CHECK POINT™ | Harmony SASE

How to Win With Harmony SASE

PARTNER SALES GUIDE

Solution Overview

Harmony SASE is a game-changing solution that delivers 10x faster internet security, full hybrid mesh Zero Trust Access, and optimized SD-WAN performance. Harmony SASE also incorporates Mobile Security, Browser Security, and SaaS Security delivering the most comprehensive SASE platform on the market.

Using Harmony SASE, MSPs can build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

Who is it for?

Harmony SASE is a great fit for different-sized companies who are managing a remote or hybrid workforce and delivering applications and services from cloud data centers. Advanced and tech-minded organizations who embrace digital transformation and are looking to simplify their networks and improve security are also an ideal fit.

The target persona is an IT decision maker such as IT or security Manager/Director/VP, CIO, CISO, etc. See role-based messaging on the last page.

Harmony SASE Advantages

Easy-to-use
The solution is easy to deploy and is managed from a single-pane-of-glass console.

Fast time to value
The solution can be deployed quickly to start connecting and protecting employees and the corporate network in less than an hour.

Cloud-native
Delivered as a cloud-native service, the solution is ideal for fully remote deployment, management, and maintenance by MSPs.

Robust
Delivered from more than 80 PoPs connected with redundant tier-1 links.

Converged security
ZTNA, web filtering, malware protection, firewall as a service, mobile security, browser security, SaaS security, and other capabilities delivered from a single platform.

Scalable
Easily add users and PoPs whenever and wherever needed.

Discovery Questions and Talking Points: Private Access

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
How are you connecting remote users to corporate resources?	Connecting remote employees to the corporate network exposes a dangerous attack surface, which can lead to breaches, ransomware attacks, data theft, and other risks.	Private Access ZTNA ensures secure remote access by micro-segmenting the network and enforcing granular user-based access to explicitly authorized applications.
How are you limiting user access only to the applications they need?	If a user's credentials are stolen, limiting the access the perpetrator has impedes their lateral movement ability and reduces the overall attack surface.	By implementing zero trust principles of lease privilege, our ZTNA enables user or group access to explicitly defined applications.
How do you ensure employees' device security?	Unsecure devices are more vulnerable to infection, which can spread to the rest of the network and critical resources.	By implementing Device Posture Check (DPC), device security compliance is determined before granting access. This includes disk encryption, active anti-virus, OS version, and more.
How do you connect unmanaged devices and contractors to company resources?	There is often a need to enable employees, contractors, or other 3rd parties, to securely access corporate resources.	Agentless zero trust network access enables secure web-based access via unmanaged devices to explicitly defined resources.
How are you authenticating users?	It's critical to make sure only authorized users have access to the network, even if their credentials are stolen.	Supports multi-factor authentication (MFA) to ensure that stolen credentials can't be used to access company resources.
How are you tracking device inventory and user activity?	Keeping track of devices and users helps detect possible network issues and suspicious activities and enables fast remediation.	Provides detailed logs of network activities and enables fast detection and remediation of any discovered issues.
How do you isolate Production/staging/internal/guest/contractor networks from each other?	Complete isolation of networks ensures a higher level of security for company resources.	Enables defining multiple isolated networks within the same account. User and group access can be limited to explicitly defined networks.
Are you planning an M&A? How will you onboard the new network?	Adding a new network as part of an M&A can be very complicated and expose security threats.	The ability to define multiple separate networks under the same account enables easy onboarding of new networks in a completely isolated and secure manner. Also solving issues of overlapping IP ranges.

