

Prevention Starts with Perception

Unparalleled prevention of all attacks across email, web browsers and cloud collaboration apps

Perception Point is on a mission to protect all organizations by isolating, detecting and remediating any cyber threat that is delivered via text, files and URLs, across email, web browsers, cloud apps and collaboration channels.



Perception Point's solution met all required KPIs in only 1 week. They prevented almost 2 dozen attacks in no time, saving the company severe potential damages. They also didn't affect the user experience as promised in the first pitch.

(CISO, Fortune 500 company)

Gartner

Recognized as a Representative Vendor
in 2021 Gartner Market Guide
for Email Security for 3rd Year in a Row*

SE Labs

#1 in Independent
Detection Testing



Patented Dynamic
Scanning Technology

Why Perception Point?

UNMATCHED PROTECTION AT THE SPEED OF YOUR BUSINESS

Perception Point's SaaS solution is powered by patented detection engines and provides a detection rate of more than 99.95%. Dynamically scanning 100% of content, including embedded files and URLs in just seconds, it eliminates your security blind spots for the best protection of your organization.

COST REDUCTION, SIMPLIFIED MANAGEMENT AND RAPID REMEDIATION WITH A FREE OF CHARGE INCIDENT RESPONSE SERVICE

An all-included Incident Response service combines machine learning, automated processes, and close engagement with our cybersecurity experts, so that every incident is analyzed and managed efficiently. The service is an extension to your SOC team and ensures continuous optimization of the system's detection rates and rapid remediation across all channels. Your management overhead is reduced and you can save up to 75% of your SOC time.



The Perception Point solution is easy and straightforward to deploy. It made an immediate impact on our day to day operation. I can't say enough about the team and how quickly they responded to questions, new feature requests or improvements. Any issue I faced was answered on the same day.

IT infrastructure manager, Finance

Unprecedented protection against any attack type

Outperforms all solutions in accuracy and speed

Unmatched detection speed & scale

Lowering dynamic threat analysis time from minutes into seconds

Scan 100% of traffic in real-time

Unlimited scale: scanning every piece of content, regardless of volume



Integrated incident response

All-included incident response serves as a force multiplier to the SOC team

Easy to use, intuitive solution

Simple, easy to operate management dashboard. No long manuals



One-click deployment

SaaS solution deploys in one click with existing security solutions



99.95%
Detection rate
















40X
Faster detection

∞
Scale

75%
SOC time saving

Eliminate Security Blind Spots with 360° Channel Coverage

Your organization is exposed to external and insider threats from email, web browsers and other cloud collaboration channels. Perception Point holistically protects your main attack vectors, allowing you to easily extend the same policies, consolidate and simplify security systems, and obtain a unified solution that isolates, detects and remediates all threats in the organization.

 Email	 Cloud Apps	 Web Browsers	 Proprietary Apps
 Office 365  G Suite  Exchange Any web-based email service	 OneDrive  SharePoint  box  salesforce  amazon S3  zendesk	 chrome  Microsoft Edge	<ul style="list-style-type: none"> > Inhouse built collaboration apps > File streams coming in through APIs > ICAP-based apps



Perception Point has allowed our team to feel at ease when it comes to OneDrive and SharePoint. There is no solution like Perception Point when it comes to offering true threat prevention for these channels.”

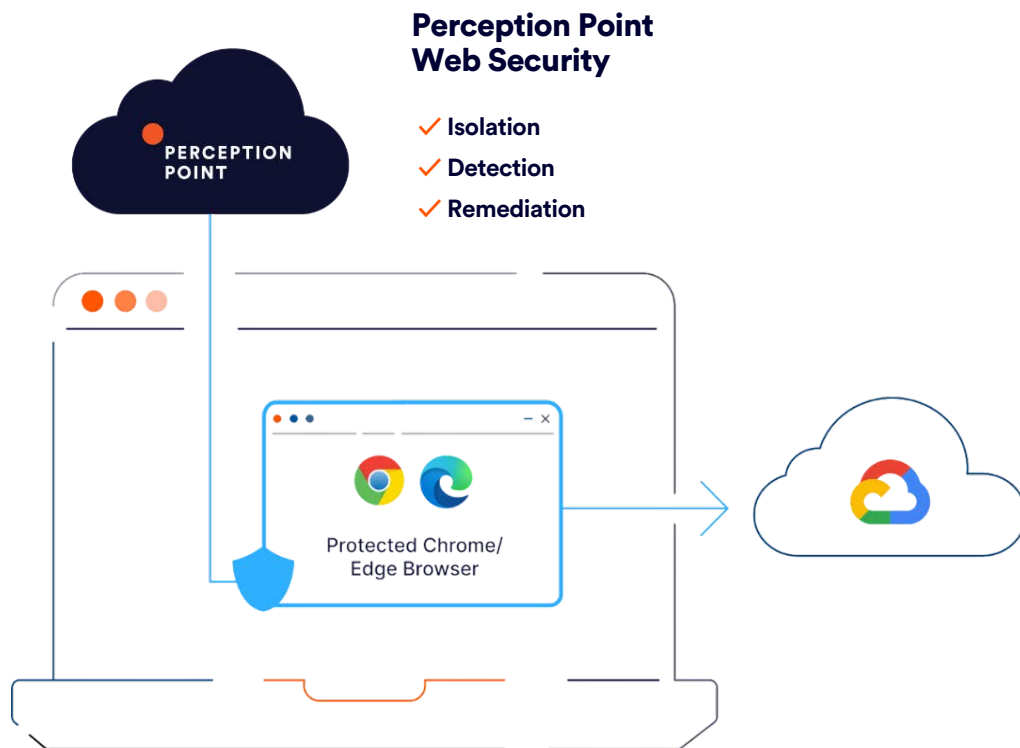
(Information Security Director, Fortune 500 company)

