

# Perception Point vs FireEye

Perception Point’s multi-layered email protection is the most robust against every type of threat, including zero days, n-days, new evasion techniques, phishing, commodity malware and more. While the comparison below is for the email channel, our solution can also be easily deployed across shared drives, messaging and any channel where content is exchanged.

## CLIENT USECASE

### Software Industry

+750 USERS

Perception Point’s Advanced Email Security solution was deployed in a medium sized software enterprise. The client is hosted on G Suite and is also using FireEye email protection. The main reasons for testing Perception Point’s offering were: (i) the discontent from the existing detection rate; and (ii) the lengthy delays in email transfer, which led to deteriorating end-user experience. By processing the same data via both FireEye and Perception Point, the client was able to easily compare the performance and detection of each vendor.

## MAIL FLOW



## Key Findings & Results

Since deployed, several different types of attacks and a significant amount of spam were missed by FireEye. Moreover, the delivery time to the end user, was cut dramatically.

Malicious Incidents	<b>+150</b>	Total Spam	<b>+18,000</b>	Email Traffic Scanned	<b>100%</b>
---------------------	-------------	------------	----------------	-----------------------	-------------

## Types Missed

- Impersonation Attacks (BEC)
- Known / Unknown Malware
- Advanced Persistent Threats
- Phishing

# Why FireEye Missed

## Visibility

No visibility at the hardware level allowing for obfuscated exploits.

## Long Delays

Leading to some clients using the solution only in detection mode.

## Embedded Content

Lacked ability to uncover malicious files and links embedded in clean files.

## Phishing

Several misses on basic phishing attacks due to only the use of Threat Intelligence.

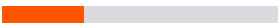















## Verdicts

Provided indecisive verdicts requiring admins to manually transfer to sandbox.

## Scale

No ability to scan 100% of traffic which leads to misses of key incidents.

## Feature Comparison

Feature	FireEye	Perception Point
Advanced Threat Module	Sandbox	<b>The HAP™</b>
Level of Visibility	Application	<b>CPU</b>
Scan Speed	~5-20 Minutes	<b>&lt; 30 Seconds</b>
Ability to Unpack Embedded Files & Urls	✗ No	✓ Yes
Method of Analysis	Statistic (Behavioral)	<b>Deterministic</b>
APT Module Capacity		
Spam / Threat Intelligence		
Phishing		
Malicious Scripts (e.g Word Macro)		
Logical Bugs in Apps		
Zero Day & Fudged N-days		
Anti-evasion Techniques		
Real-time Browser Scanning		
Next-gen Exploitation (e.g COOP)	