CHECK POINT™

Harmony Connect

BUYER'S GUIDE TO

ZERO TRUST NETWORK ACCESS

Zero Trust essentials for your most valuable assets

TABLE OF CONTENTS

INTRODUCTION:

MASSIVE WORKPLACE CHANGES SHAKE UP PRIVATE ACCESS

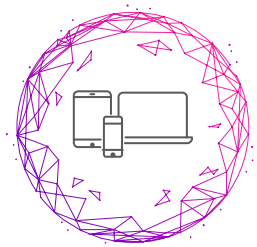
In 2020, organizations experienced a massive shift to remote and hybrid work environments. Due to the pandemic, six out of 10 organizations moved to a 100% work-from-home model almost overnight. More than a year later, 78% of them still have significant numbers of employees working from home[1] or remotely. This phenomenon dramatically increased companies' attack surfaces and security risk.

According to Check Point Research, there were 50% more attack attempts per week on corporate networks globally in 2021 compared with 2020. Ninety-two percent of executives reported their organizations experienced business-impacting cyberattacks or compromises, resulting in the loss of customer, employee, or other confidential data; interruption of day-to-day operations; ransomware payout; financial loss or theft; and/or theft of intellectual property[2].

As remote access to company networks and cloud environments became essential to business continuity, cyber attackers quickly capitalized on vulnerabilities. Attacks through employee-owned devices, supply chain partners, and weak cloud security measures have spurred the need for a new approach to secure remote access.

[1]Beyond Boundaries: The Future of Cybersecurity in the New World of Work, Forrester, September 2021

[2]Beyond Boundaries: The Future of Cybersecurity in the New World of Work, Forrester, September 2021



BYOD Increases Risk

Unmanaged, employee-owned devices pose significant risk. Because their risk posture is not known, they can easily infect networks and assets with malware and open the door to threats.
Check Point research[3] shows that while 70% of organizations allow access from BYOD, only 16% take a ZTNA approach to ensure least privilege access to sensitive data and resources.

Supply Chain Attacks Cost Big

Employees aren't the only ones who need access to corporate resources. Third-party partners, contractors, and vendors also need access to applications, servers, and databases with varying levels of sensitivity. Without secure remote access, risk increases—along with consequences. The average financial impact of a supply chain attack reached $1.4 million in 2021[4].

Cloud Environments Targeted

The move to remote work accelerated cloud initiatives for many organizations. Cloud data centers and production environments provide anywhere-anytime access but invite attack through weak security practices and exposed infrastructure and credentials. In fact, according to Check Point research, 76% of organizations use two or more cloud providers, and 26% experienced a related security incident[5].

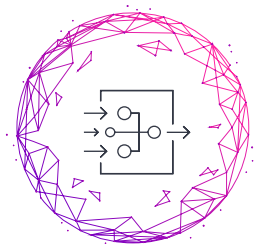
[3] Check Point Remote & Hybrid Work Security Report 2021

[4] IT Security Economics Report, Kaspersky, October 2021

[5] Check Point Cloud Security Report 2022

Admins Contend with Blindspots

With so many corporate resources accessed from different devices within and outside the office, it comes as little surprise that 48% say they have limited ability to view user logs and audit user activity[6]. Needless to say, this also translates into hampered compliance, post-breach forensics and analysis.



Legacy Architectures get Congested

With users and data increasingly residing off-premises, upkeeping connection speed becomes nearly impossible when using legacy prem-based security engines. Some organziations still backhaul all their traffic to the datacenter just for security purposes, including decryption, inspection and re-encryption of all traffic. These organizations are bound to experience downtime and lost productivity, as 46% cite scaling performance as their top administration challenge with remote access[7].

[6] CyberArk Research: Lack of Security Controls and Visibility Into User Activity Continue to Put Organizations at Risk 2021

[7] Check Point Remote & Hybrid Work Security Report 2021

TRADITIONAL REMOTE WORK SECURITY ISN'T DELIVERING

Traditionally, organizations have relied on Virtual Private Networks (VPNs) and premises-based security to secure access to networks and applications. However, they are typically deployed as one-size-fits-all solutions. Not everybody accessing company resources needs—or should have—the same level of access to applications with the same permissions. With widespread, secure remote access now a requirement for doing business, VPNs aren't keeping up.

Inability to Scale

Organizations can't quickly configure and scale VPN connections to cope with high numbers of employees suddenly locked down during a pandemic or with seasonal traffic spikes. Scaling on demand while simultaneously ensuring uninterrupted connectivity is nearly impossible without an additional huge investment.

