SECURE ACCESS SERVICE EDGE SOLUTION

With remote work on the rise, today's enterprises are highly distributed with users and applications residing everywhere. At any given time a user can simultaneously be connected to the corporate data center, a cloud SaaS app and collaborating on a video conference while looking up something on the Internet. Connecting users direct to the Internet and cloud applications instead of backhauling traffic through a data center security stack provides a better user experience, but is it secure?

To address this digital transformation, technology is emerging to converge network and security into a cloud-delivered secure access service edge (SASE). Gartner describes this need to shift the focus of network and security design from the data center to the identity of the user and device in their paper "The Future of Network Security is in the Cloud". The SASE vision is available today.

Check Point Harmony Connect redefines SASE by making it easy to access corporate applications, SaaS and the internet for any user or branch, from any device, without compromising on security.

Built to prevent the most advanced cyber attacks, Harmony Connect is a cloud-native service that unifies multiple cloud-delivered network security products, deploys within minutes and applies Zero Trust policies with a seamless user experience.

Tightly integrating with leading SD-WAN services, Harmony Connect combines client- and cloud-based protection to deliver enterprise-grade security with less than 50ms latency and a 99.999% uptime—allowing organizations to scale remote access with peace of mind.

SECURELY CONNECT TO EVERYTHING

SASE that's built to Prevent
Unify multiple core network security products

Easy to Deploy & Manage
Deploy the solution in 5 minutes and manage from the cloud

Secures Everyone
Connect any user from any device, to any application

Secure Internet Access

Harmony Connect Internet Access provides branch offices and mobile users with easy and secure remote access to the Internet and cloud applications. Connect to a globally distributed network and security service edge for the protection you need from known and unknown zero-day threats.

Prevent Known Threats with Unfied Services

With integrated security, traffic can be decrypted once and inspected in a single pass. Application Control, URL Filtering and data loss protection (DLP) enforce safe web use. Check Point's industry leading intrusion prevention system (IPS), Anti-Bot and Antivirus protect customers from known threats. HTTPS inspection safeguards companies from threats trying to hide inside encrypted HTTPS channels.

Prevent Unknown Zero Day Threats with the Industry's Best Malware Catch Rate

Preventing unknown threats before they enter your network or your user's device saves precious incident response time for your staff and minimizes the risk of a breach.

Harmony Connect Internet Access provides the world's best[1] zero-day protection through a combination of evasion-resistant sandboxing (ThreatCloud) and revolutionary AI engines an. Empowering organizations to take a prevention-first strategy to cyberattacks, Harmony Connect defends against unknown malware, C2 botnet communications and phishing.

ThreatCloud – World's Most Powerful Threat Intelligence

Comprising the largest repository of real-time, security intelligence—utilized in four billion security decisions daily—Check Point ThreatCloud is an advanced cloud-based sandboxing service that examines suspicious files to determine if they are malicious or benign before they ever enter your network or are downloaded to a user's device.

Powering Harmony Connect's zero day protection, ThreatCloud gleans cyber attack data from:

- Hundreds of millions of protected assets worldwide across cloud, endpoints and networks
- Top notch research by Check Point Research Labs
- The industry's best threat intelligence feeds
- AI enrchiment with predictive threat intelligence

Real-time Protection from the Latest Exploits (IPS)

When it comes to protecting browsers, applications (e.g. PDF readers) and systems against the latest CVEs, Check Point leads in time to virtually patch against the newest threats[2].

Our development team's solid track record in responding to new vulnerabilities ensures that organziations who have not had time to apply patches are still virtually patched and protected against the latest gaps.

Protect Sensitive Data Before It Leaks Out (DLP)

Working remotely expands your attack surface, especially as users access the internet and cloud outside the corporate firewall.

Harmony Connect's cloud DLP service blocks sensitive date before it is uploaded to other sites and services, e.g. public cloud drives, social networks etc. with granular policy configuration and integrated web application control, supporting real time inline protection to identify numerous data types.

Unified Security Management

Apply a consistent security policy to protect remote offices and users. Centrally manage cloud security service policy and threats using a browser connected to the customer's cloud tenant.

