ESG SHOWCASE

A Guide to Adopting Secure Access Service Edge Network Security

Date: March 2021 **Author:** John Grady, Senior Analyst

ABSTRACT: The shift to cloud and remote work has been massively accelerated over the last year due to global events, forcing organizations to rethink their approach to network security. As a result, secure access services edge, or SASE, has seen significant interest as a means to converge previously disparate security controls, centralize management, and push enforcement to the edge to more efficiently secure today's distributed enterprise environment. Check Point's Harmony Connect delivers on the SASE vision by unifying management and threat visibility across a range of security tools, protecting both users and applications from known and unknown threats regardless of location, and delivering a user-centric approach to security.

Siloed Network Security Tools Cannot Meet the Needs of the Distributed Enterprise

Unsurprisingly, ESG research has found that 64% of cybersecurity professionals believe that network security at the edge has become more difficult over the last two years.[1] Why is this unsurprising? The fundamental design of enterprise networks has become inverted, with users and applications increasingly residing outside of corporate offices and data centers. While this trend is not new, the pandemic has hastened not only the shift to remote work, but also cloud migration to support greater resiliency, flexibility, and agility. Organizations attempting to use existing security tools to address this new paradigm have experienced a variety of challenges, as exhibited by the strong majority indicating network security has become more difficult. Specifically, ESG's research respondents called out the following challenges with regard to network security at the edge (see Figure 1):[2]

- The sophisticated threat landscape. The difficulty in keeping up with the wide range of known and unknown threats has only increased. Attackers continue to adjust their tactics to remain a step ahead of defenders, and the rise of COVID-related attacks, especially those using ransomware and phishing, is a good example of this.

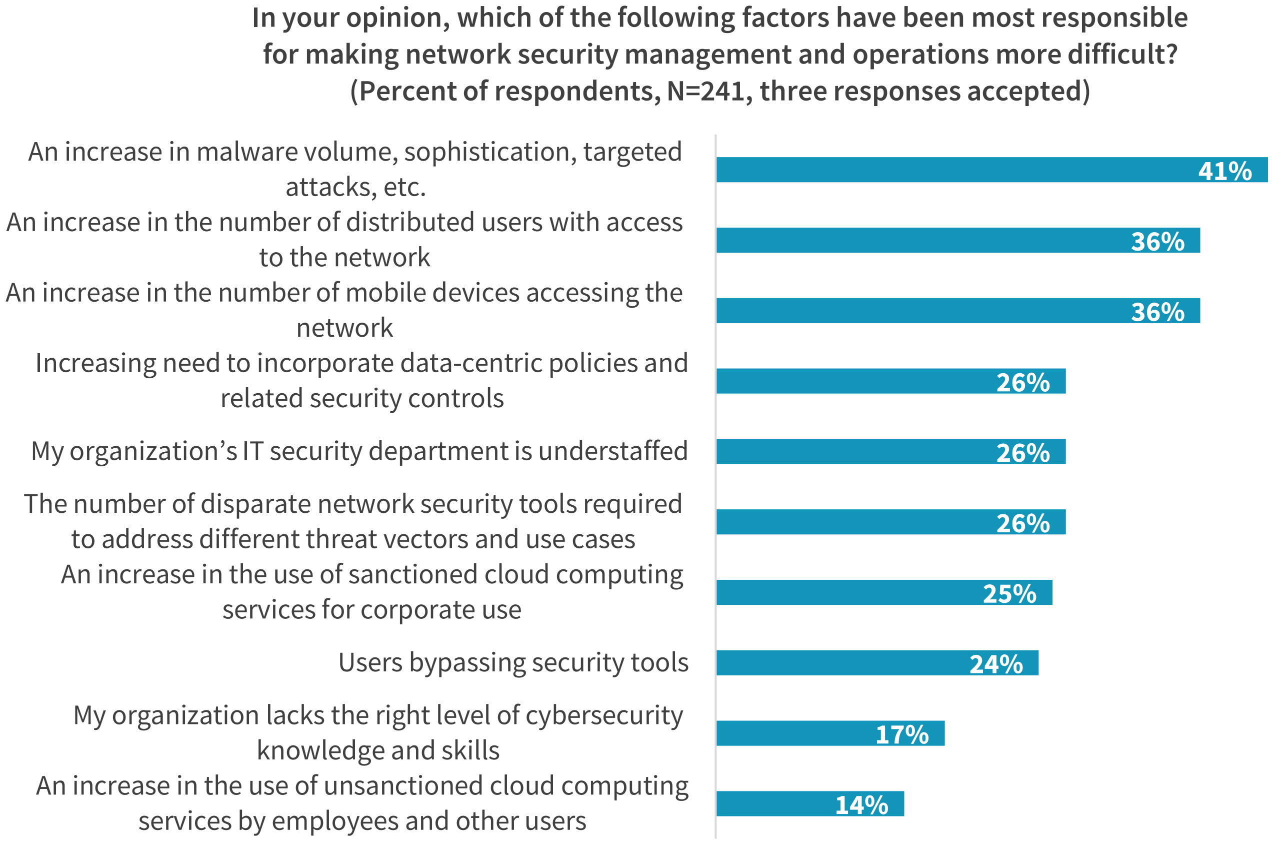
- Network complexity. The increase in cloud usage, remote work, the number and types of devices connecting to the network, and direct internet access for branches and remote users have all made providing consistent security across the entire enterprise environment more difficult than ever. This complexity affects not only security, but also performance, as existing security architectures were not built with the distributed enterprise in mind and are predicated on hairpinning traffic back through the on-premises security stack.

