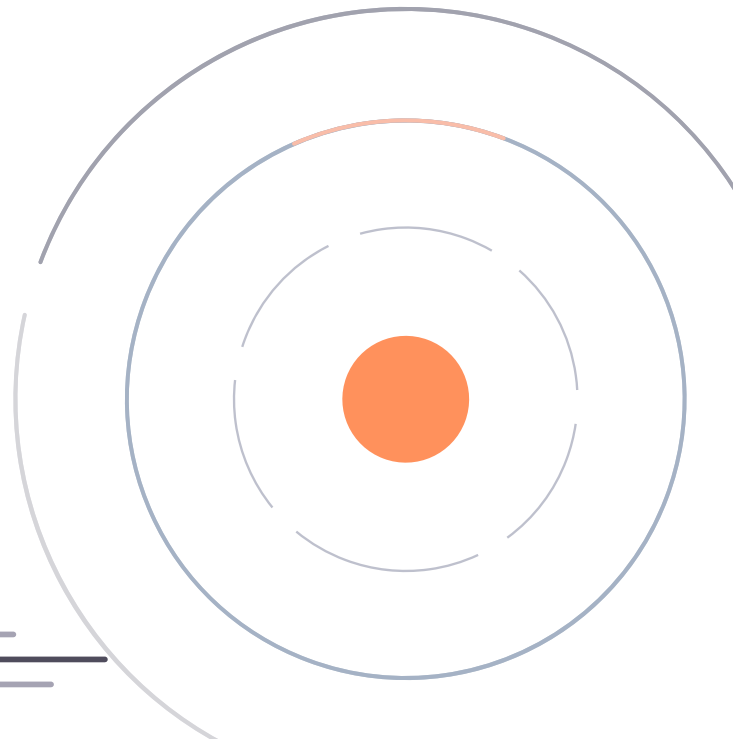




Advanced Browser Security Browser Extension

Datasheet



PROTECT YOUR PRIMARY PRODUCTIVITY TOOL WITH UNMATCHED DETECTION AND PREVENTION

Perception Point's Advanced Browser Security - Browser Extension allows you to stop any web-based threat before it reaches your end users, and protect the organization's applications, data and devices using your standard browser, without added latency, maintaining productivity and user experience.

When combined with Perception Point Advanced Email Security, you receive unparalleled detection across the main attack vectors, leveraging correlation between attacks and enhanced threat visibility.

HIGHLIGHTS

Secure your native browser, detecting and preventing phishing, ransomware, malware and zero-days from reaching the organization's endpoints.

- Best-in-class detection, including advanced phishing and malware protection
- Advanced DLP controls
- Full governance capabilities with fine-grained policy settings
- Leverages existing organizational browser
- Full compatibility with the web and the enterprise ecosystem
- Content and URL filtering
- Secured connectivity, extending Zero Trust to the Endpoint
- Visibility to organizational users, devices, browsers, and browser extensions
- Visibility to all browsing and download events
- Non-intrusive easy deployment & automatic updates
- Comprehensive incident investigation platform
- All-included 24x7 managed incident response service at no additional cost

USE CASES

SECURE RISKY ACCESS

Secure your native browser and stop ransomware, phishing and other advanced threats from reaching the organization's endpoints.



Safe browsing in any website



Content and URL filtering



Phishing prevention



Ransomware/malware and zero-days prevention

SECURE ACCESS TO SENSITIVE APPS

Secure access to sensitive applications from any endpoint, preventing data loss and malicious insiders, with multiple security, DLP & governance features.



