PERCEPTION POINT

Advanced Shared Drive Security.

Cutting-edge threat prevention for the collaboration-driven enterprise.

Highlights.

Real-time prevention
Block malicious content before it ever reaches the end user.

X-ray visibility
"X-ray" any code executed by the system for 100% visibility into malicious intent.

Deep scanning
Unpacks and follow URLs to detect evasive malicious intent.

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

Unlimited scale
Scan 100% of content, regardless of volume.

Shared Drive services
OneDrive, SharePoint, Dropbox, Google Drive, and Box.

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

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

Shared Drives: A Growing Security Blindspot.

Cloud-based shared drives are an essential productivity tool for the modern enterprise. They allow for simple and easy collaboration, no matter where people are working from. However, they also pose a significant new cybersecurity risk. Given their growing usage, they pose an attractive target for hackers, yet aren't nearly as protected as more traditional vectors like email, endpoints and networks.

Shared drives can be highly effective malware distribution platforms, whether the malicious content is coming from another channel open to the outside (like email), an insider threat, or an unmanaged endpoint from a third party. Once malicious content is on the shared drive, it can easily travel to any unsuspecting user with access.

It is not enough to just secure the data in collaboration channels, you have to ensure that the content inside these channels is clean and safe.

OUR SOLUTION:

Any threat. Any file. Any URL. Any shared drive.

Perception Point's Advanced Shared Drive Security, delivers the same robust prevention typically only available for email. Cutting-edge cloud solution **prevents malicious content (files & URLs) from being uploaded, downloaded or utilized to infect previously clean files.** Unique CPU-level visibility plus deep scanning capabilities detect the unknown attacks like zero days and n-days, pre-malware release. Multi-layered technology combines multiple threat intelligence, image recognition and static engines to prevent phishing and commodity malware.

Our service deploys in one-click, has virtually zero scanning delay, and limitless scale – so your employees can collaborate both securely and seamlessly, wherever they are.

Key Features

- Real-time prevention for OneDrive, SharePoint, Dropbox, Google Drive, and Box.
- Run-time scan and detection of all files uploaded to the shared drives.
- Pre-scan ("hunting") and detection of all historical files.
- Ability to define scan policy and extend existing security policy.
- Ability to define quarantine policy.
- Forensics of all file scans using the same tools used for email.

Contact Us

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

We're in
Boston | Tel Aviv

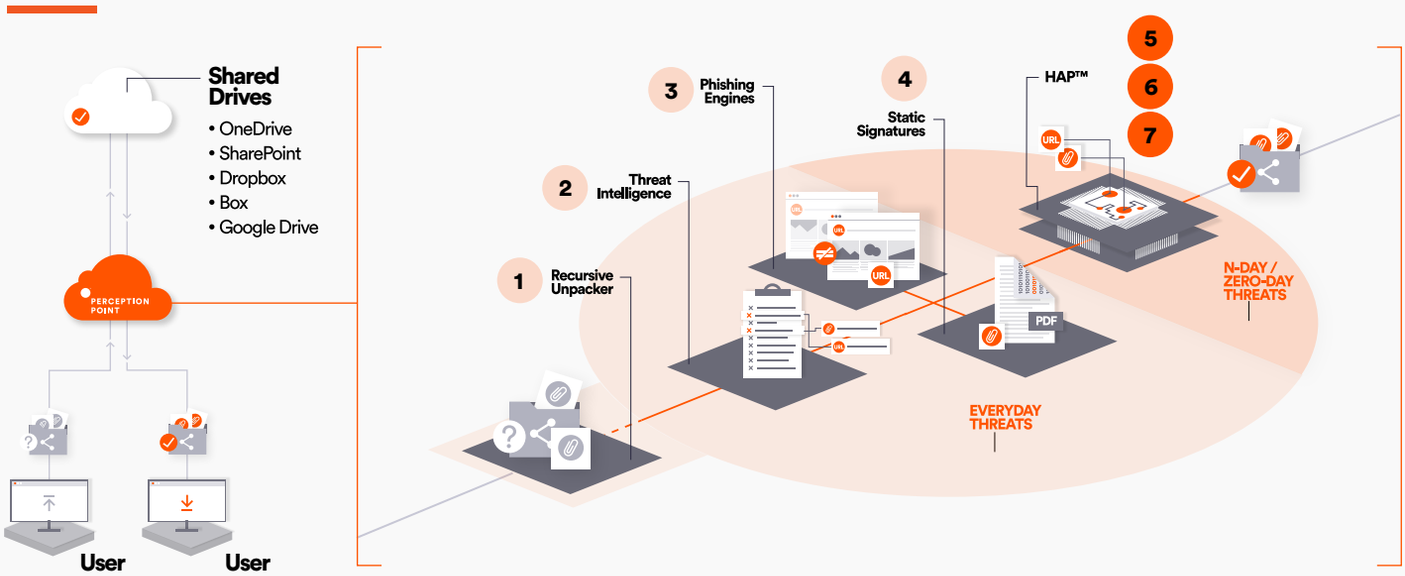
Free 30-day trial

Set-up a trial in less than an hour, with no interference or disturbance to the end user or organization.
No content will be stored and all data is encrypted.

PERCEPTION POINT

Inherent Layered Solution

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



EVERYDAY THREATS | Phishing, Commodity malware, Spam, etc:

1

Recursive Unpacker.
Unpacks the email 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 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.

Protect multiple channels with our full Advanced Collaboration Security platform.
Email, messaging, shared drives + API for any content-exchange channel

PERCEPTION POINT