CHECK POINT™

HARMONY CONNECT
CHECK POINT'S SASE SOLUTION

THE ONLY PREVENTION-FIRST
SECURE ACCESS SERVICE EDGE

CONNECTIVITY AND SECURITY NEEDS ARE EVOLVING

New work models require new security para-digms, as organizations shift from a concentrated, centralized IT model to a widely distributed one. Remote and hybrid work are the new normal. Applications reside everywhere, consumed as SaaS (e.g Office 365) or hosted on premises and cloud-based data centers (IaaS). And branch offices increasingly bypass security engines to connect directly to the cloud.

THE RESULT: COMPLEXITY IN ENSURING, MANAGING AND SCALING NETWORK SECURITY

The new perimeter, defined by cloud, mobile and remote work has signification implications on the entire organization:

Complex Management

- Scaling hardware-dependent remote access infrastructure impedes agility.

- Managing multiple point products leads to high overhead and inconsistent policies.
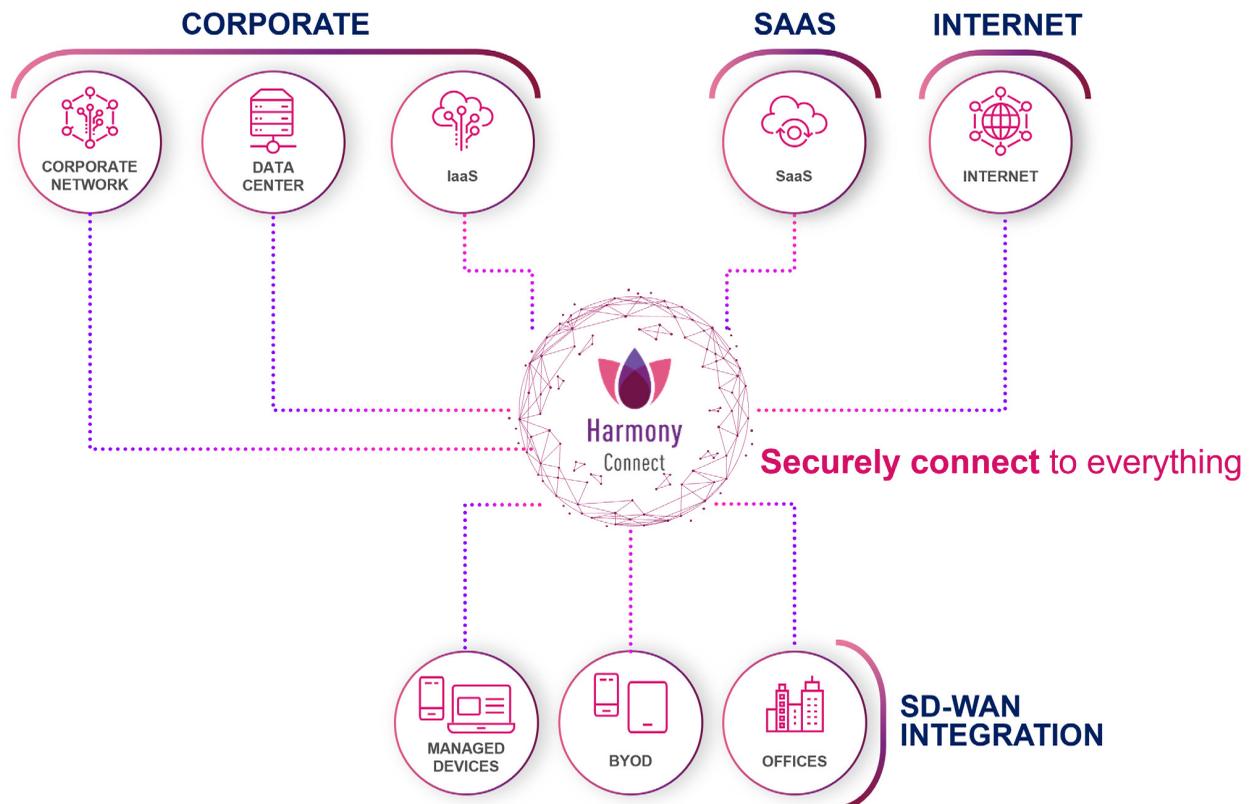
Increased Security Risk

- As users access networks and applications outside the perimeter firewall, your organization's attack surface expands.

