SASE Architecture

Architecture Reference Guide for the
Implementation of Secure Access Service Edge

Release 23-02-2021

ABSTRACT

As resources and applications shift to the cloud, on-premise data centers are no longer the core of the network, users are no longer found only in corporate offices, and remote working becomes widely accepted with COVID-19 moving the world into a new paradigm.

To meet these needs and more, enterprises are seeking advice on how to re-architect their infrastructure.

This document provides a basic understanding of SASE architecture, explains how it solves different needs of evolving organizations, and best practices for deployment.

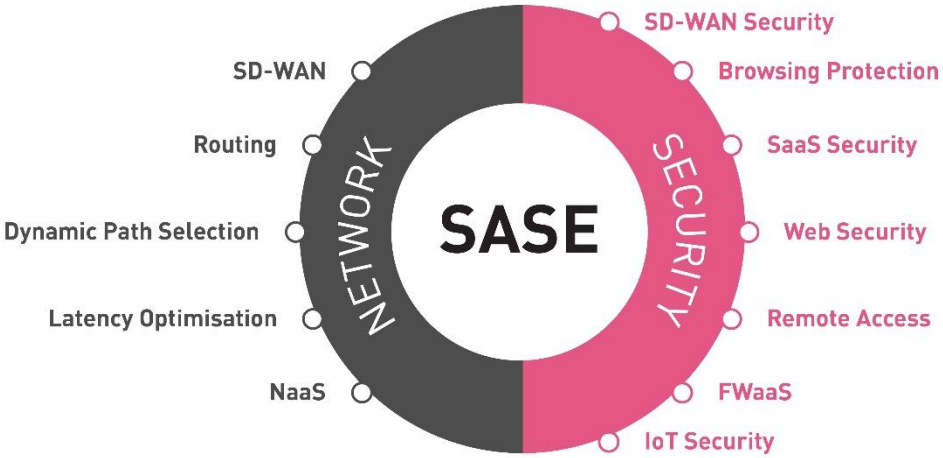
AUDIENCE

This document is written for technical readers, IT security architects, and network specialists who are venturing out into cloud territory.

Readers should be familiar with basic concepts of virtualization, networks, and have a strong understanding of security design.

TABLE OF CONTENTS

INTRODUCTION TO SASE



The acronym SASE stands for Secure Access Service Edge.

SASE describes a change in architectural principles that moves away from a traditional on-premise Data Center and shifts to a decentralized architecture. When organizations adopt SASE principles, they distribute user access to corporate resources instead of consolidating them in one place.

We view SASE as an architectural methodology that converges network and security requirements into a single cloud-centric solution that allows cloud transformation.

It is an undeniable trend that more resources are moving from the traditional Data Center to the cloud.

This is the reason why instead of routing traffic from branch offices and remote users to the Data Center, where the internet egress point was typically located, SASE recommends that users and branches should all have a direct internet breakout.

The SASE model covers a wide range of functionalities, ranging from layer 3 in the OSI model up to the application layer, as depicted in the graphic on the left-hand side.

SASE Main Components

Security

- SD-WAN Security: Sets companies dealing with a significant amount of legacy infrastructure in branch offices to stop backhauling all internet-bound traffic to the regional hub site without having to upgrade the legacy gateways, saving WAN costs without compromising security.
- Firewall as a Service (FWaaS): A cloud-based Next-Generation Firewall is a scalable, application-aware solution allowing enterprises to eliminate the challenges of legacy appliance-based solutions.
- Web Security: Secures Internet access to Web applications and resources leveraging unified Threat Prevention solutions, such as URL Filtering, Anti-Virus, IPS, Anti-Bot, and Zero-Day attack prevention.
- Browsing protection: a simple browser extension complements the cloud-based security controls and allows for full visibility into encrypted traffic, protecting against the loss of corporate data and mitigating modern-day malware such as ransomware, zero-day attacks, phishing, etc. so you can safely navigate today's menacing threat landscape.
- Secure Remote Access to Corporate Resources: Replacing traditional remote access solutions where the VPN was terminated in an on-premise Data Center, SASE Remote access no longer requires the traffic to be backhauled, improving the user experience.
- SaaS Security: Secure access to SaaS applications like Office 365, Google suite, etc. using a Cloud Access Security Broker (CASB).

- IoT Security: SASE enables IoT devices to break out to the internet directly in a secure way.

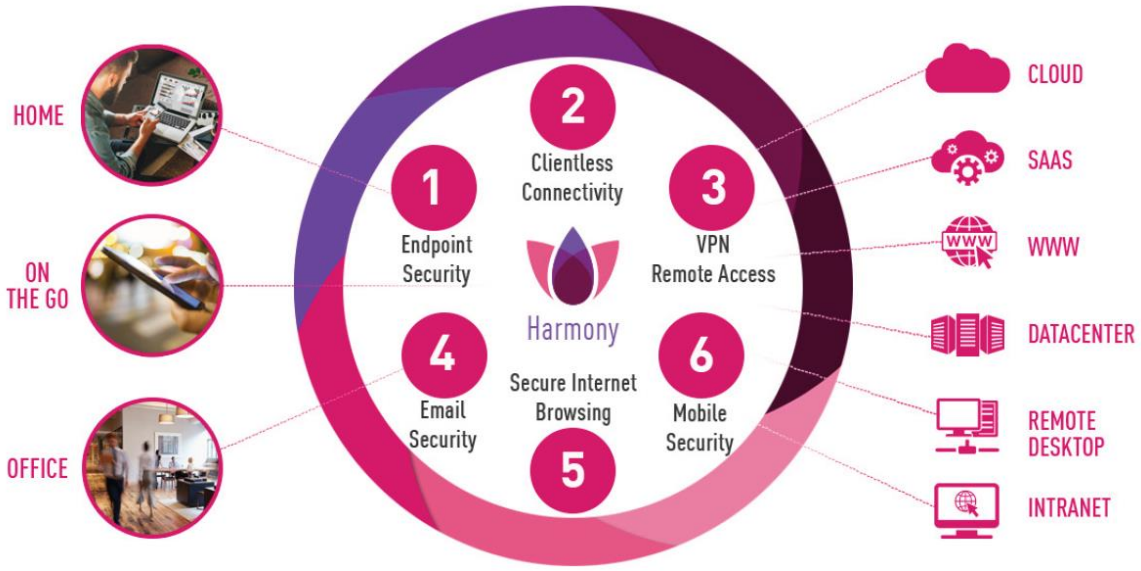
Network

- SD-WAN: Optimizing access to the Internet and Data Centers by allowing branch offices and users to break out to the internet directly and securely, significantly improving the user experience.
- Elements like routing, dynamic path selection, NaaS, and latency optimization are all essential networking features of SD-WAN, laying the foundations on which security is built.

Reasons to consider a SASE architecture		
Business Drivers	**Reducing the operational burden and cost**	With network security as a service, maintenance and upgrades are included in the monthly cost. Upgrading multiple physical gateways is time-consuming and leaves security inconsistent and lagging; converting to an FWaaS architecture and managing the entire infrastructure from a single pane of glass saves time, resources, and training as well as reduced cost. Reducing the Wide Area Network costs by retiring expensive MPLS circuits in favor of broadband internet links is a second important driver.
	Cloud-centric architecture and technology	Enterprises are looking for a zero-touch provisioning solution, which is centrally managed, easy to deploy, and scale. We would expect the majority of SASE solutions to be delivered from the cloud, reducing the need for on-premise hardware and delivery times.
	Ubiquitous access to corporate resources	During the Covid-19, many enterprises allowed their workforce to work from home. Many were pleasantly pandemic surprised to see that employee productivity went up. In a post-pandemic world, this new way of working will become the norm, and employees must be able to access any corporate resource securely and efficiently. When productivity goes up, business figures usually follow suit.
Security and User Experience Drivers	**Internet access optimization**	SD-WAN Dynamic link selection ensures the best path is always automatically chosen if multiple access circuits are present.
	Improving security and reducing threats	Increasing security to a level that can deal with Gen VI attacks, even with old EOL perimeter equipment.
	Cloud adoption	As enterprises rapidly move their data centers to the cloud, backhauling traffic to the hub site may not be the best option in terms of cost and/or latency for roaming users or for users in branch offices requiring access to (corporate) resources in the cloud. For instance, streaming audio or video is much more efficient in terms of WAN bandwidth consumption with a local breakout.
	Zero Trust Network Access	The same level of security should always be enforced, regardless of the location of the user. Whether they are in the office or roaming, a SASE architecture will constantly ensure complete session protection.

