Solution Brief

Improve Employee Productivity While Maintaining Security.

The Problem

The last year has led to an increase in the adoption of hybrid work, and an increase in cyber threats, with 70% of breaches originating on the endpoint. One of the ways IT teams have been dealing with the increasing endpoint threats is by constantly locking them down, significantly restricting employees freedom which often prohibits employees from doing their job well and causes conflicts with the organization's business leaders.
These restrictions may include:

- Browsing the full web
- Using unsanctioned SaaS apps
- Using personal apps
- Accessing content originating from 3rd parties
- Accessing sensitive enterprise apps

This conflict is exacerbated due to the shift to hybrid work and the need for more collaboration and communications tools. Accessing web sites and SaaS apps may be necessary for daily work, but they are also potential avenues that enable infiltration of malware, ransomware, and other threats into the organization, and exfiltration of sensitive data. IT and Security want to limit these web applications, but business leaders insist they are necessary productivity tools. You end up in "whitelisting hell", wasting precious resources on checking and approving a never-ending list of websites.

The Solution

Perception Point Advanced Browser Security adds enterprise-grade security to native Chrome and Edge browsers. The managed solution fuses patented web isolation technology with multi-layer advanced threat detection engines which delivers the unprecedented ability to isolate, detect and remediate all malicious threats from the web, including phishing, ransomware, malware, APTs, and more.

Untrusted, risky websites and web applications are automatically opened and used in the secured browser which is isolated from corporate data and applications. Access to sensitive corporate apps is secured via an isolated, trusted Chrome or Edge browser. This prevents data loss (DLP) from both managed and unmanaged endpoints.

The behavior of the secured browser is managed in the cloud, while all of the computing resources run locally on user endpoints. This eliminates the need to invest in a large and costly infrastructure, and provides a better local user experience in terms of speed, along with offline availability.

We add advanced security to native Chrome and Edge browsers to protect your organization against all malicious threats from the web and protect access to sensitive corporate apps.

PERCEPTION POINT

Benefits.

01

Reduce the time and money spent on whitelisting applications. attacks

02

Your team can access untrusted websites and SaaS apps, without security concerns and without added latency.

03

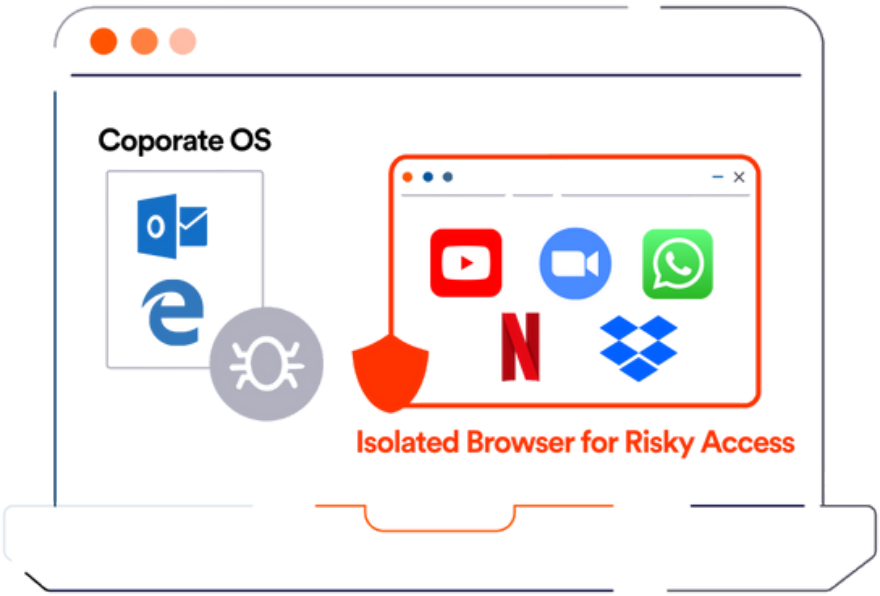
Untrusted web content is deeply scanned and opened in the secured Chrome or Edge browser, reducing the risks from viruses and other downloadable threats.

04

Productivity and connectivity applications can be opened in the secured browser so you can work without concern about introducing malware, ransomware, viruses and other issues.

05

Reduce risks from USBs and printer applications by automatically redirecting usage to the secured browser.



PERCEPTION POINT

Perception Point Advanced Browser Security - Protecting Access to Sensitive Corporate Applications and Data

Perception Point Advanced Browser Security adds enterprise-grade security to native Chrome and Edge browsers. The managed solution fuses patented web isolation technology with multilayer advanced threat detection and DLP engines which deliver the unprecedented ability to isolate, detect, and remediate all malicious threats from the web, including phishing, ransomware, malware, APTs, and more.

Perception Point Advanced Browser Security is easily deployed via a browser extension or a light agent on PC or Mac, and is managed from the cloud. There are no added cloud infrastructure or data center expenses. Access to sensitive corporate apps is secured using a trusted browser, preventing data loss (DLP) from both managed and unmanaged endpoints, protecting from insider and external threats.

Customers deploying the solution will experience fewer breaches, while also providing their users with a better user experience as they will have the freedom to browse the web, use the SaaS applications that they require, and access privileged corporate apps, confidently, securely, and without added latency.

A fully managed Incident Response service is included, free of charge to all customers. The team of cybersecurity experts manage all incidents, provide analysis and reporting, and optimize detection engines on-the-fly. The IR service drastically minimizes the need for internal SOC team resources, reducing the time required to manage and mitigate web-borne attacks by up to 75%.

> ***To learn more about Perception Point's web security solution, download Advanced Browser Security - Free, or request a demo.***

© 2022 Perception Point. All rights reserved.

Visit us: www.perception-point.io
Contact us: info@perception-point.io

PERCEPTION POINT