- Broad network access increases the risk of lateral movement and can lead to a breach.

- Supporting secure access for unmanaged and BYOD devices becomes challenging.

Poor User Experience

- Routing all internet and cloud-bound traffic to the on-prem datacenter for security inspection causes congestion, latency and downtime for users.

Fragmented Visibility

- Disparate solutions make it difficult to gain a single audit trail of all user activity, and obfuscate the organization's true security posture.

CORPORATE

CORPORATE NETWORK · DATA CENTER · IaaS

SAAS — SaaS

INTERNET — INTERNET

Harmony Connect

Securely connect to everything

MANAGED DEVICES · BYOD · OFFICES

SD-WAN INTEGRATION

HARMONY CONNECT: SECURELY CONNECT TO EVERYTHING

To secure the distributed enterprise, organizations need a Secure Access Service Edge (SASE) architecture.

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

Delivering the only prevention-focused Security Service Edge (SSE), Harmony Connect is a cloud-native service that unifies multiple network security products, deploys within minutes and applies Zero Trust access policies with a seamless user experience.

Combining client-based and cloud-based protection to deliver enterprise-grade security with less than 50ms latency and a 99.999% uptime, Harmony Connect allows organizations to scale remote and hybrid work with peace of mind.

For a full SASE architecture, Harmony Connect offers tight integrations with leading SD-WAN services.

INDUSTRY LEADING NETWORK SECURITY FOR ENTERPRISE USE CASES

Harmony Connect provides comprehensive security from the cloud to apply a zero trust policy to enterprise applications in the datacenter, IaaS or SaaS applications, secure internet access and browsing for remote users, and protects direct connections from branch offices to the cloud by securing organizations' current SD-WAN infrastructures.

BENEFITS

- Industry's best malware catch rate at 99.7% with top-rated threat prevention[1]
- Zero Trust Network Access (ZTNA) with choice of network- or application-level access to cloud and on-prem apps
- Rich clientless ZTNA; ideal for BYOD, partners, contractors, engineers and DevOps
- Full protection of remote user internet access with a cloud SWG
- Consistent branch & SD-WAN security with a Next Gen Firewall-as-a-service (FWaaS)
- Cloud Access Security Broker (CASB) with inline and API-based SaaS Security
- Consume security-as-a-service
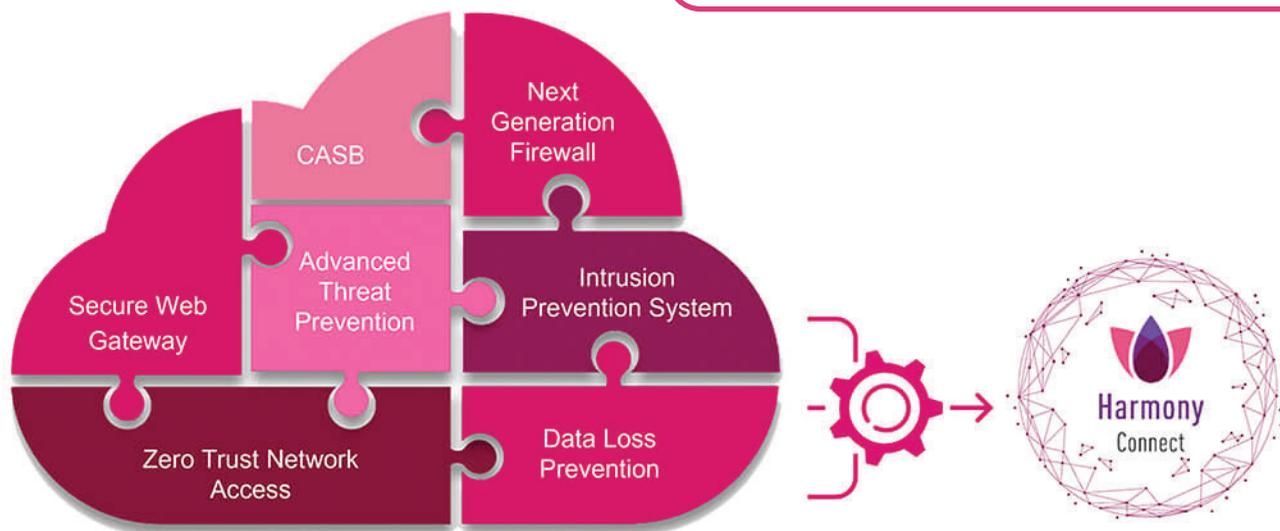
[1] Per Testing by Miercom NGFW Security Benchmark 2023

