DATASHEET

Deep Instinct
Beyond the Endpoint

WORLD'S ONLY
DEEP LEARNING
BASED CYBERSECURITY SOLUTION

PREVENTS
>99%
KNOWN, UNKNOWN, ZERO-DAY THREATS

PREVENTS THREATS IN
<20MS

ONLY
1-2 UPDATES
NEEDED PER YEAR

Prevent Attacks Across Malicious File Uploads and Downloads for Cloud, Web Gateways and Applications

The endpoint is not your only attack vector; threat actors are continually searching for new ways to infiltrate your hybrid environment. Files stored in the cloud, uploaded into your custom applications, and downloaded from the internet all expand your attack surface and increase the risk of a breach.

Through the power of deep learning, Deep Instinct meets the attacker earlier to prevent malware from being uploaded into your environment — without requiring agents. Using our deep learning static analysis, Deep Instinct scans in-transit files to ensure the integrity of your local, private, and public cloud storage, as well as your custom applications, and prevents malware at the web gateway – reducing latency and stopping more threats before they hit your endpoints.

Deep Instinct preserves the integrity of the files in your hybrid environment to ensure business continuity, improve SOC efficiency, and increase compliance by preventing known and unknown threats including ransomware, zero-day threats, and file- and script-based attacks, earlier and faster.

Deep Instinct for Cloud

With the acceleration of digital transformation, enterprises are experiencing a high volume of file transfers into and out of their public and private cloud storage.

Public cloud providers are responsible for the security of the cloud, but you are responsible for the security of what is stored in the cloud. Preventing malicious content from entering cloud storage is critical to lowering the risk that an infected file could spread malware.

Deep Instinct prevents malicious files from uploading to, or downloading from, your public or private cloud storage.

Challenge:

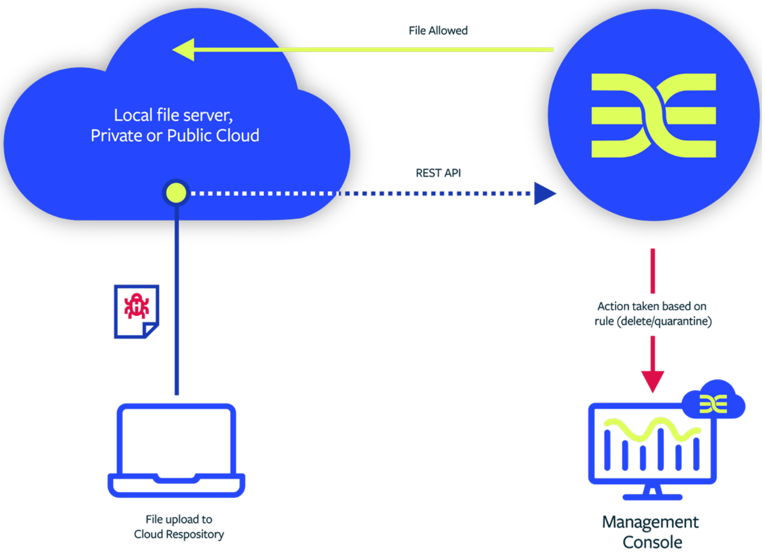
Files stored in the cloud could be malicious

- Infected files stored in the public or private cloud increase risk of a breach

Opportunity:

Ensure the integrity of the files stored in the cloud

- Reduce the risk that malware-infected files are a hidden source of infection
- Prevent malware from spreading to production systems upon download
- Lower the probability of a weaponized file executing a ransomware or other attack upon download



Benefits

- Prevents malicious files from uploading into public or private cloud storage.
- Keeps malware infected files from reaching production systems.
- Improves existing security solutions by reducing burden on the endpoint.

How it works:

When a file is uploaded to a public or private cloud, or a local file server, a trigger will call Deep Instinct to scan the file and return a verdict of malicious or benign and the file is either blocked or allowed.

Deep Instinct for Applications

To meet the needs of your business, your organization has custom-built or modified applications. Applications that require a high number of files to be uploaded and downloaded by employees or customers pose a potential risk. A challenge for organizations who modify or develop their own custom applications is that they often lack consistent security standards.

Deep Instinct scans in-transit files to ensure that they are uploaded through your custom applications and downloaded to your customers free of malware.