[1] Based on independent third party testing by NSS Labs Breach Prevention System (download report here)

[2] Based on availability of IPS protections (aka signatures) against latest CVEs in leading vendors' solutions

Securely Connect Remote Users

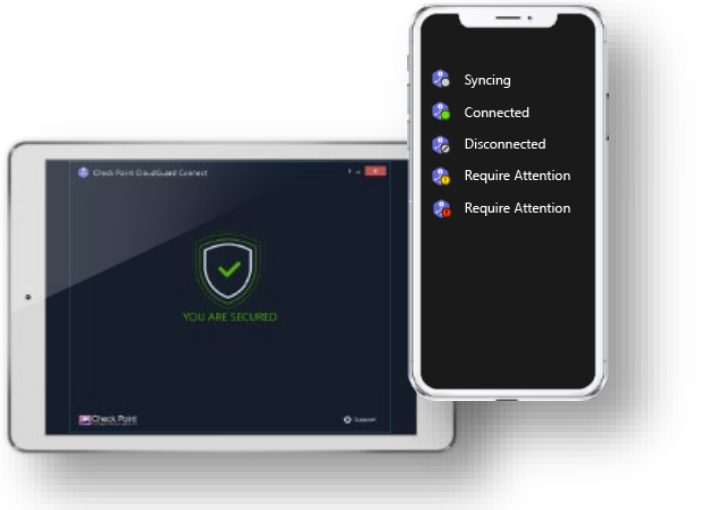
Authenticate and secure remote user connections to the Internet. A lightweight client authenticates to the cloud security service. SSO options with SAML Identity Providers such as Okta, Ping Identity, OneLogin, ADFS and Azure AD are available.

Data in transit from the client to the cloud service is private and secured in an IPsec or GRE VPN tunnel. The cloud security service inspects the connection to the Internet in a single pass according to poli

Resilient Cloud Platform

Harmony Connect Internet Access offers a fast connection for any user anywhere thanks to:

- Global network of 100+ POPs
- High availability with 99.999% uptime
- High performance1 Gbps tunnel and 50ms latency
- Integrations with leading SD-WAN and vWAN vendors: Azure, VMware, Silver Peak, Cisco, Citrix, Aruba (HPE), Aryaka, Nuage Networks (Nokia), Asavie, Cradlepoint, Versa and more



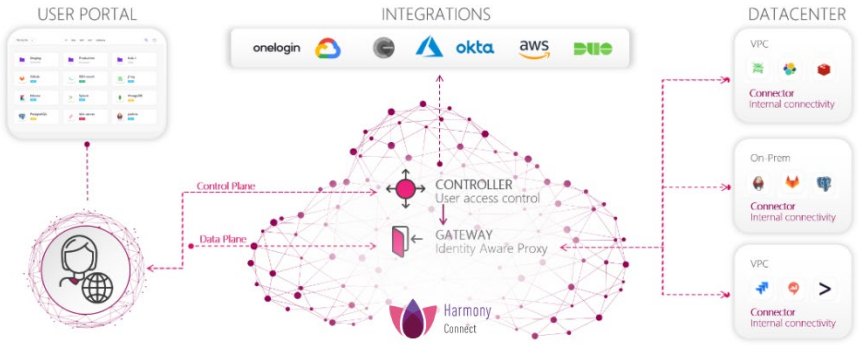
Quickly Connect Users and Offices

With a simple and easy setup process, network traffic from existing SD-WAN edge devices are tunneled over IPsec or GRE to a primary cloud-based network security service at a nearby location. A second connection provides redundancy. This ensures branch offices stay connected. Using a RESTful API, site deployment is automated and removes the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing overall CAPEX and OPEX costs.

Remote users are on boarded by deploying a lightweight client via Microsoft Group Policy Object (GPO) or by sending an email invite to users.

Secure Corporate Access

Deployed in just five minutes, Harmony Connect Remote Access offers clientless remote access to any internal corporate application residing in the data center, IaaS, public or private clouds. Our agentless solution allows teams to manage access to web applications, servers and databases in a single unified location, with full visibility on all user activity.