Zero Trust Network Access

Harmony Connect Remote Access takes only five minutes to deploy and enforces an identity-centric zero trust access policy to secure any internal corporate application residing in the data center, IaaS, public or private clouds.

By integrating with enterprise identity providers, user access is secured by single sign on and multi-factor authentication, with additional assurance offered by Harmony Connect's device posture validation.

The service comes in two flavors that can be deployed side-by-side from the same console to accommodate different use cases and personas. As detailed below, these include clientless-application level access and client-based network-level access.

CLIENTLESS APPLICATION-LEVEL ACCESS

Harmony Connect Remote Access offers clientless remote access to any internal corporate application residing in the data center, IaaS, public or private clouds. With no agent installation or management required, the clientless deployment option is ideal for BYOD and third party users, such as contractors and partners.

Thanks to intuitive access to Web, RDP, SSH and SQL-based resources, the service is both user and management friendly, while catering to the needs of diverse personnel. Business and third-party users enjoy agentless access, administrators gain complete visibility and granular in-app controls, while DevOps benefit from a wealth of cloud-native capabilities including privileged access management (PAM) and automated server onboarding.

CLIENT-BASED NETWORK-LEVEL ACCESS

Harmony Connect Remote Access also offers a client-based network-level access deployment option, delivering VPN-as-a-service that provides the power of layer-3 network connectivity, secured by customizable Zero-Trust access policy.

Ideal for employee access from any managed device, this option is more versatile in supporting applications and protocols, with embedded cloud DLP and industry-leading IPS to protect your apps from the latest vulnerabilities (such as Log4J).

For increased remote access security, network-level access is protected with device posture validation (optional), performing additional checks before access is granted.

Remote Access Service
FEATURES

Zero Trust Network Access

Choice of Layer 3 and Layer 7 access

Embedded Cloud DLP and IPS

Clientless Access to Web, SSH, RDP and SQL Applications

Choice of native RDP or web RDP access (no VPN client required)

Ideal for BYOD and Third Party Access

Full Visibility

Complete Audit Trail

Monitor All Actions

Session Recordings

Identity and Authentication

Integration with 3rd party Identity Providers
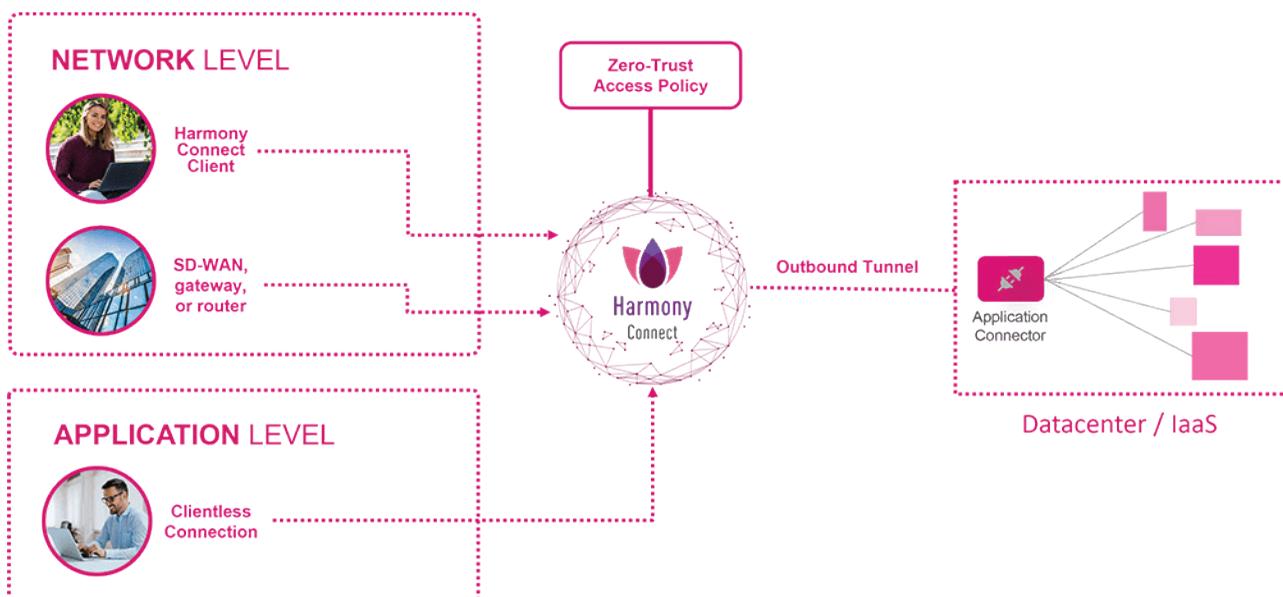
Built-in PAM and SSO