Discovery Questions and Talking Points: Internet Access

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
How are you limiting employee access to malicious websites?	Unlimited access to malicious and compromised websites exposes employees and the network to potential threats.	Web filtering inspects all web requests and blocks access to compromised or malicious sites.
How are you protecting users from downloading malware?	Downloading ransomware or other malicious content to user devices can propagate through the network and cause detrimental damage.	Malware protection scans all downloaded files and inspects for suspicious content. If malware is discovered, it is blocked and reported for further analysis.
How do you protect employees connecting from public WiFi?	Public WiFi is known to be unsecure and expose a highly risky attack surface.	Harmony SASE's agent has a unique capability to detect public WiFi and enforce secure access when used.
How are you protecting users who are not connected to the Private Access cloud service?	There are cases where users cannot connect to a cloud service due to a login issue, outage, or other reasons.	Harmony SASE Internet Access runs on the user's device and inspects all traffic without needing to connect to the cloud service.
Are you bypassing part or all web traffic to conserve bandwidth? If so, how are you protecting users from downloading malware?	Bypassed traffic is sent directly to the website, without passing through the cloud security stack, therefore leaving it unprotected.	Web filtering and malware protection are implemented on the user device and inspect all traffic, including traffic bypassing the network.
(Customers using or considering cloud SWG, e.g., ZScaler ZIA) **Are you concerned about performance issues with a cloud based SWG solution?**	Routing user traffic through a cloud data center can add significant latency and impact application performance.	Harmony SASE Internet Access enables routing traffic directly to web applications without passing through a cloud service on the way, while providing complete protection. Performance has been proven to be 10x faster than competing SWG solutions.
(Customers using on-prem SWG) **Do you need to backhaul remote user traffic to a branch office or a data center?**	Backhauling traffic adds significant latency and can dramatically slow down web applications and impact productivity.	Internet Access can route traffic directly to the cloud without any backhauling.
(Customers using or considering SSE/SASE) **Do you need to purchase and use a ZTNA/VPN in order to enable SWG for your users?**	Converged SSE/SASE solutions typically require users to connect to the corporate network in order to get SWG protection.	Internet Access doesn't require connecting users to the corporate network in order to receive SWG protection.
(Customers using or considering SSE/SASE) **Do you need to purchase bandwidth licenses to use SWG?**	Some SSE/SASE solutions require bandwidth-based licenses on top of user-base licenses, essentially paying twice for the same service.	Check Point doesn't charge for bandwidth for Internet Access. We've moved on, so should you.

Discovery Questions and Talking Points: Cloud and Network Security

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
How do you control user access to cloud applications?	As more applications and sensitive data are moved to the cloud, it becomes critical to control access to them.	Harmony SASE supports all public cloud platforms and enables granular per-application access control.
Where do you define firewall rules to protect cloud data centers?	Firewalls are as critical for protecting cloud data centers as they are for on-prem.	The solution includes a Layer 3-7, cloud-based firewall which processes all cloud-bound traffic and can enforce access rules.
How do you keep your external IP addresses hidden?	Exposing public IP addresses means anyone can use them to try to hack sensitive proprietary resources.	Hides public IP addresses, essentially making your resources invisible.
How do you limit access to trusted resources?	Accepting connections from trusted origins only greatly reduces the cloud attack surface and helps avoid breaches.	Each account is allocated a private static IP address which can be used for cloud application allowlists. All other origins will be blocked.

Discovery Questions and Talking Points: Network Performance

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
How do you ensure network performance?	Slow networks can impact application performance and reduce productivity.	Harmony SASE global mesh network is deployed across more than 80 globally distributed PoPs. Users connect to the closest PoP to ensure minimal latency and optimal performance.
How do you ensure fast connectivity to cloud resources?	Solutions that need to backhaul traffic via a physical data center add latency and impact performance.	The solution is deployed in the cloud and enables direct access to any cloud data center with minimal latency.
How do you ensure network performance for long-distance connections?	Long-distance connections (e.g., intercontinental) are prone to high latency, jitter, and packet loss, greatly impacting network performance.	Harmony SASE utilizes a private backbone consisting of at least two tier-one provider links for each PoP. This ensures fast and reliable connectivity to any cloud environment.
How do you ensure network performance for multi-cloud deployments?	Using cloud access optimization solutions (e.g., AWS Direct Connect/Azure Express Route) you are limited to the cloud provider's data centers.	Harmony SASE is a cloud platform-agnostic solution, which optimizes connectivity to any cloud data center.