CHECK POINT SASE SOLUTION: HARMONY

Harmony, Check Point's SASE's architectural model, unifies 6 cloud-based security products to keep you 100% safe. Wherever you connect from, whatever you connect to, and however you connect – Your home, your devices, your privacy and your organizational data are secured and protected from any cyber threat.
Any user, regardless of their location, or asset should be able to access any application, either corporate or public, in a secure way. Versatility, scalability, and user experience are of paramount importance.

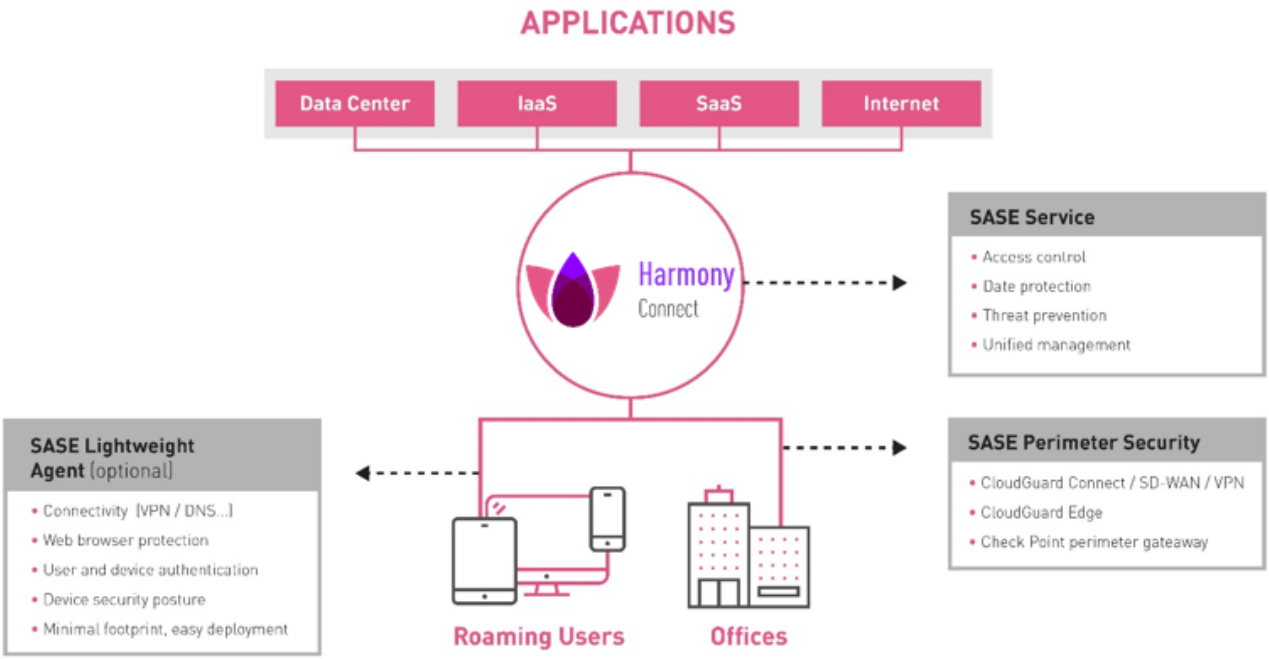


Harmony Connect - the network part - serves as a transport layer for users and devices connecting to resources and applications on the corporate network and the internet.

For secure branch office connectivity, Check Point has tight integration with most popular SD-WAN providers, establishing a best-of-breed SASE solution that provides efficient connectivity and comprehensive security capabilities.

Graphic: *Check Point's strategic SD-WAN partner ecosystem*

The security part is a unified solution based on Check Point Harmony products, the adjacency of those provides Check Point's SASE solution. All services are managed using Web UI Management, providing a single pane of glass for the Administrator.



The Check Point SASE solution

The Check Point SASE solution places security as a service in the cloud in a distributed fashion instead of enforcing it the legacy way on gateways, on-premise Data Centers, and branches. Access to corporate resources is possible directly without detours, and securely, for everyone.

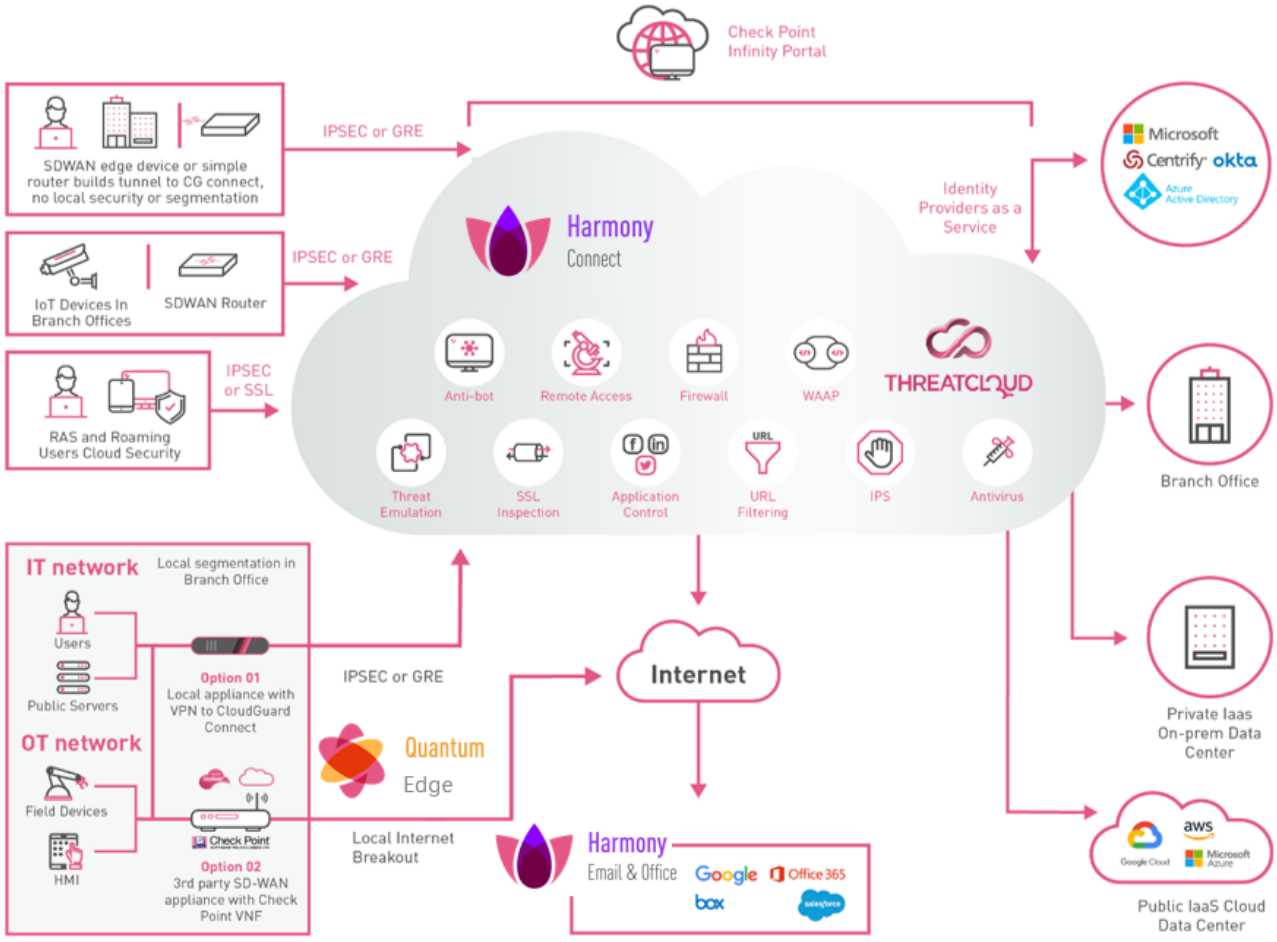
The service runs on top of the Amazon AWS and Azure infrastructure to ensure maximal availability and the best possible response times when accessing cloud resources.
This cloud-based solution does not burden IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing routers or SD-WAN deployments. With a simple and easy setup process, network traffic from existing SD-WAN edge devices are tunneled to a primary cloud-based network security service at a nearby location. A second connection provides redundancy. This ensures branch offices stay connected and removes the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing overall CAPEX and OPEX costs.