Connect in Seconds

An innovate Zero Trust network Acccess Service (ZTNA-as-a-service), Harmony Connect Remote Access provides users with an agentless, SaaS-like user experience when connecting to enterprise applications residing on-premises or in the cloud. There is no endpoint agent to install, appliances to deploy, or maintenance to perform. Access is provided in one-click from a browser to corporate applications such as web, RDP, SSH and database servers.

Simply set up a Docker container to create a connection to our cloud proxy. Connect an Identity Provider to onboard users and groups. Then define your Access Policy. You can also leverage native APIs to setup access in seconds.

Integrate with your Identity Provider

Create and manage your users, groups and access policies directly inside Harmony Connect Remote Access or integrate with your existing Identity Provider such as Azure AD, ADFS, Okta, OneLogin, Keycloak and Ping Identity.

Resilient Cloud Native Architecture

As shown in the diagram, Harmony Connect Remote Access is comprised of the following components:

- **User Portal**: provides agentless secure access
- **Control Plane**: authenticates users internally or externally via IdPs such as Okta
- **Data Plane**: a proxy providing least privileged access to web, RDP, SSH, database servers and more as set by policy
- **Application Connectors**: a Docker container or VM providing a secure outbound connection from the applications to the Data Plane

Zero-trust Network Access

Harmony Connect Remote Access provides Layer-7 access to only the applications allowed by policy after authenticating the user. Authentication and authorization is set before the user logs in. Application connectors conceal the datacenter applications from discovery and DDoS attacks.

Harmony Connect provides granular access control over and within each resource based on the dynamic and contextual assessment of user attributes and device state. A rich set of rules can be enforced across all user, servers and enterprise data stores including user commands and database queries.

Reduce the risk of lost or compromised keys by managing SSH keys in a central and secure location.

Automatically Monitor and Terminate User Sessions in Real Time

Get a full audit trail of user activity, including SQL queries, each POST and GET, and executed SSH commands. All audit logs are tied to users' accounts and devices, and can be exported to your SIEM for additional contextual data. Control access to sessions and block suspicious commands in real time. An optional feature is full video recordings of user sessions.

DevOps and Engineering Access

Engineering teams need to leverage the agility and flexibility of cloud-based development and production environments, without compromising security.

Harmony Connect secures DevOps and Engineer access through a wealth of cloud-native capabilities including:

- Privileged Access Management (PAM-as-a-service)
- Instant cloud deployment
- Automated server onboarding (AWS)
- Tag-based management
- Full audit trail and optionally session recordings

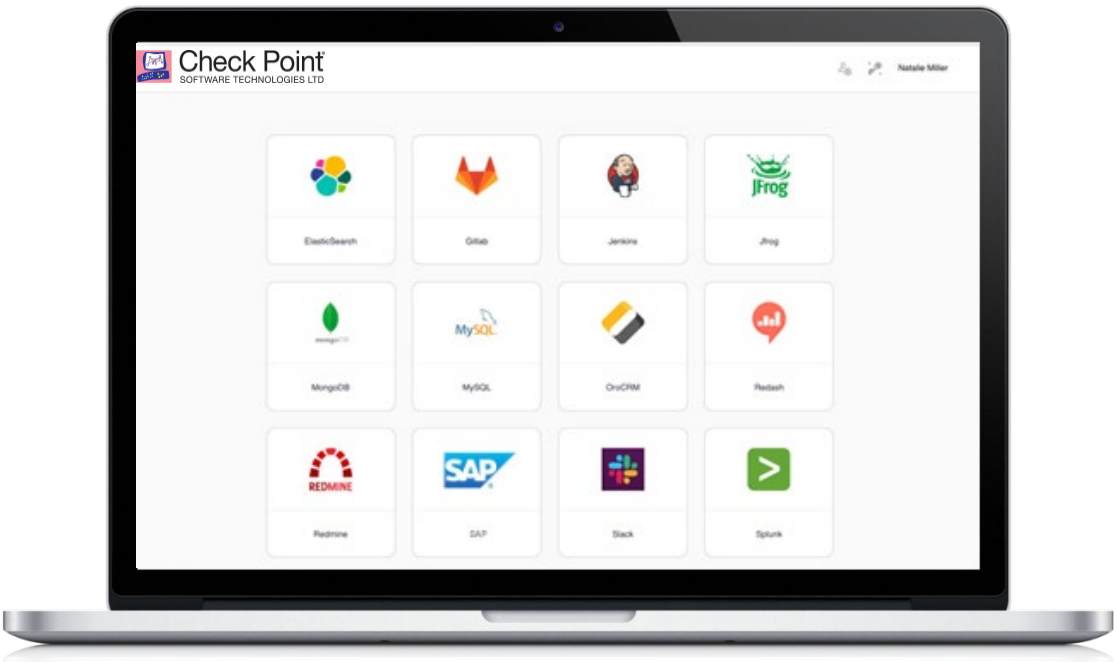
Easily provision and de-provision access to virtual machines, applications or IaaS/PaaS services as needed with secure key management and server single sign-on.