Discovery Questions and Talking Points: SD-WAN

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
Does your SASE solution natively include SD-WAN integrated with your SSE solution?	Purchasing an SD-WAN solution separately from your SSE solution adds unnecessary complexity to your environment.	Harmony SASE includes Check Point SD-WAN, unifying industry-leading security with optimized Internet and network connectivity.
Do you have branch offices where you need to optimize network connectivity and security?	SD-WAN complements SSE in on-prem settings to provide optimal speed and protection.	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.
How do Quantum SD-WAN and Harmony SASE combine to form a complete SASE solution?	To address the needs of some industry sectors (e.g., highly regulated) and organizations that maintain physical premises, the combination of SSE and SD-WAN is the ideal architecture.	The complete Harmony SASE delivers security and networking from a single service. Check Point SD-WAN and Harmony SASE combine to form a complete solution that can be managed from the Infinity cloud platform

Discovery Questions and Talking Points: Browser Security

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
How do you currently manage browser security across your organization, especially with the shift to remote work?	Ensuring your remote workforce is protected without complex setups can streamline operations and enhance security without additional overhead.	Offers seamless protection directly within the browser, ensuring secure, private browsing without the need for complex configurations, ideal for remote and hybrid environments.
Have you experienced any security breaches or data leaks through web browsers?	Understanding your exposure to browser-based threats is crucial to prevent future incidents and protect your organization's data integrity.	Provides advanced threat prevention capabilities, including real-time phishing protection and data leakage prevention, to safeguard against similar incidents.
What challenges do you face with integrating and managing multiple security solutions?	Streamlining security solutions can reduce operational complexity and close security gaps, making your defenses more robust and less prone to errors.	Integrates smoothly with existing Check Point products and third-party solutions, offering a centralized management dashboard for streamlined operations.
How do you ensure compliance with data protection regulations when employees use browsers for accessing sensitive information?	Compliance is crucial for avoiding legal penalties and maintaining customer trust.	Features advanced DLP capabilities that ensure data shared via browsers complies with regulations, enhancing data governance and compliance.

What measures do you have in place to protect against zero-day threats and sophisticated cyber attacks through browsers?	Proactively defending against emerging threats can safeguard your critical assets and give you peace of mind in the ever-evolving threat landscape.	Delivers protection against zero-day threats and sophisticated attacks with AI-powered threat prevention technologies and real-time updates.
How do you handle the security of unmanaged devices accessing corporate resources through browsers?	Unmanaged devices pose a significant risk as they often bypass traditional security measures.	Enforces security policies on both managed and unmanaged devices without the need for device management software, extending protection to all endpoints.
Can you describe your current solution's impact on browser performance and user experience?	Security solutions should not degrade performance or hinder productivity.	Operates with zero latency, ensuring that security measures do not impact browser performance or user experience.
How do you currently protect against phishing and credential theft through browsers?	Phishing and credential theft are common attack vectors that can lead to broader security breaches.	Utilizes AI-powered Zero-Phishing technology to block phishing sites and prevent credential theft in real-time.
What is your strategy for securing web searches and ensuring safe browsing?	Safe browsing can prevent access to malicious sites and reduce the risk of web-based attacks.	Ranks browser search results by safety based on reputation and corporate policy, significantly reducing the risk of accessing harmful sites.
Are employees using GenAI tools like ChatGPT or Gemini to process or share sensitive data?	GenAI tools can introduce data security and compliance risks, especially if sensitive or regulated information is uploaded or shared without controls.	Monitors and controls data transfers within GenAI tools, including uploads, downloads, clipboard, and print actions—helping ensure safe and compliant use.
What protection is in place for files downloaded via browsers?	Browsers are a common entry point for malware hidden in downloads, which can bypass traditional defenses.	Scans all downloaded files with Threat Emulation® and Content Disarm & Reconstruction (CDR), ensuring sanitized content is delivered in milliseconds.
How do you prevent the use of corporate credentials on unauthorized websites?	Credential reuse on unauthorized platforms can lead to unauthorized access and account compromise.	Detects and blocks the use of corporate credentials on non-corporate websites in real time.
Do you have visibility into security events and web threats targeting your organization?	Understanding which threats are being blocked and how security policies are performing is critical to improving protection without compromising user privacy.	Provides aggregated threat insights and policy-level reporting through the Infinity Portal—helping security teams stay informed while respecting end-user privacy.
Are all your users—regardless of browser or operating system—equally protected?	Security solutions that only work with specific browsers or operating systems leave gaps that attackers can exploit.	Delivers consistent protection across all major browsers—Chrome, Edge, Firefox, Safari, and Brave—on Windows, macOS, and ChromeOS, without requiring an enterprise browser.
Are you looking for a strong browser security solution that's lightweight, scalable and cost-effective?	Many browser security solutions are complex to deploy and expensive to scale—especially in remote and hybrid environments.	Provides enterprise-grade protection as a lightweight browser extension. It installs in seconds, requires no infrastructure changes, and reduces both operational overhead and total cost of ownership.

