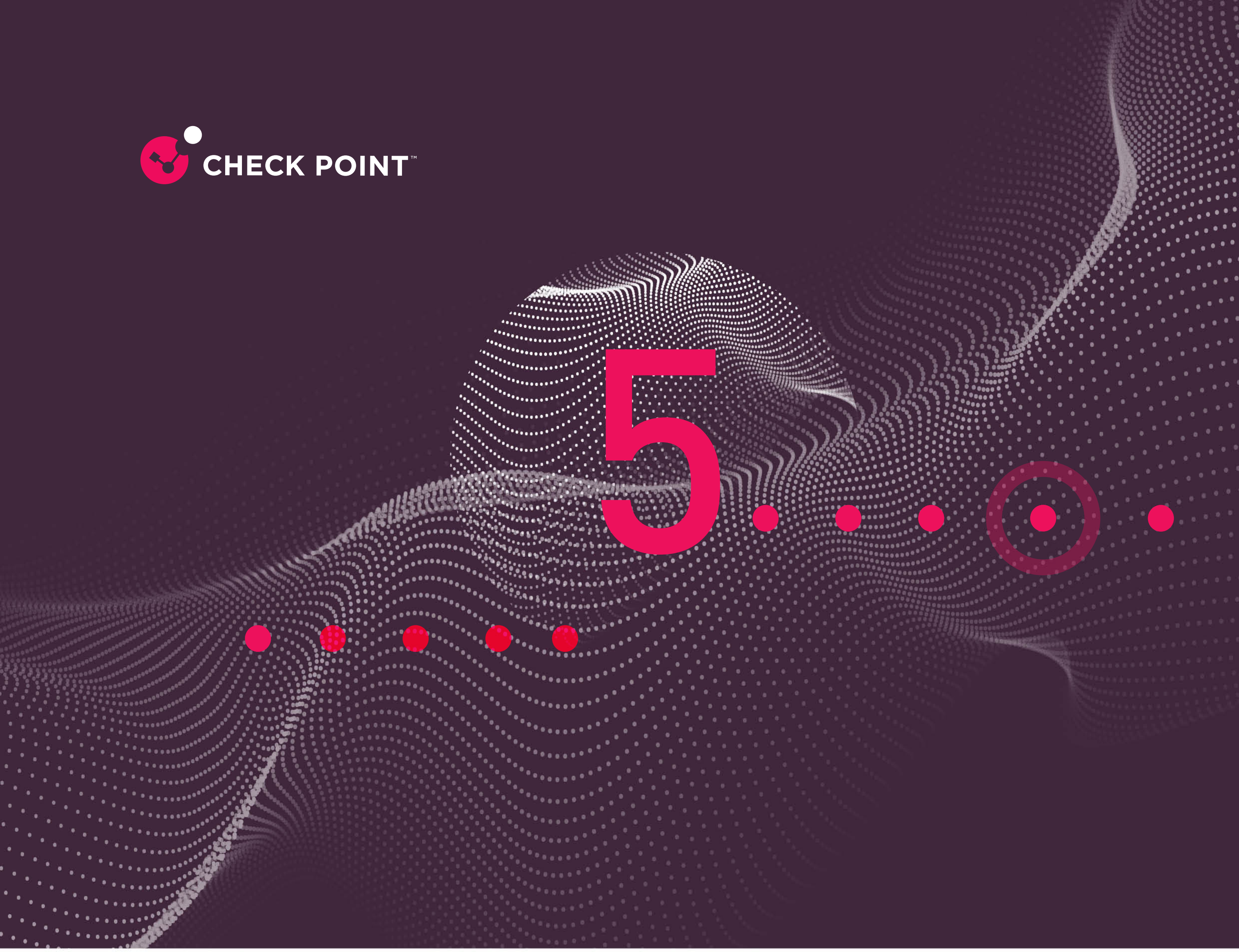

CHECK POINT™

5 STEPS TO STREAMLINE SECURITY **FOR YOUR HYBRID NETWORK**

Build unified security across your services and locations

Many organizations have embraced the shift to a hybrid work model with users connecting from both on-prem and remote locations. From the user's perspective, they just want access to the tools they need to get their work done. It's immaterial whether a resource is SaaS-based, in a public cloud, or in a company-controlled data center.

For the IT team, however, the hybrid network creates myriad challenges as new users, devices, apps, and cloud environments come online. You can almost hear IT and security leaders cringe as they consider building a towering security stack to contend with a seemingly endless attack surface.

If this scenario hits close to home, you're not alone. It's increasingly common for organizations to get caught in the network complexity trap where the IT team struggles to::

- Provide users easy access to the information and resources they need
- Maintain control over users and devices
- Manage an expanding set of SaaS apps and cloud environments
- Ensure that the network is protected against unauthorized access and internet-borne threats like malware

Seeking Security Simplicity

It is not feasible to address these challenges efficiently with a stack of security tools. Even if you had the budget, you would also need a small army of expensive security operators. In the real world, most IT teams are battling persistent staffing shortages and budgetary constraints.