[1] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.
[2] Ibid.

- Inefficient and ineffective tools. Deploying and managing different tools for different threat vectors and locations is not only costly, but also difficult to manage and can ultimately lead to security issues due to policy inconsistency and siloed visibility.

- Resource constraints. On top of all these technology issues, many organizations continue to make do with understaffed, underskilled, and underfunded security teams. When coupled with more threats, increased complexity, and ineffective tools, it should come as no surprise that we have reached a tipping point.

Figure 1. Challenges Securing the Evolving Perimeter



Source: Enterprise Strategy Group

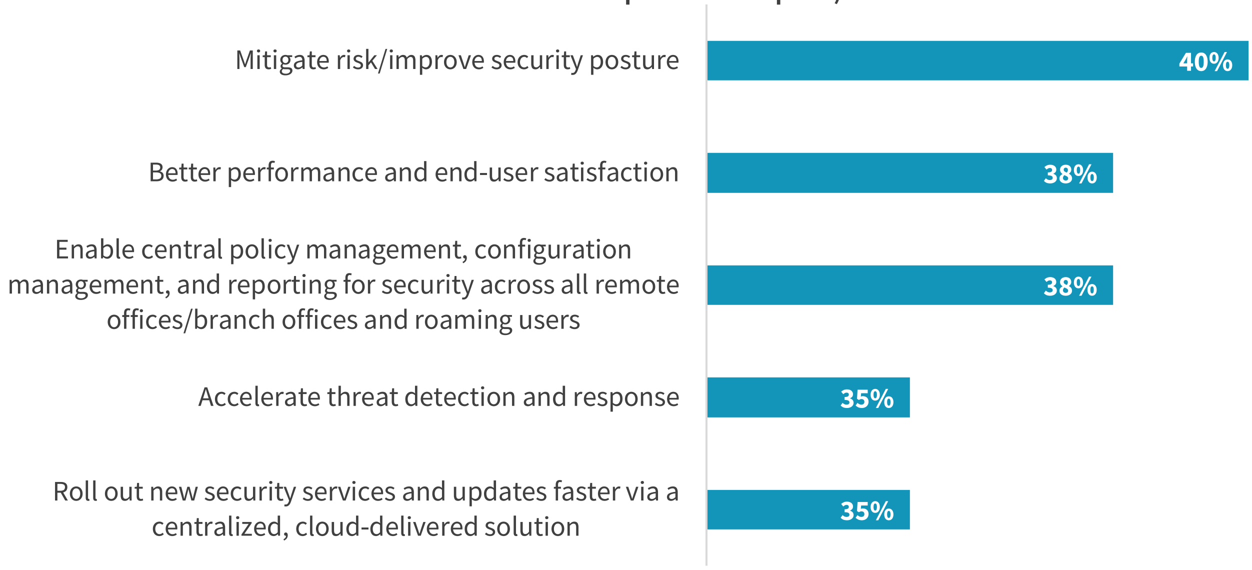
The Principles of a Converged Approach to Network Security