Third Party Access with Zero Trust

Managing partner and consultant access to sensitive data at scale is a nearly impossible task, exposing companies to potential security risk. And perimeter-based solutions provide no visibility into user activity.

Harmony Connect's innovative ZTNA-as-a-service makes it easy to secure third party access thanks to:

- Clientless architecture, with no agent required
- SaaS-like user experience from any browser
- Granular access controls, to and within apps
- Quick setup
- Lightweight posture check (coming soon)



SOLUTION SPECIFICATIONS

Harmony Connect Internet Access

Core Security Services	
Inline Security	Harmony Connect: Outbound network firewall, Application Control, URL Filtering (SWG), Content Awareness (DLP), IPS, Anti-Bot, Antivirus, SandBlast Threat Emulation (sandboxing)
Protocols Inspected	All ports, all protocols including SSL/TLS
Applications and Websites	110+ categories and granular control of 8,500+ applications
Data Types	40+ pre-defined data types including PCI, PII, HIPAA, source code and more
Use Cases	SASE solution to protect remote, mobile users and branch office Internet access from advanced threats

Cloud Services	
Branch-to-Site Connection	IPsec IKEv1, IPsec IKEv2 or GRE tunnels
Redundant Availability Zones	Yes
SLA	99.999% uptime
Availability Regions	US South-East, US North-East, US South-West, US North-West, Canada, Italy, Germany, France, Sweden, Ireland, United Kingdom, Hong Kong, South Korea, Singapore, Japan, Australia, India, Brazil, Bahrain and South Africa
Multiple Branch IP	Yes
Dynamic Branch IP	Yes
SAML Identity Providers	Azure AD, ADFS, Okta, OneLogin, Ping Identity[3]
SIEM Integrations	syslog formatted for Splunk CIM, CEF, LEEF

Performance	
Single IPsec Tunnel	Up to 870 Mbps per tunnel
Latency	up to 50 milliseconds

Branch Edge Device	
SD-WAN	Aruba SD-Branch (HPE), Aryaka, Asavie, Cisco, Citrix, Cradlepoint, Nokia Nuage Networks, Oracle Talari, Silver Peak, Versa, VMware
Other	Generic GRE or IPsec capable devices, Microsoft Azure Firewall Manager

Remote User Internet Access	
Managed Devices	Windows, macOS, Linux[2]
Routing	Direct to trusted cloud applications (see sk170299)
Unmanaged Devices	Browser access based on device posture and compliance[2]
App Deployment	Email invite or any endpoint management tool including Microsoft Group Policy Object (GPO), Jamf, Altiris, HP IMC, and more. See sk172550
Compatibility with 3rd party Apps	✓
App Port Use	UDP port 1194 (accelerated traffic option) with a fallback to TCP 443
Location Awareness	Automatically disconnect when in office
End user Deactivation	Optional requirement to use a deactivation code to suspend the App
App Security	Optional requirement to use a code to uninstall the App

[3] For details on other SAML identify providers, visit our knowledge base.

