ESSENTIAL NETWORK SECURITY: A COMPREHENSIVE CHECKLIST

The threat landscape for enterprise security is always changing and requires constant adaptation. The latest evolutionary demands for corporate networks include the cloud and remote work—environments where the old hub-and-spoke approach is less than ideal.

Cloud-based network security is purpose-built to secure resources wherever they reside.

> "There are multiple business benefits when using a cloud-based network security solution."

Cloud-Based Network Security in Brief

Zero Trust Security

Zero Trust means only permitting access to those who require it and continually verifying that each person is meeting pre-determined access policies. Zero Trust Network Access (ZTNA) secures company resources at the application level employing standard logins and MFA authorization, as well as at the device level utilizing posture checks, and context-based permissions such as time of day and location.

FWaaS

Firewall-as-a-Service works with ZTNA to prevent anyone from accessing resources without an authorized identity such as a specific user, group, or originating IP address. Just like on-premises firewalls, FWaaS defends against unwanted entry into company resources and networks.

SWG

A Secure Web Gateway (SWG) protects company employees while web browsing. It prevents outbound traffic from accessing restricted content such as gambling sites, as well as known or suspected malicious file destinations. It also scans inbound traffic for malicious web content.

High-performance connectivity

A network security solution should be responsive and provide a smooth user experience. To enable this, the solution should ideally be cloud-based with points-of-presence (PoPs) distributed throughout the globe. Companies can then choose PoPs in locations near their employees, for better responsiveness and connectivity rather than backhauling traffic through physical data centers.

Network Security Checklist

1. Map Your Network's Architecture (user devices, on-prem services and appliances, cloud services, etc.)
2. Assess Your Needs (VPN replacement, cloud firewall, Zero Trust solutions, DNS filtering, device posture check, etc.)
3. Enable SSO With MFA
4. Define Group Access Policies
5. Define Compliance Needs
6. Research Solutions Based on Assessments Above

The Checklist Explained

Map Your Network's Architecture

The first thing you need to do is assess what your corporate infrastructure looks like, be it as a list or a diagram. It's important to understand your on-premises needs such as the number of data centers your company has.

Also include all the cloud services the company uses—at least the ones you know about. Again, try to be as exhaustive as possible, not forgetting about that one Heroku app that DevOps is using.

Then it's on to endpoints. What kind of devices are your remote employees using? Is it all company-owned Macs, a mix of Windows and Mac, what about phones or tablets that might be used to access company resources? Also consider BYOD devices and what employees are currently using those for.

Locations are also a key part of assessing your needs since this will help determine the optimal PoPs to connect to.

Assess Your Needs

Next, it's time to consider what we're trying to accomplish with the move to a cloud-based network security provider. Is it purely a VPN replacement with better latency for employees spread out across multiple locations? Do you want to boost security with a modern Zero Trust approach that includes more restrictive permissions instead of providing carte blanche access to the network and resources?

What about adding a SWG for secure web access and malware protection, as well as logging activity for incident response purposes? Do you need static IPs, or access control at the DNS level?

All of these issues need to be taken into consideration. If you're moving to a cloud-based network security model from the traditional hub-and-spoke approach then we strongly recommend adopting a zero trust model. This includes Zero Trust Network Access (ZTNA) for company devices, as well as an agentless option for unmanaged devices and third-party access such as by contractors.

Enable SSO with MFA

Using an identity provider (IdP) with single sign-on (SSO) support and multi-factor authentication (MFA) is highly recommended when moving to a converged network security solution. An SSO IdP provides a better user experience that avoids the need to perform multiple logins every day. It also makes it much easier to gain visibility over logins and to group users for Zero Trust access purposes.

If you have your own homegrown identity management system then look for services that support the System for Cross-domain Management (SCIM) specification. If your company uses multiple providers, support for Security Assertion Markup Language (SAML) 2.0 is also a must.

