PERCEPTION POINT

Advanced Threat Protection for Microsoft Teams

Next-gen threat-prevention of content-based attacks leveraging Microsoft Teams

Collaboration and remote working apps are exposed to cyber threats

The new swift and dramatic change to remote working has boosted the ongoing trend in adoption of new collaboration applications, such as Microsoft Teams. These collaboration apps offer internal and external chats, file sharing, video meeting, and more. However, this change comes with a hefty price of poorer cyber security:

- **Misconception of security –** Collaboration apps are wrongfully considered safe, even though the same attacks that are used on Email, are also used through these apps.
- **Rapid adoption –** 2020 already sees 44M daily active users on MS Teams. IT teams decided to adopt Microsoft Teams in no time, leading to no clear policies or appropriate security measures taking place after a structured process.
- **Attackers capabilities –** attackers always look for the lowest hanging fruits. They don't want to work hard unless they have to. With so many layers of detection in email, and the huge adoption of collaboration application it is the new perfect way in for an attacker.

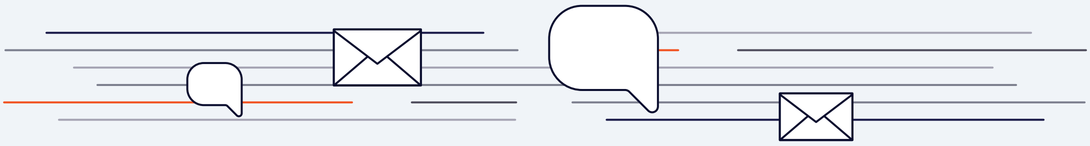
> **Like water, attackers always look for the path of least resistance – they will look for the easiest path inside your organization; in these chaotic days – it's MS Teams.**

OUR SOLUTION:

Lightning-fast Interception of Any Malicious File & URL Upon Upload

Perception Point's Advanced Threat Protection for Microsoft Teams scans all files and embedded links shared via your Teams users to intercept any attempt to use it for malicious purposes.

Our prevention-as-a-service is comprised of an advanced multi-layered threat platform, with complete 360-degree Incident Response services to monitor, identify, and prevent any content-based attack, as well as alerting your cybersecurity teams. Our solution integrates seamlessly and quickly, no long deployment process or install guides and no additional IT overhead.



Highlights.

Prevention as a Service
360-degree service. No ongoing efforts from the IT Team.

Seamless User Experience
Zero effect on business performance and end users.

Zero-touch Deployment
Fast, seamless integration with the MS Team app.

24/7 Incident Response
IR Intelligence team + machine learning algorithms continuously monitoring incidents.

Holistic View
A single, consolidated view of all incidents + real-time alerts and forensics

Privacy & Compliance
SOC-2 compliant. No data stored on servers.

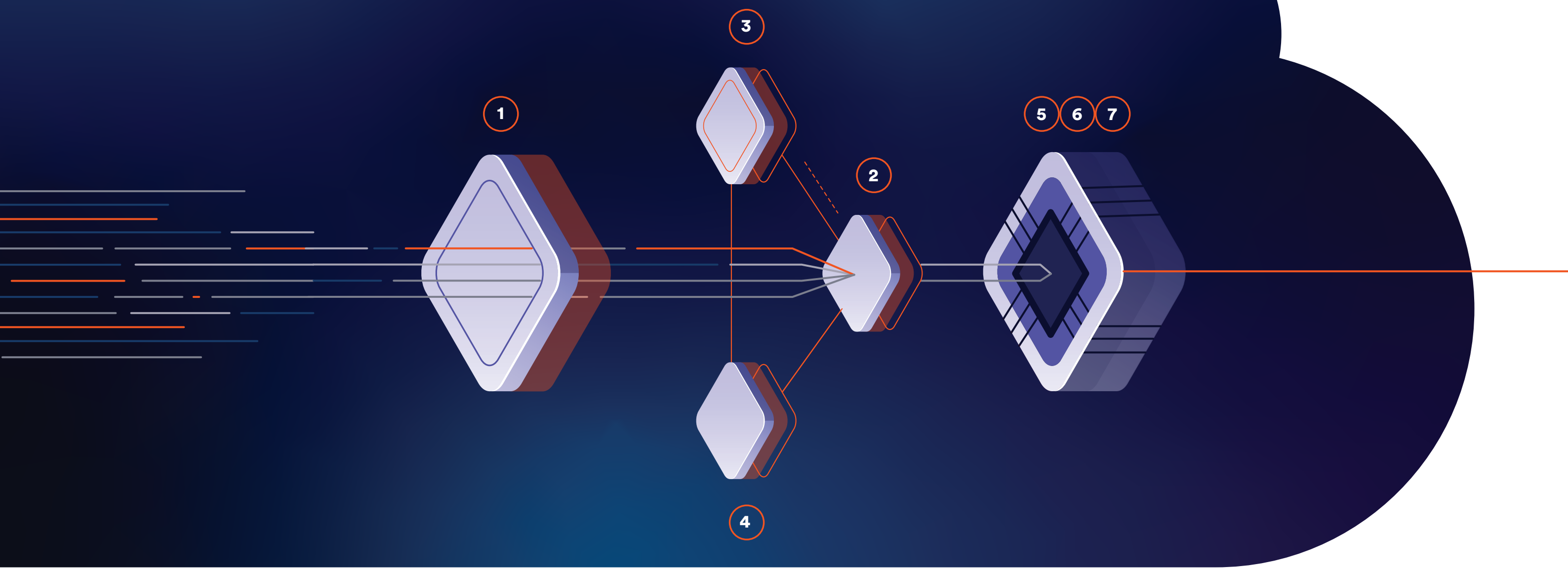
Contact Us

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

We're in
Boston | Tel Aviv

Inherent Layered Solution

Enhanced standard layers + cutting-edge APT protection for the most high-performance defense on the market.



Everyday Threats | Phishing, Malware, Impersonation, BEC, etc.

1

Recursive Unpacker.

Unpacks the content into smaller units (files and URLs) to identify hidden malicious attacks. Further extracts embedded URLs and files (recursively) by unpacking files and following URLs. All of the extracted components go separately through the next security layers.

2

Threat Intelligence.

Combines multiple threat intelligence sources with our internally devloped engine that scans URLs and files in the wild to warn about potential or current attacks.

3

Phishing Engines.

Combines best-in-class URL reputation engines and an in-house image analysis engine to identify impersonation techniques and phishing attacks.

4

Static Signatures.

Combines best-in-class signature based anti-virus engines to identify malicious attacks. In addition, we've developed a tool that acts to identify highly complicated signatures.

N-DAY/ ZERO-DAY THREATS

First Hardware-Assisted Platform (HAP™)

Unique CPU-level technology acts earlier in the kill chain than any other solution. Blocking attacks at the exploit phase - pre-malware release - for true APT prevention.

5

HAP™ (Dropper).

Employs advanced heuristics-based engine for detecting logical bugs and handling macros and scripts.

6

HAP™ (CFG).

Records the CPU while it processes the input (files and URLs) and identifies exploits by examining the entire execution flow - detecting any deviation from the normal flow of a program in order to deterministically identify malicious activity.

7

HAP™ (FFG).

Detects advanced techniques such as exploits that are written to bypass common CFI algorithms. Proprietary semantic aware control flow graphs developed for each application identify deviations of the execution flow during runtime.

Free & easy 30-day trial

just contact sales@perception-point.io

PERCEPTION POINT