CHECK POINT

YOU DESERVE THE BEST SECURITY

Harmony
Browse

COMPREHENSIVE THREAT PREVENTION FOR WEB USERS

Easily Secure Web Browsers on Managed and Unmanaged Devices

Table of Contents

Executive Summary

Too often, the workforce unwittingly puts your organization at risk when working online, using web browsers and SaaS (Software as a Service) tools for their tasks, both in the office and remotely.

This is because traditional endpoint security is not designed to protect users against the most sophisticated browser threats such as zero-day phishing websites and malware downloads or uploads.

Accordingly, robust browser security is critical for protecting users, their devices, and credentials, as well as the organization's network, applications, and data assets.

The key to overcoming the browser security challenge is comprehensive threat prevention that brings all the requisite protections for users and the organization.

In this paper we will present how you can ensure such protection, with insights about:

- The major risks in today's browser threat landscape
- The most common attack vectors
- The gaps in traditional endpoint security
- How Harmony Browse from Check Point bridges the gap with the most comprehensive, least intrusive defense against web-borne attacks.

The Browser Threat Landscape

Your network, apps, and employee devices are at a constant risk of falling prey to a wide variety of web threats. And with 85% of employees working primarily on their browsers, browser security is more critical than ever to a strong cyber posture.

However, the browser threat landscape is complex, the attacks are sophisticated, and this makes for effective protection that is particularly challenging.

Users visiting malicious sites

Employees sometimes unknowingly visit malicious websites, where they are duped into providing corporate credentials or downloading harmful files, putting the network and the organization's data at risk. Even legitimate sites can be integrated with malicious plugins that can execute an attack.

Low cyber vigilance

Lower rates of precaution-taking are common when employees seek to ensure productivity at the expense of security, both in the office and remotely. And when they spend most of their time in an unprotected browser, engaged in web-based work, they become more vulnerable to malware downloads, malicious scripts, and more.

> In a recent industry survey of 2,000 remote employees worldwide, 67% admit finding workarounds to corporate security policies to be more productive.

[1] Forrester's Security Survey, 2022

Insufficient BYOD browser protection

Even when a BYOD policy is in place, connecting these devices to corporate networks and resources still poses a major risk to the organization.

This is because available BYOD security solutions do not cover the full scope of browser threats, such as password reuse and uploading malicious files to corporate domains. Additionally, BYOD users might be reluctant to deploy an invasive endpoint security solution on their personal devices and would rather install a limited extension on their browser.

Corporate devices being used for non-work browsing

Further complicating the browser security challenge is the use of corporate devices for personal tasks and allowing household members, who are less cyber aware, to use the internet on these devices for non-work activities such as gaming and shopping.

The 4 Main Browser Attack Vectors

To protect your organization against browser-based cyberattacks, the workforce requires comprehensive protection while it is accessing the internet.

Unfortunately, traditional internet access security no longer fits today's perimeter-less business environment. They offer only partial protection and bring a negative impact to the user's browsing experience.

What organizations need is browser threat protection that is not intrusive, and which protects the user against the four main web attack vectors:

Zero-day phishing

This is where users inadvertently visit known and unknown phishing sites or impersonated corporate cloud applications and are tricked into providing sensitive data.

Credential theft

The reuse of corporate passwords on unauthorized or non-business sites enables threat actors to steal an employee's credentials.

Even just a single compromise can provide them with further access to hundreds, even thousands of business accounts and corporate assets.

52% of security incidents were caused by credential theft, the most popular entry point for breaches (DBIR 2023)

Malware downloads and uploads

This happens when users unintentionally upload infected files to the organization's web applications or download malware from harmful sites.