Clearly, today's hybrid networks require a streamlined security approach, where a small team can maintain control of the network and its users and defend against internet threats while consolidating control into as few interfaces as possible.

With that in mind, here are five useful steps to help you address the challenge head-on by streamlining your security.

1. Build a Zero Trust Security Policy

Adopting a Zero Trust model based on least-privilege is a great way to start streamlining your network security. It immediately reduces the attack surface by limiting access to resources based on role, device, and other identifiers. Using an Identity Provider (IdP) as part of this model simplifies things further. IdPs let you condition access to the network based on a simple Single Sign-On (SSO) process, giving admins the ability to automatically identify the employee behind a connection and enforce access and other security policies for each user and role.

Even better, integrating your network security solution with a SAML 2.0 IdP makes it easy to obtain visibility, as well as control access and traffic between any object, service, address, or user on the network. This unified model can also more seamlessly adapt to the nuances of a hybrid workforce with various devices, locations, and time zones.

2. Consolidate Control of Networking and Security

Managing security control for on-premises environments and users is relatively simple for administrators; however, the hybrid network is significantly more complex, incorporating multiple cloud environments and workers connecting from a range of locations and devices.

This demands a flexible, secure network infrastructure that is easy for the IT team to manage. While they were a mainstay for years, standalone VPNs – even those labeled as business solutions – are no longer up to the task, as they suffer from issues related to backhauling and constant updates. Encrypted connections are still a must, but the network must also deliver high speeds and reliability to remote teams.

While the networking part of the equation is straightforward enough, adding robust security and applying it to all users, devices, and connected environments raises the degree of difficulty a couple of notches. It requires combining all the disparate pieces – the associated ports, addresses, and protocols – to create a coordinated solution.

Modern, cloud-based networking solutions can help admins implement the type of user-centric, segmented approach necessary for easily manageable hybrid security. These solutions can connect all network resources and enable application-by-application granular access. This makes it easy to give any user access only to the specific resources they need for their role.

3. Find the Easy Wins

Streamlining security should entail identifying opportunities to boost your protection quickly and easily – and inexpensively. Opt for tools that cover multiple security controls and require minimal – or zero – ongoing maintenance.

Adding extra layers of security including 2-factor authentication and allowlisting is always a safe bet. While these tools are simple and easy to deploy, it's crucial to do it the right way. With a standalone VPN, manipulating settings to account for network nuances, regions, policies, and more is nearly impossible. It's much more practical to establish site-to-site encrypted connections that only accept traffic from authorized IP addresses.

Holistic security tools make it easy to establish and enforce security configurations on users and groups across the network, using a unified management console. For example, admins can mandate that contractors accessing a certain application must authenticate multiple times and can only access during their work hours. Or an encrypted connection can be required when a user tries to gain access via an unfamiliar Wi-Fi connection. Such tools also make it possible to remove barriers for trusted users on managed devices and familiar networks.

4. Implement it Fast

Even when an organization has identified an optimal solution for networking and security, a potential showstopper still remains: implementation. That process can be derailed by overly complex technologies, difficulties integrating the solution with existing network infrastructure and systems, and challenges ensuring that the solution can scale effectively as the organization grows.

This is the time to lean heavily on your security vendor and confirm that your expectations are in alignment. Any prolonged delays at this point can send the project down a dead-end path where it's ultimately scrapped.

Your vendor should be committed to helping you achieve value quickly and transforming your network security. This is where selecting a robust, yet lightweight converged network and security solution from a trusted vendor will pay off. It can be up and running in a fraction of the time of traditional tools, while offering better security and a streamlined user experience.

5. Unify and Monitor

Data on hybrid networks can be transmitted from resources located anywhere in the world. So holistic monitoring and data capture across all data flows is a must.

Pulling data streams together into a single view gives administrators real-time visibility into user activity and behavior and simplifies logging and analysis. Authentication, access, group and server creation, team member activity, password changes and more combine to paint the overall network security picture.

Aggregating and correlating events from across the network into SIEM visualization and analysis tools allow admins to see who accessed the network and from where, track activity, generate reports, and ensure effective security enforcement. This amplifies the effectiveness of SIEM solutions such as Microsoft Sentinel, Splunk, and others.and time zones.

Complete the checklist with Harmony SASE

Today's hybrid workforce requires fast, easy, and secure connectivity to corporate resources without any hassles. This is exactly what Harmony SASE delivers!

Instead of attempting to sync multiple solutions together, Harmony SASE provides an intuitive, converged networking and security solution that delivers fast, encrypted connections and Zero Trust access policies for users anywhere in the world.

By consolidating multiple security capabilities and providing management and monitoring from a single-pane-of-glass console, Harmony SASE streamlines security for your hybrid network.

Harmony
SASE

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