PERCEPTION POINT

Case Study: Augmenting Microsoft Defender

Global Multinational Chemical Company Deploys Advanced Email Security in a Microsoft 365 environment for employees in 80 Countries.

The Company.

Our client is a leading global industrial gases and engineering company, with over $30 billion sales. The company serves a variety of end markets including chemicals & refining, food & beverage, electronics, healthcare, manufacturing and primary metals. It provides high-quality solutions, technologies and services which are making their customers more successful and helping to sustain and protect the planet.

Challenges.

- Better protection: Advanced threat protection service was required to provide additional layers of security to augment Microsoft 365 security solutions.
- Easy integration and reduced risk: A gradual deployment process across the organization required customization.
- Scalability: Seamless expansion to absorb an additional 60,000 users, demanding a scalable cloud-native solution.

Solution.

The customer required a modern Integrated Cloud Email Security (ICES) solution that could deploy on top of Microsoft Defender and deployed Perception Point's Advanced Email Security.

Results.

57,000 users in 5 regions are leveraging the Perception Point platform to intercept all content-borne threats.
Over a four month period, Perception Point:

- Intercepted over 137,000 malicious attacks.
- Blocked over 4,260,000 spam emails.
- Scanned clean emails at an average of < 10 seconds.

Contact Us

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

We're in
Boston | Tel Aviv

Challenge:

The client is a large global company with over 57,000 users across different geographic sites. The client functions within a complex environment that poses many challenges when integrating additional security platforms. The substantial escalation of targeted cyber attacks on large scale companies made the implementation of an advanced security solution vital. The objective was clear: the client required an advanced cybersecurity solution that did not compromise performance. The client faced the following challenges:

- The client utilized a complicated Microsoft 365 environment which consisted of many rules and settings across the organization. Therefore, the client required a flexible security system that could adjust itself accordingly.
- The client's size and large number of users posed a challenge for integrating with legacy non-cloud-native platforms. The client's users were located in several regions, each with different settings and needs. Further, the client required a gradual deployment process that would not affect its users' performance or work environment.

Solutions:

- Perception Point provided a gradual and comprehensive deployment process that included a full support team with thorough understanding of office 365 settings. Our Incident Response and Customer Support teams were available around the clock to review and manage incidents, provide technical support, answer questions and resolve any issues that arose during the deployment and after.
- Perception Point provided a flexible integration process that was divided into different regions and settings. The deployment was expanded to different regions in a gradual process, while implementing different settings according to each region's needs.
- The adaptability of the Perception Point cloud-native platform allowed easy accommodation of the customer's requirements and scaling needs.
- Real time dynamic scanning of all content provided best protection without compromising performance time.

> **The most valuable features of the solution are the ones that are related to finding impersonation attacks and detecting attempts to steal credentials. In scenarios where attackers get you to follow URLs to a malicious site that looks similar to a good site, and then ask for the user credentials to try to steal them, it is very useful. It also has features for detecting branding impersonation…And specifically, when it comes to protecting our VIPs and avoiding BEC (business email compromise) attacks, that is another important part for us…It scans pretty much all content, so it's full-scale. We see in our dashboard how emails are categorized by different engines. There isn't just one engine that determines whether an email is malicious. They have a multi-engine architecture for detection of malicious emails. They provide full scanning of email.**
>
> *Director of Office365 Services*

PERCEPTION POINT

Results:

Over a 4-month period, Perception Point's security system scanned millions of files and URLs. Since then, the system has successfully blocked thousands of malicious attacks and reduced the amount of spam being sent to its employees.

Traffic:

33,105,895
Total emails scanned

91,058,966
Total artifacts scanned

0.4x
Embedded files/mail ratio

1.3x
Embedded URLs/mail ratio

Events:

>137k
Attacks prevented

4.3M
Spam blocked

94k
Most prevalent attack: Phishing

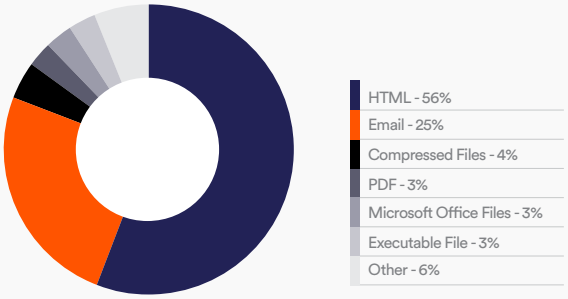
1,239
Number of advanced attacks blocked by HAP

Performance:

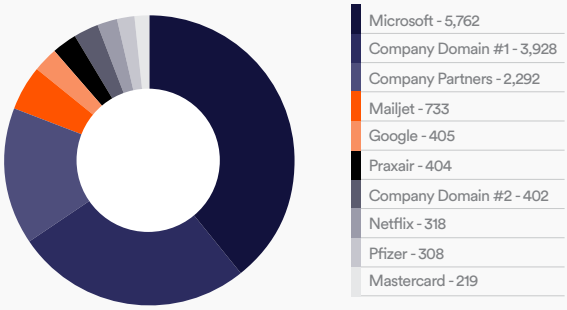
Avg. scan time for clean content: 10 seconds; 75% of content is scanned within 12 seconds

100% of content scanned dynamically

Malware Catches:



Brand Impersonation:



As can be seen above, one of the most frequent impersonations we have seen was of the Microsoft brand. As our client uses Office365, preventing phishing attempts of this sort is critical.

Summary:

Perception Point is pleased to be able to contribute to our client's advanced security protection stack. Agile deployment along with the existing Microsoft Defender, is preventing the most advanced email security attacks including phishing, BEC, ATO and zero-days before they reach the users' inboxes. Combining best protection with multi-layer advanced detection, integrated IR services and an innovative security approach, Perception Point delivers the ultimate security solution for contact-borne attacks.