Local User Directory

Credential Vaulting

Customizable Session Timeout

Device Posture Validation

Device Certificate Validation

TO LEARN MORE: Download the Guide | Sign Up for a Demo | ZTNA Web Page

NETWORK LEVEL

Harmony Connect Client

SD-WAN, gateway, or router

APPLICATION LEVEL

Clientless Connection

Zero-Trust Access Policy

Harmony Connect

Outbound Tunnel

Application Connector

Datacenter / IaaS

Internet Access for Remote Users

How do you protect your users as they browse the web for their personal use, and prevent the latest phishing and malware attacks from reaching them?

Delivering the safest browsing experience from a single intuitive policy, **Harmony Connect Internet Access** is a cloud Secure Web Gateway that blocks phishing sites in real time, prevents zero-day malware through advanced sandboxing and protects against the latest vulnerabilities and browser exploits with a cutting-edge cloud IPS (intrusion prevention system) for deep packet inspection (virtual patching).

The services inspects all internet traffic across all ports and protocols, with granular access control to 10,000+ precategorized internet and SaaS applications, including peer-topeer (P2) apps, anonymization services, and consumer VPNs. Using a single, intuitive policy, access controls are applied for users, groups and branches leveraging patented technology[2], while data is protected with an embedded cloud DLP (data loss prevention system).

Harnessing the power of ThreatCloud, which combines 30+ AI engines with big data threat intel, the service ensures that every connection is thoroughly vetted, while leveraging the Harmony Connect client for accelerated connectivity.

Secure Web Gateway
FEATURES

Threat Prevention

Zero-day Sandboxing

Intrusion Prevention System (IPS)

Phishing Prevention

Malware and C2 Bot Prevention
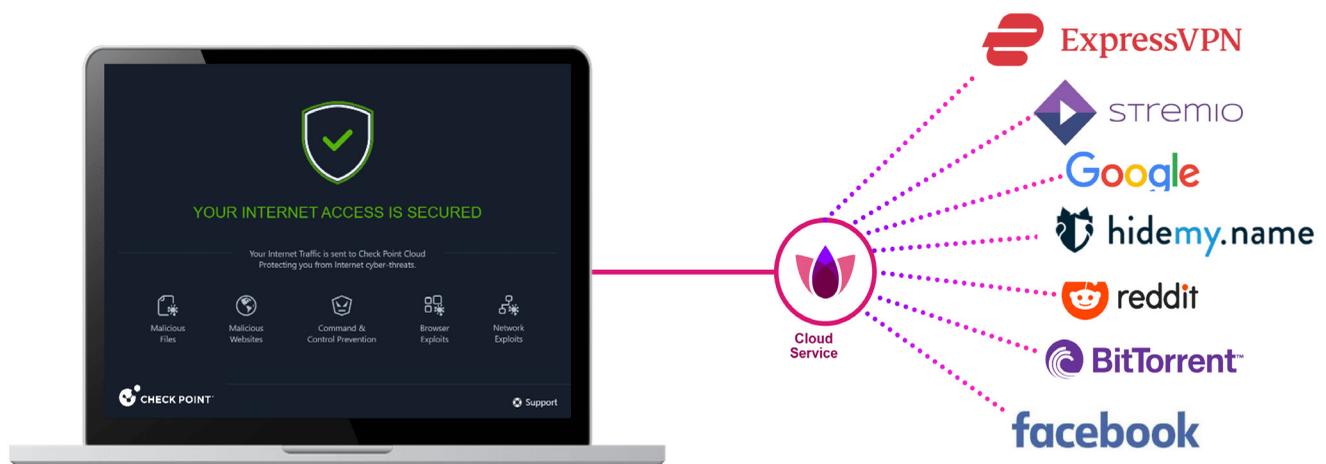
Full traffic inspection across all ports and protocols