Harmony Connect Remote Access

Core Security Services	
Clientless Architecture	Zero Trust Network Architecture, Web browser access, clientless access to corporate applications; Web, SSH, RDP and SQL
Full Visibility and Control	Full audit trail, monitor all actions, optional session recordings
PAM and SSO	Integrates with IdP for strong MFA authentication, built-in key management and credential vaulting
Use Cases	Remote employee access including DevOps and Engineering, and granular third party temporary access control

Remote Access Specifications	
Browsers Supported	any HTML5 capable browser; Chrome, Firefox, Edge, IE, Safari, etc.
Applications Supported	Web, RDP, SSH, SQL, PSQL
Identity Stores	internal or SAML IdP, SAML 2.0 IdP, LDAP, Web Services Federation (used by ADFS)
SAML Identity Providers	Azure AD, ADFS, Okta, OneLogin, Ping Identity
Key Management	✓
Infrastructure Communications	TLS 1.2
App-level SSO and MFA	✓
Application Discovery	AWS Discovery of Windows and Linux servers
Connector Options	Docker, Kubernetes, cloud image
Load Balancing/Redundancy	up to 5 connectors per account
Connector Performance	250 Mbps per connector, up to 1,250 Mbps across 5 connectors

[1] The expected additional latency for a branch in the same Harmony Connect region [2] Roadmap

Cloud Services	
SLA	99.999% uptime
Availability Regions	US South-East, US North-East, US South-West, US North-West, Canada, Italy, Germany, France, Sweden, Ireland, United Kingdom, Hong Kong, South Korea, Singapore, Japan, Australia, India, Brazil, Bahrain and South Africa
SAML Identity Providers	Azure AD, ADFS, Okta, OneLogin
SIEM Integrations	syslog formatted for Splunk CIM, CEF, LEEF

Harmony Connect Management

Management	
Cloud-hosted Web Management	Asset deployment, security policy and threat management
On-premises Management	Internet Access via a SmartConsole extension
Internet Access API	sc1.checkpoint.com/documents/latest/api_reference/
Remote Access API	docs.odo.io/reference
Log Management	Stored for 1 month (Remote Access), 2 weeks (Internet Access) by default
SOC2 Type 2 Compliance	Available on request
Privacy Statement	see sk164292

ORDERING HARMONY CONNECT SASE

DESCRIPTION	SKU[1]
Harmony Connect Remote Access - Service subscription for one user for one year	CP-HAR-RA-1Y
Harmony Connect Internet Access - Service subscription for one user for one year	CP-HAR-IA-1Y

[1] 2, 3, 4 and 5 year SKUs are available in the online product catalog.

Managed Security Service Provider (MSSP) Options

For details on subscription through MSSPs, including pay-as-you-go pricing, please contact us.

Harmony Product Suite Bundle

Harmony unifies security for users, devices and access, reducing management complexity and costs while increasing security. Purchase any three or more Harmony products or the complete Harmony bundle for less than you would pay for each product. All packages include cloud management from the Check Point Infinity Portal.

Harmony Total Suite		CP-HAR-TOTAL-1Y
✓	Harmony Connect Internet Access	CP-HAR-IA-1Y
✓	Harmony Connect Remote Access	CP-HAR-RA-1Y
✓	Harmony Email & Office	CP-HAR-EMAIL-OFFICE-1Y
✓	Harmony Endpoint	CP-HAR-ENDPOINT-1Y
✓	Harmony Mobile	CP-HAR-MOBILE-1Y
✓	Harmony Browse	CP-HAR-BROWSE-1Y

Harmony Connect:

Internet Access and/or Remote Access for clientless and client-based remote access to enterprise applications and secure Internet access for users and branch offices.

Harmony Email and Office:

Complete protection for Office 365 and G Suite to block sophisticated phishing attacks, protect sensitive business data (DLP), prevent account takeover and block malware without impacting productivity.

Harmony Endpoint:

A complete endpoint security solution including FDE, anti-ransomware, zero-phishing, malware and file-less attack protections, credential theft prevention, sandboxing and Content Disarm & Reconstruction (CDR) technologies.

Harmony Mobile:

Delivers complete mobile threat defense for your mobile workforce that is simple to deploy, manage and scale including protection from malicious apps, network protection, OS and device protection.

Harmony Browse:

In-browser protection inspects 100% of SSL traffic to prevent malware downloads, prevent phishing attacks and corporate credential reuse and block access to websites deemed inappropriate by company policies.