PERCEPTION POINT

Advanced Salesforce Security

Next gen prevention of content-based attacks leveraging the Salesforce Customer Portal.

Highlights.

Full Content Coverage
Auto scanning of all files & URLs upon upload to Salesforce.

Seamless User Experience
Fast and easy integration without impact on end users.

Easy Install
Download and upload via Salesforce AppExchange.

Holistic View
A single, consolidated view of all scans and incidents.

One-click deployment
Easy and tfast deployment on the cloud. No change to existing processes.

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

24/7 Threat Response
Expert intelligence team continuously monitoring incidents.

The CRM Threat – When Your Customer is a Security Risk

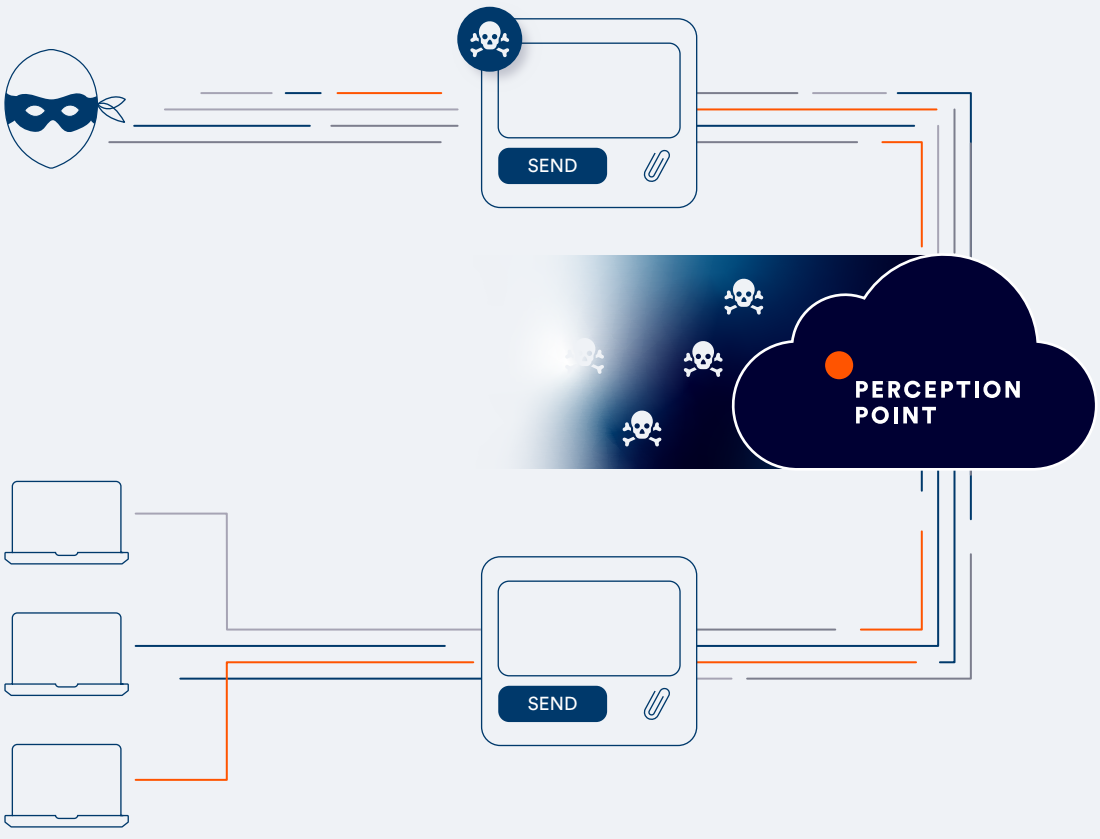
Any digital-first enterprise requires the processing of data. A lot of data. This is even more true for B2C companies which have to manage up to millions of customers at the same time. To do so they must rely on client management platforms – and foremost, Salesforce, the gold standard of CRM apps. However, this development also has created a new entry point for 21st century attackers. Relatively easily, malicious actors can disguise themselves and masquerade as "customers". Once they have gained access, the attackers can easily upload files with a malicious payload and trigger the malevolent sequence, causing severe damage to their target – either in the form of data theft or financial gains.