The SASE infrastructure is deployed in the cloud, fully managed by Check Point. The SASE functionalities in the cloud include the most sophisticated Next Generation Threat Prevention and zero-day protection mechanisms, ensuring the best possible protection against Gen V attacks, such as Application Control and URL Filtering, Anti-Bit / Anti-Virus, IPS, Threat Emulation, and Extraction along with SSL inspection capabilities and Remote Access VPN technologies.

All features of the service can be managed using a single pane of glass; either by Management as a Service (MaaS) leveraging the Infinity Web Portal or existing R80 Smart Center management system deployed on-premises.

SASE ARCHITECTURE REFERENCE

The following graphic represents the recommended Check Point SASE architecture, with several use cases as outlined below.



Note: *some features and capabilities shown above, are part of Check Point short-term roadmap and will become available during the 2nd half of 2020, e.g.: remote access to an on-prem data center via the SASE cloud service, for users or branches; branch-to-branch communication; the use of external Identity Providers as a Service.*

Use case: Security as a Service

- **Remote Access VPN to Data Center**
  Users can connect to the SASE cloud with a lightweight client, which connects to the SASE cloud over IPSEC or SSL. The traffic is secured and the user gets access to corporate resources either in an on-premise Data Center or in the public cloud. This is explained in more detail on page 15.
- **Clientless Access to Corporate Applications**
  Applications can be published to users directly thought the SASE cloud using only a browser. Assess is based on identity, which is typically provided by an Identity-as-a-Service provider. Applications will only be shown to users who have access to them, as they are hidden by default. This is explained in more detail on page 16.
- **Internet Web Access Security**
  When roaming users access the internet, they are secured by SASE cloud-based security controls, meaning these security controls do not need to be enforced locally. The lightweight agent routes all traffic to Harmony Connect in the SASE cloud where access control and threat prevention take place.

- **Harmony browser**

  The browser extension secures all web traffic before it is SSL encrypted: direct visibility into the rendered browsing content allows for zero-day protection (threat emulation and extraction) and phishing protection.

  It also permits dynamical delegation of network security functions (URLF, phishing & malware prevention) to the endpoint allowing intelligent direct internet routing without compromising security.

- **SaaS Application Security (CASB)**

  Roaming users connect to SaaS applications in the public cloud, like Office365. Check Point's SASE cloud solution secures *access* to applications. A key part of this access process is determining the identities (these originate from a 3rd party identity provider such as AzureAD) and risk level of users, as this information is used in the security policy that decides which applications users get access to.
  A second and equally important part is to provide data protection and threat prevention, both inline and out-of-band through the API integration Check Point has with SaaS providers.

Use case: SD-WAN / Branch Office Security

- **SD-WAN device connected to Check Point SASE service**

  A branch office that is equipped with an existing SD-WAN device can connect to Harmony Connect using an IPSEC or GRE tunnel, set up between the on-premise SD-WAN device and the Harmony Connect infrastructure. All access control and threat prevention features are enforced in the SASE cloud before allowing the traffic to break out to the Internet or any (corporate) resource like SaaS applications, the on-premise Data Center, or public cloud resources.
  The same setup can also be used if there is only a simple router present at the branch. As long as the on-premise device is capable of building a tunnel, the branch can be secured.

- **SD-WAN device running Check Point Virtual Machine (VNF)**

  Some of the SD-WAN vendors allow a Check Point VNF (virtual machine) to be run on routers. This allows for segmentation of the local network and inbound access to servers in a DMZ.

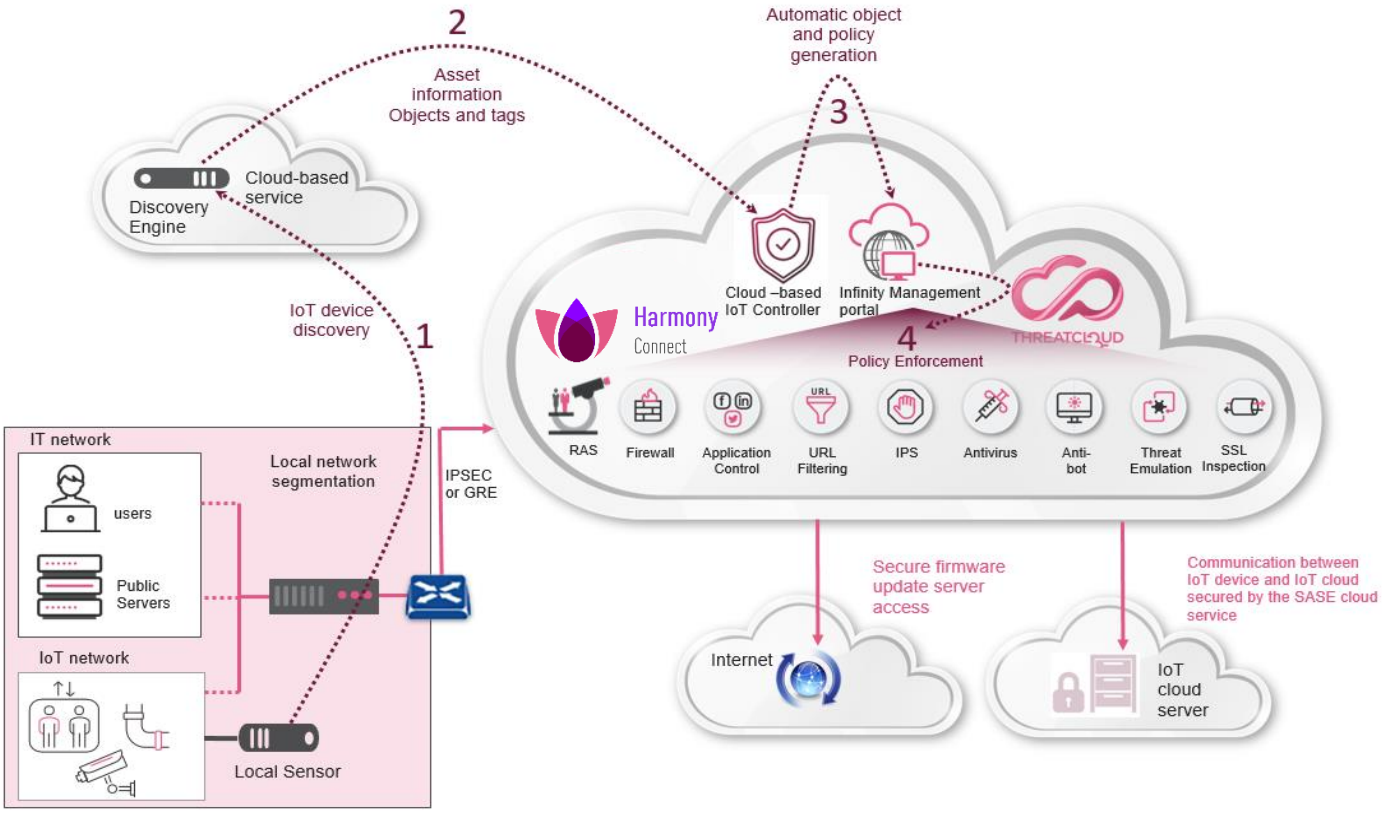
- **A Check Point gateway FW/IPS and an SD-WAN device**

  Some branch offices may have old Check Point equipment in place that is nearing its end of life, but upgrading is a time- consuming process. In these cases, advanced security features are disabled on the gateway because it is not powerful enough to run them. This leaves the branch exposed to modern-day malware. To fix this, the gateway can be kept for local segmentation purposes and the SD-WAN device can be used to build a tunnel to the SASE cloud, as in the previous example.