Malicious websites

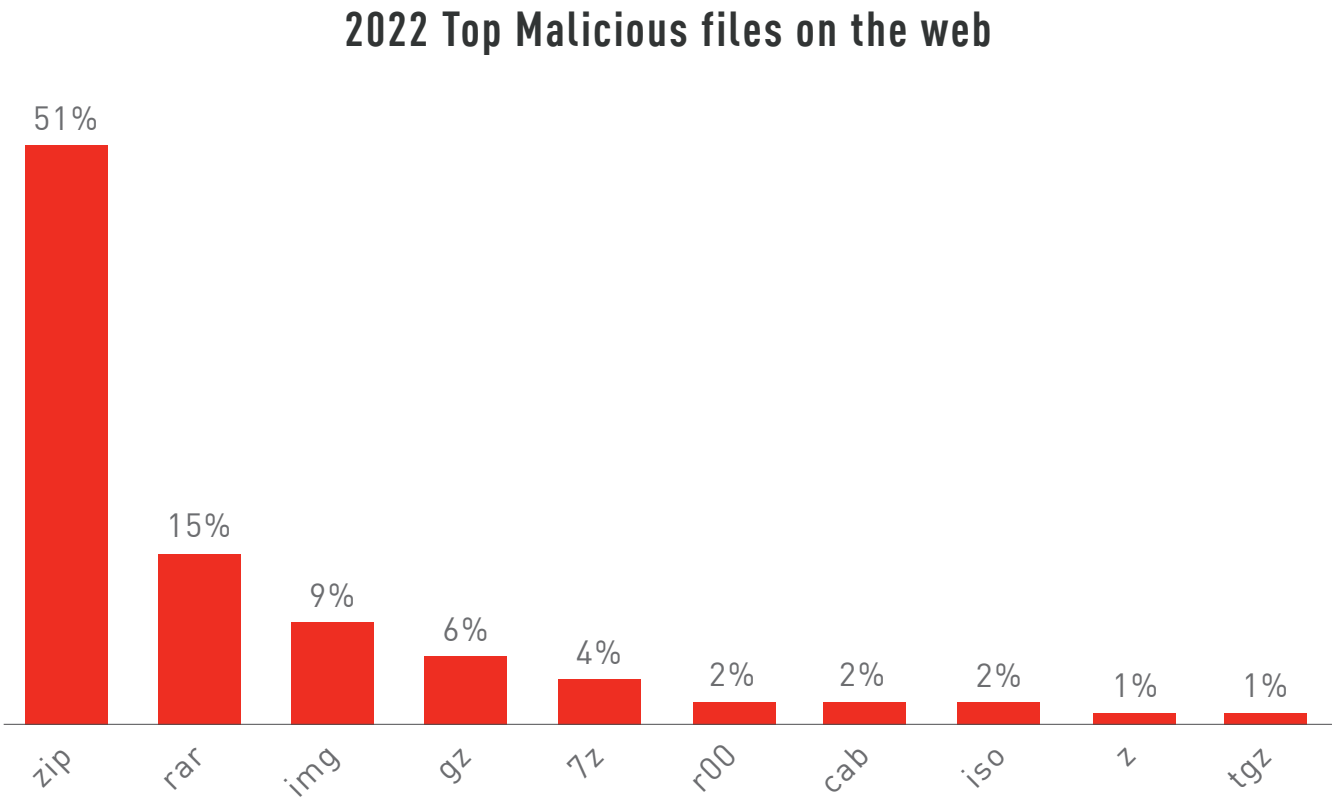
Without the ability to vet malicious websites, as based on reputation intelligence and URL filtering, it can be impossible to prevent employees from accessing malicious sites and unsuspectingly downloading compromised software, files, or programs.

The implications for organizations

More people today use the internet and web-based business applications as their main platforms for work. Unfortunately, this has not gone unnoticed by cybercriminals who are increasingly targeting web users for attack.

As noted in Check Point's 2023 Cyber Security report, Check Point Research scouts the web in real time and identifies 100,000 new malicious websites every day.

This has turned web-based work into one of the biggest threats to security, putting the organization at a greater risk than ever.



Source: Check Point's 2023 Cyber Security Report

Overcoming the Browser Security Challenge

To overcome the browser security challenge, organizations will need to eliminate the gaps in traditional endpoint security and ensure comprehensive, yet non-intrusive, threat prevention directly on the endpoint's browser.

Bridging security gaps

Today's endpoint security does not cover the full breadth of risks, such as employees accidentally downloading zero-day malware, visiting zero-day phishing sites, accessing restricted and non-compliant websites, and reusing corporate passwords for non-business web content.

Overcoming the browser challenge requires endpoint security that is comprehensive.

