

Perception Point vs Barracuda

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

Automotive Industry

PERIOD:

3 Weeks
300 Users

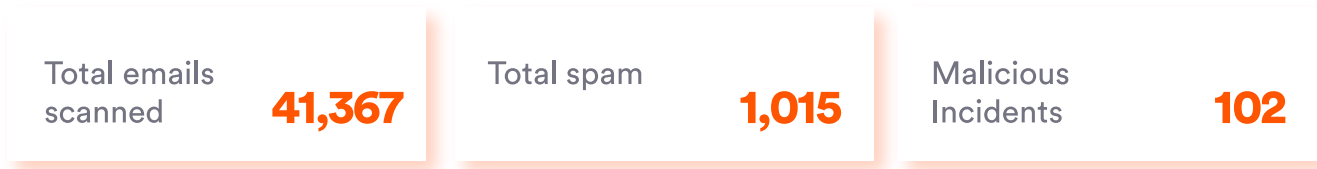
Perception Point’s Advanced Email Protection was installed in a medium sized automotive enterprise. They are hosted on Office365 and are also using Barracuda email protection. The main goal is to see what threats are currently bypassing their existing security infrastructure. Being positioned in the email-flow after Barracuda, Perception Point is then only receiving mail that has already been given a “CLEAN” verdict by Barracuda.

MAIL FLOW:



Key Findings

Over the course of three weeks, several different types of attacks and a significant amount of spam were missed by Barracuda.



Types Missed

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

Why Barracuda 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.

Feature Comparison

Feature	Barracuda	Perception Point
Advanced Threat Module	Sandbox	The HAP™
Level of Visibility	Application	CPU
Scan Speed	~5-20 Minutes	< 30 Seconds
Ability to Unpack Embedded Files & Urls	✗ No	✓ Yes
Method of Analysis	Statistic (Behavioral)	Deterministic
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)		