Access Without Visibility

A VPN-based remote access scheme usually allows broad network access, putting the organization at increased risk of lateral movement by potential threat actors. Worse, IT has no central visibility into what users are actually doing in the network or with applications.

Impractical for Third Parties and BYOD

For most organizations, it's simply not practical or desirable to install and maintain VPN clients on BYOD and partner devices.

Performance Suffers

A VPN implementation usually backhauls all traffic to the data center for security inspection. Without the ability to load-balance traffic, throughput slows down and low-latency application performance suffers. Check Point Research found that 67% of organizations cite performance problems and latency as top user complaints .

VPN-to-Cloud Complexity

VPNs don't scale easily across multitudes of servers, cloud providers, and hybrid architectures. For example, setting up numerous AWS Virtual Private Clouds (VPCs) with an on-premises VPN is complex.

Lack of Privileged Access Management

VPNs don't offer native Privileged Access Management (PAM) capabilities for privileged users and resources. This makes it challenging to enable secure access for DevOps and engineering teams to databases, administration terminals and hundreds of dynamic cloud servers and workloads.

High Overhead

Relying on VPNs to secure entire workforces, networks, and applications incurs high operational overhead. They require additional hardware, software updates, and management resources.

[5]Check Point Blog: Four Ways Remote Work Has Impacted IT Security and What You Can Do About It, July 2021

ZERO TRUST NETWORK ACCESS

Why Secure Access with Zero Trust?

Zero Trust Network Access (ZTNA) is software-defined functionality that enables secure access to networks and applications. The concept evolved from traditional security measures but flips the concept of trust on its head. Now instead of assuming that users and devices working on the network are trustworthy, a Zero Trust model is based on a perspective of "never trust, always verify." A ZTNA model:

- Authenticates every device and user, no matter where they are located
- Limits access on an application-by-application basis
- Applies granular in-app controls and authorization
- Hides unauthorized applications from the user and internet to minimize lateral movement
- Continuously monitors user activity, and enforces policy in real time

Gartner® defines ZTNA as "products and services that create an identity- and context-based, logical-access boundary that encompasses an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities. The broker verifies the identity,

context and policy adherence of the specified participants before allowing access, and minimizes lateral movement elsewhere in the network[1]."

