Check Point
SOFTWARE TECHNOLOGIES LTD

Harmony Connect

Harmony Connect Remote Access

Zero Trust Network Access for the Modern Enterprise

Harmony Connect Remote Access is a simple, secure and centralized platform that enables IT and DevOps teams to manage remote access across multi-cloud and on-premises infrastructures, without the need for VPNs. Our zero-trust architecture enables administrators to provide least privilege access to company resources while receiving full visibility on all user activity. And, unlike other approaches, Harmony Connect Remote Access is completely agentless and delivers value across the entire organization – with support for Web, SSH, RDP and database protocols.

CHALLENGE

Work has changed. Network access solutions have not. The new reality for IT and DevOps engineers is defined by the cloud, mobility, and increasing demands for agility. Yet, in spite of this new reality, companies are still using legacy access solutions like VPNs. The problem is, they are nearly impossible to manage at scale, cannot secure a shifting attack surface and provide no visibility into what people are actually doing.

BENEFITS

Least Privilege Access to Corporate Resources

Provide granular access for each corporate resource (and within each resource) based on dynamic and contextual access permissions. Easily add (or remove) applications, data centers, employees and contractors in any location, with Check Point's cloud-native access solution designed for multi-cloud, multi-site, and multi-region environments.

Receive a Full Audit Trail of User Activities

Get a full audit trail of user activity, including executed SSH commands and fully recorded sessions. Check critical actions carried out by users on their own accounts. Narrow audit logs to show specific events or users. Export logs to your SIEM for additional contextual data.

Reduce Security Risk

Provide granular access at the application layer, eliminating any network level access and mitigating the risk of network level attacks. Easily adjust and enforce access policies to block suspicious events in real-time.

Improve User Experience

Give users a quick and secure connection to any resource through their terminal, without the need to use outdated VPNs, with thick clients and unstable connectivity.

USE CASES

VPN Replacement

Today's workforce is mobile and they need access to any application, hosted anywhere, and from any device. Our zero-trust architecture replaces traditional binary security models that focus on letting good guys in and keeping the bad guys out, with a model where the perimeter moves with your users, who must be consistently authenticated and verified prior to being given access to sensitive company data.

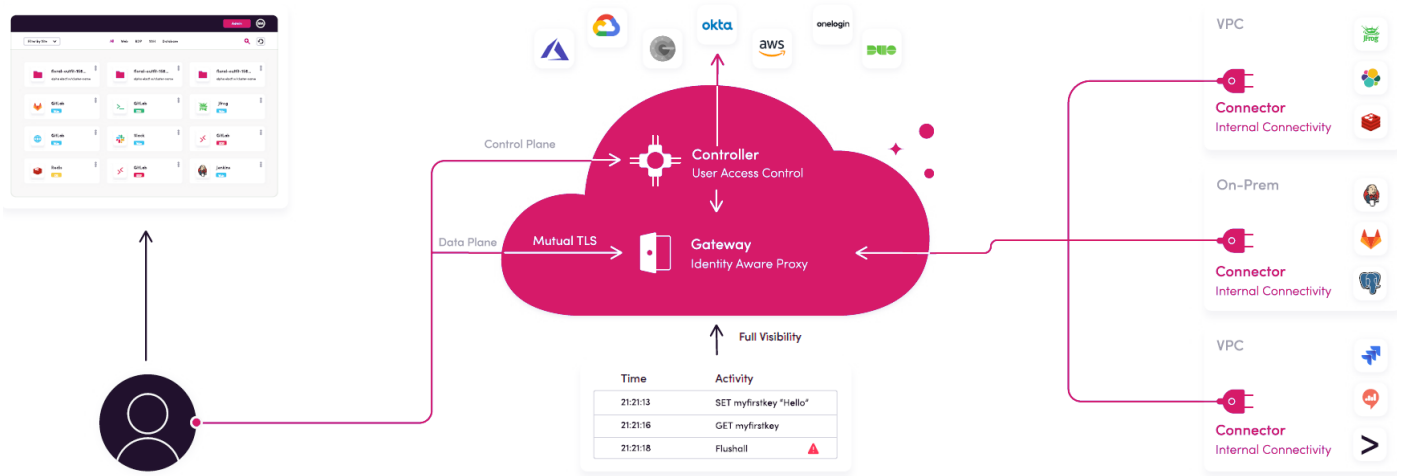
Third Party Access

Freelancers and contractors are an integral part of today's workforce, but managing their access to sensitive data is cumbersome, and exposes you to potential security risk. With Check Point, third party access to — and within — any application, server, database or environment can be easily compartmentalized and limited in both time and scope.

DevOps Access

Engineering teams need to leverage the agility and flexibility of a cloud-based development and production environments, without compromising security. Harmony Connect Remote Access provides least-privilege access to dynamic and hybrid environments with a full audit trail of all user activity. Administrators can leverage the cloud-native access platform to effortlessly provision and de provision access to virtual machines, applications and services.

HOW IT WORKS



- Check Point moves access decisions from the network layer to the application layer, eliminating the ability for attackers to roam freely in your network.
- Every user is authenticated using contextual data such as their location, device and behavioral patterns and authorized based on business policies before being given access to anything.
- Authorized users receive only the level of access needed to do their jobs. Any other resources are not only inaccessible, they are invisible.
- IT and DevOps engineers have a full audit trail of user activity with real-time notifications for suspicious activities.
- And, as a SaaS platform, the experience for the end-user is frictionless.

KEY FEATURES

Connectivity in Seconds

Leverage native API calls to setup access to new virtual machines, applications or in seconds. Provide users with agentless, SaaS-like user experience — no endpoint agents to install, appliances to deploy, or maintenance to perform.

Least Privilege Access

Based on the Software-Defined Perimeter (SDP) approach, users will be able to access a segmented part of the network only. This segment can be dynamically provisioned for each individual user or group, and is displayed uniformly across all corporate data centers.

Centralized Control

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 users, servers and enterprise data stores, including user commands and database queries.

Integrate with Existing IDP

Create and manage your users, groups and access policies directly through Harmony Connect Remote Access. Alternatively, Harmony Connect Remote Access can integrate with your existing IDP.

Forensic Visibility to User Activity

Gain full visibility into all user activity within the network. Investigate user actions with a complete web requests audit trail, query logging for Database access and fully recorded SSH and RDP sessions.

Part of Harmony Connect SASE

Harmony Connect Remote Access is part of Harmony Connect, which is redefining SASE by making it **easy** to secure access to **corporate applications**, **SaaS and the internet** for any user or branch, from any device, without compromising on security.

"Check Point has developed an elegant approach that easily layers on top of existing infrastructure while providing users with a seamless and intuitive access experience."

Steve Brasen
Research Director at EMA.

"Controlling access and maintaining visibility to both production and development environments is a complex challenge. This kind of access and control is something that no other platform has been able to give before."

Eyal Sasson
CISO of Gett