Use case: IoT Security

SASE also secures machine-to-machine communication.
A branch office can have IoT devices that need to communicate with an IoT cloud service, where the data of all IoT devices is stored, for example, surveillance cameras uploading video clips to a public cloud video storage service. SASE allows the cameras to send the footage via a VPN tunnel between the branch and Harmony Connect to the public cloud storage, ensuring integrity, encryption, and authorization of the upload process.

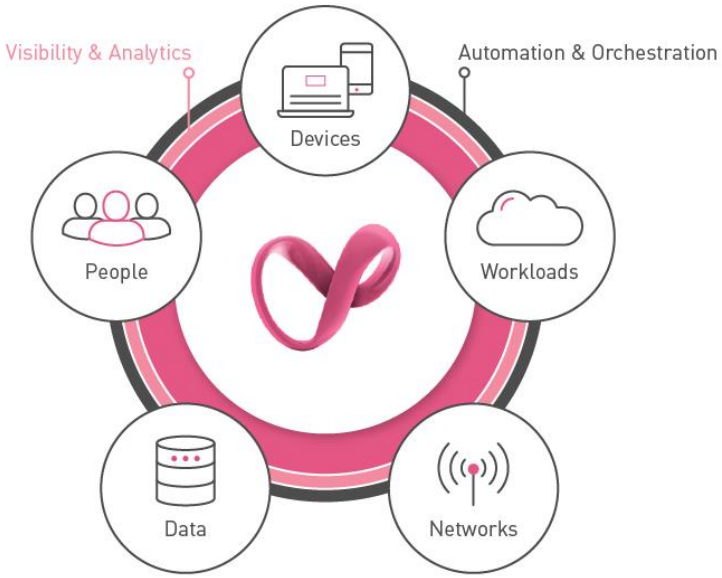
Conversely, SASE also allows for direct internet access for certain services. In the use case below: firmware updates for said IoT devices.



An additional advantage is that a local sensor in the branch office can be used to send the data it collects about IoT devices to a cloud-based 3rd party discovery engine (1), which in turn feeds this information to the Check Point cloud-based IoT controller (2). This Management-as-a-Service (MaaS) platform uses that data to automatically generate objects and policies based on the behavior and communication patterns of the IoT devices and feed them to the Infinity Management portal (3). After review by the security admin, the suggested policies can be enforced in the SASE cloud (4) or on on-premise gateways.

Alignment with the Zero Trust Model

SASE secures the communication between resources, branches, users and devices in a way that is completely aligned with the key principles of Zero Trust Network Access. By identifying users and devices, regardless of their location, the resources they need to access are secured by user-centric policies.



- **Zero trust people:**
  Identity Awareness is an essential component of SASE. User-centric policies for Harmony Email & Office ensure that the only the corporate applications a user is allowed access to, will be displayed. Identity awareness will also be used on both Harmony Connect and Quantum Edge, for user-based access control as well as threat prevention.
- **Zero trust devices:**
  The full End Point client enables on-device security protection for all employee devices, to prevent zero-day malware, malicious app installations, phishing attacks, bot attacks, and more.
  BYOD and non-managed devices (i.e. from temps or contractors) can also be used to obtain access to web-based corporate applications in a clientless scenario.
- **Zero trust data:**
  The DLP blade can be enabled on Quantum Edge, and content awareness can be enabled on Harmony Connect. Harmony Email & Office uses APIs in the cloud to enforce DLP policies to protect corporate data in the cloud.
- **Zero trust workloads:**
  Enable access control and full threat prevention for all south-north communication between users, the branch and data center, IaaS assets, and SaaS applications. Only displaying the applications to which users are supposed to have access to, is a perfect example of both zero-trust workloads and zero-trust people.
- **Zero trust network:**
  In case inbound access is required, a local appliance or Quantum Edge can be used to segment the DMZ from the user's segment and apply the necessary security controls between segments. Either the local VNF, security gateway or the Harmony Connect instance will segment the branch from the next hop, protecting the corporate network from lateral malware movements.

CHECK POINT SASE COMPONENTS

Check Point's SASE platform supports multiple security and network components, which are centrally managed using the Cloud Guard Connect management web application or console.

Check Point's SASE platform includes the following components:

- **Secure Web Gateway** – Check Point's cloud SWG is designed to protect your organization from known and unknown threats. It offers protection for users accessing the internet and SaaS applications in the office or remotely, and includes functionality of FWaaS.

  Security includes URL Filtering, application control, IPS, phishing, and malicious download prevention using SandBlast technology to prevent zero-day attacks, and DLP.

- **Network Security as a Service –** Cloud-hosted network threat prevention service, on top of existing SD-WAN deployments. The solution delivers the latest and most comprehensive cyber security available, protecting branch offices from the latest generation of targeted and advanced cyber threats.

- **Secure Access to corporate resources –** provide safe access to remote employees to corporate resources, providing the same level of security as in the office.
  Corporate resources are protected by zero-trust access based on user identity, endpoint security posture, and session risk. Access is granted based on the Zero Trust policy as well as behavioral models for users and applications. Corporate resources are protected in the data center or the private and public cloud.
  Corporate applications are also protected with advanced IPS and WAAP.

- **Anti-Bot and Anti-Virus** - Protects against malicious files, malware-infested websites, and more. The analysis uses real-time virus signatures and anomaly-based protections. Identifies and contains infections by blocking Command and Control traffic between infected hosts and a remote operator.

- **SaaS Applications Protection**

  A robust, native API based solution that provides zero-day threat protection from malicious links and attachments, anti-phishing, ID protection, and data leak prevention across cloud emails, office suites, and applications (e.g. Dropbox, Slack).

  - **Mail Security** - Check Point's Mail protection acts as the last line of defense, protecting your mailboxes from the vulnerabilities of built-in Office 365 email security. Use artificial intelligence to detect malicious content heading for your email accounts and block sophisticated phishing schemes that bypass traditional email security solutions.

  - **DNS Security** – Check Point's solution prevents access to malicious domains, at the access level. DNS Security prevents DNS exploits and tunneling, over HTTP or HTTP integrated with Threat Cloud, solution provides malicious domain blocking, for newly-registered domains related to active threat campaigns, as well as prevention against zero-phishing.

  - **Harmony Browser -** endpoint-based browsing protection compliments network SWG functions with superior protection. Browser extension provides visibility to encrypted traffic, and protection against zero-day phishing and malware attacks. The browser extension can be deployed independently, or as part of the SASE agent for PC.

  It is meant for those enterprises that need on-premises security for data privacy or data location requirements and can also be used to segment the local network.

Harmony Connect / Quantum Edge

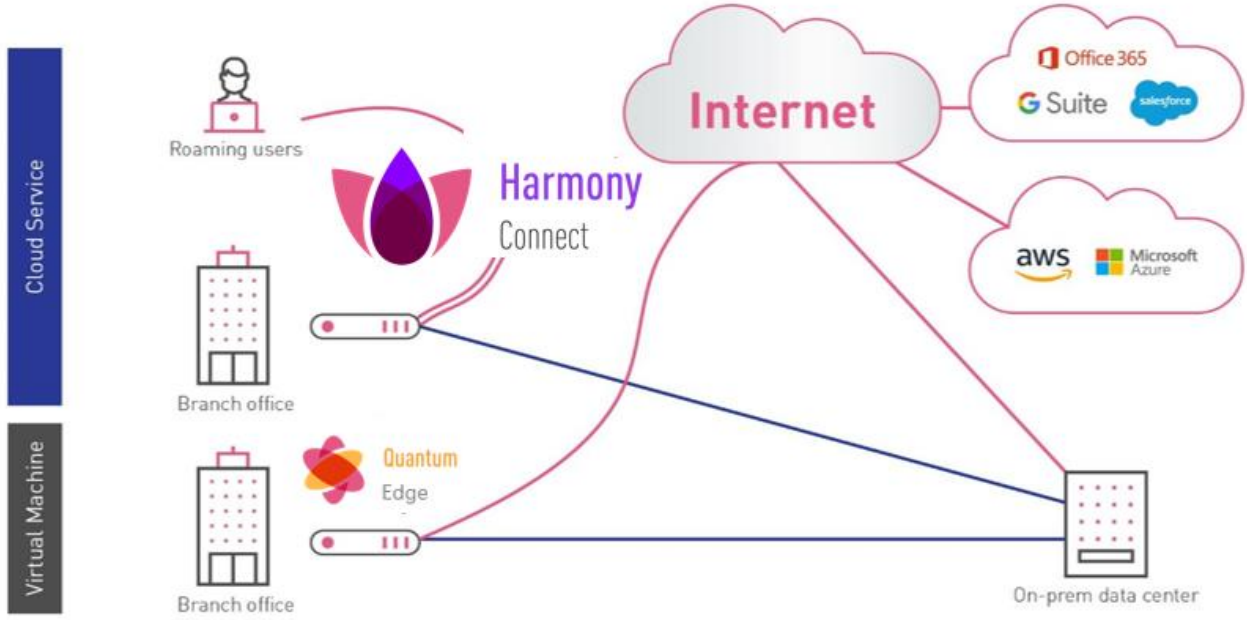
This chapter helps the reader choose between Check Point's **Harmony Connect** and **Quantum Edge** technologies and explains their ZTNA features.

