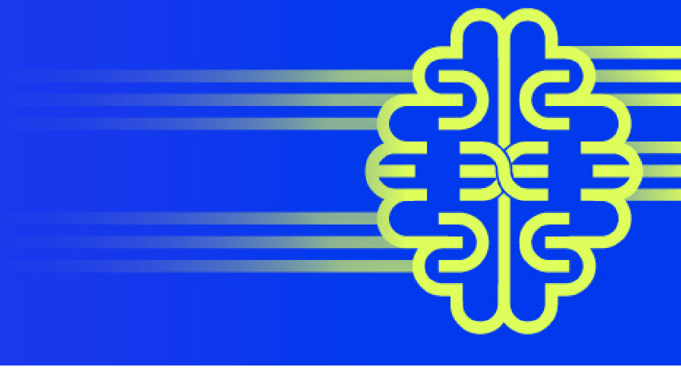
SOLUTION BRIEF

Deep Instinct Prevention Platform



STOP RANSOMWARE
BEFORE IT ENCRYPTS

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

GUARANTEES
<0.1%*
FALSE POSITIVE RATE

<20MS
MALWARE PREVENTION

There are 350,000 new pieces of malware discovered daily—and this number is growing exponentially. Zero-day, ransomware, filed-based, fileless, supply chain, and adversarial AI attacks continue to morph and evade detection, making it exceedingly difficult to prevent bad actors from infiltrating your hybrid network. An innovative prevention-first approach—made possible by deep learning—is the path forward to take back control.

With work-from-anywhere becoming the new normal combined with the continued evolution of digital transformation and distributed networks, computing has moved closer to the edge. Protecting your endpoints has never been more important.

But it's not just the endpoint. Bad actors can infect systems through files stored in the cloud, files uploaded through applications and downloaded to customers, and files your end users are downloading from the internet. Legacy AV will only prevent known threats. And EDR alone is not enough to stop the unknowns before they are executed on your network.

We must rethink our approach to prevention.

The Deep Instinct Prevention Platform

The Deep Instinct Prevention Platform stops known, unknown, and zero-day threats with the highest accuracy and lowest false-positive rate in the industry. For your organization, this means reduced risk, greater SOC efficiency, and the knowledge that attackers have lost their advantage. With >99% known, unkno wn, and zero-day threat accuracy, a guaranteed <0.1% false positive rate, plus a $3M ransomware warranty backed by Munich Re, the Deep Instinct Prevention Platform meets the promise of true prevention.

Deep Instinct prevents threats prior to execution, unlike detection and response solutions that look for behaviors after the attacker has already installed droppers and artifacts on your network. Deep Instinct's Prevention Platform reduces the risk of a breach by meeting the attackers earlier and stopping threats 750x faster than the fastest known ransomware can begin to encrypt.

Deep Instinct prevents attacks at the endpoint with end-to-end static and multi-layered dynamic analysis. To meet the attacker even earlier, Deep Instinct also prevents malware beyond the endpoint by scanning the in-transit files of your custom applications and workflows, as well as local, private, and public cloud storage and web gateways to prevent the upload or download of malicious files while ensuring the integrity of your environment.

Deep Instinct Powered by Deep Learning

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

Deep learning is the most advanced form of AI, inspired by the brain's ability to think and learn over time. Our vast neural network has been trained for more than five years on hundreds of millions of files to autonomously prevent threats.

Deep Learning differs from basic machine learning in several critical ways:

Basic machine learning requires a human domain expert, making it slow and prone to error, and is only trained on 2% of available data. Deep learning trains on 100% of available raw data and can make non-linear correlations of the data automatically. With deep learning-based neural networks specifically architected for cybersecurity, decisions are made faster, more accurately, and with much greater efficacy.

A deep learning model is self-sufficient and does not require frequent cloud updates or constant human intervention.