Challenge:

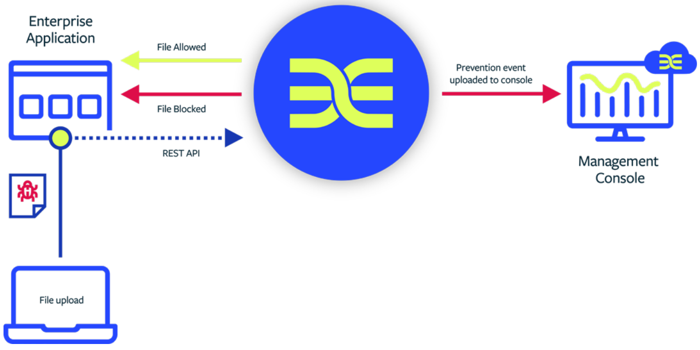
Weaponized files pose risk to users and customers

- Increased risk from both internal and external file uploads and downloads through your custom applications

Opportunity:

Decrease risk, reduce attack surface

- Meet the scale requirements for scanning high-volume applications for malware without introducing latency
- Prevent the introduction of malware into your production environments
- Increase assurance that your applications will not be a source of infection for your end users or customers



Benefits

- Reduces latency associated with traditional AV file scanning.
- Provides consistency of security standards across all applications.
- Scales to the needs of high volume transaction applications.

How it works:

When a file is uploaded through an application, a trigger calls Deep Instinct to scan the file. If the file is deemed malicious the file is blocked, and according to the policy set by the organization, the file will be deleted or sent to a sandbox.

Deep Instinct for Web Gateways

Unknown malware bypasses traditional AV defenses at the web gateway and increases the reliance on the endpoint to catch threats. Existing controls have a low probability of preventing never-before-seen threats and increase latency thus adding an .additional burden on security analysts who are already overwhelmed with alerts

If you are currently using a web proxy to filter traffic, Deep Instinct will scan files to prevent users from accessing malicious files from the internet. Deep Instinct, deployed with ICAP, will prevent the download of malicious files from the web faster and more accurately using our deep learning static engine to catch >99% of known and unknown threats.

Challenge:

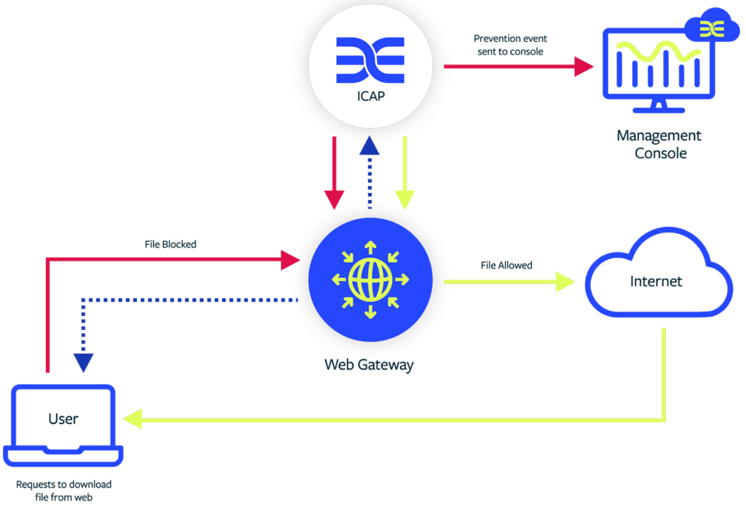
Legacy AV and ICAP solutions will not stop unknown threats

- Threats missed at the proxy are then dependent upon endpoint detection

Opportunity:

Reduce the burden on the endpoint

- Reduce the operational and investigation cost of existing endpoint solution
- Reduce latency associated with file scans to improve user experience
- Provide greater protection with your existing infrastructure



Benefits

- Prevents a greater number of known and unknown threats at the web gateway.
- Improves end user experiences by reducing latency associated with Legal AV solutions.
- Reduces malware at the endpoint and the burden on security analysts overwhelmed with alerts.

How it works:

Your internal user requests access to a file from the internet. That request first hits the proxy and is then offloaded to the ICAP Server to make the benign vs malicious decision instantaneously and the file is either returned or denied. The end user will see the request come back or see a request denied message.

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.