PERCEPTION POINT™

ADVANCED BROWSER SECURITY DATASHEET

Refreshing Browser Security & Control

Perception Point's extension integrates with any browser to protect your employees and SaaS apps against web-borne attacks and data-loss, and allows you to regain control over your users' last ungoverned app.

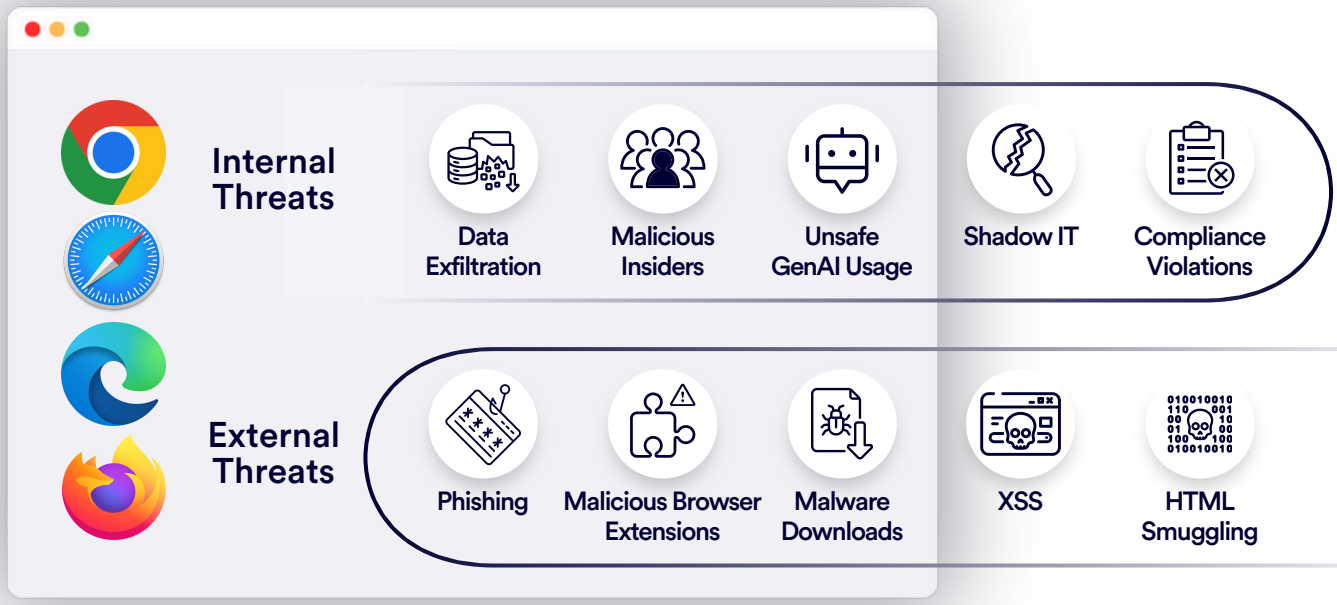
WHY ENTERPRISE BROWSER SECURITY?

The browser has become the de-facto workspace of the modern organization. It is the most used application with users spending the bulk of their working hours switching between one tab to another to communicate, collaborate and complete tasks. As the "windows to the web", browsers present fundamental security and IT challenges:

Highly Targeted Attack Surface: Browsers are prime targets for cyber attacks that easily bypass traditional security measures like firewalls and Secure Web Gateways (SWG) and only detonate in the target's browser. From evasive zero hour phishing attacks to malware and zero-day exploits, threat actors leverage the native accessibility of browsers to circumvent detection and launch attacks on users and endpoints.

A Source for Data Loss: Designed inherently for information access and sharing, browsers are also a critical vector for data exfiltration. Whether through inadvertent actions by employees (e.g. GenAI usage) or deliberate maneuvers by malicious insiders/3rd parties, browsers are often the means for the unauthorized transfer of sensitive data outside the organization.