To address the changing enterprise environment and resulting security challenges, a new architecture for network security has emerged. Secure access services edge (SASE) represents a convergence and re-platforming in the cloud of previously siloed point tools. SASE solutions natively include or integrate with SD-WAN tools to automate the deployment of security services during branch office provisioning and enable consistent, secure connectivity across the WAN. These approaches have seen a significant increase in interest over the last 12 months, with ESG research finding that 68% of organizations use or are likely to consider SASE solutions. The top factors driving this interest in SASE include improved security, better performance, and more efficient management (see Figure 2).[3]

[3] Source: ESG Master Survey Results, Transitioning Network Security Controls to the Cloud, July 2020.

Figure 2. Top Five Drivers for SASE Adoption[4]

Of the following outcomes, which are the most important in driving your organization's interest in an elastic cloud gateway solution? (Percent of respondents, N=376, multiple responses accepted)



Source: Enterprise Strategy Group

Adopting a SASE architecture does not necessarily require replacing existing tools. In fact, because it's such a large initiative, organizations should first look at how their existing tools can support a SASE approach to begin seeing benefits in the short term, while working towards a full SASE implementation over time. Specifically, there are a handful of key requirements organizations should seek when considering solutions supporting a SASE architecture.

Centralized Management

Writing redundant policies across multiple tools, some with overlapping functionality, prevents administrators from focusing on more proactive tasks and is prone to error. In fact, with regard to the challenges associated with using a number of siloed point tools, 38% of ESG research respondents cite operational inefficiencies, and 32% report misconfigurations arising due to inconsistent policy management across different tools.[5] With workers accessing corporate resources from different locations and devices, policies should be written once and follow the user wherever they may connect from. Further, integrating these security controls with SD-WAN tools ensures consistency across the entire corporate environment (both on the WAN and off) and ensures policy is migrated efficiently as branch offices are provisioned.

38% of ESG research respondents cite operational inefficiencies, and 32% report misconfigurations arising due to inconsistent policy management across different tools.

[4] At the time of this research, the term "elastic cloud gateway (ECG)" was used rather than SASE, though it was defined in the same way SASE would be.

[5] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.

Defense-in-Depth/Multi-Layered Security

To address the broad spectrum of threats employed by attackers today, organizations need a layered preventative approach to protect users from web, email, and file-borne attacks and applications from compromise and misuse.

83% of respondents indicate that advanced threat protection capabilities are required or important to SASE approaches, the highest percentage reported for any tool or function.

In fact, 83% of respondents indicate that advanced threat protection capabilities are required or important to SASE approaches, the highest percentage reported for any tool or function.[6] Traditional signature-based capabilities combined with reputational assessments can filter out known bad threats. However, advanced capabilities such as sandboxing and isolation are increasingly required to prevent unknown attacks. To ensure applications are not exploited by compromised users or bad actors, IPS deep packet inspection, web application, and API protection (WAAP) should all be considered integral components to prevent malicious activity.

Cloud-based, Consistent Enforcement at the Edge

To facilitate this efficacy, policies must be enforced consistently regardless of location and occur close to the user at the edge to maintain a strong experience. This often requires a cloud-centric approach. The legacy model of backhauling traffic to the on-premises security stack can introduce unacceptable latency, especially when that traffic is ultimately destined for the cloud. Regardless of what device or location the user is accessing the internet or corporate applications from, their experience should be seamless, consistent, and secure. As shown in Figure 2, while the top outcome organizations seek through SASE approaches is mitigating risk and improving security posture (cited by 40% of respondents), it is closely followed by the 38% of respondents anticipating better performance and end-user satisfaction.[7]

Zero-trust tenets

Zero-trust strategies have seen an increasing interest for many of the same reasons that have driven SASE adoption. With users and resources shifting outside of the network perimeter, location has become meaningless with regard to determining trust.