OUR SOLUTION:

Intercepting Any Malicious Files or URL Upon Upload

Perception Point's Advanced Salesforce Security scans all content uploaded to your customer portal to intercept any attempt to use it for malicious purposes, before it reaches the end user employee. The multi-layered solution employs unique anti-evasion algorithms to identify even the most hidden objects and processes each of them separately through three unique static layers and the proprietry HAP layer, making sure no attack gets into your system.

As part of a partnership with Salesforce, the solution is available on the AppExchange and can be easily installed directly on your service. No additional IT costs nor overhead.



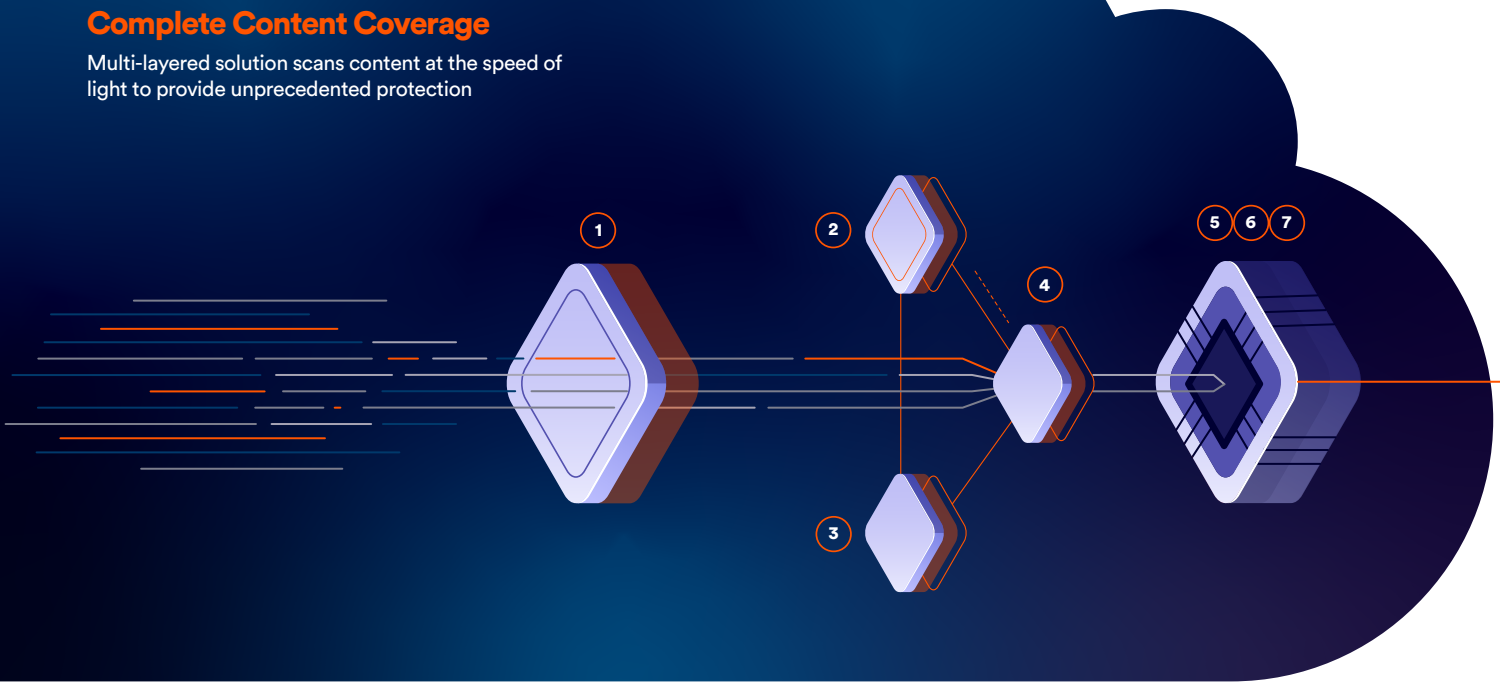
Contact Us

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

We're in
Boston | Tel Aviv

Complete Content Coverage

Multi-layered solution scans content at the speed of light to provide unprecedented protection



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.