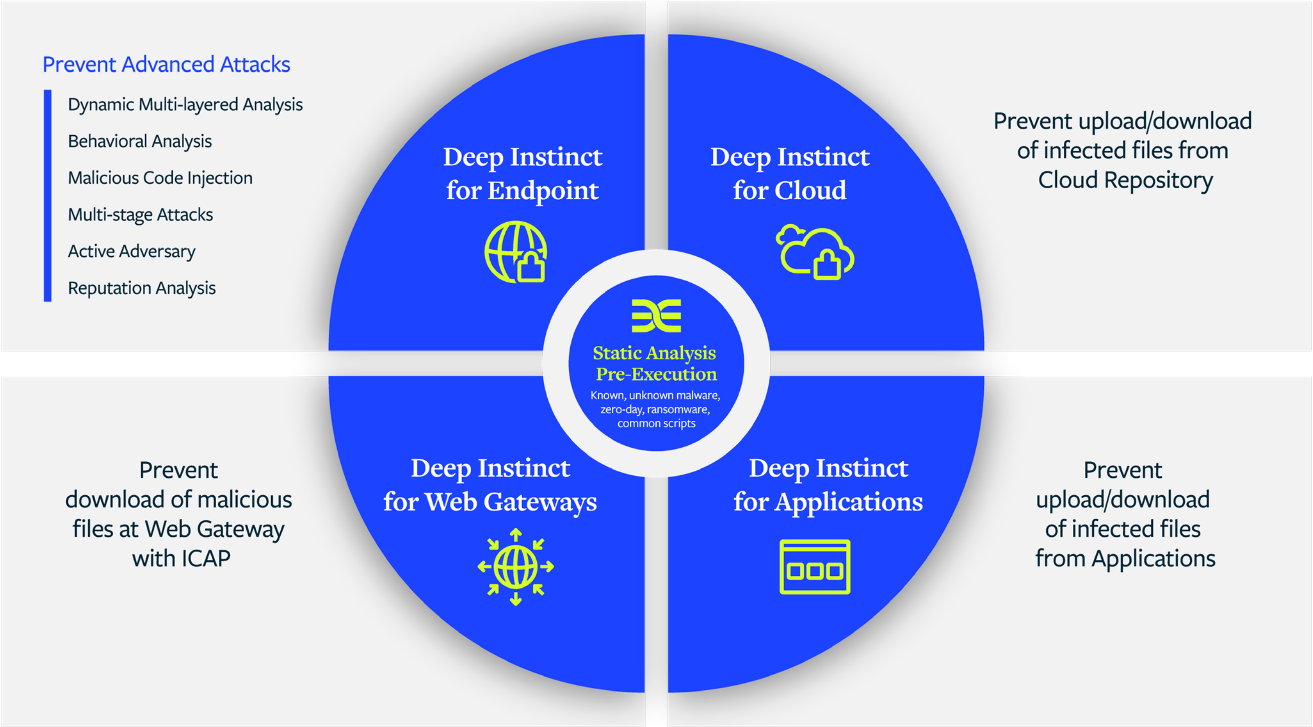
Ultimately, deep learning is what will enable organizations to make prevention a reality, predicting and stopping threats before they execute and compromise your environment.

Product Differentiators

- Integrates with existing security solutions to improve efficiency, effectiveness, and focus on what really matters – stopping attacks.
- Reduces burden on security teams to sift through false positives
- Improves threat hunting capabilities with high-fidelity alerts and suspicious activity rating

*Applies to endpoint only.

The Deep Instinct Prevention Platform



Prevent Advanced Attacks

- Dynamic Multi-layered Analysis
- Behavioral Analysis
- Malicious Code Injection
- Multi-stage Attacks
- Active Adversary
- Reputation Analysis

Deep Instinct for Endpoint

Deep Instinct for Cloud

Prevent upload/download of infected files from Cloud Repository

Static Analysis Pre-Execution

Known, unknown malware, zero-day, ransomware, common scripts

Prevent download of malicious files at Web Gateway with ICAP

Deep Instinct for Web Gateways

Deep Instinct for Applications

Prevent upload/download of infected files from Applications

Deep Instinct for Endpoint

Deep Instinct for Endpoint provides end-to-end, multilayered security. The moment an attacker attempts to land a malicious payload on their target endpoint, Deep Instinct prevents it – before it executes

Pre-execution: Static Analysis

Prevent >99% of known and unknown malware, including ransomware, zero-day, filed-based, and script-based attacks with Deep Instinct's static analysis engine.

