HARMONY SASE

10X Faster Internet Access | Full Mesh Private Access
SaaS Security | Secure SD-WAN

Harmony
SASE

Security Is Expanding Beyond the Perimeter

Hybrid work and cloud transformation demand security to expand beyond the traditional network perimeter.

While companies adapt their enterprise network for the distributed workforce, they must also adapt their network security controls:

- The data center has expanded to the cloud with 90% of organizations currently using two or more public cloud services.[1]
- Hybrid work is here to stay per 51% of organizations[2], making it critical to ensure least privileged access to sensitive corporate applications across cloud, offices and data centers.
- As branches connect directly to the cloud for faster connections and lower costs, the adoption of SD-WAN is growing and expected to reach 70% by 2026.[3] These direct connections to ISPs and MNOs also need to be secured.

Not only do security controls need to be adapted, but they also need to be unified. Unsurprisingly, a "Gartner survey shows 75% of organizations are pursuing security vendor consolidation."[4]

By consolidating their security management, organizations can lower their TCO, streamline day-to-day administration, ensure consistent policy enforcement and avoid compliance blind spots.

Meet Harmony SASE

Unified 10x Faster Internet Security, Zero Trust Access, SaaS Security, and SD-WAN

BENEFITS

- Single-vendor SASE with a unified console for your entire on-prem and cloud firewall estate
- Blazing-fast secure Internet access for remote users and branch offices
- Localized browsing experience with tighter security and improved privacy
- Zero Trust Access with full mesh connectivity between users, branches and applications
- Powerful visibility and control over SaaS application use within your network
- Optimized SD-WAN connectivity with full branch-level security and leading threat prevention
- Fast deployment and intuitive administration

While organizations are shifting to SASE, their current solutions break the user experience with slow connections and complex management.

Offering a game-changing alternative, Harmony SASE delivers 10x faster internet security combined with full mesh Zero Trust Access, SaaS Security, and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

With a local browsing experience supporting tighter security and privacy, Harmony SASE boasts innovative on-device network protections and secures any enterprise application with an identity-centric policy that accommodates everyone: employees, contractors, and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized internet and network connectivity, ensuring uninterrupted web conferencing thanks to seamless link failover and a built-in steering policy for over 10,000 applications.

1 Enterprise Strategy Group Complete Survey Results, 2023 Technology Spending Intentions Survey, November 2022. All Enterprise Strategy Group research references are from this survey results set unless otherwise noted.
2 Forrester.com: It's Time To Discard Outdated Conceptions Of The Office, J.P. Gownder, VP, Principal Analyst, SEP 7 2022
3 Comsoc.org - Gartner: changes in WAN requirements, SD-WAN/SASE assumptions and magic quadrant for network services
4 Gartner.com Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022, September 13, 2022

Blazing-Fast Secure Internet Access

Harmony SASE Internet Access delivers blazing-fast, secure internet access for remote users and branch offices. Thanks to a combination of cloud and on-device network protections, the service offers a localized browsing experience with tighter security and improved privacy by avoiding cloud latency and compliance concerns.

- **Comprehensive protection** - Delivers on-device network protection, web filtering, threat protection and more
- **Blazing-fast browsing** - Thanks to on-device inspection, users avoid routing traffic through the cloud for security as well as the associated latency, complexity and privacy concerns. The result is a superb browsing experience with increased speed, privacy & compliance
- **Browser security** - In-browser data loss prevention (DLP), file sanitization, and protection against phishing, corporate password reuse, and malicious search results
- **Quality of connectivity** - Sites enjoy reliable and fast internet connections thanks to Harmony SASE's global private backbone built on tier-1 network providers with middle-mile acceleration

Full Mesh Zero Trust Access

Harmony SASE Private Access lets you connect users, sites, clouds and resources with a Zero Trust Network Access (ZTNA) policy. Create an advanced full mesh global cloud network and apply least privilege access to any enterprise resource.

- **Zero Trust access for any user from any device to any resource** - Apply least privileged access to any enterprise resource with a contextual identity-centric policy that accommodates both internal and external identities. Secure BYOD, partners and consultants with agentless access, and validate device posture for managed devices.
- **Reliable, high-performance connectivity** - Delivers reliable connectivity with a full mesh global private backbone of 80+ PoPs.
- **Seamless deployment -** Create and edit networks that interconnect your sites, data centers, clouds, and users managed from an intuitive cloud console

Mobile Security

Mobile Security extends the power of Harmony SASE to mobile endpoints, delivering a seamless, secure experience for users on the move.