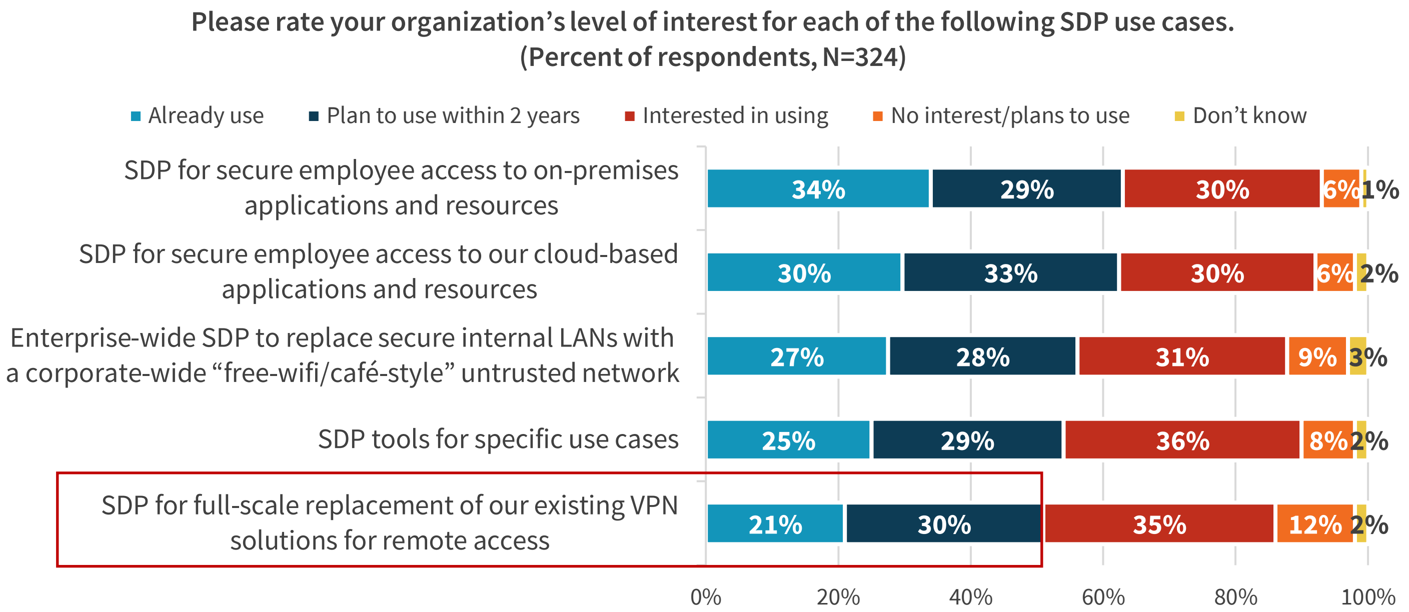
51% of organizations are using or plan to use zero-trust network access as a full-scale replacement for their VPN solutions for remote access.

As a result, there is a need to shift to an identity-centric model, granularly restrict access to what is explicitly permitted, and continuously monitor and reevaluate access even after it has been initially granted. In the context of SASE, zero-trust network access (ZTNA), sometimes called software-defined perimeter, delivers these capabilities and has emerged as a common starting point for SASE adoption. While many organizations focus on specific use cases such as providing secure access to cloud environments or applications, securing third-party access to corporate applications, and supporting merger and acquisition (M&A) activity, ESG research has found that 51% of organizations are using or plan to use zero-trust network access as a full-scale replacement for their VPN solutions for remote access (see Figure 3). Unlike traditional solutions that enforce security at the perimeter, ZTNA enforces security rules at the application, protocol, and command level, eliminating network-layer risks.

[6] Ibid.

[7] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud,* July 2020.