[1] Gartner, Market Guide for Zero Trust Network Access, ID G00730534

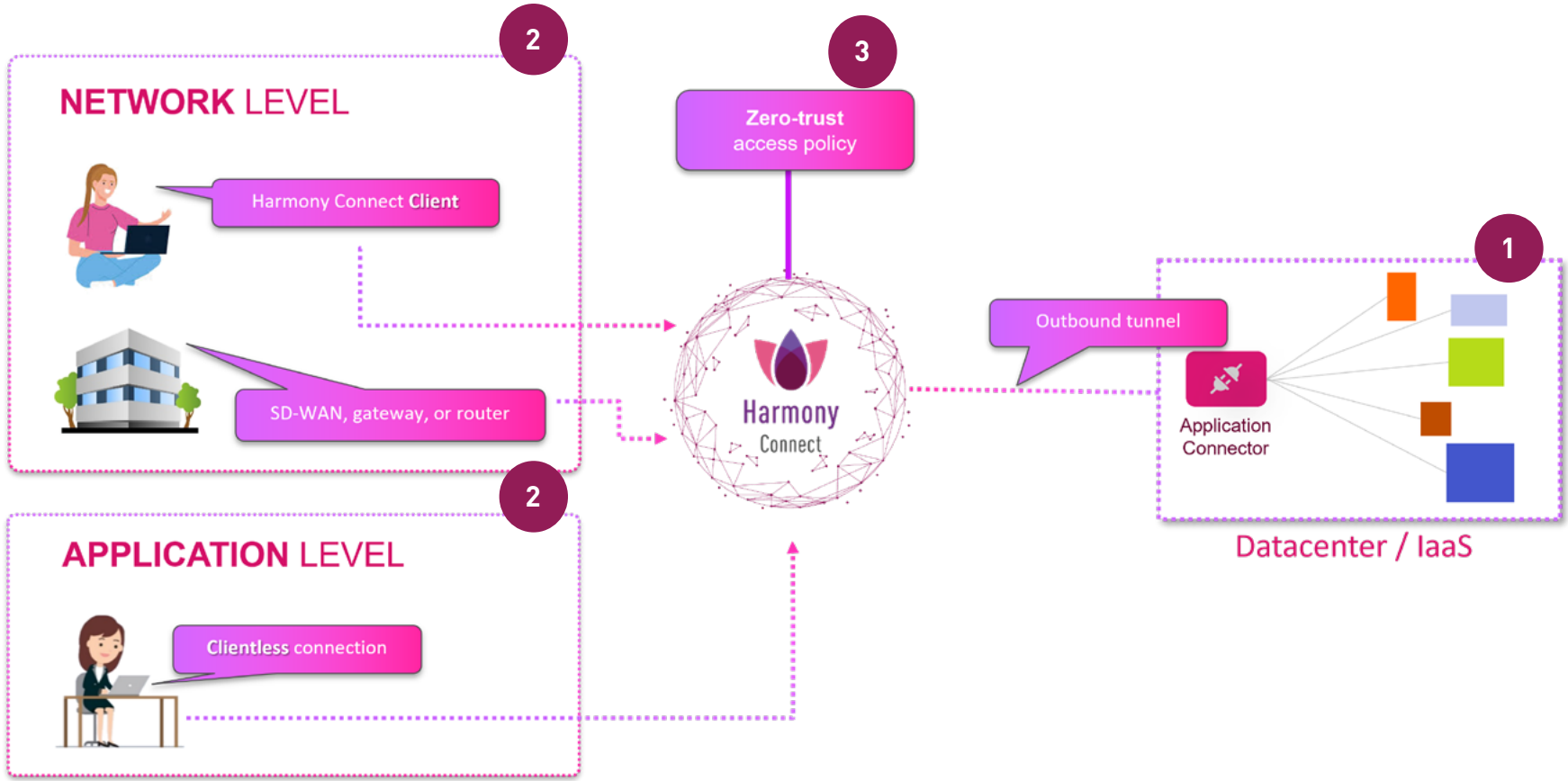
Endpoint vs. Service-Initiated Zero Trust

In the realm of Zero Trust Network Access, Zero Trust can be endpoint-initiated or service-initiated. Endpoint initiated connections rely on a client installed on the user's device for providing authentication and authorization information to the cloud-based trust broker.

On the other hand, "A service-initiated architecture," as explained by Tech Target, "uses a connector appliance to initiate an outbound connection to the ZTNA provider's cloud where identity credentials and context requirements are assessed, eliminating the need for an endpoint software agent."

Regardless of its implementation with or without a client, by deploying a single connector for each datacenter, network segment or virtual private cloud (VPC), all access attempts to the resources behind the connector are vetted and controlled by the cloud trust broker to enforce zero trust policies.

Two Access Modes, **Single** Architecture



How Zero Trust Works

Here's how zero trust access architecture works:

1 **Application Connector** - A Zero Trust service connector, or application connector software, is deployed in the relevant network, network segment, datacenter, IaaS or cloud production environment. In segmented networks, a connector is deployed in each segment. The Connector is a lightweight container, that can be deployed in a matter of seconds with a simple command-line. The connector creates a secure outbound-only tunnel to the cloud trust broker service. This creates a `data center darkening' effect, where all private applications are hidden from view and not visible to the internet.

2 **Zero Trust Access** - There are two options to connect your users:

- Application-level Access - Users connect using only a browser or with their existing RDP or SSH software. Users first authenticate to the ZTNA service using their current identity provider or directly to the service itself. Layer 7 application-level access may be delivered as clientless access - with no need for a VPN client in order to connect. Application-level access uses cloud-based reverse proxy technology to publish applications.
- Network-level Access - Network-level access is a VPN-as-a-service technology. It enables secure layer-3 network connectivity. This access mode is available for both users and offices. To connect, a lightweight client or agent is used. Offices connect to the cloud service using IPSsec from an edge device. Typically, this is an SD-WAN router.

3 **Zero Trust Service** - Regardless of how users connect, their access into the datacenter or cloud environment is always subject to an organization's zero-trust access policy, enforced by the cloud trust broker.

Zero Trust Must-Haves

Regardless of the approach taken, be it layer 3 network-level access or layer 7 application-level access, key zero trust principles that should be supported include:

- User-based access policies
- Device security posture validation
- Use of a trust broker that sits between the user and the application
- Application-based access policies (not just network-level ones)
- No direct access to the corporate network
- Private applications are not visible to the Internet
- Simultaneous connections to different locations

More than simply a VPN replacement, ZTNA is becoming a critical element of standardized security architectures because it ensures any user on any device—whether inside or outside the organization's network—is authenticated, authorized, and continuously validated for security configuration and posture before being granted or maintaining access to applications and data.

