ADVANCED EMAIL PROTECTION

Perception Point vs Mimecast.

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.

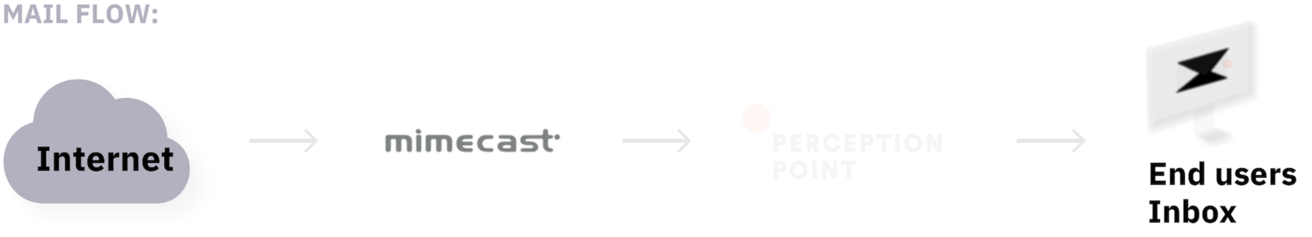
CLIENT USE CASE

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 Mimecast. The main goal is to see what threats are currently bypassing their security. Being positioned in the email-flow after Mimecast, Perception Point is then only receiving mail that had already been given a "CLEAN" verdict.

PERIOD: **1 Week. 150 Mail Boxes.**

MAIL FLOW:



Key Findings.

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

Total emails scanned	80,048
Spam	619
Malicious Incidents	21

Types Missed:

Phishing

Known / Unknown malware

Hidden embedded malicious links / fil

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

Why Mimecast 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	Mimecast	Perception Point
Advanced Threat Module	Sandbox	**The HAP™**
Level of Visibility	Application	**CPU**
Sandbox Scan Speed	~5-20 Minutes	**< 30 Seconds**
Ability to Unpack Embeded 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 & Fudded N-days	⬛⬛⬛⬛	🟧🟧🟧🟧
Anti-evasion Techniques	🟧⬛⬛⬛	🟧🟧🟧🟧
Real-time Browser Scanning	⬛⬛⬛⬛	🟧🟧🟧🟧
Next-gen Exploitation (e.g COOP)	⬛⬛⬛⬛	🟧🟧🟧🟧