CHECK POINT

Harmony SASE – Battle Card

Q1 2025

Major Components

Harmony SASE – Unified, Cloud-Delivered Network Security

Private Access – A Zero Trust Network Access (ZTNA) solution that controls access to company resources using granular application-level rules based on individual users or groups. It also includes contextual rules such as device posture check for enhanced security.

Internet Access – Prevent users from unknowingly visiting malicious websites, guards against users downloading internet-sourced malware. Hybrid architecture allows for flexible deployments, and the ability to bypass cloud processing for optimized performance and without sacrificing security

Mobile Security – Comprehensive security against advanced mobile cyberattacks, safeguards corporate data, secures access to internal resources, ensures employee privacy and productivity

Browser Security – In-browser protection against zero-day phishing, corporate credential reuse, malicious file downloads, and data leakage (even through GenAI apps) without compromising speed or privacy

SaaS Security – Get a complete mapping of your SaaS ecosystem, with misconfiguration detection, timely alerts, and automated threat response

SD-WAN – Optimized multi-link application-aware traffic routing with auto-steering based on jitter, packet loss, and latency. Plus, a full branch-level security stack with industry leading threat prevention.

Zscaler Challenge Questions

Drive the sales cycle by addressing business challenges, not feature analysis.

- Are performance issues slowing down your workforce and impacting productivity?
- Do you think managing multiple consoles will impact team efficiency and increase risk?
- How do you ensure secure remote access for BYOD and contractors without complicating the experience for users and IT?

Palo Alto Challenge Questions

- How do you ensure secure remote access for BYOD and contractors without complicating the experience for users and IT?
- Are you worried about unmanaged internet traffic creating security blind spots?
- Do slow network and security changes delay business growth and agility?

Key Features

- **Infinity Portal Management –** Manage remote and internet access seamlessly in a single-pane-of-glass with the rest of your Check Point portfolio
- **Zero-Phishing Protection –** 90% of phishing websites are live for just one day—we can detect and block these sites in real time
- **Faster secure Internet access –** Avoids cloud latency through on-device inspection
- **Full Mesh Connectivity –** Any-to-any connectivity including server-to-server and cloud-to-cloud
- **Clientless access for BYOD and third parties, *e.g.* partners and contractors –** SaaS-like user experience from a web-based portal with no agent, appliances to deploy, or maintenance to perform
- **Global, high-performance connectivity –** More than 70 PoPs worldwide, with Tier-1 connectivity, reserved bandwidth, and expansive peering
- **Layer 3-7 access control –** Applications and resources access control on network and application level (layers 3-7)
- **Gen AI Protection –** Uncovers which generative AI tools are used by your workforce, assesses risk, and uses AI-powered data classification for DLP
- **Advanced Threat Protection –** Multi-layered protections including web filtering, DNS filtering, malware protection, threat sandboxing, anti-bot, and secured Wi-Fi traffic
- **Zero Trust Security –** Granular, least-privilege application access reducing exposure and lateral movement
- **Fast, Seamless Deployment –** Deploy your cloud-based network, bring it online, and connect employees, fast
- **Broadest Protocol Support –** Go beyond HTTPS with support for RDP, SSH, and VNC as well
- **Static IP Addresses for Each Customer –** IP addresses are private to you and can be used for whitelisting SaaS applications

CHECK POINT

Harmony SASE – Battle Card

Q1 2025

	Comparison Matrix	Harmony SASE	Prisma SASE	Zscaler ZIA + ZPA	Cisco Secure Connect
Private Access	Full Mesh Connectivity	A	A	A	
	Device Posture	B	B		A
	Native RDP Support (clientless users)				
	Clientless User Posture Checks (Date, Time, IP, Country, OS, Browser)	6/6	0/6	0/6 B	2/6
Internet Access	Secure Browsing Speed	C	C		
	Malware Prevention Rate[1]	99%	74%	83% C	96%
	Security for Bypassed Traffic[2]		D		
	Zero-day Phishing Protection	D			B
	GenAI Access Control	E			
	Threat Extraction (CDR)		E		
	DLP				
Platform	Ease of Deployment	F	F	D	C
	Dedicated Static IPs				D
	In-House SD-WAN	G		E	
	Price 1Y + Support[3]	$238/User[4]	$247/User[5]	$400/User[6]	$324/User[7]

