

ADVANCED BROWSER SECURITY

MULTIPLE SECURITY LAYERS PROTECT YOUR ENTERPRISE FROM EVERY BROWSER-BASED THREAT



Digitization, hybrid work models, and adoption of web-based SaaS apps have made the browser a prime attack vector for adversaries. Phishing pages, malicious downloads, harmful plugins and internal threat actors - easily evade traditional security solutions leading to ransomware incidents, financial losses and severe data breaches.

Perception Point adds enterprise-grade security to standard browsers (Chrome, Edge, Safari, etc.) fusing **Advanced Threat Detection** with Browser-level **Governance** and **DLP** controls. The Advanced Browser Security extension provides organizations of all sizes with unprecedented ability to detect, prevent and remediate any browser threat while maintaining user productivity and native browsing experience.



KEY BENEFITS



Secure your organization's endpoints against any browser-based threat



Prevent data loss and protect the access to your sensitive SaaS applications



Retain user productivity with a familiar, fast and seamless web browsing experience



Reduce IT friction, overhead and cost per user

PERCEPTION
POINT



Browser Protection is Active

Your browser is protected against advanced web threats

GAPS IN TRADITIONAL WEB AND BROWSER SECURITY

Legacy architectures like Secure Web Gateway rely on basic detection models and are insufficient for preventing advanced browser threats. The fact that they are positioned in the network level means they have limited visibility and control over what's going on in the application/browser-level (what the users actually see and do). This partial "blindness" exposes organizations to the ever-growing threat landscape consists not only of external attacks like phishing websites or malicious downloads but also insider threats and data leakage via the browser.

Common browser security solutions like Remote Browser Isolation (RBI) or Virtual Desktop Infrastructure (VDI) introduce significant delays, hinder user productivity, create IT overhead, and tend to be costly.

PROTECT FROM EXTERNAL THREATS, DATA LOSS AND MALICIOUS INSIDERS

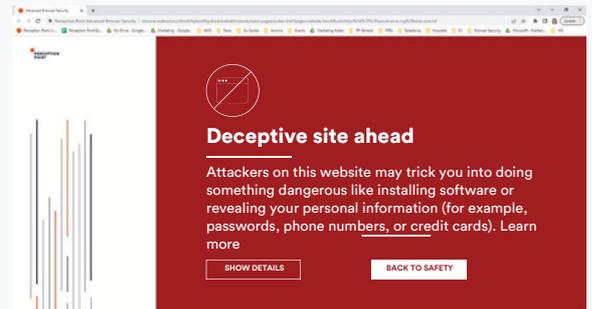
Advanced Browser Security by Perception Point solves today's browser security challenges for a multitude of cases:

SAFE BROWSING

Protect the organizational browsers, detecting and preventing phishing, ransomware, malware and zero-days from reaching your endpoints.

Use Cases

- Secure access to risky websites
- Phishing prevention
- Ransomware/malware prevention
- Content and URL filtering

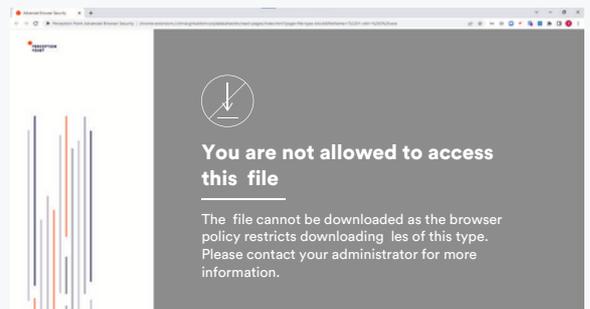


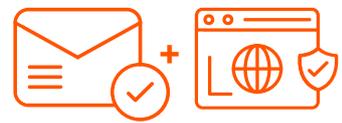
SENSITIVE ACCESS

Protect access to corporate sensitive applications from any endpoint, preventing data loss and malicious insiders, with granular security, DLP & governance capabilities.

Use Cases

- Privileged and sensitive app access
- 3rd party vendors & partners
- BYOD & unmanaged devices
- Extend Zero Trust to the endpoint
- Access SaaS and internally-developed apps
- Customer care and call centers





THE ULTIMATE COMBO - ADVANCED EMAIL + BROWSER SECURITY

Secure your data and endpoints with a browser-centric solution offering unparalleled web and email protection synergy. Combining Perception Point's market leading Advanced Email Security and browser protection elevates threat prevention to new heights.

Correlating Cross-Channel Evidence to Stop the Most Evasive Threats



Deployed in the browser, the extension views threats from the user's perspective, rendering the most sophisticated evasion techniques ineffective. "Geofencing", IP or time based tactics designed to evade email scanning are prevented in seconds once the user clicks the malicious link. In addition, evidence and context gathered from email (e.g. sender, domain, files) is leveraged to enhance detection of web threats - and vice versa!

Tracing Attacks Back to their Source and Identifying Impacted Users



Combining real-life user browsing data with email events allows security professionals to easily and visually "connect the dots" and investigate the impact of an attack or an ongoing incident: Which users inserted their credentials? Who clicked/downloaded the malicious content? What unsanctioned SaaS apps do my users use?