Discovery Questions and Talking Points: Mobile Security

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
What mobile security measures do you currently have in place, and how do they address different types of mobile threats, such as QR code attacks and malware from app downloads?	Malicious actors continue to increase the sophistication and variety of attacks targeting mobile devices, requiring advanced security capabilities.	Harmony Mobile provides comprehensive protection against mobile threats, including advanced scanning for malicious QR codes and secure app downloads.
What challenges have you faced in implementing effective security measures for personal devices used for work purposes?	Implementing BYOD security is crucial for managing the risks associated with personal devices in the workplace.	Harmony Mobile ensures secure access and data protection on personal devices, aligning with your BYOD policy requirements while maintaining user privacy.
Are common misconceptions about mobile security impacting your security strategy?	Addressing misconceptions is essential for ensuring that security measures are properly understood and adhered to by all employees.	Harmony Mobile provides clear, user-friendly explanations of security protocols and their importance, helping to dispel common misconceptions.
How do you currently manage and secure the applications installed on corporate mobile devices? What measures are in place to protect against network-based attacks?	App and network security help protect mobile devices against a wide range of attacks.	Harmony Mobile offers robust app management and network protection features, ensuring that only secure apps are used, and data transmissions are safe.
How do you ensure compliance with mobile security policies across all devices, especially in a diverse device environment?	Ensuring that devices comply with security standards helps reduce the risk of data breaches and other security incidents.	Harmony Mobile provides comprehensive compliance tools that enforce security policies consistently across all mobile devices.
Does your current solution provide real-time protection against zero-day phishing attacks?	Zero-day phishing attacks are unpredictable and can bypass conventional security measures, posing a significant risk to mobile security.	Harmony Mobile leverages AI/ML-based technology to provide real-time detection with the highest catch rate and low false positives, ensuring robust protection against emerging threats.
How do you protect against malicious file downloads across all file types?	Mobile devices are increasingly targeted with malicious files that can compromise data and system integrity.	Harmony Mobile offers comprehensive protection by scanning and blocking malicious downloads, ensuring a safe mobile environment as part of its 360-degree protection strategy.
Are you currently able to mitigate threats before they impact the user?	Preventing threats before they occur reduces potential damage and enhances overall security posture.	Harmony Mobile uses a multi-layered approach with automatic remediation actions to quickly address vulnerabilities and prevent exploits in real-time.
How do you handle vulnerability management and CVE reporting?	Effective vulnerability management is crucial for maintaining the security integrity of mobile devices.	Harmony Mobile provides full CVE reporting and assessments, allowing for proactive management of vulnerabilities and ensuring devices are always protected against known threats.
Does your current solution integrate with a SASE platform to provide risk-based conditional access for SaaS services and corporate resources?	Integrating mobile security with SASE enables a unified security posture that adapts to the risk level of the device and user behavior.	Harmony Mobile, coupled with Harmony SASE, assesses the full device posture and implements risk-based conditional access, ensuring secure and compliant access to SaaS services and corporate resources.