1. Based on 2025 Miercom Enterprise & Hybrid Mesh Firewall
2. bypassed traffic. = Traffic not usually steered to the cloud PoPs (e.g video conferencing, Google FQDNs, Microsoft apps, etc.)
3. Price for the lower tier (up to 100 users). SD-WAN price is not included.
4. Internet Access Essentials+, and Private Access Premium
5. Prisma Access Enterprise + DLP + SLS (Strata Logging Service). A dedicated static IP option is not available.
6. Zscaler Platform bundle. *Sandbox & Cloud firewall requires additional add-ons*.
7. Cisco Secure Connect Complete Advantage *Does not include reserved IPs for tenant ($5,500 per year per tenant)

Competitive Advantage

Harmony SASE

A. **Zero Trust Access with full mesh connectivity between users, branches and applications.**
B. **Continuous device posture checks including antivirus, disk encryption, certificate, OS version and more.**
C. **Hybrid SASE solution (On-Device+Cloud), results in Faster secure browsing compared to Cloud-Only SASE**
D. **Real-Time 0-day Phishing prevention, protect all users from 0-day phishing links and sites**
E. **Control users' access to GenAI applications to reduce associated risks**
F. **Easily create and manage networks that connect your sites, data centers, clouds, and users.**
G. **SD-WAN Unifies industry-leading security with optimized Internet and network connectivity**

How to Compete Against...

paloalto NETWORKS

A. **Hidden cost approach** – Full mesh connectivity (Net Interconnect) is only available as an add-on for the highest bundle. Cortex Data Lake, additional ZTNA connectors & service connections require add-on licenses.
B. **Limited device posture check capabilities** - Posture checks are performed only once an hour.
C. **Low browsing speed and high latency** since the traffic must be routed through the cloud.
D. **No internet security for bypassed traffic** – Traffic that is usually not steered to the cloud PoPs (e.g. video conferencing, Google FQDNs, Microsoft apps, etc.) will not be inspected, resulting in a security risk.
E. **Missing CDR** – No sanitized files support via Prisma Access
F. **Complicated deployment** - Onboarding a new Service Connection to access corporate resources requires significant time and expertise (more info). There are multiple profiles, profile groups and policies to set

zscaler

A. **Limited corporate connectivity -** Only support user-to-app connectivity.
B. **Lacks posture checks for clientless users** – Increases the risk on the corporate resources.
C. **Low Malware prevention rate** – only 83% malware block rate in Miercom Enterprise & Hybrid Mesh Firewall
D. **Complicated to deploy -** Requires configuring IDP twice (ZIA and ZPA). Moreover, connect corporate resources for secure private access only available by app connector (IPSec tunnels are not supported).
E. **Limited SD-WAN solution** – Zscaler's Physical appliances are limited to a small branch, Supporting as low as 1 Gbps. Additionally, limited to L3/4 (No L7). Do not support OSPF, BGP, MPLS, and other protocols.
F. **Hidden cost approach –** Zscaler's new licensing model requires numerous add-ons (Sandbox, Cloud Firewall, Advanced DLP, and more) which are not included in their highest-tier bundle "Zscaler Platform"