Figure 3. Plans for Zero-trust Network Access (ZTNA) Adoption[8]



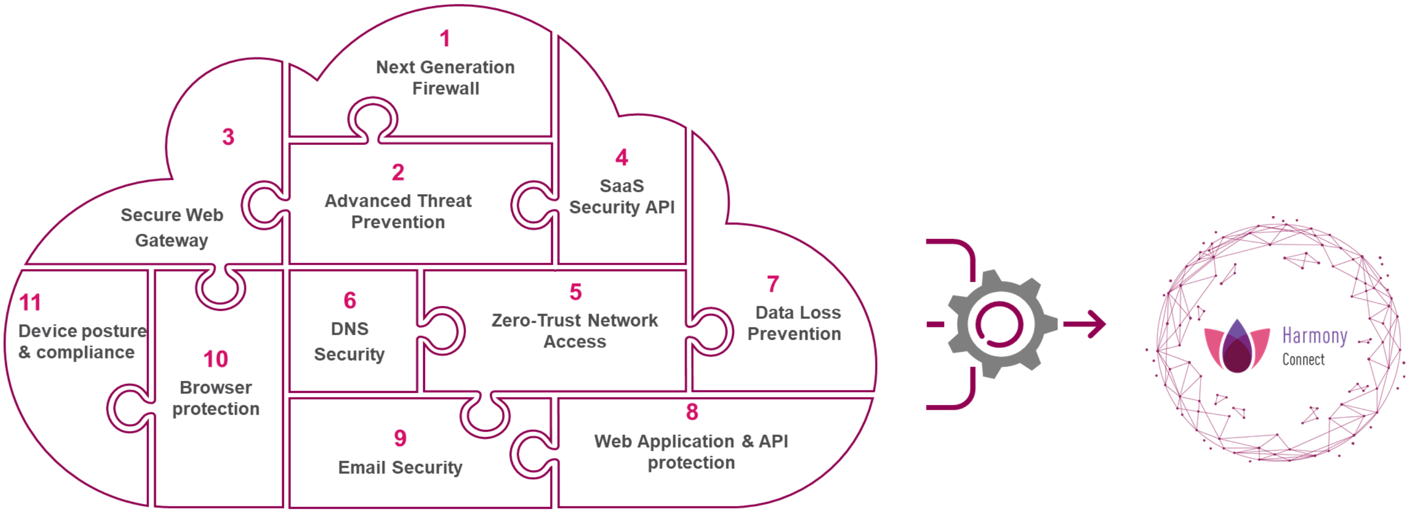
Source: Enterprise Strategy Group

Check Point's Harmony Connect as an Approach to SASE

Harmony Connect is Check Point's SASE solution. The offering provides a unified, cloud-native service for securing user access to corporate applications, SaaS, and the internet, with end-to-end threat prevention, unified management and threat visibility, and a user-centric experience. The solution builds on Check Point's strong network security heritage and includes ZTNA capabilities from its recent acquisition of Odo Security. The Harmony Connect cloud consists of over 100 points of presence (PoPs), providing service level agreements (SLAs) for <50ms latency and 99.999% uptime. Further, by integrating out-of-the-box with numerous leading SD-WAN solutions, organizations can leverage their current SD-WAN infrastructure to gain a better enterprise-wide security posture, while maintaining high-connectivity through WAN acceleration and intelligent routing for path optimization.

[8] Zero trust network access (ZTNA) and software-defined perimeter (SDP) are often used interchangeably and, based on the definition used in the scope of this research, should be considered synonymous.

