PERCEPTION POINT

Advanced Email Security.

Cutting edge threat prevention for the modern enterprise

Highlights.

Real-time prevention
Block malicious content before it ever reaches the end user.

X-ray visibility
"X-ray" any code executed by the system for 100% visibility into malicious intent.

Deep scanning
Unpack files and follow RULs to detect evasive malicious intent.

Zero delay
In-line engines work in a matter of seconds. Up to 40x faster than sandboxes.

One-click deployment
Easy and fast deployment on the cloud. No change to existing processes.

Unlimited scale
Scan 100% of email traffic, regardless of volume.

Email services
Office 365, Gmail, any cloud email service, Exchange.

Privacy & compliance
SOC2 compliant. No data stored on servers.

24/7 Threat response
Expert intelligence team continuously monitoring incidents.

Contact Us

www.perception-point.io
info@perception-point.io

We're in
Boston | Tel Aviv

The Urgent Need For Next Gen Email Security.

Email is the source of 91% of targeted attacks and despite there being many exsiting email solutions, most companies remain highly exposed. On one hand, sophisticated hackers are continuously innovating and can now evade even the latest sandbox technologies.
On the other, multiple deployments have resulted in a chaos of solutions driving increased costs, complexity, and delays. There is an urgent need for next gen technology that is far more effective against the full threat landscape, while also being aligned to the modern cloud-driven enterprise.

OUR SOLUTION:

Faster Interception + Holistic Protection.

Our Advanced Email Security combines cutting edge threat prevention with the speed, scale and flexibility of the cloud. We've built in multiple scanning engines and threat intelligence for enhanced protection against known attacks like phishing, spam and commodity malware.
For advanced threats, **we've invented the first technology to combine hardware visibility with software agility** to see what leading solutions miss. Propriety software algorithms x-ray code at the CPU-level to intercept attacks at the earliest stage possible - the exploit - before malware is even delivered.

Our cyber security as a service deploys in a single click, analyzes up to 40x faster* and has limitless scale to always scan 100% of your traffic.

* ~30 seconds analysis time vs. 7-20 minutes by leading sandboxes

Zero Day, N-day, & Everyday Threat Coverage.

Our platform protects your business from the full range of attacks contained in any file or URL. Coverage includes:

Everyday Threats	N-day Threats	Zero-day Threats
Signature-based attacks	Masked attacks & unpatched software	Unknown vulnerabilities
Spam, Phishing, commodity malware	Exploits leveraging known vulnerabilities. Altered signatures prevents detection.	Exploits leveraging unknown vulnerabilities in Office, Adobe and browsers.

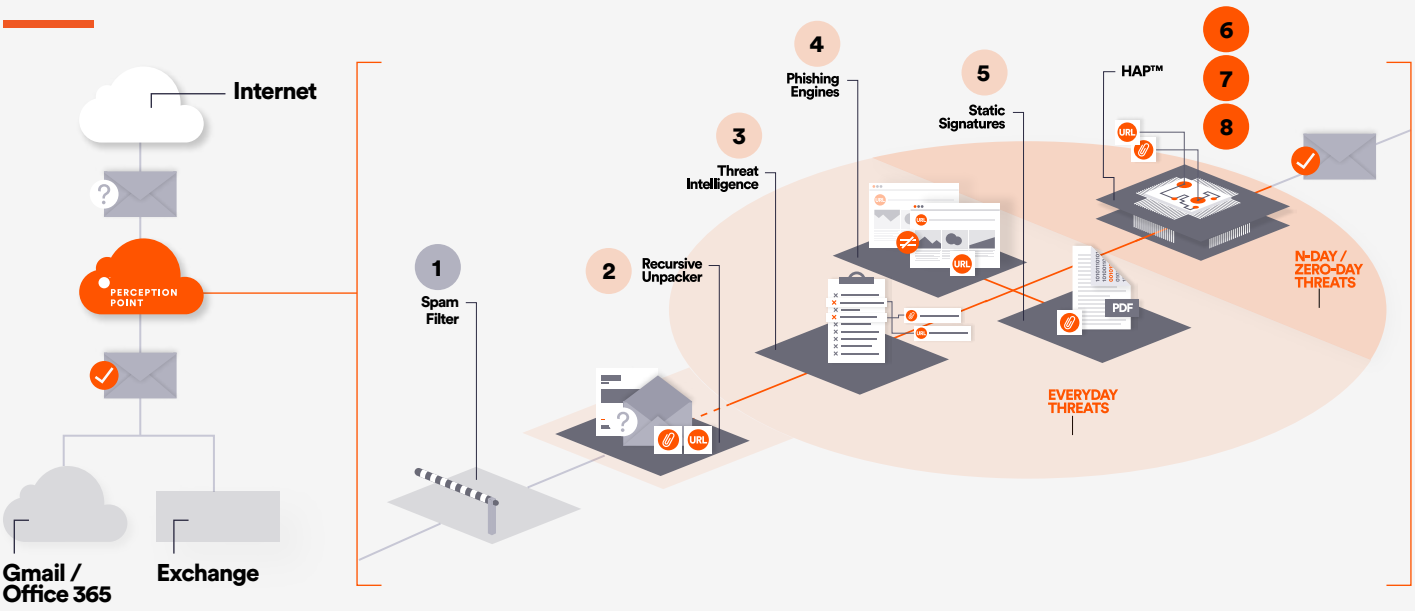
Customer Quote

> *"Integrating Perception Point's platform into our Office365 was quick and seamless with absolutely no impact to our email service levels.* ***In less than a month they've already blocked a potentially damaging attack*** *that could have easily tricked our users and caused a serious disruption. It's rare that I see immediate returns that quickly."*

CISO, Healthcare

Inherent Layered Solution

Enhanced standard layers + cutting-edge APT protection
for the most high-performance defense on the market.



EVERYDAY THREATS | Phishing, Commodity malware, Spam, etc:

1

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

2

Recursive Unpacker.
Unpacks the email into smaller units (files and URLs) to identify hidden malicious attacks. Further extracts embedded URLs and files (recursively) by unpacking files and following URLs. All of the extracted components go separately through the next layers.

3

Threat Intelligence.
Combines multiple threat intelligence sources with our internally devloped 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 anti-virus engines to identify malicious attacks. In addition, we've developed a tool that acts to identify highly complicated signatures.

N-DAY/ ZERO-DAY THREATS

First Hardware-Assisted Platform (HAP™)

Unique CPU-level technology acts earlier in the kill chain than any other solution. Blocking attacks at the exploit phase - pre-malware release - for true APT prevention.

6

HAP™ (Dropper).
Employs advanced heuristics-based engine for detecting logical bugs and handling macros and scripts.

7

HAP™ (CFG).
Records the CPU while it processes the input (files and URLs) and identifies exploits by examining the entire execution flow - detecting any deviation from the normal flow of a program in order to deterministically identify malicious activity.

8

HAP™ (FFG).
Detects advanced techniques such as exploits that are written to bypass common CFI algorithms. Proprietary semantic aware control flow graphs developed for each application identify deviations of the execution flow during runtime.

Free & easy 30-day trial

just contact sales@perception-point.io

PERCEPTION POINT