deep instinct™

CASE STUDY

SECURE HIGH VOLUME FILE UPLOAD

Fortune 50 financial services organization uses Deep Instinct to validate the integrity of millions of application file uploads every day

RELIABLY AND QUICKLY SCAN MILLIONS OF FILES PER DAY IN

<20MS

WITH NO IMPACT ON BUSINESS OPERATIONS

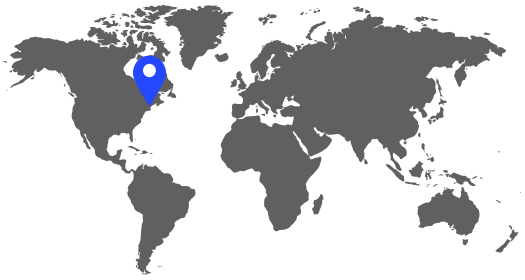
PREVENT UNKNOWN THREATS IN FILE UPLOADS BEFORE THEY REACH THE ENDPOINT

LOWER RISK AND ENSURE BUSINESS CONTINUITY WITH REDUCED LATENCY AND ELIMINATION OF SANDBOXING

The Company

Multinational financial services institution

Industry: Financial Services
Company size: Enterprise
Existing security solution: Antivirus



Attacks come from many different touchpoints within an organization. Endpoints are an important protection point, but it's become necessary to stop an attack earlier, long before it reaches the endpoint.

One often-ignored gap is the files that enter an organization through custom business applications. The enterprises that scan files for malicious content often do so for compliance reasons but continue to be at risk of a compromise because current solutions are slow and ineffective at stopping unknown threats, like ransomware, new malware and variants, and zero-day threats.

The Need: Faster, Accurate and More Reliable Prevention of Malicious File Uploads

This Fortune 50 financial services organization has customers, employees, and other third parties who regularly upload files to transact business around investments, loans, and hiring. Millions of files containing a variety of sensitive data – customer, payment, and other protected information – are uploaded and stored every day from hundreds of their custom business applications.

Every file upload is potentially malicious, as attackers weaponize documents, like Office and PDF files. Malicious documents, if uploaded, are one of the most prevalent attack vectors early in the kill chain. As attackers increase evasion and exploitation techniques, they commonly use malicious files as a first stage dropper. Because files are suitable for targeting organizations (trivial landing surface).

The Company was using a traditional antivirus solution to scan the files, but the legacy product lacked efficacy, introduced latency, and consumed a high number of resources. The traditional antivirus (AV) solution could not handle the wide variety of file types that needed to be scanned. This not only affected the user experience, but also required vast resources to run and maintain the solution.

As files were passed through the AV solution, the number and size of files meant that scanning and sandboxing malware could take up to five minutes per file, an unacceptable SLA for employees and customers, ultimately impacting business continuity that explicitly put them at risk of negatively impacting employee productivity.

In addition, typical AV solutions only scan three to five percent of the actual file, lowering the efficacy of the tool and making false positives and false negatives far too common. Virus scanning was massively resource-intensive, with server CPU utilization regularly clocking in at 90%. On top of the delays and the expense, the traditional AV product could not guarantee that it could stop known threats, let alone ransomware or zero-day exploits.

Because of an ongoing validation conducted by the Company's IT teams on a multitude of solutions, they understood the value of Deep Instinct's unmatched efficacy to prevent both known and unknown malware. It was proven that Deep Instinct provided a better way to scan their uploaded files, ensure the integrity of their storage, and lower their risk.

The Solution: Deep Instinct Prevention for Applications

The Company's security team identified that Deep Instinct Prevention for Applications could better protect against weaponized files and reduce latency to improve security and provide a better user experience, while at the same time improving their ability to meet compliance and do so with unmatched speed and efficacy.

Through the power of deep learning, Deep Instinct enables the Company to meet the attacker earlier by preventing malware from being uploaded to storage through their custom applications. Deep Instinct's low false positive rate was a critical success factor for the solution.

Using deep learning static analysis, Deep Instinct scans in-transit files as well as script content like DDE, Excel 4.0, and dynamic script loading, to validate the integrity of uploaded files before they are stored and downloaded. The documents are scanned in their entirety without flattening content or reducing functionality. Preventing the file from storage means that the malicious content will never reach the endpoint, eliminating the risk.

For example, a mortgage application may require a prospective homeowner to upload a file for review. Deep Instinct scans the file before it is allowed to be stored or retrieved. This protects not only the Company from a malware infection, but their customers as well when the file is sent back for review.

Deep Instinct Prevention for Applications provided the Company with a highly flexible solution that does not require an agent to be implemented. Using a REST API, the Company can point the Deep Instinct solution at any custom application they choose providing resilience to unknown attacks and exploits.

Deep Instinct scans files for known and unknown threats and returns a malicious or benign verdict in less than 20 milliseconds. If the file is clean, it is allowed to be stored. If the file is identified as malicious, it is prevented or otherwise directed according to the Company's compliance and security policies.

The Results

Ensure business continuity by stopping malicious file uploads

Deep Instinct Prevention for Applications is scanning millions of documents per day that are uploaded through several hundred custom business applications. This scale combined with Deep Instinct's less than 20 millisecond speed to prevent, ensures that there is no disruption to the business. By stopping malware before it hits the endpoint, the Company can reduce the attack surface and improve compliance. The Company is protected as are its customers—without any impact to the user experience.

- Reliably and quickly scan millions of documents per day in under 20ms (per file)
- Improve user experience with near zero latency
- Meet attacker earlier by preventing weaponized files from storage

Lower resource requirements

As an agentless solution, Deep Instinct Prevention for Applications doesn't place a burden on the Company's custom applications or require any changes to the existing infrastructure. The solution eliminates the need to run files in a sandbox which speeds up the scanning process. A false-positive rate of <0.1%, provides the security operations team with time back to focus on the threats that matter most.

Deep Instinct's API is seamlessly incorporated into the organization's business and security workflow. Each business unit can adapt the workflow to meet its individual requirements.

The flexibility of Deep Instinct API-based solution means that the Company can add new applications and monitor the activity.

- Provides flexibility by integrating into existing infrastructures
- Works with existing workflows and products as an agentless, API-based solution
- Improves SOC operations with low false positives and greater threat accuracy

Greater visibility into emerging risk

The Company has greater visibility into emerging risk and has created a portal to track all of its Deep Instinct-protected applications. The Company can gain insights on their custom applications that are most targeted by attackers, so it can proactively protect against emerging threats. The flexibility of the Deep Instinct solution makes it easy to add new applications for scanning.

- Insights into which custom applications are more targeted by attackers
- Reduces risk from known and unknown threats like ransomware and new variants
- Gain understanding into custom application file activity

Summary:

The Fortune 50 Company adopted Deep Instinct's API-based, agentless solution to solve a critical need to improve efficacy, meet compliance and reduce risk from weaponized files. With a low false positive rate of 0.1% and improved threat prevention efficacy, the Company is able to scan millions of files per day with zero impact on end users. Deep Instinct's prevention platform provides prevention on the endpoint and beyond to stop attackers earlier, shrinking an organization's attack surface and lowering their overall risk.

"The scale, speed, and flexibility of Deep Instinct Prevention for Applications enables Fortune 50 financial services to protect against the growing risk of malicious file uploads from hundreds of critical business applications. "

Request an online demonstration of the Deep Instinct Platform

See how Deep Instinct can help protect your organization in this live demonstration of our solution capabilities against unknown threats.

REQUEST A DEMO

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.