- **Zero-Phishing Protection** to block phishing across all apps, including zero-day threats
- **Safe Browsing and Anti-Bot** to prevent access to malicious sites and C2 servers
- **App Protection** using AI, sandboxing, and anomaly detection to stop malicious apps
- **File Protection** with real-time sandboxing to block malware before it reaches storage
- **Wi-Fi and DNS Security** to detect man-in-the-middle attacks and enforce DNS policies
- **Device Posture Checks** to block access from non-compliant devices
- **Zero-touch deployment** via your MDM (Mobile Device Management) or UEM (Unified Endpoint Management) platform.
- **User privacy and experience preserved** - No performance impact or data collection

SaaS Security

Harmony SASE provides comprehensive visibility into your SaaS applications ensuring complete coverage of your cloud environment.

- **Shadow SaaS insights** that expose hidden risks by creating a complete mapping of your organization's SaaS interconnectivity, including every application, plugin, and API
- **Extensive reporting** covering services, integrations, users, and tokens, with actionable insights and recommendations to enhance your security posture
- **Automated threat prevention** that blocks data theft, supply chain attacks, and account takeover using behavioral indicators and threat intelligence
- **Fast time-to-protect** with AI-based anomaly detection that automatically stops and alerts you to anomalous activity, leveraging machine learning and historical data on SaaS activity within and across organizations

- **Reduced SaaS attack surface** by improving native SaaS security settings, managing identity permissions, fixing misconfigurations, and disabling unused credentials
- **Automated compliance maintenance** with alerts and fixes for compliance mistakes as well as changes in your supply chain, ensuring tight regulatory adherence

SD-WAN Unified with Industry-Best Security

Check Point SD-WAN unifies the best security with optimized internet and network connectivity, ensuring uninterrupted web conferencing thanks to seamless link failover and an automated steering policy, combined with robust management and site protection.

- **Smooth Web Conferencing** - Subsecond WAN link failover with support for broadband internet, 5G cellular and MPLS connections
- **Automated Steering Policy** - Optimized routing for 10,000+ applications and users, with auto-steering based on link health including jitter, packet loss, latency
- **Mature management and security** - Zero-touch provisioning with a full branch-level security stack and industry-leading threat prevention

Enterprise Browser

For organizations that require secure access and advanced protection for unmanaged devices, Harmony Enterprise Browser isolates web sessions, enforces security posture, wipes data on exit, and prevents lateral movement – all without a persistent agent.

- **Strong data isolation** – Isolates corporate apps and data from the host device, preventing unauthorized data transfers
- **Integrated DLP controls** – Prevents unauthorized data exfiltration via downloads, copy-paste, printing, or screen captures, with options such as on-screen watermarks
- **Agentless posture checks** – Verifies the security posture of the device before granting access, despite the absence of a persistent agent
- **Full session recording, visibility, and auditing** – Provides complete visibility and reporting for user actions