Consider some of the following factors:

- The importance of owning a platform vs. using it as a service
- The necessity of inbound access to public servers in the branch
- The ability to use cloud services for security vs. having a strict policy restricted to on-premise solutions only

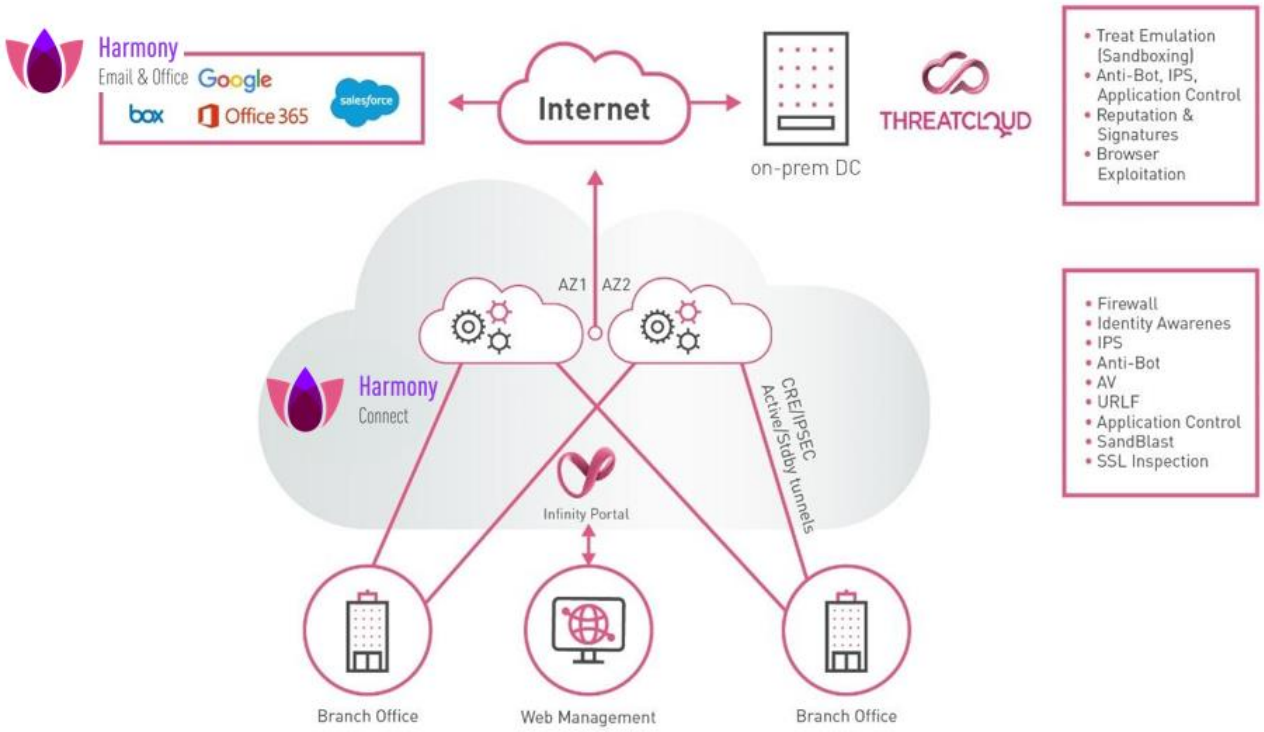
Harmony Connect is a native cloud service that requires no dedicated security hardware on-premise.
It can also be used as an FWaaS solution for roaming users and also allow them to access resources in an on-prem Data center.

Quantum Edge is a Check Point VNF running on 3rd party SD-WAN hardware. Both solutions allow branch offices to break out to the internet without the need to backhaul the traffic back over the WAN to the hub site where the internet egress point would traditionally reside.



When to consider Harmony Connect

1. In cases where old security Customer Premise Equipment (CPE) in the branch cannot immediately be replaced with modern hardware, for any reason. There is a need for a local internet breakout in the branch, but the CPE is not powerful enough to enforce all required security controls typically enabled at the perimeter.
2. As long as the CPE is capable of building an IPsec or GRE tunnel to a Check Point Harmony Connect instance, all security controls can be enforced in the cloud instead of on the CPE, and the branch office obtains a secure local internet breakout.
3. The choice has been made for a specific 3rd party SD-WAN vendor and their products are not designed to run a Check Point VNF image on them. As in the previous case, the SD-WAN device only needs to build a tunnel to the Harmony Connect instance and route all the traffic over the tunnel to obtain a secure local internet breakout.
4. Harmony Connect can also be used to provide roaming users with secure internet access without having to deploy a fat agent on their machines; a lightweight client will provide secure access to all resources, or even clientless for non-managed devices.



The Harmony Connect security as a service solution offers the following advantages:

- Auto scaling
- No operational hassle: no need to worry about upgrades and provisioning of hardware
- Cost reduction: the WAN costs will decrease as traditional expensive MPLS circuits are replaced by VPN over cheap broadband connections
- Better user experience for internet-bound traffic (i.e. SaaS) by eliminating additional latency caused by backhauling via the hub site

Specifications:

Check Point's Harmony Connect is a cloud-hosted network threat prevention service offering a maintenance-free, comprehensive, affordable security solution for branch offices and roaming users. Harmony Connect seamlessly delivers the latest and most comprehensive cybersecurity available, protecting branch offices from the latest generation of targeted and advanced cyber threats.

Harmony Connect doesn't burden IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing routers or SD-WAN deployments. With a simple and easy setup process, network traffic from existing SD-WAN edge devices is tunneled to a primary cloud-based network security service at a nearby location. A second connection provides redundancy, ensuring branch offices stay connected and removing the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing overall CAPEX and OPEX costs.

Cloud Services	
Branch-to-Site connection	IPsec IKEv1, IPsec IKEv2 or GRE tunnels
Availability regions	US South-East, US North-East, US South-West, US North-West, Canada, Germany, France, Sweden, Ireland, United Kingdom, Hong Kong, South Korea, Singapore, Japan, Australia, India, Brazil, Bahrain

Software	
Latency	Up to 50 milliseconds1

Performance	
Single IPsec tunnel	Up to 1 Gbps per tunnel

(1) The expected additional latency for a branch in the same Harmony Connect region

When to Consider Quantum Edge

1. Local segmentation is a requirement: An example could be a manufacturing facility where the IT network needs to be segmented from the OT network
2. Inbound access to public servers is required at the branch office
3. There is a need for specific telco features on the SD-WAN hardware that are unavailable on Check Point solutions

The Quantum Edge product offers the following advantages:

- Hosting local public servers in the branch in a secure way
- Dynamic path selection: The SD-WAN appliance will choose the best circuit for any given session

Specifications:

Quantum Edge is a lightweight virtual image of the Check Point Branch Office Security Gateway. Within a minute of powering on the virtual security gateway, your branch office is protected.

Quantum Edge security gateways are deployed through the SD-WAN management console. This tight integration reduces deployment time, effort, and costs. When Quantum Edge is deployed on SD-WAN or uCPE equipment, the Quantum Edge virtual security gateway is configured, automatically connected, and ready to be centrally managed and monitored by the customer's domain in cloud-hosted SMP or the headquarters' R80 Security Management.