Privileged and sensitive app access



3rd party vendors & partners



BYOD & unmanaged devices



Extend Zero Trust to the endpoint

KEY FEATURES

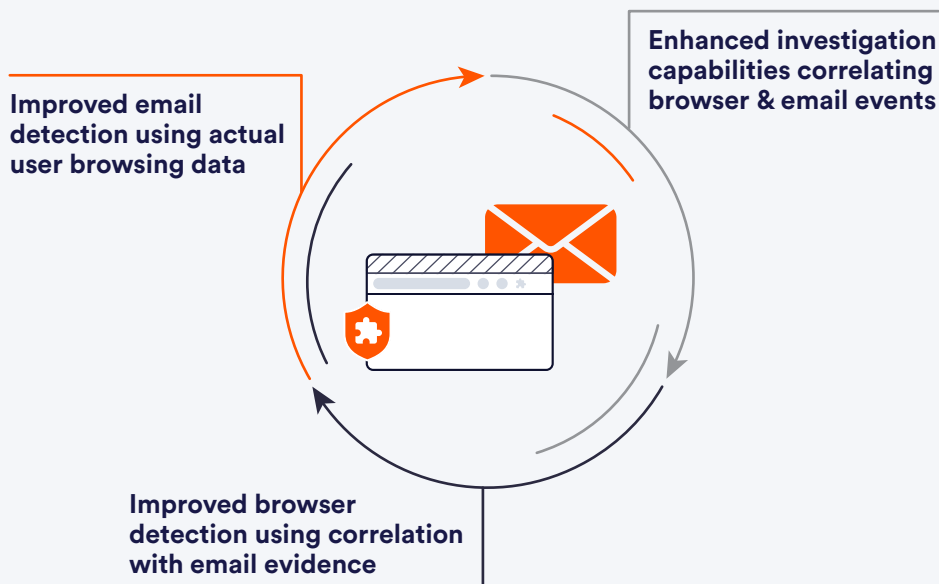
UNPARALLELED DETECTION

The browser extension is powered by an award-winning detection platform, composed of 7 layers of proprietary patented detection - including image recognition, ML/AI algorithms, next-gen sandbox, anti-evasion mechanism, and more. Scanning 100% of content dynamically, it is much more than an anti-virus or a Secure Web Gateway, protecting browsers against any web threat, including phishing, ransomware, malware, advanced threats, insider/3rd party threats, and more.



MAXIMAL PROTECTION ACROSS THE MOST TARGETED VECTORS: WEB BROWSER & EMAIL

Perception Point enhances detection & remediation capabilities by correlating malicious threats across the web browser and email, intercepting advanced attacks that couldn't be caught otherwise. Examples include flagging URLs the user tries to access through the browser, even if they are not malicious, but came from suspicious email sources; Remediating malicious emails that contain a URL that was only identified as malicious by actual user browsing; and more.



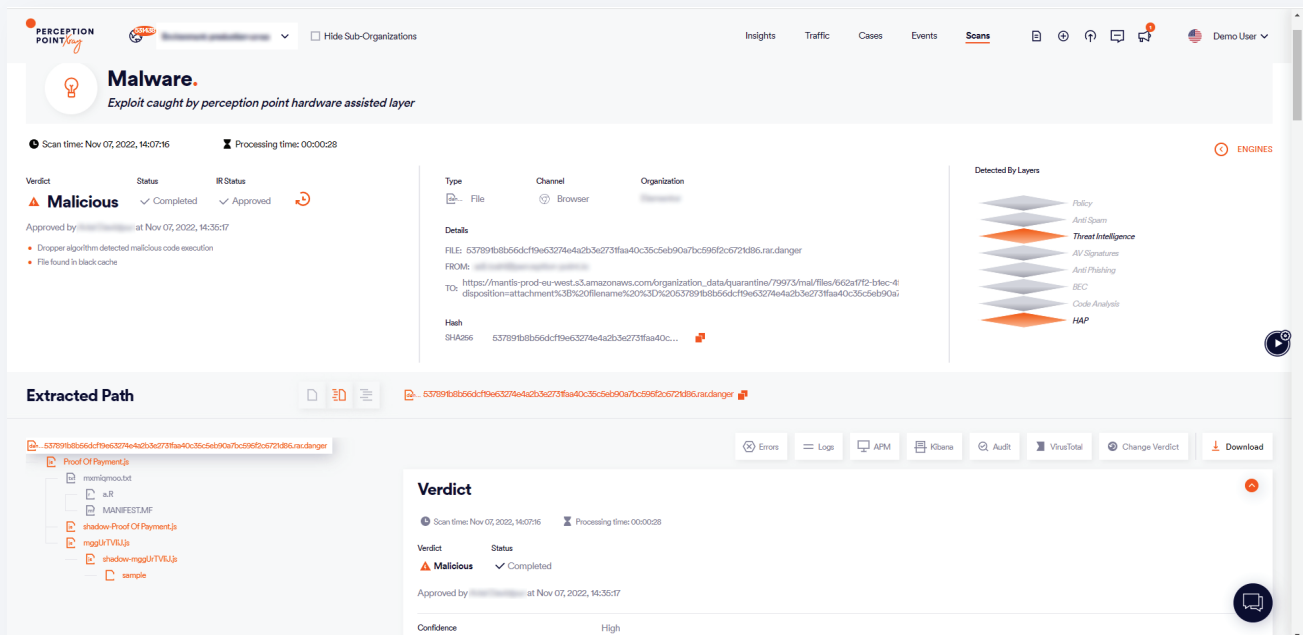
KEY FEATURES

DATA LOSS PREVENTION

DLP is both simplified and robust with Perception Point's Advanced Browser Security solution. The solution allows security teams to control access to sensitive web apps, including clipboard controls, printing controls, download controls, watermarking, and more. It can also optionally audit user activity on sensitive web apps, including an audit log for accessed URLs and downloaded files.