A Governance Blindspot: The interactions between your users and their browsers represent a significant blindspot for endpoint and network security solutions. This lack of visibility leaves IT teams unable to enforce security policies or detect anomalous user activities within the browser application.



Introducing Advanced Browser Security

Perception Point's enterprise browser security solution integrates with any browser via a lightweight extension to ensure dynamic protection and governance with zero impact on user experience or browsing quality, empowering employees to work and maintain productivity while staying secure.

Stop attacks at the point-of-click

Leveraging textual and image recognition AI models, proprietary anti-evasion, and a patented sandbox, to instantly identify and prevent web-borne threats. From evasive zero-hour phishing sites to malicious file downloads and cross-site scripting (XSS) exploits, Perception Point neutralizes them at the point-of-click.

Enforce safe access & prevent data loss

Equipping security and IT professionals with a comprehensive suite of tools and granular web policies to enable and enforce safe access to enterprise web apps and SaaS platforms while preventing sensitive data loss and risky behaviors across both managed and unmanaged devices.

Get visibility and control over the browser

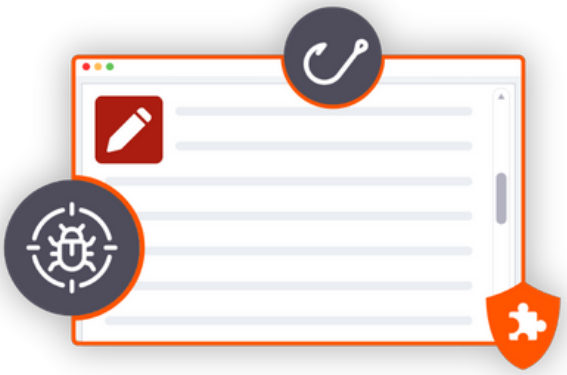
Unlocking browser-level control and effective monitoring capabilities across all of the organization's browsers from one intuitive cloud console. Allowing for web-content filtering, remediation of risky browsing events, clear visibility to unsanctioned apps and browser extensions in use, and more.

PERCEPTION POINT™

Use Cases & Features

SAFE BROWSING

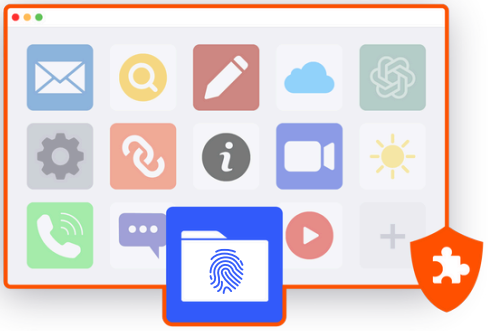
Prevent phishing, evasive malware, zero-days, and harmful browser extensions from compromising your users and data in real time.



- Anti-phishing via image recognition models (detecting logo impersonation, login forms, brand favicons, etc.)
- Full dynamic scanning of all file downloads, recognized by SE Labs as best-in-class file detection
- CPU-level sandbox - HAP™* (ransomware, zero-day exploits, etc.)
- Recursive file unpacking (anti-evasion)
- ML models to detect and prevent malicious HTML snippets
- Malicious URL detection
- HTML smuggling prevention
- Detect XSS attempts
- Block uncategorized websites & risky website categories

SAFE ACCESS & DLP

Enforce safe access to your SaaS and web apps, stop deliberate and accidental data leaks, malicious insiders and 3rd party threats.



- Require the extension as a condition to accessing enterprise web apps via conditional access**
- Granular clipboard controls to limit risky behaviors across sensitive sites and apps
- Granular download/upload controls
- Safe GenAI/ChatGPT enablement (sensitive content detection, user warning, etc.)
- Watermarking - deterring users from capturing on-screen sensitive data
- Real-time PII detection in user data submission (conditional warn/restrict, regex-based)
- PII detection in downloaded files (NER/LLM-based)
- Anomalous mass data exfiltration detection
- Shoulder surfing protection - blur sensitive websites while not in use
- Optionally audit all file uploads
- Anti-tampering - restrict developer tools use

BROWSER GOVERNANCE

Transform any browser into a secured workspace with granular browser-level controls and 360° visibility.

