CHECK POINT™

COMPREHENSIVE THREAT PREVENTION FOR WEB USERS

COMPREHENSIVE THREAT PREVENTION FOR WEB USERS

85% of employees work primarily on the web browser, where they easily fall victim to phishing attacks and malware downloads.

Browser security is available as part of Harmony Endpoint. It protects web users from malware, credential loss, and data leakage. It offers an additional security layer to your endpoint solution to enforce corporate internet access policies across managed and unmanaged devices. Your employees are protected from zero-day phishing sites, reusing corporate passwords, and uploading/downloading malicious files.

Threat Prevention
Last line of defense against web-borne attacks

Rapid deployment
Fast time to value without user disruption

Comprehensive Security
Across managed and unmanaged devices

Harmony

Main Capabilities

- Zero-day phishing protection
- URL filtering
- Malicious web protection
- Sandbox
- File sanitization (CDR)
- Corporate password protection

Why Browser Security?

- Secure user credentials on the web
- Enhance your endpoint security with additional web protection
- Prevent files from spreading malware to the organization
- Restrict access to malicious websites
- Prevent risky clicks based on website reputation
- Secure users working with web apps

Our Customers Love Us

Browser security solutions for zero day threats

Harmony Browse is a well rounded web security solution. Using of harmony browse, it has enhance our organization's security by preventing users to fall prey to malicious and phishing website as these would already have been blocked. Harmony Browse capabilities are scanning and emulate the files on browser level. It is able to block 99.9% of the threats.

read more >

IT MANAGER
★★★★★

Gartner
Peer Insights.

Please visit Peer Insights to read and write reviews.
gartner.com/reviews

Gartner Peer Insights. ★★★★ 4.3

Leader PeerSpot ★★★★ 4.5

READ OUR REVIEWS

Learn more about Browser Security or sign up for a free trial