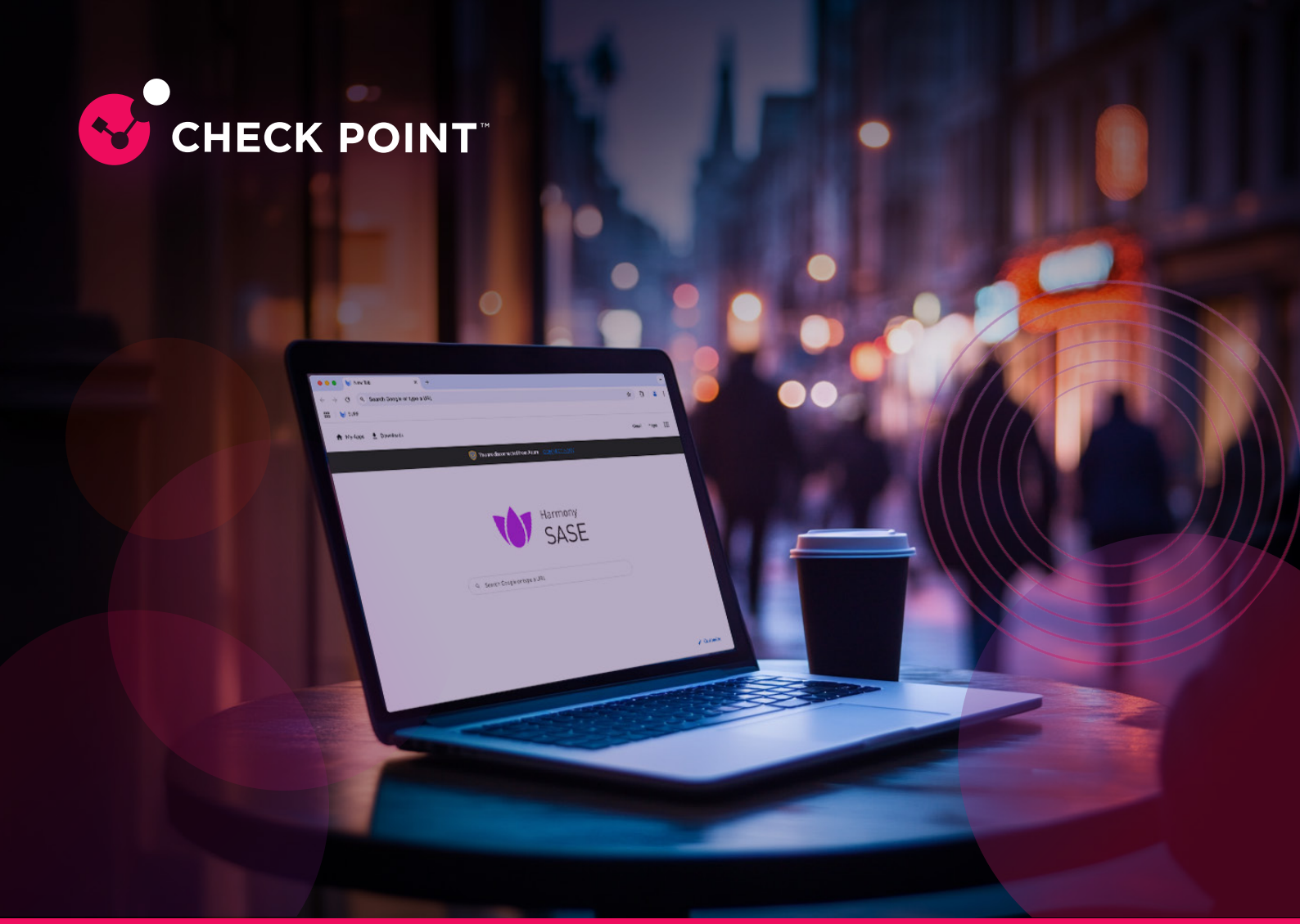
CHECK POINT™



Zero Trust at the Edge:
Securing Unmanaged Devices with the Harmony SASE Enterprise Browser

As the modern enterprise grows more distributed and reliant on contractors and employees with BYOD, unmanaged devices have emerged as a critical security blind spot. Traditional solutions like RBI and legacy VPNs have limitations when it comes to data control, visibility, and device hygiene. Check Point's Harmony SASE Enterprise Browser is purpose-built to fill this gap.

Installed on unmanaged devices, the Chromium-based browser acts as a dissolvable Zero Trust agent. It provides advanced data isolation, posture enforcement, session monitoring, and integrated DLP.

Designed for sensitive use cases such as BYOD, contractors, and temporary workforces, the Enterprise Browser complements Agentless ZTNA by delivering added control where enterprises need it most.

Unmanaged Devices: The Last Security Gap

Whether it's a contractor working from a personal laptop or a full-time employee on BYOD, unmanaged endpoints pose a major security challenge. These devices are a black hole for security visibility. It's difficult to know if they have a working antivirus solution, encryption, or updated OS versions. Any of these issues would make them vulnerable to malware, ransomware, and other advanced threats.