Software	
Security	• Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, • Antivirus and SandBlast Threat Emulation (sandboxing)

Performance					
VMware SD-WAN	Edge 520v	Edge 620	Edge 640	Edge 680	Edge 840
Threat Prevention	100 Mbps	100 Mbps	350 Mbps	500 Mbps	550 Mbps

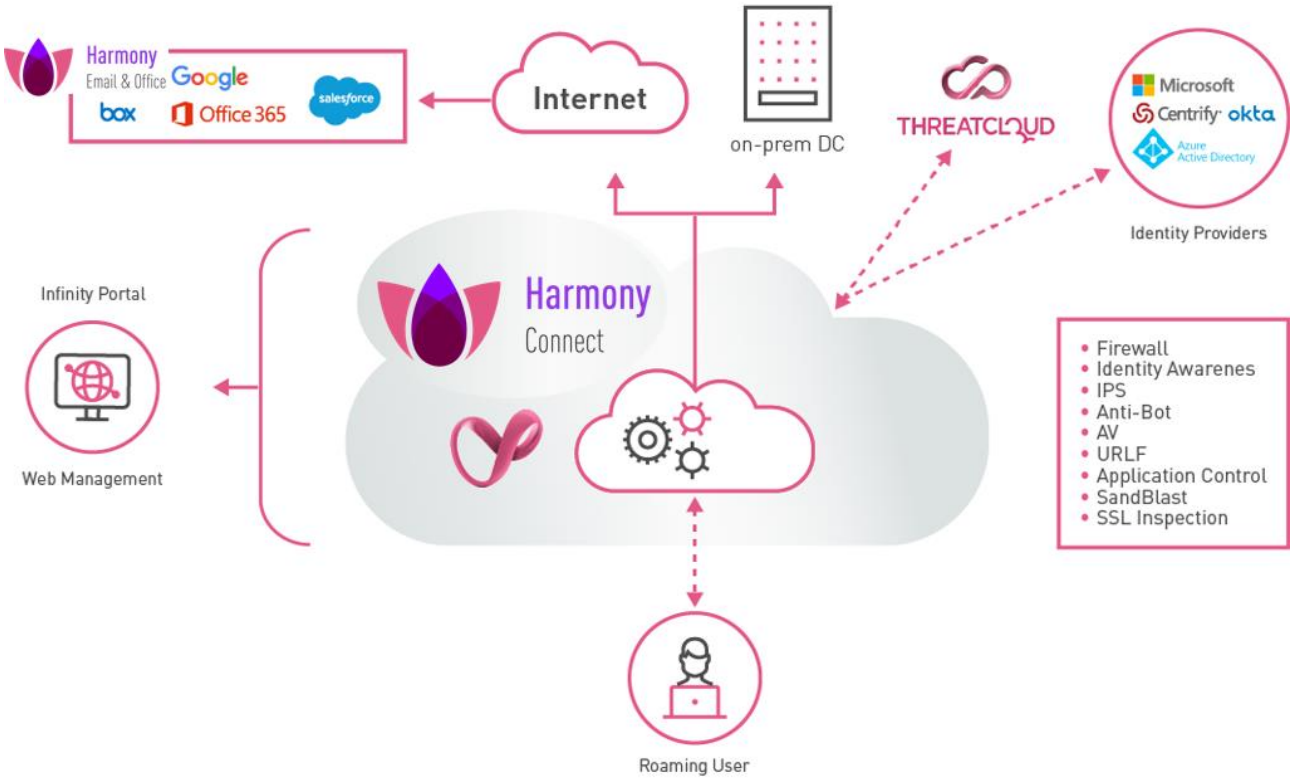
Note: The VMware SD-WAN Edge image configuration is set to 2 cores

Branch Edge Device	
VMware SD-WAN	Edge 520v, 620, 640, 680, 840
Cisco Enterprise VNF	ENCS 5104, ENCS 5412

Remote Access for Corporate Applications

Remote access to corporate applications is a primary need for all remote users. It has traditionally been done using VPN to the data center/office perimeter GW from the client side. This solution may load the perimeter GW, will require an endpoint agent, and may give too wide permission to the users on the internal network, and all its resources.

The solution is to design the access based on the principles of Zero Trust Network Access (ZTNA), which is part of the overall SASE solution.



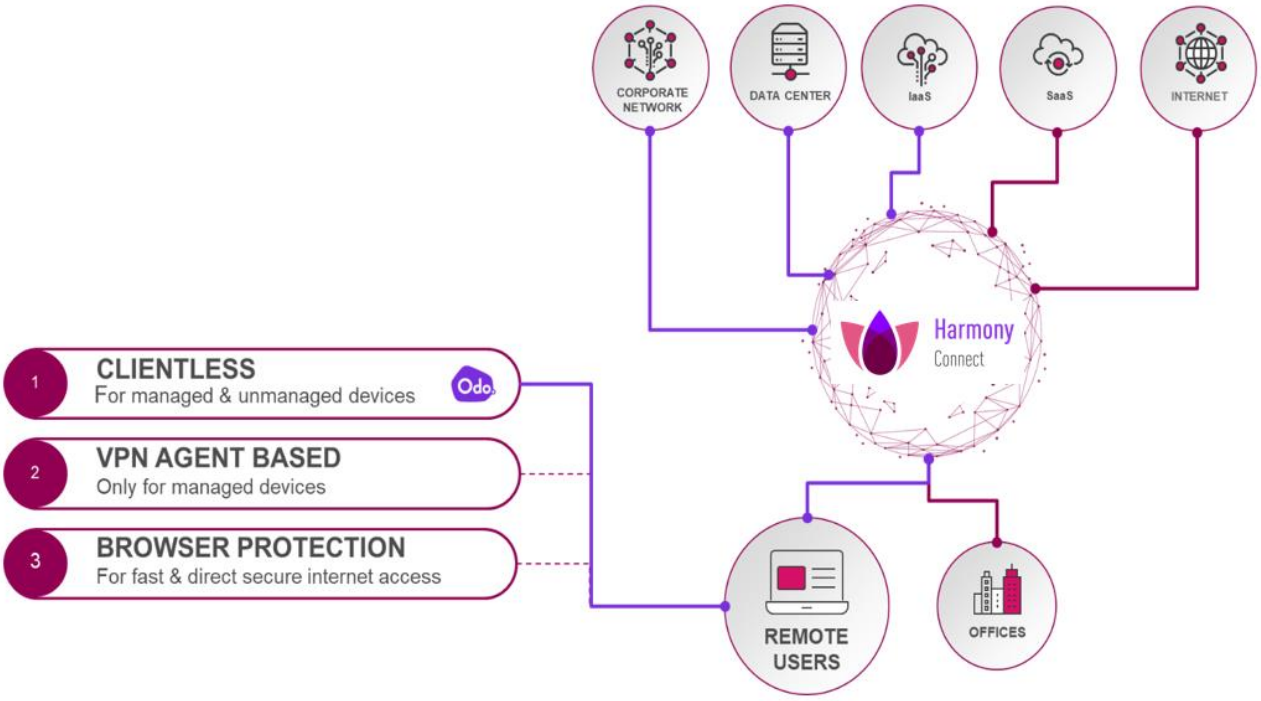
Zero Trust is a set of principles, that are implemented as part of an SDP (Software Defined Perimeter) architecture. The SDP architecture, as part of the SASE solution, will provide corporate access as a service to applications such as Web, RDP, SSH and Databases. In other words, it will manage access to corporate applications (in data centers), for all users, in a granular and flexible way.

SASE ZTNA application will support the following features:

- Least privilege access – minimum privileges to all users by default, while unauthorized applications and services are completely blackened.
- Inspection and authentication in the application level (IP agnostic)
- Continuous authentication and authorization per user per application
- BYOD friendly - clientless access to corporate applications

- Secure access using advanced threat prevention mechanisms and data protection engines
- Full visibility on all network activity

Corporate Access can be deployed in a clientless mode for unmanaged devices, with a lightweight VPN agent for managed devices, or with the Harmony Browser extension.



The blue lines in the diagram above mark the functionalities covered by Odo, as explained in the Clientless Remote Access below.

