PERCEPTION POINT

Advanced Threat Protection for Web Apps & File Uploads

The Content Security Gap of Web Apps

Content sharing and file uploads have long become a vital function in digitized organizations. It is an essential element in collaboration and productivity of the workforce as well as in conducting business and providing services. Commercial and internally developed web apps and services help organizations to easily connect with customers, partners and even unregulated online users. By allowing external content to be shared into the business environment, such channels also represent a security risk, creating an additional attack surface for malicious threat actors to target and compromise. While companies invest heavily in their network and email security architectures - web apps remain inadequately protected and a security blindspot.

An evasive malware is embedded within a CV document and meant to reach Gina, the company's HR recruiter. When sent to gina.hr@your.company.com your advanced email security solution may be able to detect it on time but what happens if the resume gets uploaded directly to a "careers" portal or sent via the chat bot on your website?
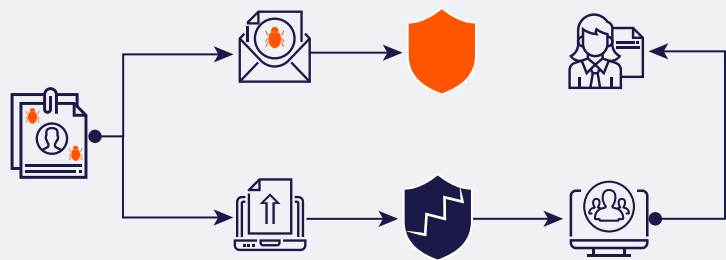
Traditional Detection is Inadequate

Single antivirus engines may be quick to verdict and can handle large scopes of uploads, but they do not provide sufficient detection against evasive or unknown threats. Additionally, solutions that integrate traditional sandbox technology can be more effective against advanced attacks but their lack of scalability and added latency (minutes to verdict) make them unacceptable for most business flows. Other approaches like CDR may be a good fit for some use cases but are limited in supported file types and content usability.

It is recommended that you assess your risks and exposure to attacks and add the required protection that will serve the organization at any scale without impacting business, and regardless of the type of content shared.

A modern security solution is required.

Perception Point: Intercept Any Threat While Keeping Business as Usual

Perception Point's cloud-native solution is designed to hermetically secure any business flow that involves external file-streams or user-generated content; protecting against phishing, malware, ransomware, advanced persistent threats, zero-day exploit attempts and more.

The award-winning platform employs multi-layered advanced threat detection algorithms that identify even the most evasive attacks. Every piece of content gets inspected through all of the detection layers, including a next-gen sandbox that dynamically scans 100% of the traffic (including embedded files and URLs) on your web apps in seconds to prevent malicious content from infiltrating the organization.

Unprecedented protection
Prevent the transmission of any malicious file, URL or social-engineering attack with >99.95% proven detection rates

Rapid Deployment
Deploy in minutes on any content source or web application

Unmatched Speed
Dynamically scan 100% of the traffic in seconds

Privacy & Compliance
Comply with all data regulations: GDPR, HIPAA, and SOC-2 TYPE II

Unlimited Scale
Analyze millions of files with no latency; with integrated fail-safe mechanisms

Managed Incident Response
Save resources with an all-included IR team, a 24/7 force multiplier to any SOC

Secure Any Content-Sharing Flow

Web portals for external users, customer support forums, partner management interfaces, job application forms, chat apps and 3rd party content sharing solutions, are just some examples of the tools your company may use to effectively communicate and collaborate with users outside of the organization.

IN-HOUSE APPS	THIRD PARTY SOLUTIONS (ICAP SUPPORTED)	
	Security Appliances	Commercial Apps
Uploads to SaaS solutions	WAF	SAP, MICRO FOCUS
Support channels	CASB	Akamai, citrix
Customer/vendor interfaces	Gateways	Kiteworks, ISILON SYSTEMS
Ad-hoc collaboration tools	Web proxies	ORACLE
Forums		
Chat applications		
Claims portals		

Deploy in Minutes with Any Web App

Perception Point easily integrates with any web app or security proxy via REST API or ICAP deployment to boost your security posture and provide best in market threat detection for any content shared to your corporate environment.

REST API

Using REST API calls to ensure maximal scalability and availability, shared content on your web applications gets submitted to Perception Point for deep forensics and analysis.