Figure 4. Check Point Harmony Connect for SASE

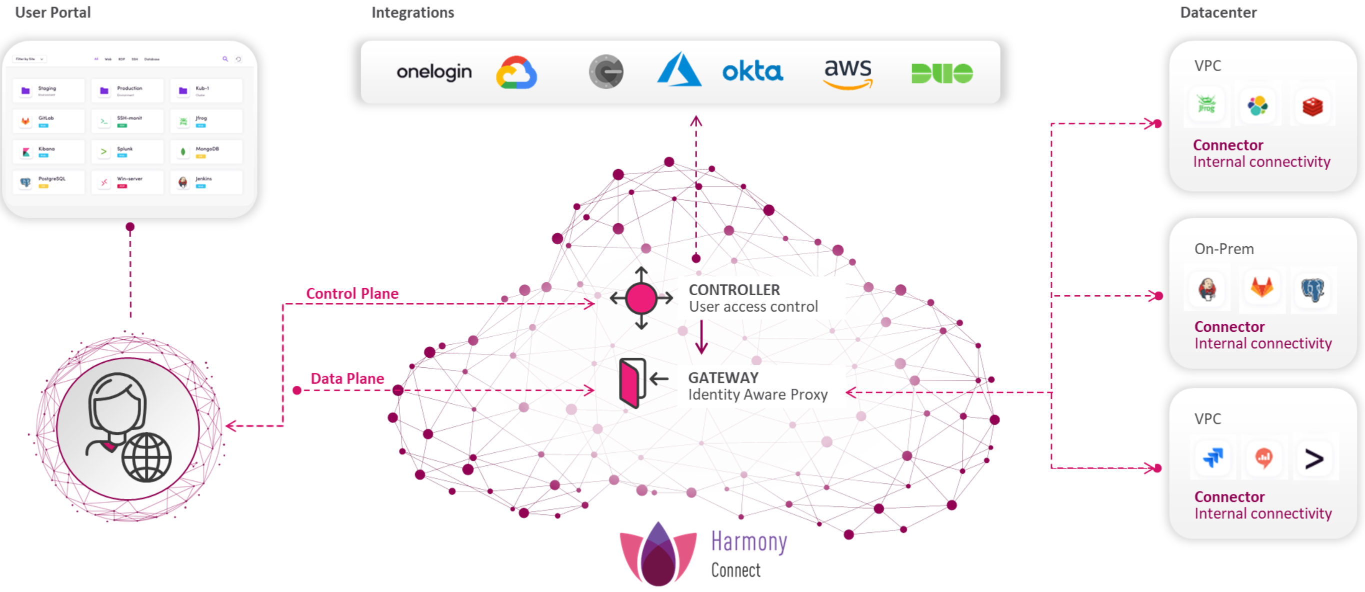


Source: Check Point

Unified Security

Harmony Connect unifies 11 security controls, including next-generation firewall, advanced threat prevention, secure web gateway, cloud access security broker, zero-trust network access, data loss prevention, and browser isolation, among others (see Figure 4). Further, a mix of native and API integrations with leading SD-WAN providers, including VMware, HPE, Citrix, and others, supports one-click provisioning of security for branch offices. Through an integrated approach, organizations can implement the SD-WAN of their choice or maintain their existing SD-WAN investment if one is already in place. The platform supports a zero-trust approach through a controller/gateway-based ZTNA architecture (see Figure 5). The controller integrates with a number of third-party identity solutions to authenticate users and broker access through the identity-aware proxy, separating the control plane from the data plane to ensure users have access only to those applications for which they are authorized, and applications are invisible to the public internet. Harmony Connect's centralized management console supports forensic visibility across all user activity through extensive logging and session recording capabilities. Additionally, security teams are provided a unified view of the threats impacting the organization's environment.