- Known malware
- Unknown malware & variants
- File-based attacks
- Zero-Day
- Ransomware
- Common Scripts

On-execution: Dynamic and Behavioral Analysis

Using a multi-layered approach to prevention, Deep Instinct employs additional dynamic analysis layers to detect and automate responses to the most advanced threats, including the following:

- Fileless attacks like malicious code injection and credential theft
- Advanced scripts like unknown shellcode
- Multi-stage attacks
- Active Adversarial AI attacks

In addition, Deep Instinct provides additional context to understand the severity and tactics of a threat, including:

- Suspicious events for threat hunting
- MITRE ATT&CK mapping

Post-Execution: Automated Analysis

In the last layer of automated analysis, Deep Instinct can override prevent decisions based on reputation or policy.

All prevented events are sent to the Deep Instinct console and can be integrated with your SIEM, SOAR, EDR, or other security solutions via REST API, Syslog, or SMTP.

Deep Instinct: Beyond the Endpoint

In-transit file scanning

Deep Instinct understands that the endpoint is not your only attack vector. Malicious files can unknowingly be uploaded to your hybrid, distributed environment, or downloaded to your customers.

Deep Instinct prevents malicious files by scanning files in-transit to ensure the integrity of your local, private, and public cloud storage and your custom applications, and prevents malicious file downloads at the web gateway.

Deep Instinct for Cloud

Infected files stored in public or private clouds increase the risk of a breach upon download.

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

Deep Instinct for Applications

Your organization is at increased risk from both internal and external file uploads through your custom applications.

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

Deep Instinct for Web Gateways

Legacy AV and ICAP solutions will not stop unknown threats at the web gateway.

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 connects with the ICAP protocol to become the ICAP server and uses our deep learning static engine to catch >99% of both known and unknown malware.

DATASHEET

deep instinct™

Deep Instinct for 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

Preventing Unknown Attacks in <20ms

Today's adversaries have time on their side—you don't.

From the moment malware executes on the endpoint, it's a race against time to stop it. Traditional security solutions struggle to detect and respond quickly to unknown threats, taking minutes, hours, or even days—during which time the malware has succeeded, and your environment has been breached. Legacy AV, signature, rule, and heuristics-based tools can prevent known attacks but are largely ineffective against unknown and zero-day threats.

Deep Instinct prevents ransomware and other known, unknown, zero-day threats in <20ms – before an attack can execute on the endpoint.

With a lightweight, agent-based solution, Deep Instinct for Endpoint prevents >99% of known and unknown malware, dramatically reducing false positives, improving the effectiveness of your existing security solutions, and lowering your organization's overall risk. Your security teams will spend less time responding to benign alerts and more time focusing on higher-value priorities like threat hunting, patching, and hardening your defenses.

The Deep Instinct Difference: Deep Learning vs Machine Learning

Endpoint Detection and Response (EDR) solutions rely on basic machine learning. This approach requires the attack to begin executing before it can be detected. Ransomware, for example, begins to encrypt in 15 seconds, but the average EDR solution can take minutes or hours to detect —too long to prevent a breach. By the time EDR tools detect an attack, droppers and artifacts have already installed on your network endpoints.

With multiple deep learning engines, Deep Instinct's multi-layered approach to prevention provides the highest efficacy and the fastest detection and prevention. This applies to both known and never-before-seen malware, as well as fileless, in-memory, and script-based attacks. Deep Instinct can also detect suspicious behavior to improve your threat hunting, investigation, and root-cause analysis.

Product Benefits

- Prevents known, unknown, and zero-day threats in <20ms
- Saves security teams time by dramatically reducing false positives to <0.1%
- Ensures malware does not execute on your endpoint
- Stops multi-stage, complex ransomware attacks
- Enacts layered prevention against the most complex attacks
- Protects against adversarial AI
- Does not require cloud lookup

Deep Instinct for Endpoint

The moment an attacker attempts to land a malicious payload on their target endpoint, Deep Instinct for Endpoint prevents it—before it executes.

Deep Instinct has pioneered the use of deep learning in cybersecurity to prevent known and unknown malware, zero-day exploits, ransomware, and common script-based attacks for the broadest range of file types, faster and with fewer false positives versus security tools that rely on signatures, heuristics, or basic machine learning.