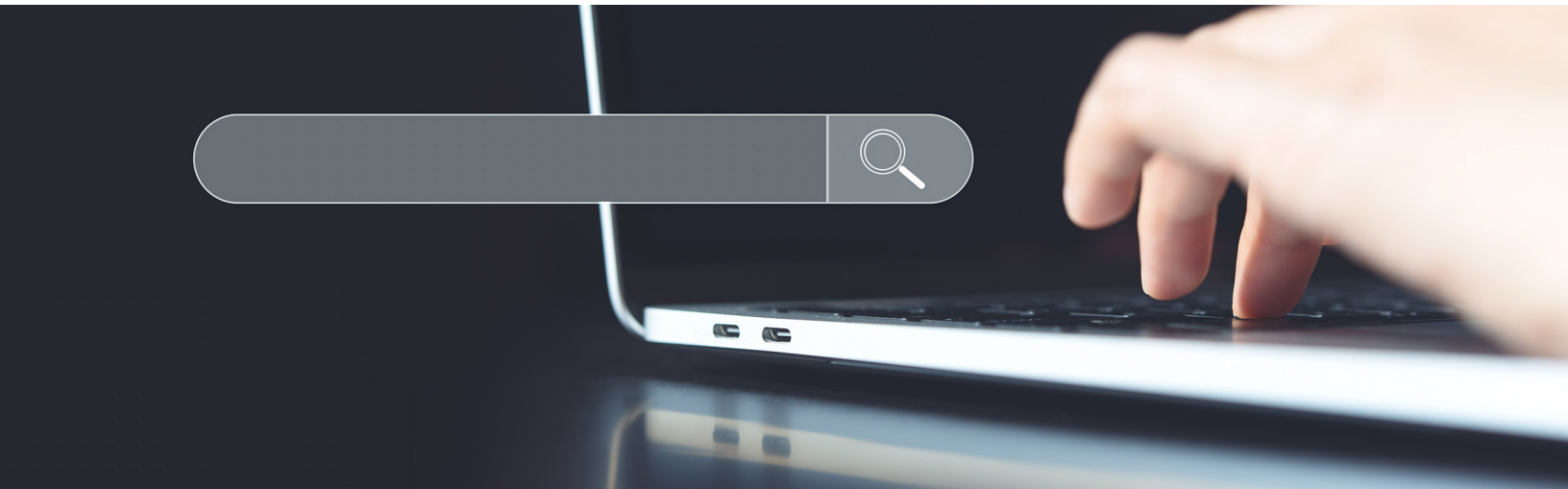
Eliminating the need to reroute traffic

Moreover, many security solutions usually sit in the datacenter as appliances and not on the user's device. This means that internet traffic needs to be rerouted from the endpoint to the datacenter for threat scanning.

Not only does this approach bring a negative impact on browsing speed, disrupting productivity, but many organizations that use such solutions still suffer from phishing frauds or users clicking a malicious download.

To mitigate the risk, organizations need to recalibrate their internet access security approach to avoid routing traffic through a data center.

Instead, protection should be ensured directly from the endpoint's browser.



How Harmony Browse Can Help

Harmony Browse is a modern web security solution that is comprehensive and non-intrusive, bringing the strongest protection against web-based attacks without compromising productivity.

Comprehensive threat prevention

The solution provides web users with the fastest and safest browsing experience while protecting them against all internet-based threats, with:

Comprehensive Threat Prevention for Web Users

Zero-Day hishing Protection	Malicious Download Protection	Malicious File Upload Protection	Password Reuse Protection
Credential Theft Protection	URL Filtering	URL Reputation Classification	Real-time Threat Intelligence

Fast and easy deployment on the browser

The solution is deployed quickly from Check Point's platform as an extension within all major web browsers to all your users, hence speeding up implementation, reducing management overhead, and eliminating complexity.

By inspecting all SSL traffic directly on the endpoint, it eliminates the need to reroute traffic. This unique in-browser endpoint protection means no additional latency nor impact on the user experience.

Powered by ThreatCloud AI

Harmony Browse is powered by ThreatCloud AI, a real-time global threat intelligence platform that monitors networks around the world for emerging threats and vulnerabilities, including zero-day.