Access Control

Cloud Firewall

URL Filtering

Customer and Non-Enterprise Apps (10,000+)

Data Protection

Cloud DLP

Granular Policy

Predefined Data Types

TO LEARN MORE: **Download the Guide** | **Sign Up for a Demo** | **SWG Web Page**

[2] For example, USPTO 11411924

Cloud Access Security Broker (CASB)

Outside the confines of the corporate firewall, how do you protect your users and data from the threats posed by day-to-day use of SaaS applications and shadow IT?

Harmony Connect serves as a Cloud Security Access Broker (CASB) offering both in-line and API-based SaaS security with rich DLP capabilities, granular zero trust SaaS access and authorization controls, and visibility into both authorized and unauthorized SaaS usage.

The service ensures that every file uploaded, downloaded and shared is thoroughly inspected and vetted for threats, while adhering to enterprise policy, leveraging the power of ThreatCloud, which combines 30+ AI engines with big data threat intelligence.

The service is delivered in two complementary modes, which can be managed side-by-side: API-based security for authorized enterprise applications and in-line SaaS security for the longtail of SaaS apps used, including shadow IT apps.

API-based SaaS security

API-based SaaS security offers more granular data protection controls and threat defense mechanisms for select SaaS apps. This includes preventing data leakage and threat propagation via file-shares such as OneDrive, Google Drive and Dropbox, as well as within chats on Teams, Slack, Zoom and other collaboration apps.

Inline SaaS security

Inline SaaS security offers more granular app and in-app access controls for thousands of SaaS applications and shadow IT, including policy relating to accessing, uploading, downloading, editing, and file sharing via SaaS apps across audio, video, messaging and files.

SaaS Security
FEATURES

SaaS Visibility

SaaS App Discovery
Shadow IT Cloud Usage
Authorized Cloud Usage
Logging
Alerting

Access Control

Credential Mapping
Authentication
Single Sign On
Authorization
Alerting

Rich Data Protection

Cloud DLP
Advanced Granular Policy e.g. upload, download, share, edit, chat, video, audio
Predefined Data Types

Threat Protection

Zero-Day Sandboxing
Intrusion Prevention System (IPS)
Full Traffic Inspection across all ports and protocols
Phishing Prevention
Malware Prevention
Content Disarm and Reconstruction (CDR)

INLINE SaaS SECURITY

10,000+ apps

SaaS API SECURITY

Internet and Cloud Access for Branch Offices

As companies with multiple branch offices and retail locations connect directly to the internet and cloud using their software-defined wide area network (SD-WAN) infrastructure, they need a way to prevent threats from entering their branch and retail networks. Offering comprehensive Secure Web Gateway features (as above), and deployed in minutes, **Harmony Connect Internet Access** offers tight integrations with leading SD-WAN vendors using advanced APIs, allowing consistent security to be enforced across thousands of sites with just a few clicks.