Figure 5. Check Point Harmony Connect Zero Trust Network Architecture



Source: Check Point

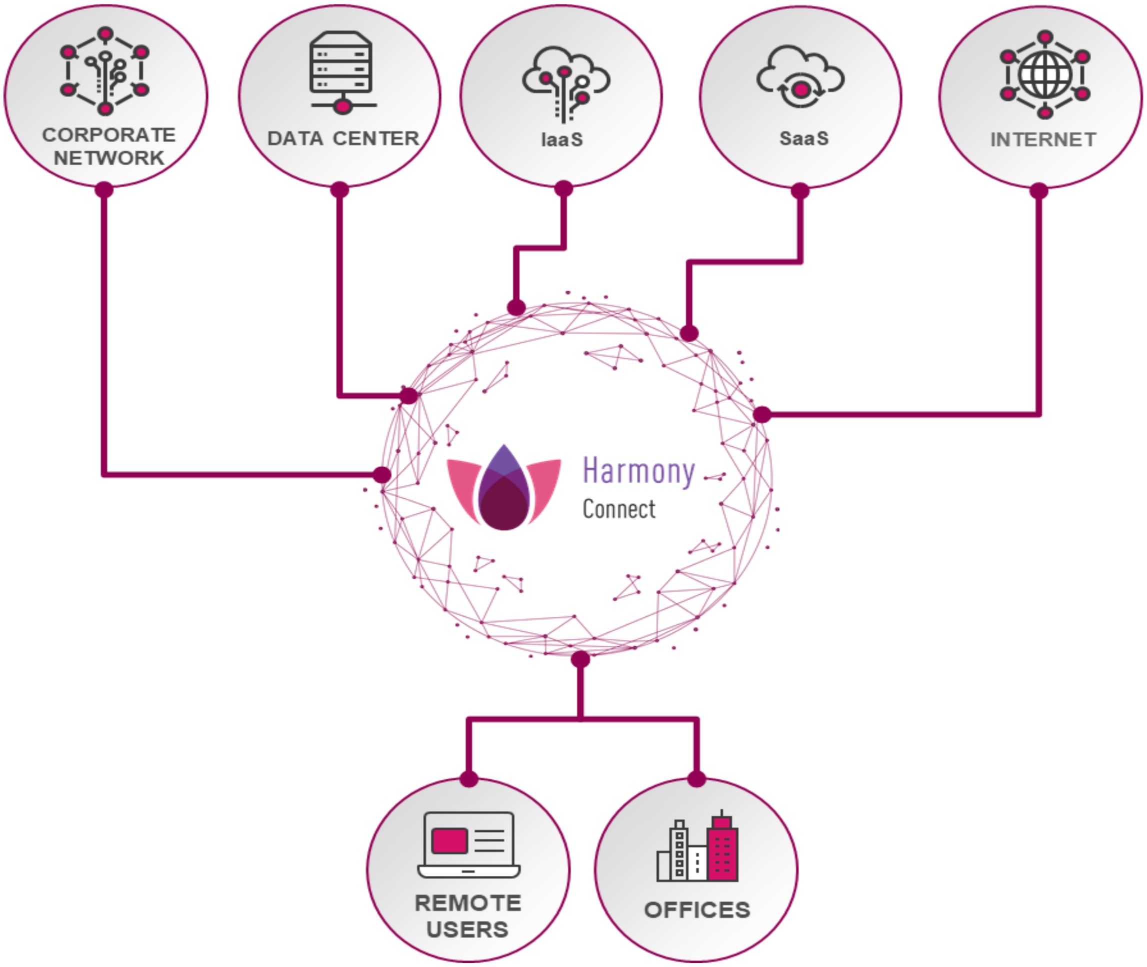
End-to-end Threat Prevention

Harmony Connect provides protections for both users and applications. Anti-malware, anti-phishing, and anti-ransomware signatures are coupled with reputational assessments for URL, IP address, and domains for core protection. Additionally, sandboxing, document sanitation, content disarm and reconstruction (CDR), and browser isolation are included to defend against unknown attacks. In addition to web application and API protection, Harmony Connect provides IPS for virtual patching and identity-based access control to defend applications.

User-centric Experience

Harmony Connect supports both clientless and client-based deployments across managed and unmanaged devices. Device posture assessment is available across both options, though more telemetry can be gathered through the client-based approach. In the clientless model, browser-based application access is provided through direct link-based access or a portal for corporate applications, supported by single sign-on to simplify user access. By supporting both client and clientless approaches, Harmony Connect addresses a diverse set of use cases, including those that require a clientless approach such as access for third-parties, contractors, and M&A. Finally, the solution's in-browser protection allows users to directly access the internet without traversing the Harmony Connect cloud. This further reduces latency and provides on-device SSL visibility for threat prevention without impacting user privacy. This approach prevents malware downloads, phishing, and password exposure on the device itself.

Figure 6. Check Point Harmony Connect Coverage



Source: Check Point

The Bigger Truth

The introduction of SASE represents a significant transition for network security. While much of the broader IT landscape has been quick to adopt cloud-centric approaches, network security has remained predominantly appliance-based. The distributed nature of the modern enterprise necessitates a new, cloud-supported approach. This is not to say that organizations can or should transition all their network security tools to the cloud at once. Use-case-specific considerations (such as scaling remote access to corporate applications, securing remote web browsing, or moving to cloud-based applications), regulatory concerns, and existing infrastructure investments will continue to necessitate a hybrid approach for most organizations. Vendors such as Check Point that provide a flexible set of solutions can allow customers to take an iterative approach to SASE and make the transition to cloud at their own pace, over time.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188