Check Point SASE:

Triple Threat Protection for the New Perimeter

The modern enterprise faces numerous challenges to network security. Company data and other resources are now served via the cloud, SaaS is replacing on-device applications, the browser is replacing dedicated clients, and the workforce is more distributed than ever before.

Securing the modern corporate network requires a new approach that goes beyond the traditional perimeter: This is the promise of Secure Access Service Edge (SASE). Instead of securing offices, SASE secures individual users, and access on an application-by-application basis. This new approach allows for even more granular security than is typical for traditional deployments.

SASE has robust capabilities for inspecting user traffic for threats. It also uses a zero trust approach for access requests that is context aware and goes beyond a simple username and password.

However, most SASE solutions, while providing a high level of security, lack visibility into the browser, which for most employees is their window into the corporate network and the wider world.

Business-critical applications were either built for the web as a Software as a Service platform (e.g. Google Docs, Salesforce, Asana), or provide a web alternative to the desktop application (e.g. Office 365, WebEx, and Adobe Creative Cloud).

That's why the vast majority of people rely on the browser for their everyday work activities. Whether it's writing a memo, creating a slide deck, managing the customer database, or carrying out research, the browser is at the center of modern work.

From a single interface, you can move between tasks, collaborate in real-time, and manage workflows without needing to switch between applications. This seamless experience has been a key factor in the widespread adoption of remote work, where the browser serves as the bridge between remote workers and their corporate resources.

This advance in productivity and flexibility brings with it some serious challenges to network security. The browser is, by design, built to execute code from numerous sources at once. This is what provides us with capable web apps and rich user experiences, but threat actors can also use it as an entry point into your network.

Temporary web page file downloads, third-party ads, or a document embedded with malware are all potential attack vectors.

To combat these threats, SASE requires built-in browser security. Desktop agents monitoring network traffic, network appliances governing a network, or cloud-based inspection points can easily miss advanced and well-crafted threats directed at the browser.

Introducing H_3 SASE: Check Point's Hybrid Triple-Layer Solution

Check Point SASE's hybrid approach closes the gap for network threats with inspection elements in the browser, the network, and the cloud. Whether your team is connecting to company resources, browsing the web, or accessing cloud applications, they are protected from emerging threats at each touchpoint.

It starts with the desktop agent, our primary window into the company network. Residing on the device, the desktop agent is packed with threat prevention capabilities to ensure threats don't get through such as ransomware, keyloggers, and zero-day threats.

Next, we have inspection points in the cloud with our network of more than 70 (and growing) points-of-presence (PoPs) around the world. These global PoPs enable fast, secure connections to cloud applications, SaaS, and on-premises resources with built-in security to prevent malicious actors and threats from entering the network.

Finally, we have in-browser security with a multitude of threat prevention and data loss prevention measures. Check Point SASE browser security provides admin teams with visibility into the browser and is powered by Check Point's ThreatCloud AI.

The brains behind all of Check Point's products, ThreatCloud combines the latest AI technologies with big data threat intelligence to identify and prevent attacks. ThreatCloud aggregates and analyzes big data telemetry and millions of Indicators of compromise (IoCs) every day making over 2 billion security decisions daily. The result is the fastest block rate in the industry for known and unknown threats, with near-zero positives.

The H_3 SASE Advantage

- **Hybrid architecture** provides greater flexibility with security in the desktop agent, the cloud, and the browser
- **2X Faster** secure Internet access means your workforce isn't slowed down by poor connection speeds
- **Full mesh networking** allows you to customize Check Point SASE to your needs with any-to-any connections including users to resources, and resources to resources
- **Unified solution** that's built right into the Check Point Infinity Portal alongside the rest of your Check Point deployment

Advanced Browser Security Features

- **Clipboard Control** monitors user actions and prevents sensitive data from being copied and pasted to generative AI services such as ChatGPT, Claude, and Copilot
- **Safe search** ensures the browser's safe search feature is active to filter our problematic content from search results
- **Safe search results ratings** inform users whether the sites that appear in their search results are considered safe based on ThreatCloud data
- **Corporate password protection** prevents the workforce from reusing the same passwords they use at work on other sites thereby reducing the chances of those passwords being exposed in a data breach

Browser security fits into your current workflow with no interruptions or requirements to replace their current browsers. It's also adaptable to managed and unmanaged devices, meaning you can distribute it to employees, as well as third-party contractors handling company data in the browser.

Using these three layers, Check Point's H_3 SASE approach enhances a company's security posture with visibility into user traffic at three different points. This can also help improve regulatory compliance, and it enables your team to manage and monitor network security from a unified dashboard, Check Point's Infinity Portal.

The H_3 SASE approach is flexible enough to suit multiple use cases for employees, BYOD employees, and third-party contractors. Both BYOD and contractors, for example, use unmanaged devices to interact with your environment.

You can give them access to the company resources they need such as access to a building system or a particular server via Agentless Zero Trust Network Access. This functions as a dedicated web portal where anyone using an unmanaged device can login, access the application they need without having greater access to the network.

In addition, unmanaged devices can be protected by adding browser security to ensure DLP standards are maintained, and that users remain secure while accessing company data.

Managed devices, meanwhile, receive more complete security with monitoring at all three security touch points. This means greater access to company resources based on Zero Trust Access rules, faster connection speeds over our private global backbone, cloud and on-device options for Internet security, among other benefits.

Check Point SASE also grows with your company. Since it's cloud delivered, Check Point's SASE can scale up on demand as needed when your workforce expands. A cloud-based solution also means you automatically gain access to new features as they're released, and with ThreatCloud AI powering your threat protection you always have the latest threat intelligence securing your network.

Discover how Check Point's H_3 SASE can secure your network.

Book a Demo

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