Clientless Remote Access

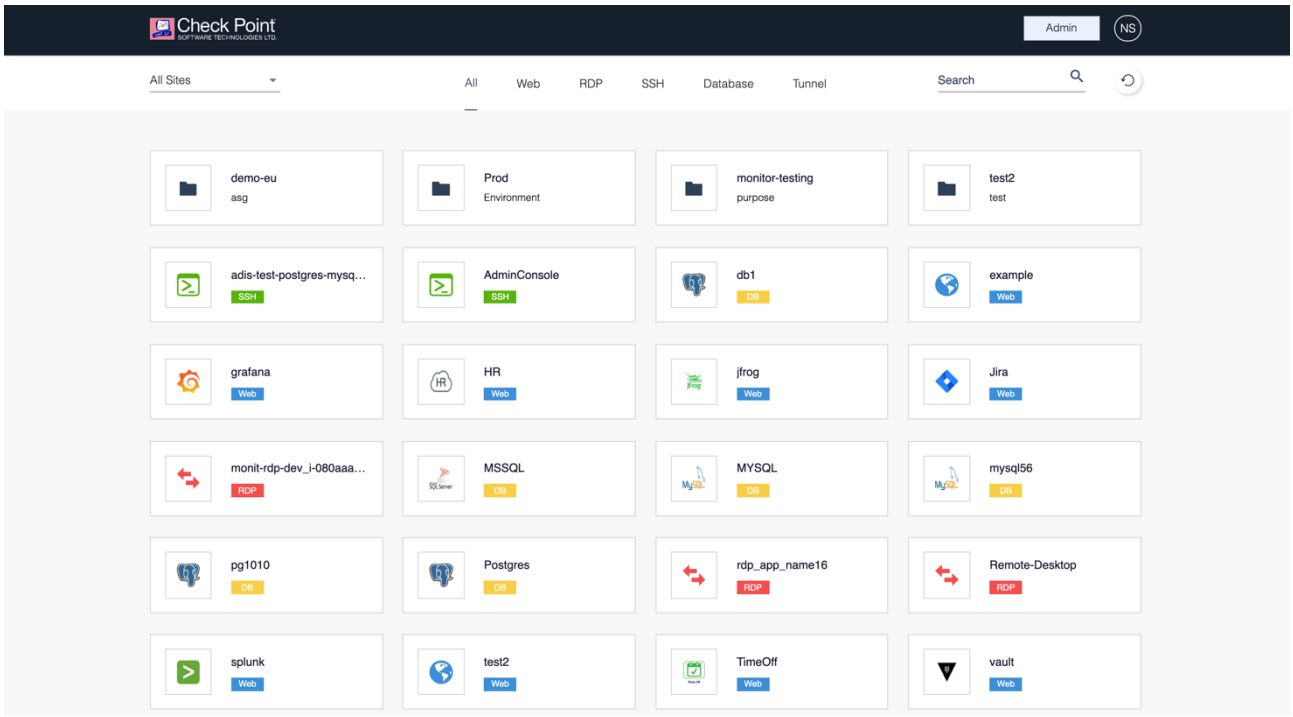
In September 2020, Check Point acquired Odo, a Tel-Aviv based start-up that developed a cloud-based, clientless SASE technology that delivers secure remote access.

Unlike traditional secure remote access solutions, this technology enables:

- Users to easily connect through a unified portal to wide range of applications such as remote desktops, web applications, database servers, cloud and corporate servers, with no client or software installation.
- Security administrators to easily deploy the solution in less than five minutes from the cloud. They also gain enhanced visibility including full audit trail of user activity.
- Zero Trust Architecture – Define granular access policy to give the right people in the right context, the least privileged access to applications and reduce the attack surface

Odo has developed innovative technology that provides clientless remote access – it enables users to connect remotely and securely to corporate applications, without requiring the user to install a connectivity agent like a VPN client.

Using the technology, users can remotely access corporate applications and remote desktops by using just a web browser. The technology currently supports access to web applications, RDP, SSH and databases.



The solution from a user's point of view in their browser.

Odo's solution is delivered as a cloud service, making it very easy for customers to deploy.

The technology addresses the following key use cases:

- **VPN replacement:**

  Provide zero-trust remote access to corporate applications that are delivered as a cloud service, and are easy to deploy and manage.
- **BYOD and third-party access:**

  Secure clientless access for unmanaged devices: employees with BYOD, contractors, etc.
- **DevOps access:**

  Addresses the need of DevOps and development teams to access cloud environments securely and easily from any device and at any scale.

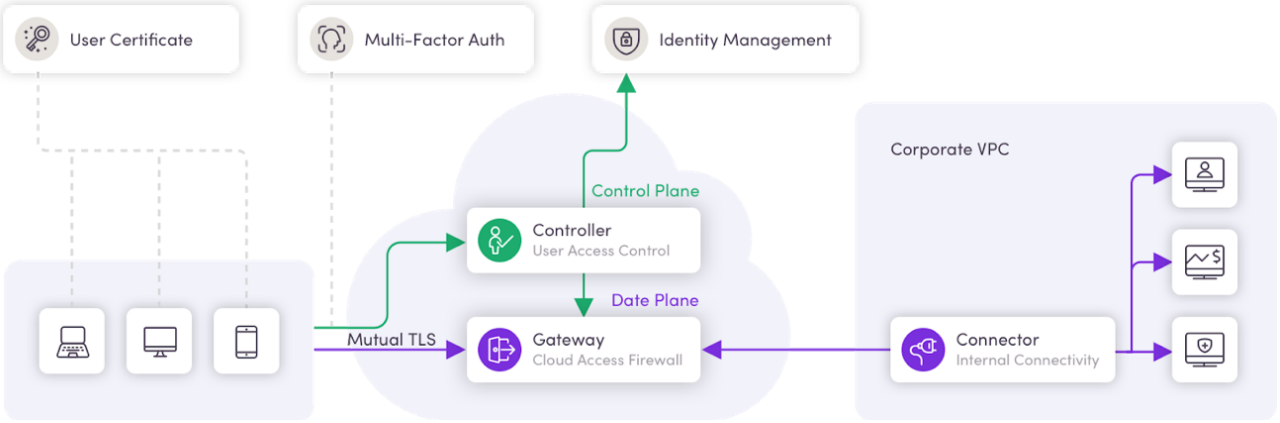
Features include:

- Automated discovery of cloud resource
- Dynamic access policy automatically provides granular access based on asset tags
- Cloud-based Privilege Access Management (PAM), with built-in key management and single-sign-on services

The architecture Odo developed is based on Zero Trust Network Access (ZTNA) and Software Defined Perimeter (SDP) principles. This means the solution is inherently secure through:

- Strict separation between the control-plane and the data-plane.
- No incoming connections to the data-center – facilitated through on-premises Application Connector technology that can be deployed in a few seconds.
- A least privilege application-aware access policy, with user identity and authentication tightly integrated with identity providers (Azure AD, Okta, Ping Identity and more).
- Application-level visibility and full session recording of user activity.

Architecture components:



1. Controller

The controller is the entity authorization end-point. It specifies who has access to what resources through a simple policy framework that factors in contextual data such as user attributes and device state. Policies can be tuned for each team or individual for more granular access management.

Through the controller, the system administrator can:

- Use the dashboard to create and edit policies with ease
- Get full visibility on user activity through a detailed activity log
- Manage device inventory
- Maintain identities locally or integrate with external IDPs
- Manage SSH keys

2. Gateway

A network tunneling gateway. Every user request flows through the gateway for consistent authentication and authorization, as well as providing a unified monitoring and logging point. This component makes sure validated users see only the applications they have permission to see, while the rest of the resources are not only inaccessible, they are completely invisible.

The gateway is in charge of the following attributes:

- Access Gateway for Web and SSH
- Contextual firewall
- End-to-end encryption
- Network blackening

3. Connector

The only network leg in the internal site. This component is a docker image and connects to the gateway through a reversed tunnel and effectively makes the organizational DMZ redundant by being the only access point to the site.

