PERCEPTION POINT

ADVANCED EMAIL PROTECTION

Perception Point vs Proofpoint.

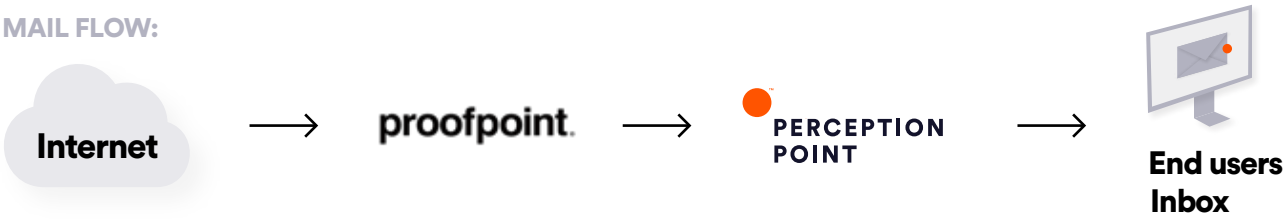
Perception Point's multi-layered email protection is the most robust against every type of threat, including Zero days, N-days, new evasion techniques, phishing, commodity malware and more. While the comparison below is for the email channel, our solution can also be easily deployed across shared drives,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

CLIENT USE CASE

Financial Institution.

Perception Point's Advanced Email Protection was installed in a medium-sized financial institution. They are hosted on Office 365 and are also using Proofpoint. The main goal is to see what threats are currently bypassing their security. Being positioned in the email-flow after Proofpoint, Perception Point is then only receiving mail that had already been given a "CLEAN" verdict.

MAIL FLOW:



Key Findings.

Over the course of one week, several attacks and a significant amount of spam were missed by Proofpoint.

Missed attacks: LODA MALWARE | CVE-2017-0199 | CVE-2017-8759 | EMOTET MALWARE

LODA MALWARE ANALYSIS:

Malicious File Name
Payment receipt.**docx**

Type of Attack
Advanced Persistent Threat **(APT)**

Detection Engines

Analysis

- An attempt to evade AVs by using several advanced techniques.
- An attempt to run Loda malware in the form of an executable file.
- An attempt to steal personal data, such as usernames and passwords.
- Collect system information such as process name and system information

Recursive Unpacker	Threat Intelligence	Phishing Engines	Static Signatures	**HAP™ Dropper**	HAP™ CFG	HAP™ FFG

How Perception Point stopped the attack:
Perception Point's "Unpacker" engine was used to unpack the email into smaller units (files and URLs) to identify hidden malicious attacks. Subsequently Perception Point's Dropper algorithm then picked the attack. The Dropper detects logical bugs in applications and malicious scripts (e.g. macros) in office documents. Unique heuristic engine that scans the execution flow for prohibited code paths (CPU Level data).

Why Proofpoint missed:

Visibility
No visibility at the hardware level allowing for obfuscated exploits.

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

Verdicts
Provided indecisive verdicts requiring admins to manually transfer to sandbox.

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

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

Feature Comparison.

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