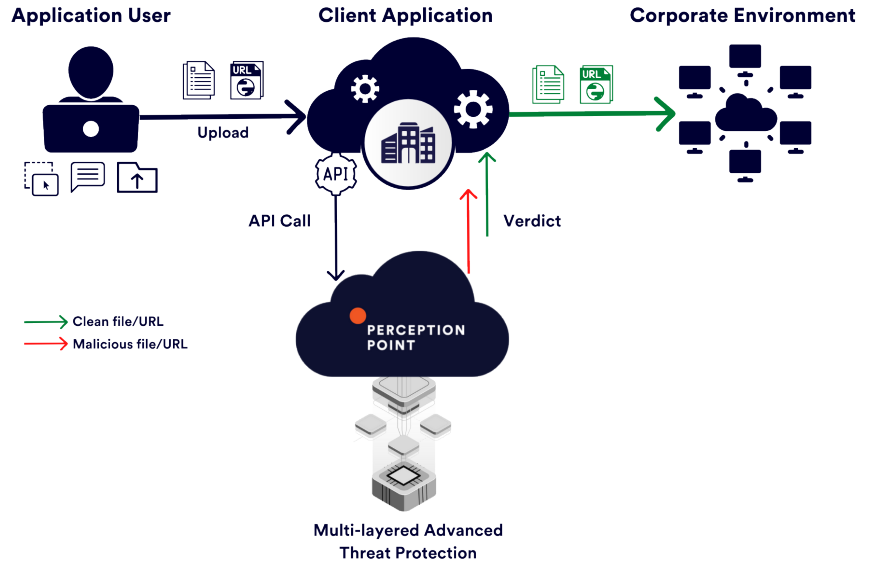Within seconds, Perception Point provides a clean or malicious verdict to the client application, which in turn, removes any malicious content.

Application User **Client Application** **Corporate Environment**

Upload

API Call

Verdict

→ Clean file/URL
→ Malicious file/URL

API

PERCEPTION POINT

Multi-layered Advanced Threat Protection

ICAP

Perception Point can seamlessly connect with any application or infrastructure that supports the Internet Content Adaptation Protocol (ICAP) and employ multi-layered detection. The integration is performed via a simple installation of Perception Point's ICAP Connector in the customer environment.

In addition, the ICAP protocol allows organizations to leverage their investment in existing proxy solutions like CASB or WAF and to easily add advanced threat protection on top of them.

Content Source **ICAP Supported Product** **Corporate Environment**

ICAP Connector

Request

Response

→ Clean file
→ Malicious file

PERCEPTION POINT

Multi-layered Advanced Threat Protection
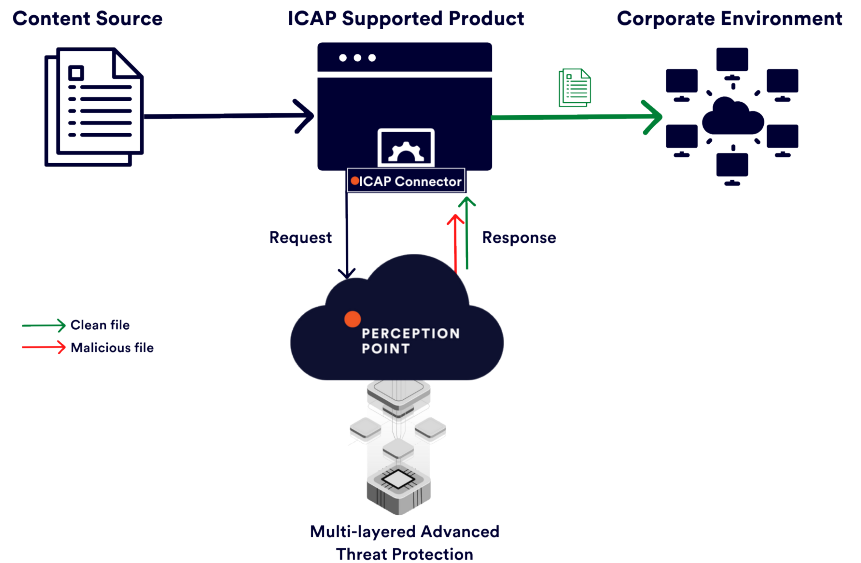
Unprecedented, Award-winning Advanced Threat Detection