Harmony SASE Feature Overview

Feature	Description
Zero-trust Network Access / Private Access	
Network access	Supports all protocols, full mesh access in any direction, all connections subject to policy with posture and identity
Agentless web access	Supported with reverse proxy, option for URL alias and customer certificate
Agentless enterprise browser	Zero Trust access for unmanaged devices with corporate data sandboxing and DLP protections including session recording and watermarking
Agentless RDP access	• Web Interface (HTML RDP), or native RDP agent (configurable options) • Support multiple screens, local printing • Security control option to limit copy-paste and printing • Configurable RDP security mode and authentication
Agentless RDP with dynamic access control	Use a single access rule, to establish a dynamic access policy that determines which specific RDP host is assigned to each user, based on IDP attribute
Agentless VNC access	Web interface
Agentless SSH access	Web interface
Device posture validation checks	Endpoint Security, Certificate, Disk Encryption, File exists, registry key, process running, windows security center, domain membership
Posture validation profiles	Multiple profiles, support all OSs
Continuous validation	Yes, configurable intervals
Additional zero-trust validations (access context)	Geo-location, Date and Time, OS, Browser
DNS filtering	Cloud resolver with DNS filtering
Firewall	Identity-based Firewall-as-a-Service
Secure Internet Access	
Malware protection	Scan all downloaded files and web components
Sandbox protection	Utilizing Check Point Threat Emulation technology and ThreatCloud AI [1]
Content Disarm and Reconstruction (CDR)	Utilizing Check Point Threat Extraction technology and ThreatCloud AI [1]
Zero-day phishing protection	Utilizing Check Point Zero-Phishing technology and ThreatCloud AI [1]
URL reputation protection	Utilizing Check Point Anti-Bot and ThreatCloud AI
URL filtering	Utilizing Check Point's URL categorization with 110 categories
HTTPS inspection	Yes
DLP	
Predefined data types	700+ including PCI, PII, HIPAA, source code and many more [1]
Supported data object types	Pattern, Keyword, Dictionary, Weighted Words, Template, File attribute [1]
Microsoft Purview sensitivity labels	Supported [1]
OCR analysis	Supported [1]
Cloud Service	
SLA	99.999%
Cloud Points-of-Presence (PoPs)	80+ global POPs, privately owned
Cloud backbone	Private backbone consisting of at least dual tier-1 providers at each PoP for fast connectivity across our network
Multiple cloud networks per customer	Support for multiple networks per account for more flexible network architectures and faster M&A consolidation
Full mesh connectivity in any direction	Full mesh cloud-based networking enables seamless private access connectivity in any direction (e.g. data center to branch, branch to user, etc.)
Network-to-Site connection	Connect from any device using IPsec, or connect with Connector software
Network-to-Site protocols	IPsec IKEv1, IPsec IKEv2, Wireguard, OpenVPN
Redundancy	Support for redundant tunnels to separate availability zones or regions

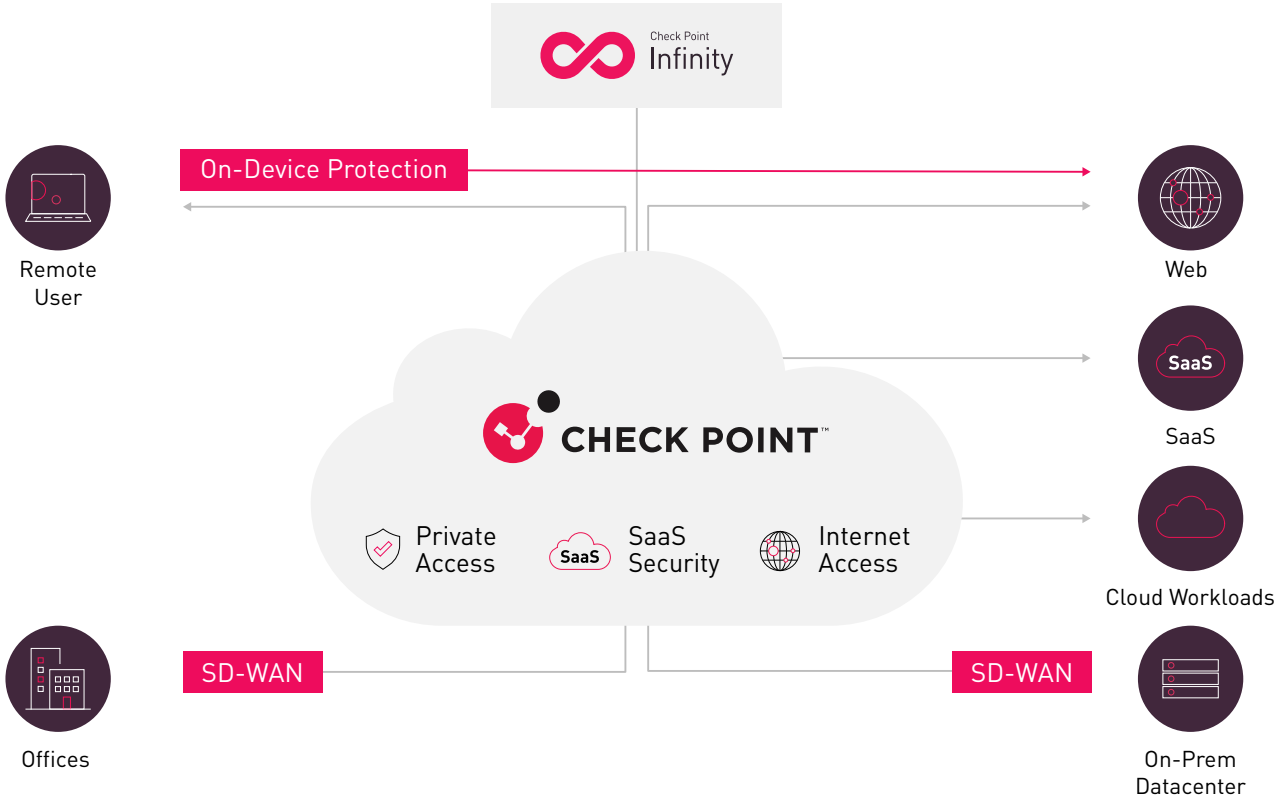
Requires the following license: (1) Browser security. (2) SaaS security. (3) Collaboration security.