Selected Customers



Advanced browser-based detection and isolation lets your users access the web without exposing enterprise data to risk

Perception Point's Advanced Browser Security is easy to deploy, with a browser extension for advanced detection capabilities or a secured browser, adding VM-based isolation to Chrome/Edge on Windows or Mac. You can prevent all threats from the web and ensure enterprise apps are accessed via a trusted Chrome/Edge Enterprise browser.

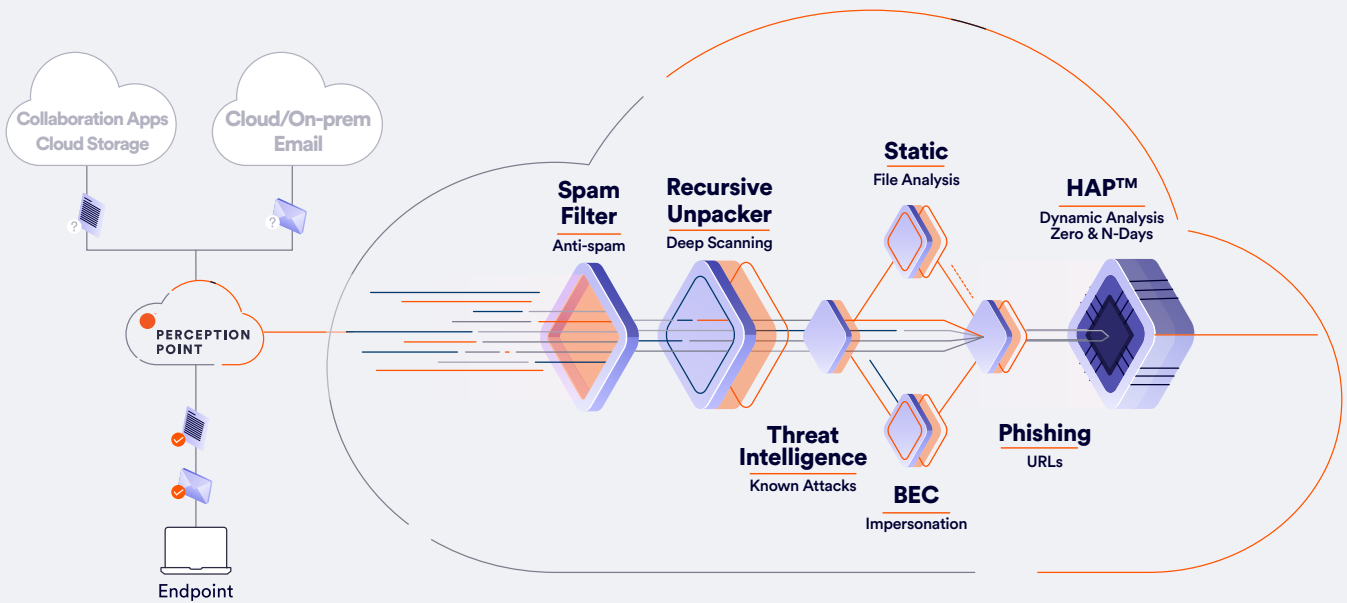


Perception Point has reinvented how organizations can isolate applications and data on users' devices and, by doing so, significantly reduce the risk on the endpoint."

Adm. Michael Rogers, Former Director of the NSA

Protect Your Organization with Unprecedented Advanced Threat Detection

Perception Point is a pioneer in advanced threat detection. Our platform recursively unpacks every piece of content and rapidly scans all text, files and URLs with multiple advanced detection engines. 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, from commodity attacks to advanced threats.



1

Spam Filter (Email Only)

Receives the email and applies reputation and anti-spam filters to quickly flag an email as malicious.

2

Recursive Unpacker

Unpacks the content into smaller units (files and URLs) to identify hidden malicious attacks, extracting embedded URLs and files recursively by unpacking files and following URLs. All of the extracted components go separately through the next security layers.

3

Threat Intelligence

Combines multiple threat intelligence sources with our internally developed engine that scans URLs and files in the wild to warn about potential or current attacks.

4

Phishing Engines

Combines best-in-class URL reputation engines and an in-house image analysis engine to identify impersonation techniques and phishing attacks.

5

Static Signatures

Combines best-in-class signature based antivirus engines together with proprietary technology to identify highly complicated signatures.

6

BEC

Prevention of payload-less attacks that don't necessarily include malicious files/URLs, e.g. spoofing, look-alike domain, display name deception.

7

HAPT™ (Hardware-assisted Platform)

Next-gen sandbox proprietary 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 advanced attack on both Windows and macOS environments. This layer provides unprecedented detection against malicious code execution in scripts and executable files, zero-day and N-day vulnerabilities, logical bugs, next-gen exploitations, ATO and more.