MANAGEABILITY

Perception Point's Advanced browser security solution is managed in a user friendly dashboard where admins can both gain insights into status of devices, users and policies, and perform required actions. Users are provided with in-depth forensics view of all security incidents, allowing a drill-down to any incident, correlation between attacks, and remediation actions. Customers also receive a fully managed 24x7 Incident Response service, free of charge, drastically reducing the need for SOC team resources.



[Example of a browser attack containing buried malware, detected by Perception Point's next-gen sandbox]

GOVERNANCE

Perception Point's Advanced Browser Security solution allows security teams to set various browser governance policies, such as defining which file types are allowed to be downloaded and which website categories are accessible to users. It can also provide visibility into installed browser extensions and other browser information.

DEPLOYMENT & UPDATES

The solution is easily deployed to remote end users through any MDM or browser management solution, e.g. Google Workspace and Microsoft Endpoint Manager. It can also be deployed in a self-service way through the Chrome Web Store, authenticating users via existing identity providers or via email verification codes. It's centrally-managed via a modern cloud-based management console and continuously updates, to stay ahead of evolving cybercriminal techniques and tools.

TECHNICAL SPECIFICATION

Threat Vectors	<ul style="list-style-type: none">▪ Protection against phishing, malware, ransomware, advanced threats, insider/3rd party threats▪ Market leader in detection capabilities according to independent benchmarks by SE Labs
Malware & Ransomware Protection	<ul style="list-style-type: none">▪ Full dynamic scanning of all downloaded files in near-real-time▪ Multi-layered detection engines▪ Recursive file unpacking▪ Patented HAP technology to detect zero-day exploits and vulnerabilities in files
Phishing & Malicious Website Protection	<ul style="list-style-type: none">▪ ML-based dynamic detection of phishing/malicious websites▪ Image recognition to detect brand impersonation attempts▪ Dynamic collection of evidence from the user's browser for the highest level of accuracy▪ Anti-evasion technology▪ Uncovers threats hidden in SSL and TLS encrypted communications
Data Loss Prevention	<ul style="list-style-type: none">▪ Granular clipboard controls to limit copy and paste operations across websites/web apps▪ Download controls to prevent downloading of sensitive files▪ Printing controls for sensitive content▪ Watermarking to deter users from taking photos/screenshots of sensitive content
Browser Governance	<ul style="list-style-type: none">▪ URL filtering to block/allow websites based on categories/URLs/IPs▪ Visibility into user-installed browser extensions▪ Limit which file types users can download▪ Browser inventory and version information
Manageability	<ul style="list-style-type: none">▪ Cloud-based management console▪ User inventory▪ Configure threat protection in silent/warn/block modes▪ Customizable block pages▪ Automatically assign policies based on user properties (e.g. SAML attributes)▪ Automatic updates▪ Dashboards and reporting▪ User and admin auditing▪ SIEM integration▪ Role-based access control▪ Identity provider integration (via SAML)

TECHNICAL SPECIFICATION

Forensics & Incident Response	<ul style="list-style-type: none">▪ An included 24x7 incident response service powered by cybersecurity experts▪ In-depth forensics view of all security incidents▪ Cross-channel correlation and remediation of security incidents (e.g. remediation across all protected organizational cloud channels)
Compliance	<ul style="list-style-type: none">▪ SOC2▪ GDPR
Supported Browsers	<ul style="list-style-type: none">▪ Chrome▪ Edge▪ Safari
Supported Operating Systems	<ul style="list-style-type: none">▪ Windows▪ MacOS▪ ChromeOS▪ Linux
Deployment & Updates	<ul style="list-style-type: none">▪ Silent installation via any MDM or browser management system▪ Self-service install by users via email▪ Operating in the background in silent/transparent mode (configurable)▪ No tunneling of traffic required▪ The browser extension is automatically updated by Perception Point (configurable)



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.