[6]Gartner Market Guide for Zero Trust Network Access, February 17, 2022

SEVEN ESSENTIAL ZTNA CAPABILITIES

How to Choose the Best ZTNA Solution

As organizations seek to replace VPNs to gain flexibility and reduce risk, there is a growing number of ZTNA solutions emerging in the market. Here are seven things to consider when evaluating ZTNA solutions for your environment.

Ensure Support for All Users

The ZTNA solution should secure access for all users—employees with managed devices, BYOD devices, third-party partners, engineering teams, and DevOps users. Client-based access capabilities are ideal for securing employees using managed devices. For employees using their own devices e.g. BYOD, mobile devices and third-party partners, look for a clientless architecture to enable secure access to target resources without requiring the installation and management of an agent. Access should be easy and intuitive for a good user experience.

Be sure to also consider basic Privileged Access Management (PAM) requirements for engineering and DevOps teams who need access to multi-cloud environments and single sign-on (SSO) into private resources, such as servers, terminals, and databases. Basic PAM tools may include SSH key management, credential vaulting and user session recordings.

> **[ZTNA] grants access based on the identity of the humans and their devices—plus other attributes and context, such as time/date, geolocation, device posture, etc.—and adaptively offers the appropriate trust required at the time.**
>
> *Gartner Market Guide for Zero Trust Network Access*[1]

TIP

Consider piloting a ZTNA solution for a specific use case, such as third-party partner access to specific portals or DevOps access to multi-cloud environments.

[1] Gartner, Market Guide for Zero Trust Network Access, by Aaron McQuaid, Neil MacDonald, John Watts, Shilpi Handa. Gartner is a registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Ensure Support for All Target Resources

Ensure the ZTNA solution will support all of the organization's critical applications and resources. Web apps are typically easy to support when enabling zero trust (ZT) remote access. However, most organizations also need to enable ZT access to SSH terminals, SQL databases, remote desktops (RDP) and servers—which often rely on dedicated, protocol-specific reverse proxies for layer 7 application-level access. DevOps and engineering teams need ZT access to Infrastructure-as-a-Service (IaaS) offerings, cloud production environments, microservices, and virtual private clouds. If the organization relies on homegrown applications with nonstandard protocols or legacy environments, Layer 3 network-level access or a VPN-as-a-Service (VPNaaS) capability will be required.

> **Some ZTNA vendors have chosen to focus their developments on supporting web application protocols only (HTTP/HTTPS). Carrying legacy applications and protocols through a ZTNA service could prove to be more technically challenging for vendors to develop and for customers to deploy.**
>
> *Gartner Market Guide for Zero Trust Network Access*

TIPS

- *Ask how the solution specifically supports high-priority private applications.*
- *How does the vendor suggest supporting lower-priority applications, such as on-premises data center resources, IaaS, or virtual private clouds?*

Ensure Rapid Rollout and Time-to-Value

Gartner says that "Organizations cite VPN replacement as their primary motivation for evaluating ZTNA offerings, but find that justification comes from risk reduction, not from any cost savings." Significant risk reduction is of huge value, but so is rapid deployment for security and IT teams.

Look for capabilities such as out-of-the-box integration with your organization's identity providers (IdPs) or verify support for identity integration standards like SAML 2.0 or SCIM. Intuitive, granular policy configuration enables any team member to be productive quickly, without requiring extensive training. As an example, watch how to deploy clientless ZTNA in 15 minutes for fast time to value.

TIPS

- *Ask about length of time needed for deployment.*
- *Ask to see how to define and enforce new policies.*
- *Ask how many consoles are required.*
- *Is any additional hardware or software required?*

Ensure Easy Operation

IT and security talent shortages make it essential to choose a ZTNA solution that delivers maximum value with minimum maintenance and no need to hire additional staff. Ensure efficient management by choosing a strategy and services that create a frictionless experience for the team. Cloud-based solutions with a unified console are easy to use and deliver visibility across all ZTNA use cases, enabling teams to be productive immediately without extensive training or a learning curve.

Cloud-based ZTNA services eliminate the need to maintain hardware and software. Internal teams achieve business resiliency without the need to manage backup, restoration, disaster recovery, and high availability resources.