INTEGRATES WITH LEADING SD-WAN VENDORS

Microsoft Azure · CISCO · nuagenetworks From Nokia · velocloud Now part of VMware · aryaka · ORACLE Talari · CITRIX · cradlepoint · VERSA NETWORKS · aruba a Hewlett Packard Enterprise company · silver peak · Extreme networks

Firewall-as-a-Service
FEATURES

Setup & Management

Integrates with your current SD-WAN infrastructure

Consistent policies across 1000s of branches

Secures a new branch in less than 5 minutes

Threat Prevention

Zero-day sandboxing

Intrusion Prevention System (IPS)

Phishing prevention

Malware and C2 bot prevention

Full traffic inspection across all ports and protocols

Access Control

Cloud Firewall

URL Filtering

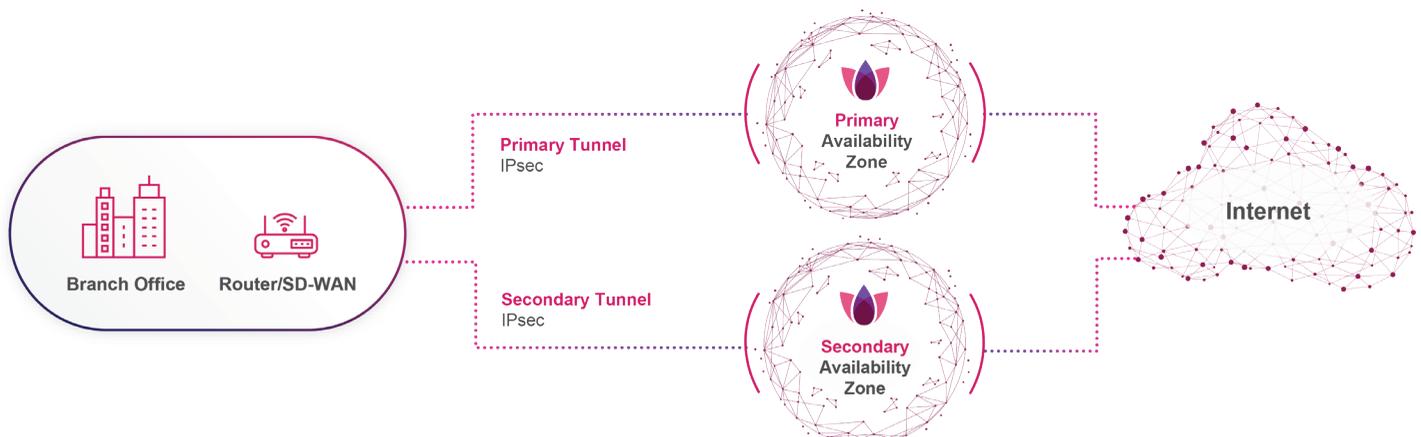Application Control (10,000+ Apps)

Data Protection

Cloud DLP

Granular policy

Predefined data types

TO LEARN MORE: **Download the Guide** | **Sign Up for a Demo** | **FWaaS Web Page**

Branch Office   Router/SD-WAN

Primary Tunnel IPsec

Secondary Tunnel IPsec

Primary Availability Zone

Secondary Availability Zone

Internet

ORDERING HARMONY CONNECT SASE

DESCRIPTION	SKU
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
Harmony Total Suite – Service subscription for one user for one year for all Harmony products: • Harmony Connect Internet Access • Harmony Connect Remote Access • Harmony Email & Collaboration • Harmony Endpoint • Harmony Mobile • Harmony Browse	CP-HAR-TOTAL-1Y

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

TECHNICAL SPECIFICATIONS
For Harmony Connect technical specifications, partners and customers can visit the Check Point Support Center here: sk179269.

HARMONY TOTAL - 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.

MANAGED SECURITY SERVICE PROVIDER (MSSP) OPTIONS
For details on subscription through MSSPs, including pay-as-you-go pricing, please contact us.

Discover Harmony: The First Unified Solution for Users, Devices and Access

Harmony Connect is part of the Check Point Harmony product suite, the industry's first unified security solution for users, devices and access. Harmony consolidates six products to provide uncompromised security and simplicity for everyone. It protects devices and internet connections from the most sophisticated attacks while ensuring Zero-Trust Access to corporate applications—all in a single solution that is easy to use, manage and buy.

Visit us at: https://www.checkpoint.com/harmony/connect-sase/

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com