CHECK POINT | netskope



Extending Zero Trust from the device to the application

Check Point Mobile Security + Netskope One SASE

Executive Summary

Mobile devices are now a primary path into corporate SaaS and private applications. Yet they remain the least visible endpoint in most Zero Trust architectures. Netskope secures how users connect. Check Point Mobile Security decides if their device is safe enough to connect at all.

Together, the two products close the mobile blind spot. Unprotected, risky, and compromised devices stay out. Trusted users, on managed or bring-your-own-device (BYOD) phones, get secure access to the tools they need.

The Challenge

- **Secure access service edge (SASE) and Zero Trust Network Access (ZTNA) platforms** authenticate the user and secure the access but have little insight into whether the device itself is compromised.
- **Mobile risk is dynamic**—a device can become risky minutes after it gets access.
- **Console and app sprawl**—teams stitch together mobile threat defense (MTD), unified endpoint management (UEM), and SASE tools. This slows response and puts multiple apps and VPNs on the same devices.
- **BYOD and unmanaged devices** fall outside the mobile device management (MDM) and UEM signals that most SASE platforms rely on.

The Joint Solution

Check Point's on-device detection engine pairs with the Netskope One SASE access control plane. Mobile risk telemetry decides, in real time, if a session to SaaS or private on-premises resources is allowed, restricted, or blocked.

A minor issue may still permit access to a low-sensitivity app. The same issue on a high-sensitivity system automatically triggers a restriction or a full block, with no manual action.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

How The Integration Works

- **Detect.** Check Point Mobile Security continuously evaluates device, app, and network posture with its Behavioral Risk Engine and ThreatCloud AI intelligence.
- **Define policy by sensitivity.** Security teams set posture requirements per resource, user group, or data classification—not one fleet-wide threshold.
- **Evaluate.** Each access attempt gets a verdict for that specific resource: allow, restrict, or block.
- **Prevent.** Netskope combines the Check Point device posture verdict with identity, location, and data sensitivity. Then it applies the matching ZTNA, cloud access security broker (CASB), or secure web gateway (SWG) action.
- **Remediate.** The app guides users to fix the issue, for example to remove a malicious app or reconnect on a trusted network. Access returns automatically when the device meets the posture requirement.

One App, Split-Tunnel Routing

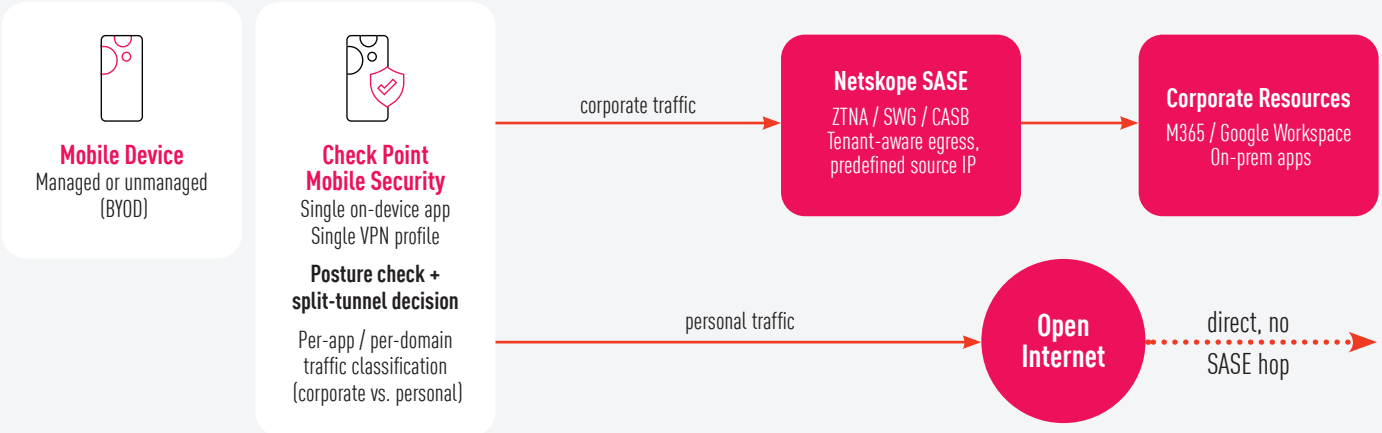
A single on-device app handles posture assessment, conditional access, app vetting, and active protection against phishing, malware, and network threats. The same app routes corporate traffic to Netskope One SASE over certificate-based mutual TLS (mTLS), and Netskope applies access policy.

One app for end users. Less work for IT. No separate MTD and SASE clients to manage.

Only corporate traffic, to SaaS and private on-premises systems, goes through Netskope. Personal traffic goes straight to the internet: better privacy, lower cost, one VPN profile.

Split-tunnel routing: corporate traffic to Netskope One SASE, personal traffic direct to the internet.

Split-Tunnel Routing: One VPN, Two Destinations



Only corporate-destined traffic traverses Netskope SASE.
Personal traffic (social media, streaming, personal browsing) goes straight to the internet—preserving user privacy and experience, reducing SASE infrastructure load and cost, and keeping a single VPN profile for simple, centralized device management.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Key Use Cases

- **Secure BYOD access to SaaS.** Access to sanctioned apps, controlled in real time by on-device risk.
- **Stable source IP for allow-listing.** A consistent egress point lets organizations enforce Microsoft 365 and Google Workspace IP allow lists for managed and BYOD devices alike.
- **Risk-aware access to private apps.** ZTNA sessions depend on device trust, which keeps compromised phones off sensitive systems.
- **Network-attack containment.** A detected man-in-the-middle (MitM) attack or rogue access point automatically restricts that device's sessions until the threat clears.

Business Value

Closes the mobile visibility gap. Brings Check Point mobile threat detection into your SASE architecture.

True Zero Trust, continuously verified. Access reflects current device risk, not a one-time compliance check.

Extends coverage to BYOD. Risk detection runs on the device, managed or not. On managed devices, UEM installs the access certificate automatically. On personal devices, users can install it manually.

Real-time response. Enforcement follows detection automatically, which shortens the time between compromise and containment.

Why Check Point and Netskope

Check Point brings deep on-device detection of app risk, OS exploits, and network attacks, with access policy set for each resource, not for the whole fleet. Netskope brings Netskope One SASE, with consistent policy across SaaS and private apps. Together: one Zero Trust outcome, from device to application.

Next Steps

Do you use Netskope One SASE and need to close the mobile risk gap, especially on BYOD and unmanaged devices? Contact the Check Point and Netskope teams. Together, we scope a proof of concept, validate the workflow, and define the right access actions for your mobile fleet.

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

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

© 2026 Check Point Software Technologies Ltd. All rights reserved.