- Installed browser extensions discovery, governance and risk analysis, leveraging both reputation data, static analysis and dynamic sandbox-based analysis of extensions
- Risky extensions detection and automatic disablement
- Web login events monitoring
- Browser inventory and version information
- Password-reuse monitoring & alerts
- Website categories, content and URL filtering and restriction
- Restrict downloads (per file type, website category, etc.)
- Seamless deployment/offboarding for contractors and 3rd party users.
- IdP SSO integration
- Customizable end-user notifications, warnings, etc.

*patented
**patent pending

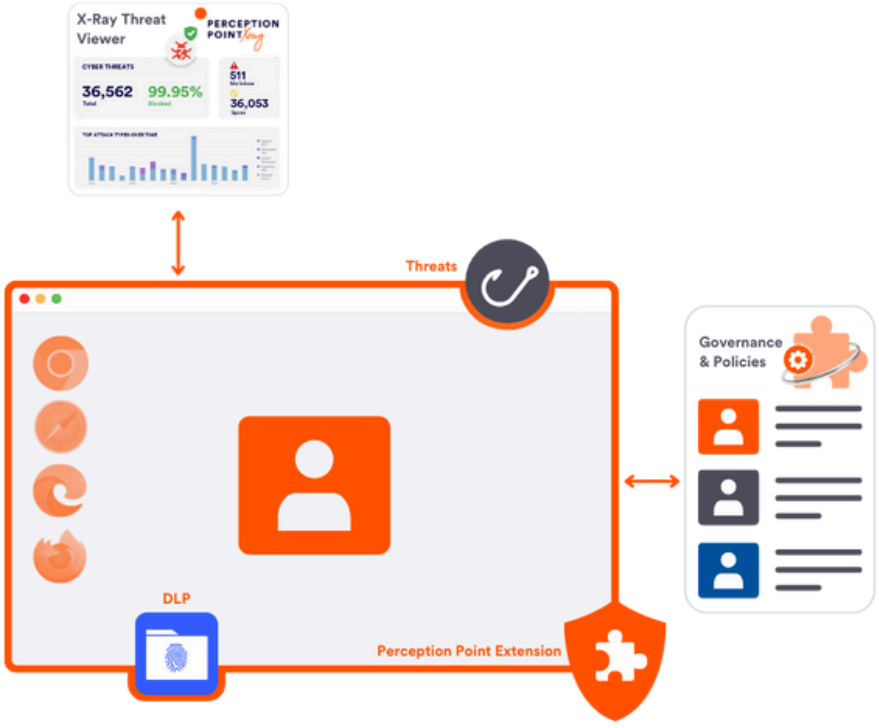
PERCEPTION POINT™

How Does it Work?

Extension: Deployed across any browser on both managed and unmanaged devices, with multiple deployment options to comply with different IT requirements (unattended/silent deployment via UEM, IdP integration, script-based, manual/automated email-invites etc.)

Admin Console - X-Ray: Perception Point's admin console provides full threat analysis and remediation capabilities, empowering security teams with detailed insights of malicious or risky behaviors, comprehensive forensic information of prevented attacks, and unique cross-channel cases and context

Admin Console - Governance & Policies: Configure and manage how the Perception Point extensions operate in your enterprise. The console allows admins to govern end-users and devices, develop and maintain web policies and DLP rules, and more.



THE ULTIMATE COMBO: EMAIL + BROWSER SECURITY

Secure your users and data with unparalleled web and email protection synergy. Combine Perception Point's market leading Advanced Email Security with the Advanced Browser Security extension to elevate threat prevention to new heights.