CISCO

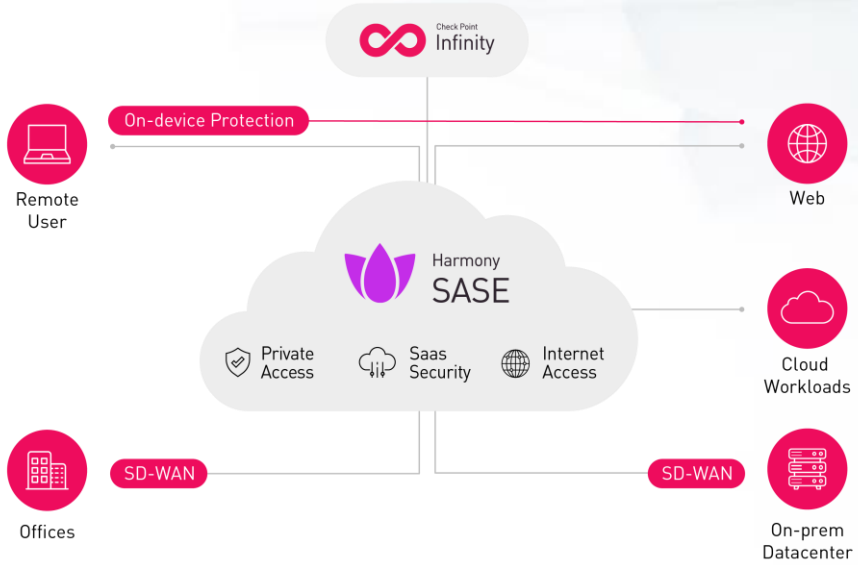
A. **Limited device posture checks capabilities -** Device posture checks are performed only prior to the connection and not periodically. Lacks validation of existing files, running processes, registry keys, and more.
B. **Lacks 0-Phishing protection** – Cisco Secure Connect can not handle 0-day phishing attacks
C. **Complicated to deploy** – Connect corporate resources for secure remote access only through IPSec tunnels. lacks an option for a VM-based connection.
D. **Dedicated private IP is only available as an add-on license** ($5,500 per year), and has technical limitations
E. **Limited cloud PoP availability** – Cisco provides only 30 PoPs, while Harmony SASE offers 70+ PoPs worldwide.

Harmony SASE – Battle Card

Q1 2025

TARGET AUDIENCE AND QUESTIONS TO ASK

CIO or CISO	DIRECTOR of IT / INFOSEC	IT MANAGERS
How are you protecting your organization for ransomware and other malicious threats?	Is your organization adopting Zero Trust? How does remote access fit into your Zero Trust plans?	Have you had scalability or user experience challenges with your existing VPN architecture?
How are you reducing your attack surface when migrating to cloud?	How are you ensuring secure access to the public cloud? What about unmanaged devices?	How do you define firewall rules to protect cloud data centers?
What is your plan for obtaining complete visibility into your on-prem and cloud assets access?	How are you protecting users who bypass the SWG cloud service to improve latency (e.g. video conferencing)?	Are you suffering from performance issues with your current SWG solution?



OBJECTION HANDLING

How are you protecting SaaS applications without CASB?	Harmony SASE provides SaaS access control via the firewall-as-a-service capabilities. Access can be defined per-user/group and per-SaaS application. We also provide API-based SaaS mapping to discover Shadow SaaS integrations.
How does Harmony SASE secure internet traffic that isn't tunneled?	Harmony SASE's hybrid approach uses on-device security to **keep internet traffic protected**, even when it isn't routed through a cloud PoP. Many other solutions leave bypassed traffic **unprotected.**
Won't an on-device SWG affect the performance of my employee's laptops (CPU, memory, battery life)?	Our agent-based SWG is efficient and causes **minimal strain on user devices**. It has a very small memory footprint, and extensive testing has shown 1%-2% of CPU utilization. This is also reflected in little to no impact on battery life.

SALES ENABLEMENT RESOURCES

Success Story
- An American energy solutions manufacturer needed to rapidly abandon their legacy VPN. Read the case study
- Learn how finance firm NQM Funding easily scaled its network to keep up with its growing business across the U.S. Read the case study

Product Information
- Harmony SASE Datasheet
- Request a Demo
- Customer Sales Presentation

SASE White Papers
- The Essential SASE for Enterprises eBook
- Securing Microsoft and Entra ID with Harmony SASE
- Harmony SASE H3
- The Work from Anywhere Checklist for IT Managers

Need more info?

Partners - partners-sase@checkpoint.com **| non-Partners -** cp-sase@checkpoint.com