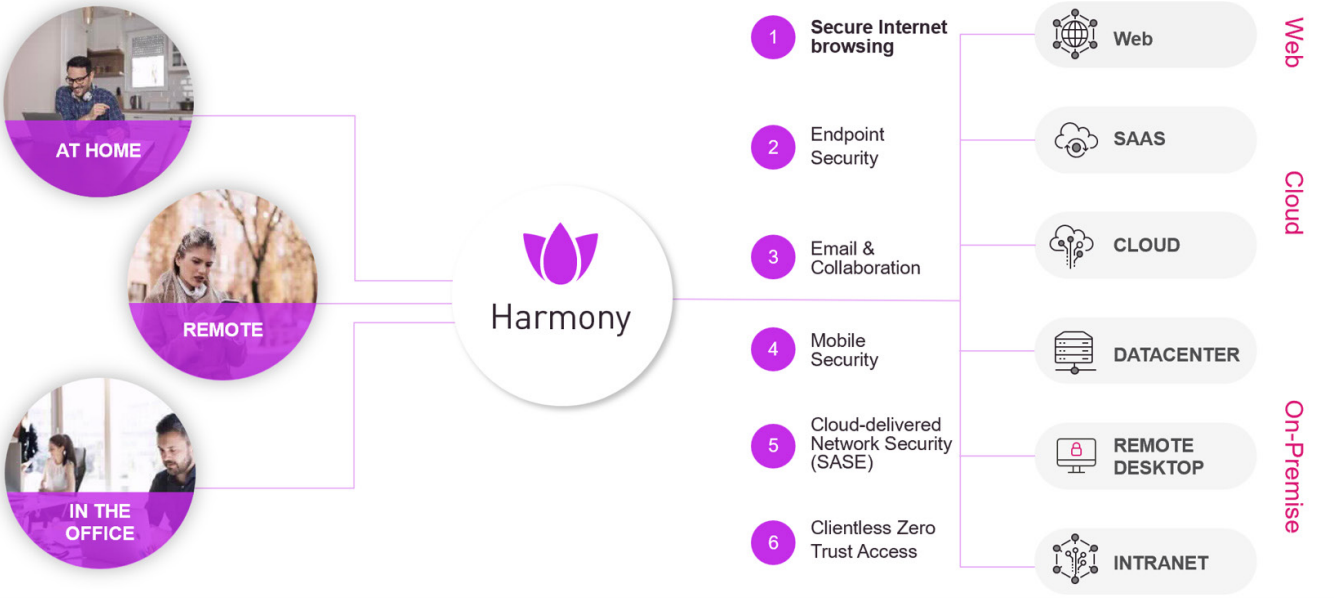
ThreatCloud AI highlights

150,000 connected networks	Millions of endpoint devices	2 million websites and files inspected daily	Dozens of external feeds and crawling the www and social media	Unique Machine Learning algorithms detecting 650,000 suspicious domains daily

Part of the Check Point Harmony Product Suite

Harmony Browse is part of the Check Point Harmony product suite, the industry's first unified security solution for users, devices, and access. It consolidates six products to protect devices and internet connections from the most sophisticated attacks while ensuring zero-trust access to corporate applications, all in a single solution that is easy to use, manage, and buy.

The Harmony Suite: 360 protection for users and organizations



The Harmony Browse difference

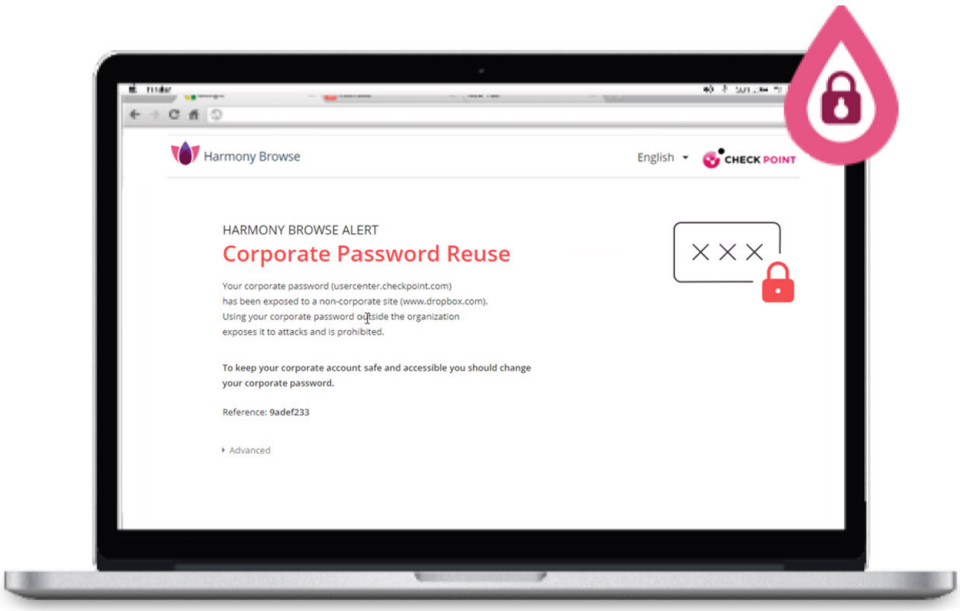
Comprehensive protection	Fast time to value without disruption	Last line of defense
• Centralized security across every browser • Enforcing policies on managed and unmanaged devices • Reducing risk associated with BYOD policies and third parties	• Deployed in seconds from the Check Point Infinity Portal, shared management platform • Seamless integration with Harmony Endpoint and third-party vendors	• AI-powered threat prevention with Check Point global threat intelligence by ThreatCloud AI to prevent existing and zero-day web threats