Discovery Questions and Talking Points: SaaS Security

QUESTION	WHY IT'S IMPORTANT	HOW HARMONY SASE CAN HELP
Are you confident in your ability to prevent SaaS data leaks or data exposure?	It's critical to evaluate current security measures and awareness of potential vulnerabilities within SaaS applications.	Harmony SaaS provides comprehensive security measures to prevent data leaks and exposure by continuously monitoring and securing connections.
How do you prevent SaaS supply chain attacks today?	This helps assess the robustness of their security strategy against complex threats that exploit third-party services and software.	Harmony SaaS mitigates the risk of supply chain attacks through automated termination of risky SaaS connections and fast discovery of unsanctioned connections. This prevents threat actors from exploiting connected SaaS platforms like Microsoft 365 or Salesforce.
Have you experienced a security incident due to a SaaS misconfiguration?	SaaS misconfigurations can lead to significant security incidents.	Harmony SaaS identifies and alerts on misconfigurations with comprehensive reporting, reducing the risk of security incidents. It helps expose SaaS security policy gaps and provides single-click remediation to close them.
How do you keep your SaaS ecosystem compliant with [industry regulation]?	Compliance with industry regulations is not just about legal necessity but also about maintaining trust and integrity in handling data	Harmony SaaS ensures seamless regulatory compliance by automatically discovering all integrated SaaS services, remediating security gaps, and maintaining tight compliance with regulations. Automated alerts and fixes for compliance mistakes are part of the service.
Would you know if security issues arose in your SaaS ecosystem?	Prompt detection and response to security issues will help minimize damage to the organization	Harmony SaaS's machine learning engines automatically detect and stop threats by identifying anomalous behavior, ensuring that any security issues are promptly addressed and mitigated.
Do you have any process to manage connections and API Keys?	Proper management of connections and API keys helps prevent unauthorized access and data breaches	Harmony SaaS includes processes to manage connections and API keys effectively, with capabilities to detect and prevent API key misuse in real-time, ensuring secure and controlled access to SaaS services.
What services are you most critical or concerned about?	Identifying your critical services are critical helps prioritize security efforts and resource allocation	Harmony SaaS prioritizes the security of all connected SaaS services, especially those handling sensitive data and critical operations. It provides insights and prioritized recommendations to reduce the attack surface and secure these critical services.
Do you have a way of seeing the whole SaaS landscape across your tech stack?	SaaS applications are an integral part of the organization's tool set.	Harmony SaaS provides a comprehensive view of the entire SaaS landscape, including every API, application, and plugin. This visibility helps in managing and securing the sprawling ecosystem of SaaS applications and integrations.
Could you detect and prevent API key misuse in real time?	Detecting and preventing API key misuse in real-time is crucial for maintaining the security integrity of SaaS applications.	Harmony SaaS can detect and prevent API key misuse in real-time through continuous monitoring and security controls, safeguarding against unauthorized access and potential security breaches.
Can you automatically discover all new connected services, and the behavior between them?	Automatic discovery of new services and their interactions is key to managing shadow IT and ensuring that all integrations are secure.	Harmony SaaS automatically discovers all new connected services and analyzes the behavior between them to ensure secure and compliant SaaS operations. This capability helps in quickly identifying and mitigating any potential risks in the SaaS ecosystem.

Role-based Messaging:

LEVEL	ROLE	OBJECTIVES	MESSAGING
CIO / VP / Director	Decision Maker	• Enable business • Meet budget • Regulatory Compliance • Protect the business	• Robust (Availability, performance, low risk) • Cost effective (OPEX, predictable, pay-as-you-go, consolidates multiple products) • Compliance w/ leading regulations and standards (SOC2, HIPAA, GDPR, etc.) • Security (complete coverage and network protection)
IT Manager / Admin	Influencer	• Fast time to deploy • Get stuff done • Reduce workload	• Ease-of-use, quick learning curve, fast deployment time • Single-pane-of-glass, simple RCA and incident resolution • Reduce maintenance work (auto updates of SW, patches, signature files) • Easy integrations (IdP, SIEM) • Stability (Availability, easy debug)
CISO	Decision Maker / Influencer	• Not get fired • Security posture • Compliance • Meet budget	• Security (Reduce attack surface with automatic updates, WiFi, MFA, DPC, SWG, static IP) • Compliance (SOC2, HIPAA, GDPR, etc.) • Positive ROI vs risk

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