PERCEPTION POINT

Advanced Internal Email Security

Preventing any type of email-borne threat, even from within your organization

Highlights.

360-degree Email Security
Complete your email security suite to protect against internal email threats.

Static & Dynamic Scans
7 different layers work together to ensure no malicious email slips by.

Near-zero delay
Active scanning of internal email without causing delays to your ongoing operations.

Scale agnostic
Scanning 100% of traffic. No shortcuts.

One-click deployment
Deployed quickly. No IT fuss or overhead.

Privacy & Compliance
SOC-2 compliant. No data stored on servers.

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

Internal Email Scanning – Why it's a Must

By 2023, 65% of organizations will scan internal traffic for advanced threats*. Contrary to popular belief, the days when email-borne threats stem only from external parties are long gone. As attackers become more and more sophisticated, they are implementing more innovative ways to cause damage. One of their newer and more successful methods is by gaining authenticated access to a real employee's email account and operating freely from within the organization.

Once an attacker is inside, he can do almost anything – spread malware through the organization, encourage employees to give away credentials via phishing links, or even directly target the financial department to wire transfer money.

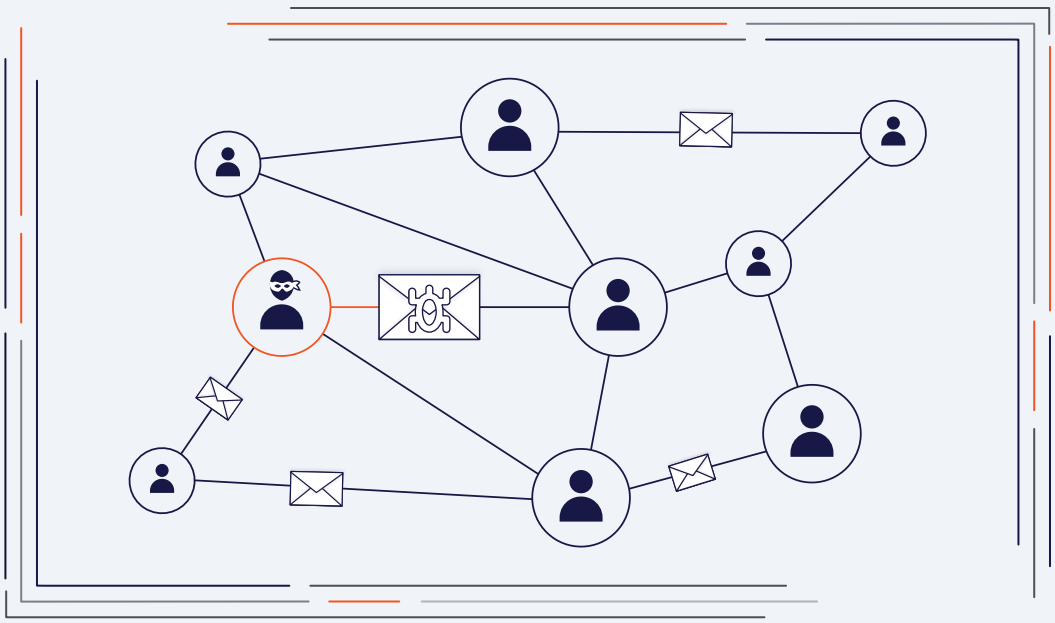
It's now clear that preventing only external email-borne attacks is simply not enough. Internal security must be enhanced by deploying advanced solutions that prevent Account Take Overs (ATO) and lateral phishing attempts.

OUR SOLUTION:

Scanning Intradomain Email Traffic for Maximum Security

Perception Point's Internal Email Security delivers the best protection against any type of intradomain threats – files, URLs and text-based attacks. Our layered solution combines multiple engines that work together to intercept spam, phishing, malware, BEC-based or highly advanced attacks.

Cloud-native solution coupled with ultrafast algorithms ensure threat prevention in real-time with near zero delay in email traffic. No scale limits, no impact on user experience.



*Gartner 2019 Email Security Market Guide.

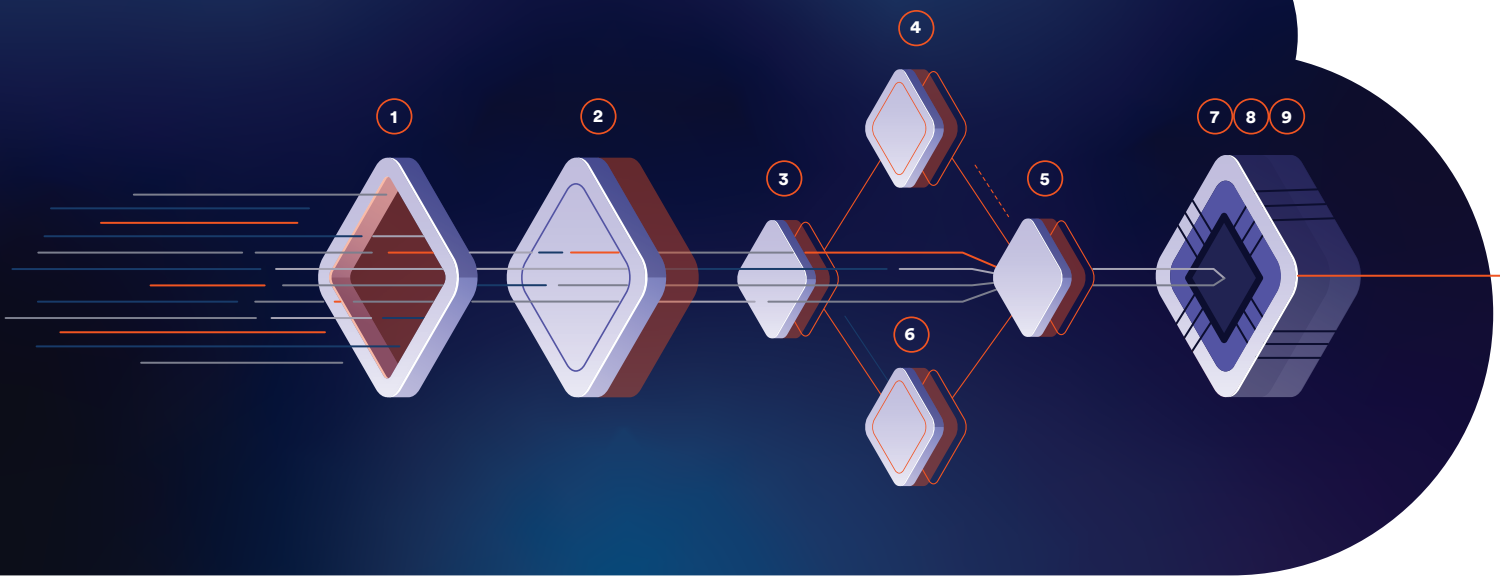
Contact Us

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

We're in
Boston | Tel Aviv

Inherent Layered Solution

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



Everyday Threats | Phishing, Malware, Impersonation, BEC, etc.

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. Further extracts 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 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.

6

BEC

Prevention of payload-less attacks including spoofing, look-alike domain and display name deception.

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.

7

HAP™ (Dropper).

Employs advanced heuristics-based engine for detecting logical bugs and handling macros and scripts.

8

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.

9

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.