Bringing 6 Powerful Browser Protections

With comprehensive threat prevention Harmony Browse enables the six drivers of powerful browser protection.

Securing user credentials on the web

Harmony Browse prevents the re-use of corporate passwords and blocks zero-day phishing sites designed to steal user credentials.



Harmony Browse password reuse prevention

By utilizing Check Point's Zero-Phishing® technology it identifies and blocks both known and unknown phishing sites. Sites are inspected within the user's browser, analyzing page visuals, text, domains, and more. If the site is found to be malicious, the user is blocked from entering their credentials.

Credential protection is further bolstered by real-time analysis of threat indicators by ThreatCloud AI. This includes domain reputation, links, IP, and similarity to legitimate web pages.

The result is the broadest phishing protection in the market.

Preventing files from spreading malware

Harmony Browse removes threats in real time from downloaded web content and protects against the upload of advanced threats to the organization's assets.

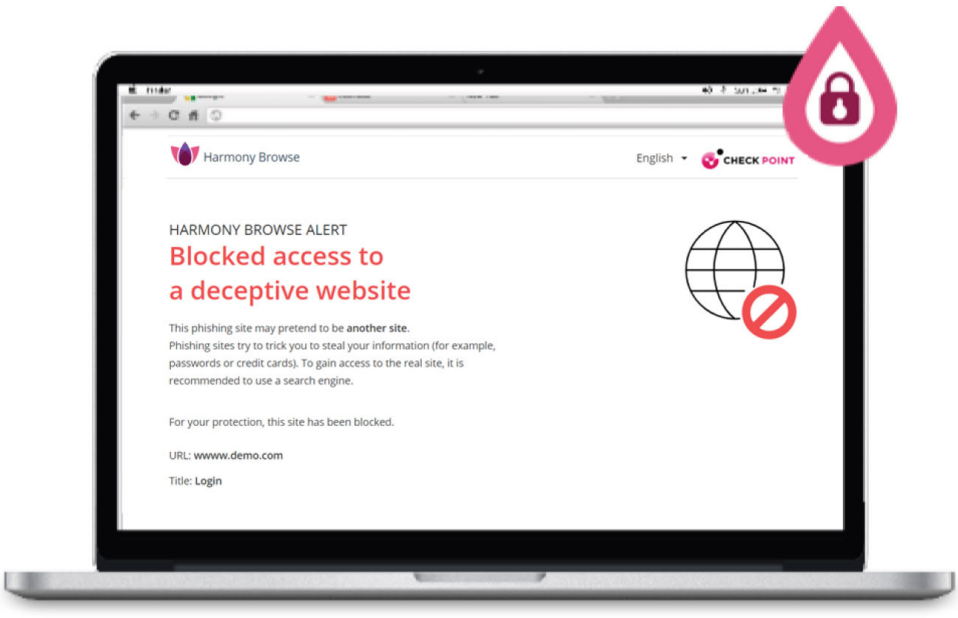
Every file downloaded through a browser is sent to the Threat Emulation® sandbox to inspect for malware. Simultaneously, Check Point's proactive Content Disarm and Reconstruction (CDR) technology, Harmony Threat Extraction®, delivers a sanitized version of the file in milliseconds. Together these technologies block all the NSA's Top 25 CVE.

Harmony Browse also prevents users from unknowingly uploading malicious files or other types of content to the organization's web applications.

Preventing zero-day attacks on web browsers

Reducing the attack surface

Access to malicious websites is restricted by blocking those that are categorized as malicious (e.g., phishing), where internet access policies are enforced as based on simplified policy management and URL filtering.

