

## 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 files 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.

### Supported 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.

## Contact Us

[www.perception-point.io](http://www.perception-point.io)  
[info@perception-point.io](mailto:info@perception-point.io)

### We're in

Boston | Tel Aviv

# Advanced Cloud Storage Security.

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

## Cloud Storage: A Growing Security Blindspot.

Cloud-based file sharing apps 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 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.

Cloud Storage apps 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 file sharing service, 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 cloud storage.**

Perception Point's Advanced Cloud Storage 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 file sharing service.

Pre-scan (“hunting”) and detection of all historical files.

Ability to define scan policy and extend existing security policy.

Ability to define quarantine policy.

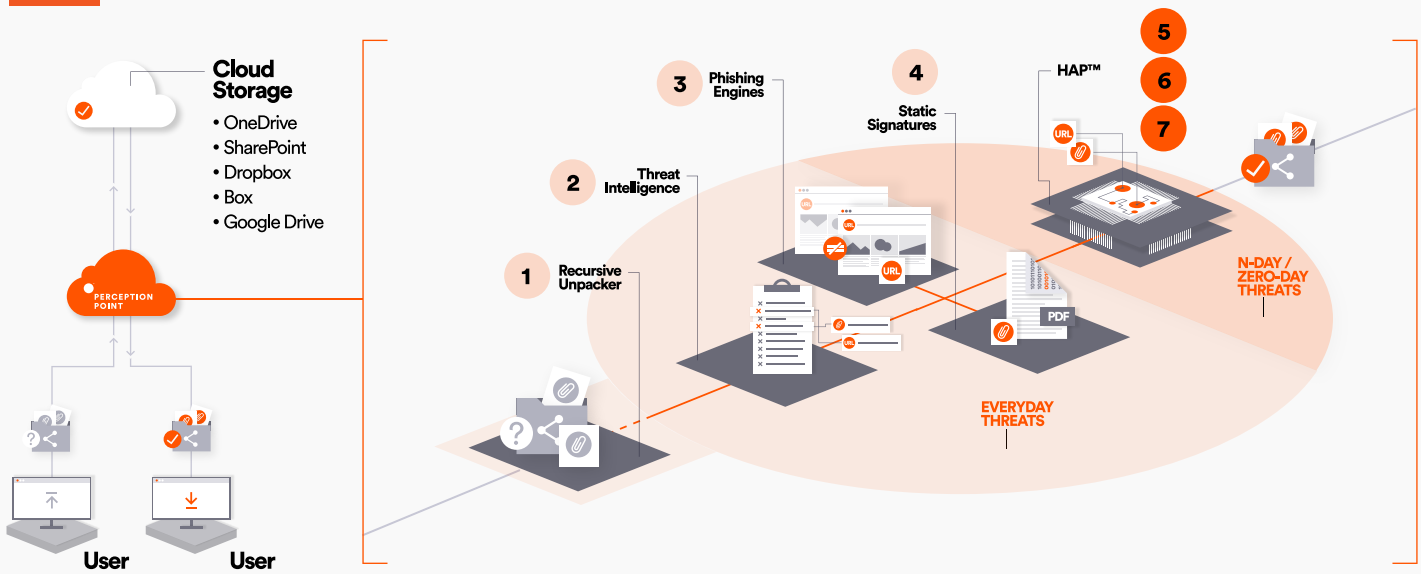
Forensics of all file scans using the same tools used for email.

## Free 30-day trial

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

## 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 file into smaller units to identify hidden malicious attacks. All of the extracted components go separately through the next layers.

2

#### Threat Intelligence.

Combines multiple threat intelligence sources with our internally developed 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

#### Hardware-Assisted Platform (HAP™)

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 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 CF1 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, CRM, Cloud Storage + API for any content-exchange channel