Predict and Prevent: Pre-execution Static Analysis

Prevent >99% of known and unknown malware including ransomware, zero-day, file-based, and script-based attacks with Deep Instinct's static analysis engine.

- Known malware
- Unknown malware & variants
- File-based attacks
- Zero-day exploits
- Ransomware
- Common Scripts

Static Analysis File Types

- PE
- PDF
- Office
- Macro
- RTF
- SWF
- JAR
- TIFF
- Fonts
- Mach-O
- ELF
- APK
- JTD
- HWP
- LNK

Script Control Coverage

- PowerShell
- JavaScript
- VBScript
- Macros
- HTML applications (HTA files)
- rundll32

On-Execution: Dynamic and Behavioral Analysis

Using a multi-layered approach to prevention, Deep Instinct employs additional layers of dynamic and behavioral analysis to detect and automate responses to the most advanced threats, including the following:

- Fileless attacks
- Remote Code Injection (Reflective .NET, Reflective DLL)
- Known, Unknown Shellcode
- Credential Theft
- Anti-AMSI Bypass
- Credential Dumping
- Spyware, including banking trojans, keyloggers, and droppers
- Advanced scripts like unknown shellcode
- Multi-stage attacks
- Active Adversarial AI attacks

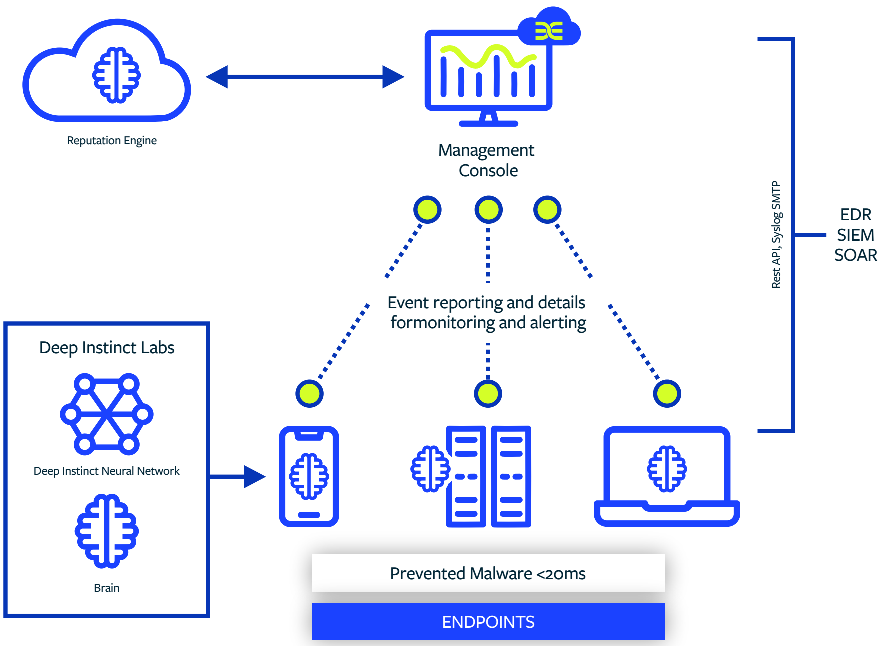
In addition, Deep Instinct provides context to understand the severity and tactics of a threat:

- Alerting on suspicious events for threat hunting
- Mapping to MITRE ATT&CK for threat context
- Conducting reputational analysis

Post-Execution: Automated Analysis

Deep Instinct includes optional automated and reputational analysis which can override decisions based on policy and imported allow lists.

Product Architecture



Automate Responses and Integrate with SIEM, EDR, SOAR

All prevented events are sent to the Deep Instinct Console and malware is instantly classified to provide context into the attempted attack. Organizations can enact a manual or automated response to achieve the following:

- Isolate the machine
- Quarantine/Delete/Restore
- Update policy: allow and restore (Hash, Certificate, Folder, Script, Process)
- Terminate the process
- Clean the registry to remove persistence
- Send prevented events to a sandbox for further analysis

Deep Instinct integrates with your SIEM, SOAR, EDR or other existing security tools via REST API, Syslog, and SMTP to improve investigation, remediation, and threat hunting.

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 can be customized to present what is most important to the authorized end user.

Built-In Reporting
Automated and ad hoc threat and trend reporting.

