatures, the cloud, or require threat intelligence feeds. Maintains the same high efficacy in online and air-gapped configurations.

Compliant and Private
Protects data privacy and meets compliance mandates and industry regulations by design.

Deep Instinct Prevention for Applications



Example: An end user uploads a file through a custom web application. The file is sent to the DPA Scanner and a verdict is returned in <20ms.*

Meeting Enterprise Scale with low TCO

- Scales to scan tens of millions of files per day
- Easily tailors to IT, DevOps, and application workflows
- Infrastructure costs reduced through efficient use of resources
- Full privacy with only the file hash ever leaving the environment

Enhancing User Experiences with Near-Zero Latency

- Extremely low latency
- Malicious vs benign verdict returned in <20ms*
- No cloud check or threat intelligence feed required to provide a verdict

Reducing the Burden on the SOC Team

- Low false positives lead to fewer and higher fidelity alerts
- Updates infrequently with an average of 3x per year
- Very low maintenance requirements

Preventing Unknown Malware with the Highest Efficacy

- >99% unknown threat efficacy
- Ransomware, zero-day, file, and script-based attacks prevented, pre-execution
- Does not require rules or signatures to make decisions
- High efficacy maintained when onine

Technical Specifications

SUPPORTED fiLE TYPES

Documents

- **PDF**
- **Office Files**
  - Docx
  - Xlsx
  - pptx
  - doc
  - xls
  - ppt
  - Hwp
  - Docm
  - Pptm
  - mht
  - sylk
- **RTF**

Web & Archives

- **WEB**
  - HTML
  - JavaScript
  - CCS
- **Archives**
  - zip
  - xar
  - 7z
  - Tar
  - rar
  - Jar
- **Compression**
  - .gz
  - .bz2

Executables

- **PE 32/64**
  - exe
  - dll
  - sys
  - scr
  - ocx
- **ELF 32/64***
- **Mach-O**
- **.o**
- **.so**
- **bundle**
- **dylib**

Media

- **Image**
  - JPEG
  - PNG
  - BMP
  - TIFF
- **Audio**
  - MP3
- **Video**
  - AVI
  - MOV
  - MP4
- **Fonts**
  - tff
  - otf

Other

- **EICAR**
- **Email**
  - eml
  - msg
- **Lnk**
- **Disk Images**
  - DMG
  - ISO99960
- **Application Files**
  - DWG
  - AI
  - EPS
- **Text**
  - CSV
  - XML

PRODUCT SPECS

- Platform, OS, and device agnostic
- Easily integrates alerts with EDR, MDR, XDR, SIEM and SOAR
- Deploy on premises or in the cloud
- Max file size support: 1TB
- Archive size limit: 50GB
- Integrate anywhere via REST API or ICAP
- Supports Kubernetes, OpenShift, and EKS
- Up to 180 MB/second throughput per pod**
- Optional cloud reputation engine

deep instinct

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.