Remediating Web and Email Incidents Rapidly from a Centralized View



Better detection and faster remediation of Account Takeover events thanks to browsing login events visibility. Malicious files or URLs discovered by the extension "in the wild" are automatically remediated from the organization's inboxes and other channels - all is done via the Perception Point's unified and SSO-friendly platform

DETECTION LAYERS

Spam Filter (email only)

Applies reputation and anti-spam filters to quickly flag spam content

Threat Intelligence

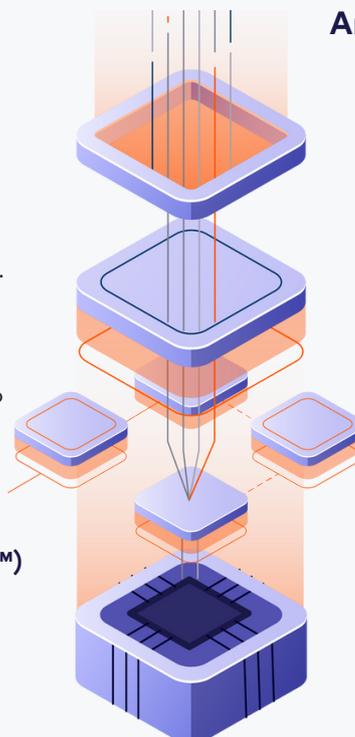
Combines multiple threat intelligence sources with a unique internally developed engine that scans URLs and files in the wild.

Static Signatures

Best-in-class signature based AV engines to identify malicious attacks enhanced with novel proprietary algorithms that act to identify highly complicated signatures.

Hardware-Assisted Platform (HAP™)

Patented CPU-level technology acts earlier in the kill chain than any other solution. Blocking attacks in near real-time at the exploit phase – pre-malware release/execution.



Anti Evasion - Recursive Unpacker

Unpacks content into smaller units (files and URLs) to overcome evasion techniques and identify hidden malicious attacks. All of the extracted components go separately through to the next detection layers.

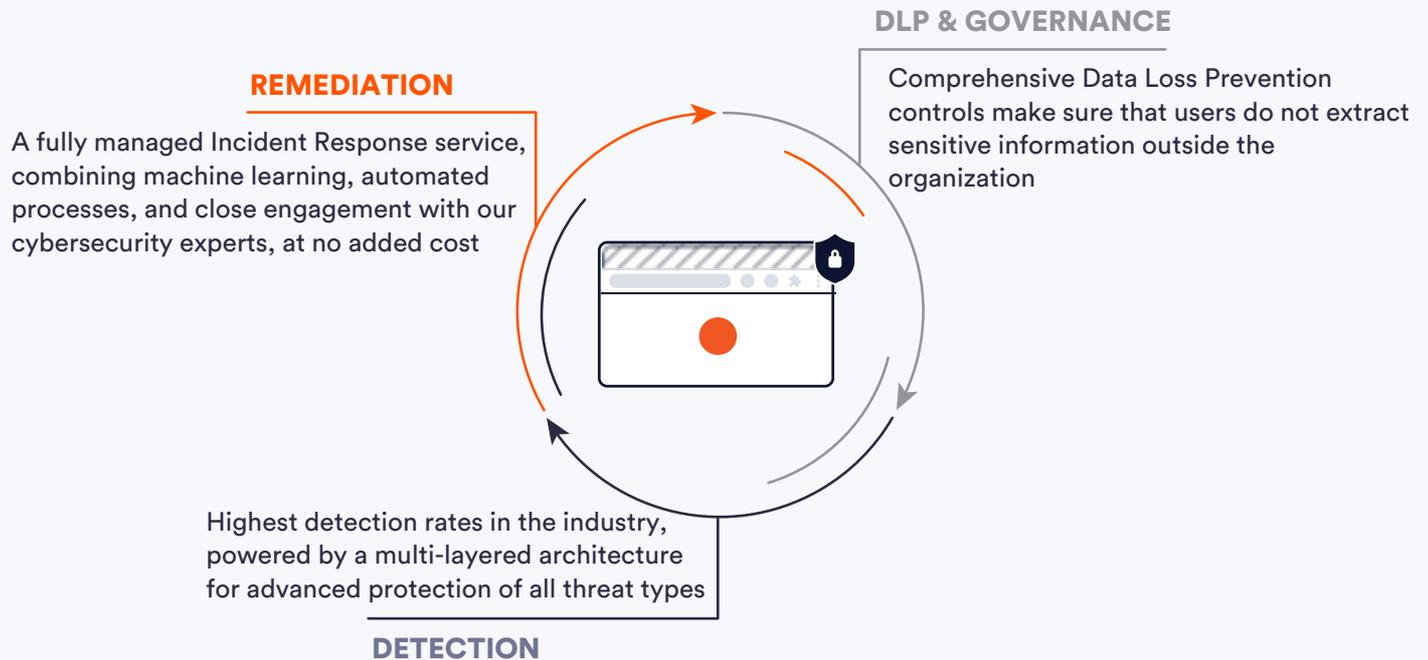
Phishing Engines

Best-in-class URL reputation engines coupled with Perception Point's in-house image-recognition models to identify phishing attacks, spoofed pages and brand impersonation.

BEC & Account Takeover

Correlates contextual and behavioral anomalies to analyze and intercept Account Takeover attempts and remediate breached users.
BEC - email only

OUR PILLARS



About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection and response to all attacks across email, web browsers and cloud collaboration apps. The solution's integrated incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights for best protection.

Deployed in minutes, the cloud-native and easy-to-use service outperforms legacy systems to prevent phishing, BEC, spam, malware, Zero-days, ATO, and other advanced attacks before they reach end-users.

Fortune 500 enterprises and organizations across the globe are protected by Perception Point.

To learn more about Perception Point, visit our [website](#) or follow us on [LinkedIn](#), [Facebook](#), and [Twitter](#).