True Multi-Tenancy
Native multi-tenant solution for Partners, MSPs, and MSSPs keeps all data safe and isolated from cross-contamination and administers multiple environments from one, centralized console.

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.

Supported Virtual Environments

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

Supported Systems

Windows
macOs
Android
Chrome OS
Linux

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.

DATASHEET

deep instinct™

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.

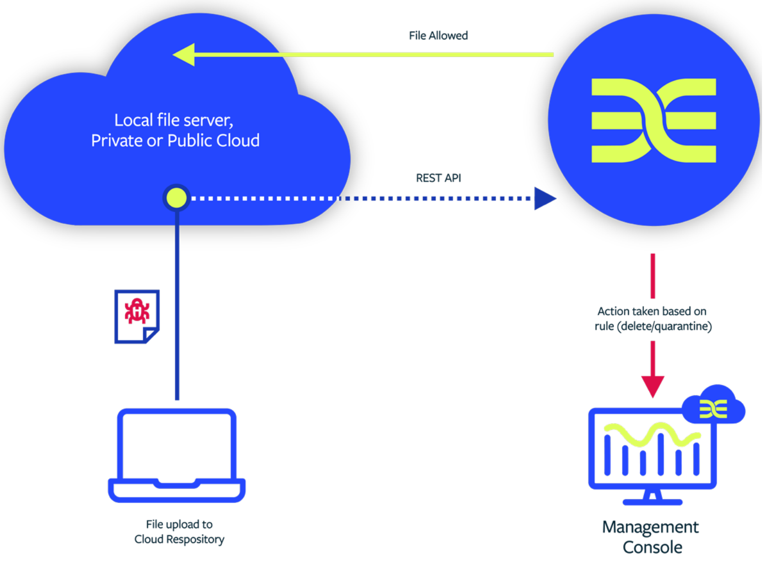
Deep Instinct prevents malicious files from uploading to, or downloading from, your public or private cloud storage.

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:

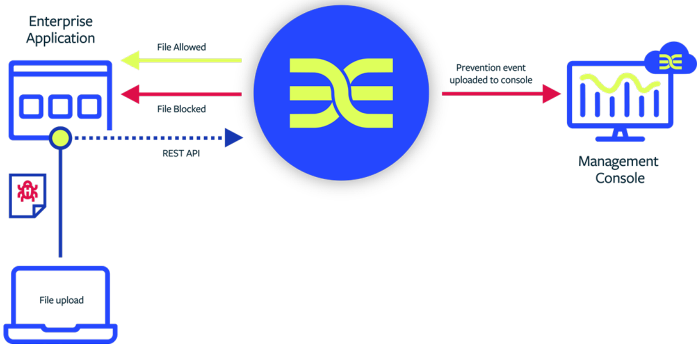
Weaponized files pose risk to users and customers

- 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:

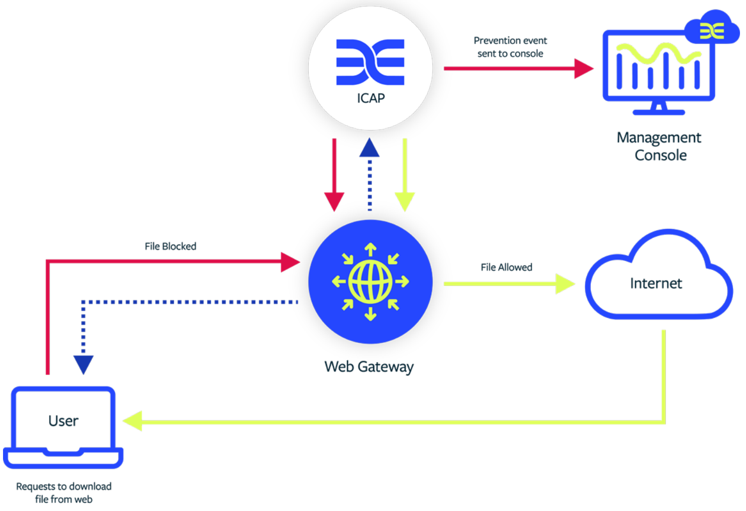
Legacy AV and ICAP solutions will not stop unknown threats

- 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.