Correlating Cross-Channel Evidence to Stop the Most Evasive Threats

Scanning threats from the user's point of view renders the most advanced evasion techniques ineffective. Geofencing, CAPTCHAs, password-protection or time-based tactics designed to evade detection are prevented in real-time once the user encounters the malicious website/payload on the browser. Contextual evidence gathered from email (e.g. sender, domain, etc.) is leveraged to enhance detection and users' awareness of web-borne attacks - and vice versa.

Tracing Attacks Back to Their Source and Identifying Impacted Users

Combining live 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 apps do my employees use?

Rapid Remediation of Browser and Email Incidents + Enhanced Email DLP

Faster, more efficient remediation of "phished" users and Account Takeover incidents with login events monitoring and visibility. Weaponized files or URLs scanned by the extension "in the wild" get automatically remediated from all inboxes. Warn or prevent end users from email-related data exfiltration, audit sensitive email attachments (e.g. employee offboarding) and receive email DLP alerts.

PERCEPTION POINT™

Uncompromising Workspace Security & Productivity

Superior Detection
AI-powered threat detection with proven accuracy of 99.95%. 100% of file downloads are scanned dynamically using a multi-layered architecture.

Rapid Agentless Deployment
Onboard employees and contractors easily via a lightweight browser extension compatible with any standard browser.

Workspace Security-Ready
Leverage with Advanced Email Security and cloud app protection, to holistically protect your user-centric attack vectors against advanced threats.

Centralized Control
Configure and enforce all website rules and policies from Perception Point's intuitive cloud management console.

Unhindered User Experience
Allow your users to continue working with their existing browsers. Unless a web-borne threat is detected, they won't feel the extension is there.

Managed Browser Security
An all-included incident response and support service alleviate the overhead and fully support your SOC/IT teams or MSP staff 24/7, to provide enterprise-grade browser security and save up to 75% in operational resources.

Technical Specifications

Manageability

- Cloud-based management console & user inventory
- Dashboards and reporting
- Configure threat protection mode (silent/warn/block)
- Customizable UX for end-users (warnings, toast messages, block pages, etc.)
- Identity provider integration (via SAML)
- Automatic policy assignment based on user properties (e.g. SAML attributes)
- Role-based access control (RBAC)
- User and admin auditing

Forensics & Incident Response

- An all-included 24×7 incident response service powered by cybersecurity and web security experts
- In-depth forensics view of all security incidents and cases
- Correlation of browser and email events (Advanced Email Security)
- Cross-channel correlation and remediation of security incidents (e.g. remediation across all protected cloud channels)

Compliance

- SOC2
- GDPR
- ISO 27001
- HIPAA

Supported Browsers

- Google Chrome
- Microsoft Edge
- Firefox
- Safari
- Any other Chromium-based browser (e.g. Opera, Brave, Arc, …)

Supported OS

- Windows
- MacOS
- ChromeOS
- LinuxiOS (preview)

Deployment & Updates

- UEM solutions (Microsoft Intune, JumpCloud, Jamf Pro, and Google Workspace)
- Self-service install by users via email invite
- Operating in the background in silent/transparent mode (configurable)
- Automatic updates (configurable)
- No tunneling/remote browsing/proxying web traffic
- Compatible with any existing VPN/proxy/network infrastructure

PERCEPTION POINT™

About Perception Point

Perception Point is a leading provider of AI-powered threat prevention solutions that safeguard the modern workspace against sophisticated threats. The unified security solution protects email, web browsers, and SaaS apps. By uniquely combining the most accurate threat detection platform with an all-included managed incident response service, Perception Point reduces customers' IT overhead, improves user experience, and delivers deep-level cybersecurity insights.

Deployed in minutes, with no change to the organization's infrastructure, the cloud-native service is easy to use and replaces cumbersome, traditional point systems. Perception Point proactively prevents phishing, BEC, ATO, malware, spam, insider threats, data loss, zero-days, and other advanced attacks well before they impact the end-user. Fortune 500 enterprises and organizations across the globe are protecting more and managing less with Perception Point.

Visit Us: perception-point.io
Contact Us: info@perception-point.io