> For cloud-based ZTNA offerings, scalability and ease of adoption are additional benefits.
>
> *Gartner Market Guide for Zero Trust Network Access*

TIPS

- *Request a demo of the management console and how easy it is to enforce policy and monitor user activity.*
- *Ask for actual results from other customers or browse customer reviews.*

Ensure High Performance and Service Availability

Whether ensuring secure access for users within a metropolitan area or in locations around the world, the ZTNA service must deliver close to 99.999% uptime and high performance backed by Service Level Agreements (SLAs). Review a vendor's SLAs, particularly if the organization operates across time zones or continents. Look for a global network of points of presence (PoPs) with redundancy in each zone. Location-based routing can accelerate connectivity for users to ensure high application performance.

> Well-designed ZTNA services include physical and geographic redundancy with multiple entry and exit points to minimize the likelihood of outages affecting overall availability. Furthermore, a vendor's SLAs (or lack thereof) can indicate how robust they view their offerings. Favor vendors with SLAs that minimize business disruptions.
>
> *Gartner Market Guide for Zero Trust Network Access*

TIPS

- *Ask about SLA guarantees for service availability and updates.*
- *Quantify expected latency to identify any potential impact on application performance.*
- *Ensure the service has availability zones near headquarters, branch offices, manufacturing facilities, retail stores, and other points of presence.*
- *Determine which industry audits and certifications (such as SOC 2 recognition) are necessary for your compliance requirements and whether the vendor complies.*

Ensure Zero Trust Security Soundness

In a least-privilege access model, users, applications, and devices are given only the minimal level of access required to perform their job or function. This helps limit an attacker's lateral movement if they successfully breach defenses.

To support zero trust from unmanaged devices, look for ZTNA solutions that separate the control and data planes to enable true least-privilege access to applications and other resources. Applications should be hidden from view until the user is authenticated with context to prevent malicious insiders or compromised accounts from moving laterally. Applications also are hidden from the public internet, preventing attackers from exploiting corporate resources.

To support zero trust from managed devices, look for ZTNA solutions that offer additional security context, such as device posture checks that check for security hygiene, such as corporate domain membership and the presence of up-to-date anti-virus software. Gartner says that "Optimally, user and device behavior are continuously monitored for abnormal activity, as described in Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) framework." Look for a zero trust solution that can continuously monitor factors such as device health, user activity, data access, and others. Policy changes also should be enforced in real time.

ZTNA solutions provide deeper visibility and control than traditional VPN solutions. Look for a solution that provides granular in-app controls, such as read-only and write permissions, and enabling policies at the command and query levels. The ability to report on groups, users, and application usage with access to video session recordings provides deep visibility and allows teams to quickly adapt policies or take other appropriate action.

ZTNA solutions that include other robust security features boost overall security effectiveness. Check for features such as integrated advanced sandboxing and cloud intrusion prevention systems (IPS) to detect and prevent exploitation of known vulnerabilities and exposures. Integrated cloud data loss prevention (DLP) capabilities prevent leakage of sensitive date to social media, internet and web apps—allowing the organization to define what data is sensitive.

TIPS

- *Ask how the solution specifically ensures least-privilege access.*
- *Ask how the service prevents threats and protects sensitive data.*
- *Does the solution offer in-app controls, such as read/write permissions, or command and query-level policies?*
- *Does the solution provide a granular audit trail?*
- *Are video session recordings supported?*

Part of a Future-Ready Security Service Edge

With the need to simplify management and consolidate point products, the concept of a Security Service Edge (SSE) is gaining traction. This approach creates an extensible future-ready, single-vendor cloud-based solution that encompasses a range of technologies that have historically been viewed as separate solutions. These include secure web gateway (SWG), ZTNA, and cloud access security broker (CASB) technologies.

As organizations move toward ZTNA strategies, they should consider how their ZTNA solutions can be extended to other use cases. For example, can the solution secure branch access? Can it secure Internet access for remote users? Can it secure access to web and SaaS applications, in addition to private applications? Looking towards the future, securing remote ZTNA is a critical step toward enabling a larger zero trust security architecture.