Define Group Access Policies

Once you have your identity provider worked out and implemented it's important to consider user group permissions for your future Zero Trust Network Access approach. Sales and marketing may need access to Salesforce, for example, but those departments don't need access to the codebase on GitHub, or the production database for the website. These kinds of finely segmented permissions make it easier to control who has access to what, and limit the impacts of a breach should the worst happen.

Define Compliance Needs

Compliance is a key concern for any business that works in sensitive industries like healthcare, or a company doing business in Europe that must comply with local laws.

Even if you know your compliance requirements well, listing them all (ISO 27001 & 27002, HIPAA, GDPR) is a key step before looking at any service provider.

Research Solutions Based on Assessments Above

Once you've got everything figured out in terms of infrastructure, needs and goals, and compliance requirements, you have an excellent list to take with you during product research.

There are many different options to consider here as well. Do you want a full Software-as-a-Service (SaaS) or Network-as-a-Service (NaaS) platform where all deployment is taken care of by the service provider, or do you want something more DIY and customizable?

Most companies want a service that reduces the burden on their IT teams so they can spend more time monitoring for threats, and assisting end users.

Nevertheless, there are cloud solutions that require more manual deployment; however, these companies tend to be pure cloud VPN or Zero Trust solutions without additional components such as cloud firewalls and secure web gateways–key factors for a complete cloud-based network security solution.

Check Point Harmony SASE Checks All the Boxes

Check Point Harmony SASE is a full-featured, cloud-based network security solution that can help segment your resources, and keep your employees and data secure. Our ZTNA solution allows companies to continually verify that employees are meeting authentication standards for accessing company resources with DPC and context-based checks.

The platform also supports the major single sign-on identity providers including Google, Jumpcloud, Microsoft's Azure Active Directory, Okta, and OneLogin. There is also SCIM support for those with homegrown SSOs, and SAML 2.0 for companies that use multiple providers. Check Point Harmony SASE's platform can help you meet compliance burdens for ISO 27001 and 27002, HIPAA, SOC 2 Type 2, and the GDPR. Finally, the Check Point Harmony SASE platform can build a network for your company in minutes and have you up and running in just a few hours, depending on company size.

"Check Point Harmony SASE's full-featured, cloud-based network security solution checks all the boxes."

What Cloud-native Network Security Can Do for Your Business

There are multiple business benefits when using a cloud-based network security solution. It's fast to deploy since there is no hardware burden for your internal team. Deployment is just a matter of choosing the best PoP locations for your cloud network and connecting your services.

There are also significant cost savings since a cloud-native solution helps you do away with expensive appliances such as SD-Wan, VPN, and branch office firewalls. The reduction of hardware also relieves your team of significant maintenance time for urgent security patches, operating system upgrades, and, in some cases, malware signature updates.

There's also no need to worry about oversubscribing with Check Point Harmony SASE since you only need to purchase the number of seats you need. Then as the needs of the business grow you can expand your requirements at the click of a button. Compare that to the legacy approach where "forklift upgrades" to more costly machines with greater capacity are the norm.

Reaching Internal Consensus

If there are other stakeholders that need to get onboard with your move to cloud-native network security we suggest showing them what the day-to-day benefits will look like from tools such as ZTNA (our ZTNA datasheet can help you there).

Another option is to show a scenario of what a potential breach would look like without a cloud-native network security approach versus having one in place. Imagine a hacker obtaining employee login credentials from a marketing employee, for example, and how they wouldn't be able to use that login to break into the codebase or HR records–or gain access at all if location and time-of-day contexts are used.

Contact us today to set-up a demo to see the Check Point Harmony SASE platform in action, or start building your secure network right away via our intuitive dashboard.

Meet Check Point Harmony SASE

2x Faster Internet Security | Zero Trust Access | SD-WAN

The internet is the new corporate network, leading organizations to transition to SASE. However current solutions break the user experience with slow connections and complex management.

Offering a game changing alternative, Check Point Harmony SASE delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud-delivered network protections, Check Point Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

CHECK POINT | Harmony SASE