Security teams struggle to enforce corporate policies or gain visibility into what happens on these devices. Allowing sensitive data to flow freely between cloud apps and uncontrolled endpoints is risky, especially in regulated industries where compliance and audits are non-negotiable.

That's where the Harmony SASE Enterprise Browser comes in.

A Secure Browser for the Untrusted Endpoint

Check Point's Harmony SASE Enterprise Browser creates a Zero Trust workspace on unmanaged devices. It is a standalone, secure browser that users download and install like any other application. Once the session ends, all browser data is automatically wiped from the device.

This ephemeral approach aligns with the concept of a "dissolvable agent": a lightweight client that enforces security policies only when needed. By isolating enterprise activity from the rest of the operating system, the browser prevents lateral movement, data leakage, and policy circumvention.

The Enterprise Browser enables remote access with posture checks, session logging, and integrated DLP—all without requiring a persistent agent. It's the ideal solution for securing access with devices you don't own or control.

The browser provides a policy-enforced environment for unmanaged devices, extending security controls to devices the organization doesn't own. IT teams can enforce any ADMX-based Chromium policy within the browser, including disabling password management, casting, and other features to align with corporate security requirements.

Key Capabilities

1. **Strong Data Isolation**
   The browser creates a secure container where enterprise apps and data are kept separate from the underlying OS. This prevents unauthorized transfers of information between corporate and personal environments.
2. **Data Loss Prevention (DLP)**
   Admins can enforce strict controls to prevent:
   - Uploading sensitive data to unauthorized destinations
   - Downloading files to local storage
   - Copy/paste of protected content
   - Printing or screen capturing

   Downloaded files can be encrypted and scanned before access, while on-screen watermarks discourage screen capture by an external device. All of this occurs within the browser, eliminating the need for full endpoint control.

   The browser also blocks the use of password managers and prevents the persistence of passwords, ensuring that user credentials cannot be saved locally or reused maliciously.

3. **Agentless Device Posture Check**
   Before allowing access, the browser checks device posture attributes such as:
   - Antivirus presence
   - Disk encryption status
   - Operating system version
   - Running processes and certificates

   This is done without installing a persistent agent, making it suitable for unmanaged devices.

4. **Full Session Visibility and Auditing**
   The browser records key events, such as:
   - Navigation history
   - Application usage
   - CPU and latency metrics
   - User actions, keystrokes, and session recordings

   These insights support compliance efforts and accelerate incident investigations in the event of a breach.

The Harmony SASE Enterprise Browser enables organizations to apply these visibility features thoughtfully and selectively, based on role, context, or sensitivity of the applications in use. These capabilities are especially valuable when monitoring privileged users or supporting internal governance policies. Session data and logs are designed to support audit and compliance workflows while maintaining administrative control over when and how monitoring is applied.

Additionally, the browser is built to block man-in-the-middle (MITM) attacks, helping to protect web sessions even on insecure networks.

How It Fits in the Harmony SASE Architecture

The Harmony SASE Enterprise Browser connects seamlessly to Agentless ZTNA applications, providing users with a consistent, secure login experience via SSO.

While Agentless ZTNA is ideal for low-risk scenarios, the Enterprise Browser steps in where enhanced control is required. This includes use cases involving contractors, regulated data access, or insider threat concerns.

This layered approach to access control ensures security teams can apply the right level of protection based on risk, context, and device type.

Use Cases: Real-World Security for Untrusted Devices

Third-Party Contractors
Use the browser to grant temporary access without risking data exfiltration. Restrict downloads, monitor user behavior, and kill sessions instantly if necessary.

BYOD in Regulated Environments
Maintain compliance with HIPAA, GDPR, and NIS2 by enforcing data isolation and capturing audit trails on personally owned devices.

Short-Term Projects and M&A
Deploy secure access instantly, without waiting for device provisioning or shipping.

Privileged User Access
Enhance security for developers, admins, or support staff by restricting tool usage and monitoring for abnormal activity.

Why Not Just Agentless ZTNA?

Agentless ZTNA remains a powerful tool for frictionless access-and it's often enough. But for organizations that need tighter control, visibility, and enforcement, the Enterprise Browser adds critical capabilities:

- Isolated browser sessions
- Download restrictions
- Session recording
- Copy/paste blocking

Benefits Across the Enterprise

CISOs gain greater assurance in data protection strategies for untrusted endpoints.

Security Teams can enforce posture-based access and track every user action.

IT Admins gain centralized control over unmanaged endpoints-without needing full device ownership.

BYOD Employees and Contractors enjoy fast, familiar access with minimal disruption.

Securing What You Don't Own

Hybrid work isn't going away, and neither are unmanaged devices. Enterprises need a secure, scalable way to protect data accessed outside their traditional perimeter.

Check Point's Harmony SASE Enterprise Browser offers exactly that: a Zero Trust browsing environment that empowers businesses to embrace BYOD and third-party access without compromising security. Paired with Agentless ZTNA and the broader Harmony SASE solution, it provides the flexibility and protection modern enterprises require.

Discover how Check Point Harmony SASE and our Enterprise Browser can transform your BYOD and third-party security strategy.

Talk to an Expert

