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 11 security products, deploys within minutes and applies Zero Trust policies with a seamless user experience.

Tightly integrated with leading SD-WAN services, Harmony Connect combines browser- 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 11 security products with ZTNA and top-rated threat prevention

Easy to Deploy & Manage

Deploy the solution in 5 minutes and manage from the cloud

Secure your Everyone

Connect any user, any device, any application, securely from the cloud

Secure Internet Access

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

Unify Services to Reduce Complexity

With integrated security, traffic can be decrypted once and inspected in a single pass. Application Control, URL Filtering and Content Awareness (DLP) enforce safe web use. 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 Threats

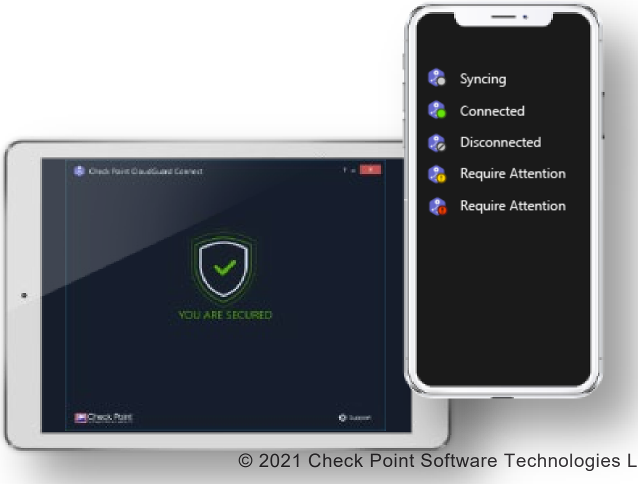
Preventing threats before the damage is done saves staff valuable time when responding to threats. Check Point SandBlast Zero-Day Protection is a cloud-hosted sandboxing technology where files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network.

Unify 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.

Securely Connect Remote Users

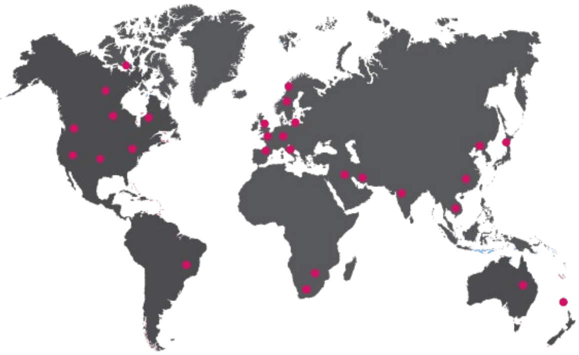
Authenticate and secure remote user connections to the Internet. A lightweight client authenticates to the cloud security service. SSO options with SAML Identity Providers such as Okta, Ping Identity, OneLogin, ADFS and Azure AD are available.



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

Resilient Cloud Platform

Global network of 100+ POPs
High availability with 99.999% uptime
High performance1 Gbps tunnel and 50ms latency
Integrations with leading SD-WAN vendors; VMware, Silver Peak, Cisco, Citrix, Aruba, Aryaka, and more



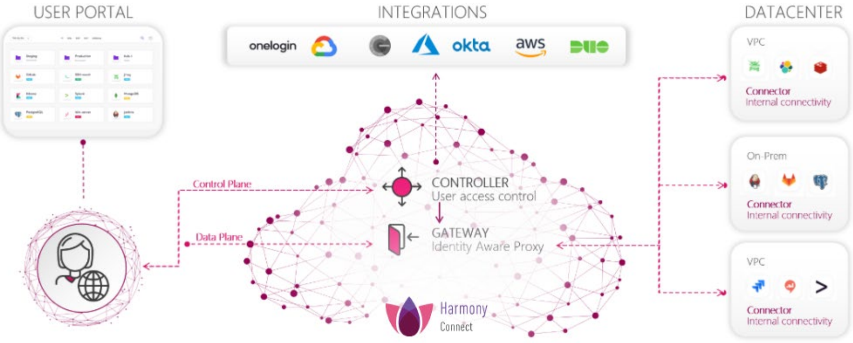
Quickly Connect Users and Offices

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 near-by 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

Check Point's Corporate Access platform helps IT and DevOps engineers to simplify, secure and scale network access across multi-cloud and on-premises infrastructures. 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

Corporate Access provides users with an agentless, SaaS-like user experience. 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 on-board 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 through Corporate Access or integrate with your existing Identity Provider such as Azure AD, ADFS, Okta, OneLogin, Keycloak and Ping Identity.

Resilient Cloud Native Architecture

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

Check Point Corporate 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. Also application connectors conceal the datacenter applications from discovery and DDoS attacks.

Corporate Access 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.

Monitor Application Use

Get a full audit trail of user activity, including 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.

Control DevOps and Engineering Access

Engineering teams need to leverage the agility and flexibility of cloud-based development and production environments, without compromising security. Corporate Access Privilege Access Management (PAM) provides automated cloud asset discovery, tag-based policies, secure key management and SSO session recording. Administrators can leverage the cloud-native access platform to effortlessly provision and de-provision access to virtual machines, applications or IaaS/PaaS services as needed.

.

SOLUTION SPECIFICATIONS

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
SIEM Integrations	syslog formatted for Splunk CIM, CEF, LEEF
Software	
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 8,000+ applications
Data Types	40+ pre-defined data types including PCI, PII, HIPAA, source code and more
Performance	
Single IPsec Tunnel	Up to 1 Gbps per tunnel
Latency	up to 50 milliseconds[1]
Management	
Cloud-hosted Web Management	Asset deployment, security policy and threat management
On-premises Management	via a SmartConsole extension
API	sc1.checkpoint.com/documents/latest/api_reference/
Branch Edge Device	
SD-WAN	VMware, Silver Peak, Cisco, Citrix, Aruba SD-Branch, Aryaka, Versa
Other	Generic, Microsoft Azure Firewall Manager
Device Security	
Managed Devices	Windows, macOS, Linux[2]
Routing	Direct to trusted cloud applications
Unmanaged Devices	Browser access based on device posture and compliance[2]
Browser	Browser Extension[2]
Corporate 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 Identity Providers	Azure AD, ADFS, Okta, OneLogin, Keycloak
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
API	docs.odo.io/reference

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

ORDERING HARMONY CONNECT SASE

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

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