> The market is increasingly converging toward an SSE agent-based architecture for the majority of deployments. We are also seeing increased demand for agentless-based deployments in the case of unmanaged devices and/or third-party access. Security and risk management leaders will need to ensure that their chosen vendor supports both approaches to cover the most common use cases.
>
> *Gartner Market Guide for Zero Trust Network Access*

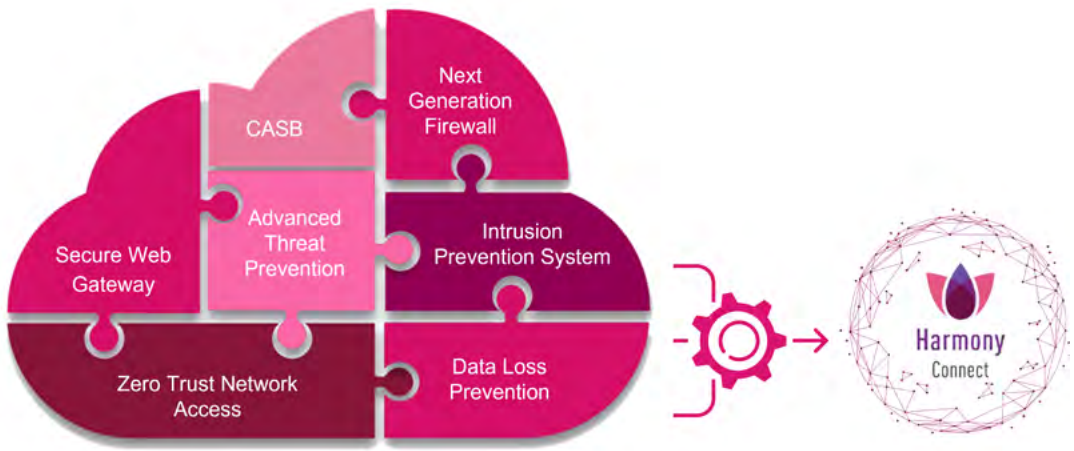


Figure 3: Core Network Security services with Zero Trust - Harmony Connect

TIP

Ask if the solution is part of a broader SSE offering.

HOW CHECK POINT HELPS

Discover Harmony Connect

Check Point Harmony Connect delivers a 100% cloud-based SSE solution, complete with ZTNA, VPN-as-a-Service, Secure Web Gateway, SaaS Security, and branch FWaaS. Harmony Connect redefines SSE by making it simple to securely connect to corporate applications, SaaS and the internet for any user or branch and from any device anywhere.

Harmony Connect Remote Access - ZTNA Your Way

Harmony Connect Remote Access takes only 15 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. These include:

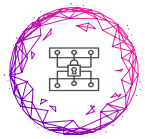
- **Clientless Application-Level Access:** This option applies intuitive ZTNA to web applications, databases, remote desktops, and SSH servers with granular in-app controls using application-level (Layer 7) reverse proxies in the cloud. It is ideal for securing remote access by employee-owned devices and third-party partners since no agent is required. This option also enables secure access for engineering and DevOps teams who need rich, cloud-native automation capabilities and basic PAM tools for multi-cloud and private servers.
- **Client-based Network-level Access:** This VPN-as-a-Service option uses the power of Layer-3 network connectivity secured by Check Point's zero-trust access policy. It is ideal for securing employee access from managed devices. The client-based option offers exceptional versatility in supporting applications and protocols, and it includes embedded cloud DLP and industry-leading IPS to protect apps from the latest vulnerabilities, such as Log4J.

Why Harmony Connect Remote Access

Check Point has built zero-trust capabilities into its solutions for almost 30 years. As a result, Check Point Harmony Remote Access provides the deepest level of zero-trust features and controls of any remote access solution with a breezy user experience for administrators and end-users alike:

Powerful ZTNA Platform

Simple 100% cloud-based deployment



Choice of application- or network-level access

Unified management with single client for internet and private access

VPN-as-a-service with embedded cloud DLP and cloud IPS

Simple all-inclusive pricing with lower TCO

Unique clientless ZTNA Experience

Clientless access with no agent required

Versatile RDP Access

Granular in-app controls at the command and query level

PAM-as-a-service for multi-cloud and private servers

Optional Video recording

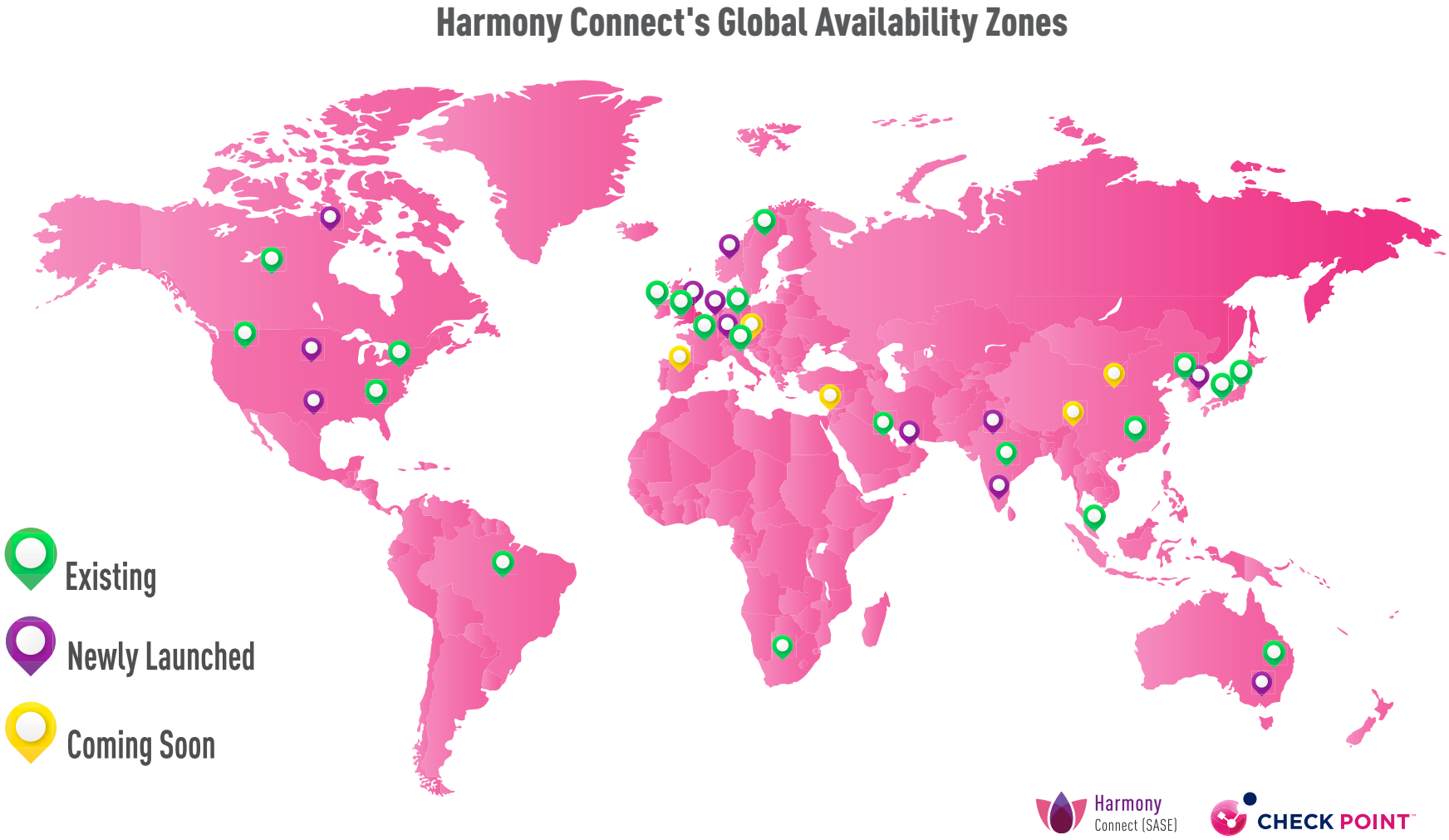


Figure 2: Ensure High Availability - Global Availability Zones for Harmony Connect - Security Service Edge

Each availability zone contains two redundant Points of Presence (PoPs). For the latest global zones, please see Check Point's support center

Explore what Harmony Connect Remote Access can do for you

ZT corporate access

Looking to scale remote access with agility? Learn how to implement zero trust corporate access quickly and easily.

Learn how >

3rd party access

Can you trust your contractors and partners with your most sensitive portals and networks? With zero trust, there's no need.

Learn why >

DevOps access

DevOps and engineers regularly connect remotely to critical production environments in the cloud and on-prem.

Explore how >

Ready to get started

Watch overview >

Live Demo >

Harmony Connect

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

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.

About

Check Point Software Tchnologies Ltd.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

To learn more about us, visit: www.checkpoint.com

Contact us

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: 800-429-439 / 650-628-2000

Fax: 650-654-4233