Feature	Description
User-to-Site protocols	Agent: Wireguard, OpenVPN
Dedicated cloud IP per customer	Standard for all customers, enables IP-whitelisting for zero-trust access to SaaS
SD-WAN integration	Integrated with Check Point SD-WAN. Connect with 3rd party SD-WAN via IPsec
Dynamic Routing	Yes, using BGP
Data residency	United States, European Union
SASE Agent	
Supported platforms	Mac, Windows, Linux, iOS, Android, Chromebook
On-device network security - Hybrid SASE	Network security controls for Internet Access (SWG) are enforced within the agent (optional), and subject to customer policy, are routed directly to the internet service without cloud routing. This capability enables users to experience their native internet speed and delivers internet performance that is double that of traditional SSE/SWG services which force all traffic through the cloud.
Split tunnelling	Yes
Disconnect when in trusted networks	Yes
Connection protocol	Wireguard or OpenVPN - configurable
Prevent user sign-out	Yes, option to issue one-time disconnect code
Connect on launch	Yes, Configurable
Connection notification	Yes, Configurable
Control agent upgrade	Yes, Configurable per OS
Automatic Wi-Fi security	Yes, Configurable
Automatic log-out	Configurable
Identity Management	
Supported IDPs	Microsoft Entra ID, Okta, Google Workspace, Active Directory, Generic SAML (OneLogin, JumpCloud, etc.)
Authentication	SAML 2.0
Identity Management	SCIM
Multiple IDPs	Yes
Local user database	Yes
Reset user password	Yes
SaaS API Security	
SaaS application catalog [3]	10,000+ SaaS applications Display per application: Name, Description, Publisher/Vendor, Category, Website, Risk Assessment, Certification, Privacy Policy, Terms
SaaS application discovery	Discovered SaaS applications are categorized, monitored and assigned a risk score
SaaS visibility and monitoring [3]	Extensive reporting covering services, integrations, users, and tokens, with actionable insights and recommendations
SaaS Anomaly Detection [3]	Yes
Supported SaaS apps: Threat Prevention and SSPM [3]	Asana, Atlassian, AWS, BambooHR, Bitbucket, Box, Dropbox, Freshdesk, GitHub, GitLab, Google Workspace, HubSpot, Jira, Microsoft OneDrive, Microsoft SharePoint, Microsoft Teams, Monday, Okta, OneLogin, Ping Identity, Salesforce, ServiceNow, Slack, Smartsheet, Zendesk, Zoom
Supported SaaS apps: DLP and Threat Prevention[2]	Microsoft OneDrive, Microsoft SharePoint, Microsoft Teams, Google Drive, Dropbox, Box, Slack, Citrix ShareFile [3]
Logs and reports	
Log retention	3 months by default, extended period available at an additional cost
Event forwarding to SIEM	Supported using syslog
Activity monitoring	Active sessions, User activity, Web and remote access and threat prevention, Audit Logs
Certification	
SOC2 Type 2 Compliance	Certified
ISO 27001, ISO 27002	Certified
ISO 9001	Certified

Requires the following license: (1) Browser security. (2) SaaS security. (3) Collaboration security.

Single-Vendor SASE

with Unified Management and Threat Prevention



Discover Harmony SASE

Don't compromise on an excellent user experience to secure your shift to hybrid and cloud.

To see it in action sign up for a demo of Harmony SASE.

To learn more visit: www.checkpoint.com

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