Perception Point is a pioneer in advanced threat detection and has been rated #1 in independent lab testing for its detection capabilities time and time again. The different engines leverage state of the art detection algorithms using computer vision, machine learning, and various dynamic and static methods to intercept every type of threat, ranging from commodity attacks to unknown, advanced threats.
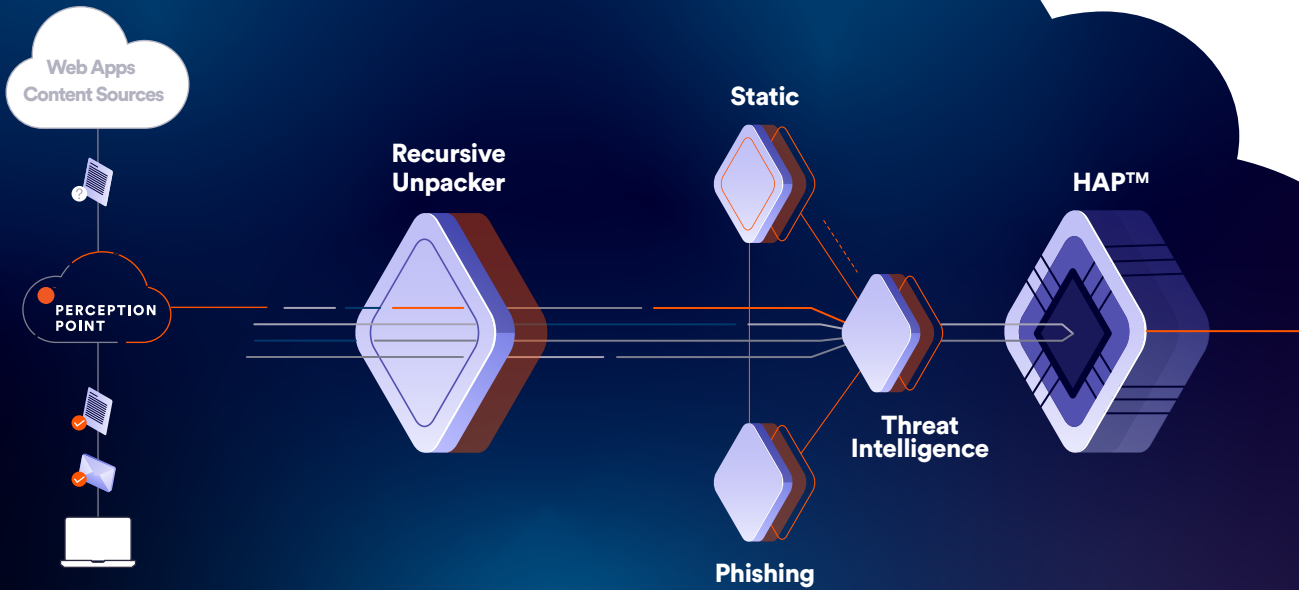
1

Recursive Unpacker

Unpacks content into smaller units (files and URLs) to identify embedded malicious attacks. All of the recursively extracted components then go individually through the next detection layers.

2

Static Signatures

Combines industry's best antivirus engines to identify malicious attacks together with proprietary technology for detection of highly complex signatures.

3

Anti-Phishing Engines

Integrates novel AI algorithms such as image recognition and lexical analysis with best-in-class reputation engines.

4

Threat Intelligence

Combines multiple threat intelligence sources with a homegrown engine that scans URLs and files "in the wild" to learn about current and potential attacks.

7

HAP™

Next-gen patented sandbox engine that is composed of software algorithms using CPU-level data to access the entire execution flow, right from the processor, to deterministically intercept any type of unknown or evasive attack on both Windows and macOS environments.

This proprietary layer provides unprecedented detection against malicious code execution in scripts and executables, zero-day and N-day vulnerabilities, logical bugs, next-gen exploitations and more.

About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation isolation, detection, and remediation of all threats across an organization's main attack vectors - email, web browsers, and cloud collaboration apps. The solution's natively integrated and fully managed incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights; providing proven best protection for all organizations.

Deployed in minutes, with no change to the enterprise's infrastructure, the patented, cloud-native and easy-to-use service replaces cumbersome legacy systems to prevent phishing, BEC, spam, malware, zero-days, ATO, and other advanced attacks well before they reach end-users. Fortune 500 enterprises and organizations across the globe are preventing attacks across their email, web browsers and cloud collaboration channels with Perception Point.

To learn more about Perception Point, visit our website, or follow us on LinkedIn, Facebook, and Twitter.

Visit us: www.perception-point.io
Contact us: info@perception-point.io

PERCEPTION
POINT