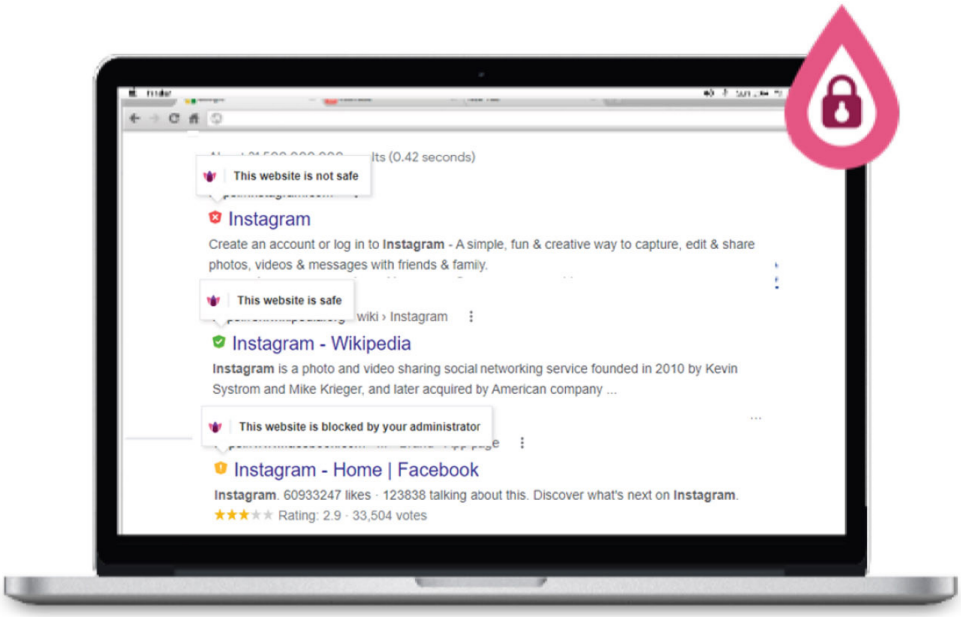


Malicious site protection

With URL filtering, Harmony Browse controls access to millions of websites by category, users, groups, and machines, protecting users from malicious sites and enforcing a safe web browsing experience.

Preventing risky clicks

Website reputation intelligence and URL filtering prevents users from clicking on malicious links or accessing a link blocked by the corporate policy, which is defined by the admin in Harmony Browse.



Preventing risky clicks

When a user performs a search through a search engine, the results will be marked with colored icons: green – safe; red – unsafe; orange – blocked by company policy.

This way, the security ramifications of human error are profoundly reduced.

74% of cybersecurity breaches involve the human element – error, misuse, and social engineering (DBIR 2023)

Securing users working with web apps

Harmony Browse offers browser security for users working primarily from their web browsers, as 85% of the workforce accomplishes their daily tasks on SaaS applications directly from the web browser. Harmony Browse is also suited for the education sector where most users study with a Chromebook. The integration with Google Suite is seamless, increasing protection against zero-day attacks while working with web apps

Protecting corporate devices and BYOD

The solution delivers the last mile of defense with an extra layer of security against phishing and zero-day threats for both company and employee-owned laptops.

In Conclusion

Web browsers today serve as the primary interface between users, an organization, and the internet, making browser security a strategic imperative.

Traditional endpoint security, however, does not cover the complete range of web-born threats, including the most sophisticated attacks such as zero-day phishing and malware downloads. And with the increased rates of such attacks, securing browsers has become a major challenge for the organization's security leaders and teams.

Harmony Browse overcomes the challenge with comprehensive, AI-powered threat prevention for web users, protecting endpoints directly from the browser, bringing simplicity and speed, and avoiding impact on productivity.

Harmony Browse key capabilities and benefits

- Prevents users from visiting zero-day phishing sites, downloading zero-day malware, accessing non-compliant websites, re-using corporate passwords for non-business web content, and more
- Fast web browsing with zero latency by eliminating the need to reroute traffic through the cloud for inspection
- Enforces corporate internet access policies across managed and unmanage devices
- Single management over different platforms and browsers
- Easy to deploy using an innovative extension directly into the browser
- Eliminates the risk from BYOD policies or from third-party contractor network access
- Enforces user data privacy, keeping browsing history private to comply with data privacy regulations

To see how **Check Point Harmony Browse**
can help you ensure protection of your organization's web users
we invite you to book a demo here.

To **learn more**, visit our website.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com