The connector provides:

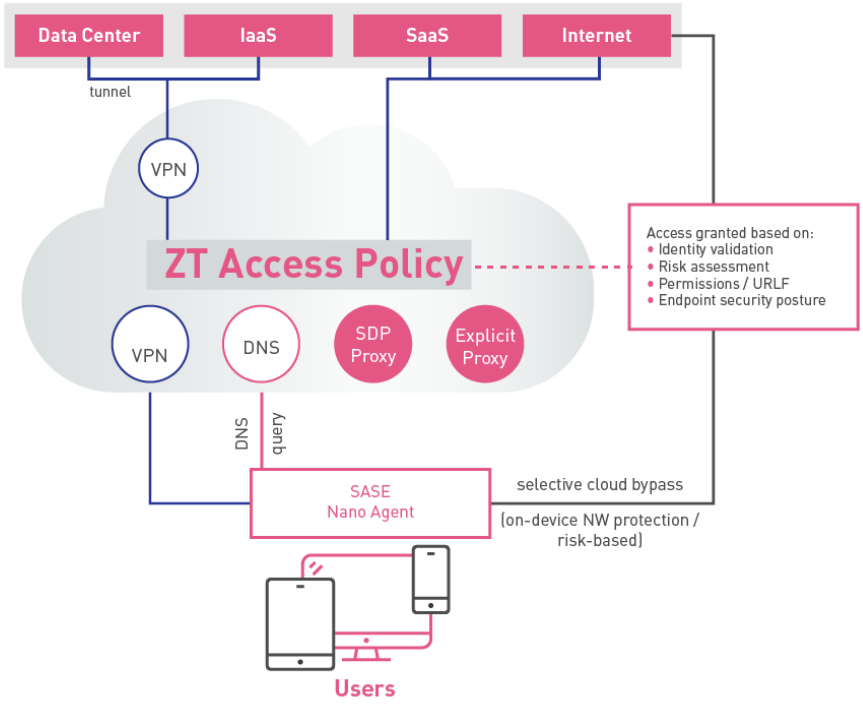
- Application-level (layer 7) access
- Cloud and region agnostic

4. Clients

The solution is completely clientless.

Lightweight Client

The lightweight agent routes all traffic to the closest Harmony Connect instance where all necessary security controls are enforced before the user is allowed to access any corporate resource or the internet, as with branch offices.



This means the endpoint, as well as the data and application, is protected but requires an agent to be installed. It ensures the same level of security for the users, regardless of their location. At the same time, the client also allows for a bypass path for specific types of traffic to break out to the internet directly, such as streaming services, thus avoiding a detour via the SASE cloud.

The lightweight Agent also adds an additional layer of DNS security to the ZTNA functionality.

DNS security reroutes corporate DNS queries to Check Point, allowing the following:

- Malicious domain prevention using Check Point's ThreatCloud
- DNS exploit prevention
- DNS tunneling prevention
- Prevention of infected hosts from communicating back to their command & control servers
- Check Point’s ThreatCloud proactively discovers and prevents access to newly-registered domains related to active threat campaigns and exploit kits
- Access control policy for domains using your own definitions as well as with 115 predefined categories by Check Point
- Zero phishing by defining domains of interest to prevent access to lookalike domains

Harmony Browser extension

It is also possible to use the SandBlast browser extension, preventing the download of malicious files, without the need for an agent to be installed. The functionality of the browser extension includes

- **Threat Emulation:**
  Detect malicious behavior by running files within a secure virtual environment.
- **Threat Extraction:**
  Obtain immediate and safe access to documents by removing potentially malicious elements or converting the downloaded file to PDF. Users can download the original file once Threat Emulation completes.
- **Phishing protection:**
  Zero Phishing is an innovative Anti-Phishing product, protecting corporate users and administrators from Zero-day phishing sites and Password/identity theft

Remote Access to Corporate Resources Using the Public Cloud (ZTNA)

Following the worldwide outbreak of COVID-19 in March 2020, remote access solutions have become a critical requirement for organizations. Under today’s circumstances many workers have their own broadband connections at home with WiFi networks capable of supporting network speeds like those found in the office. This makes it possible for employers to leverage their workers' home networks for connectivity to the edges of corporate resources. However, home networks are often shared with family members, fully rely on untrusted public backbones, and can be entirely unprotected. Connecting remote employees to corporate systems therefore requires additional layers of security to ensure the confidentiality, integrity, and availability of corporate data and systems.

Under a new approach, Check Point's ZTNA strategy is to allow remote access communications without deploying traditional gateways in the public IaaS. This new method facilitates global coverage to be reached through proximity algorithms.

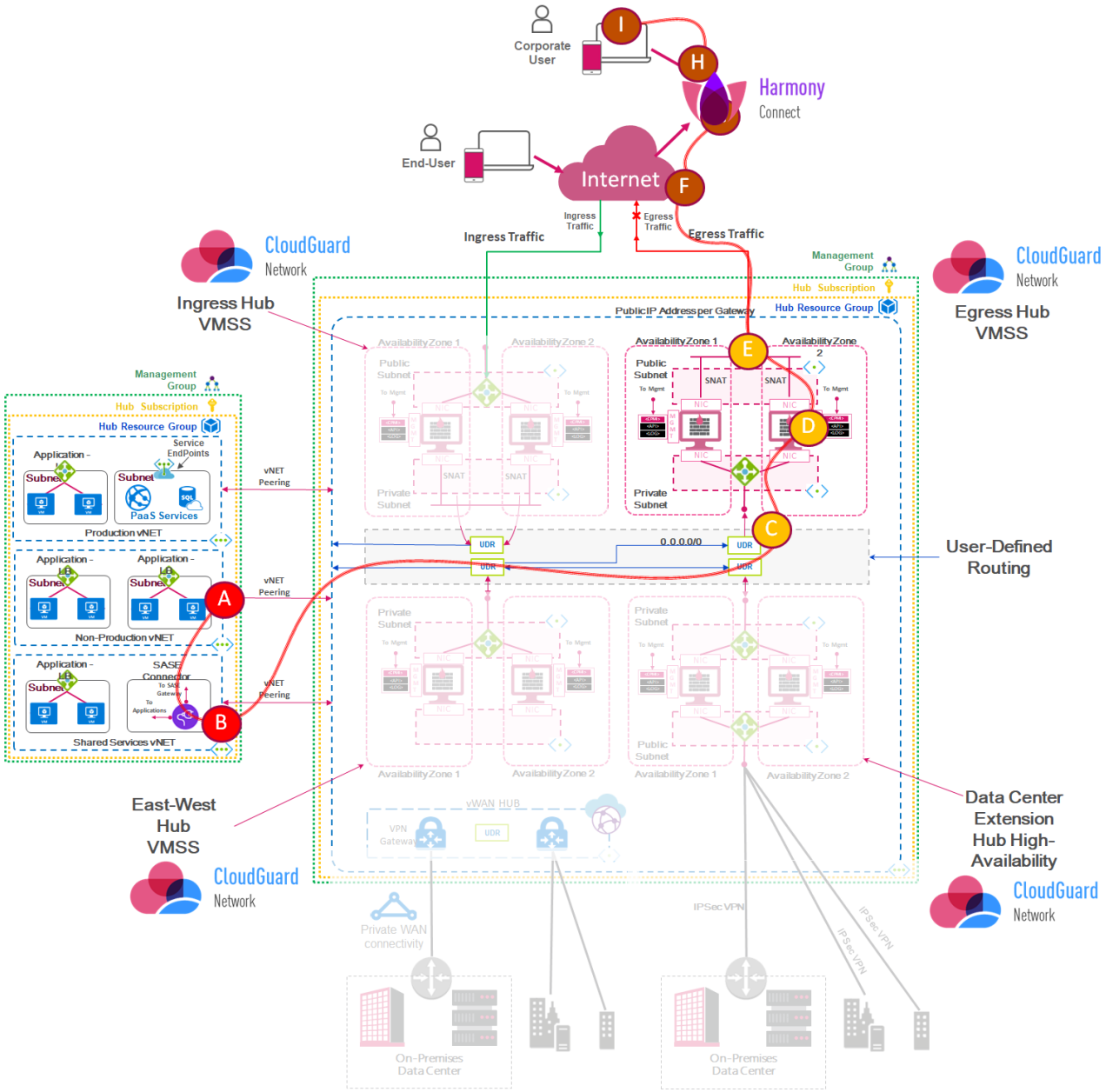


Figure 1: Remote Access through Check Point SASE – Microsoft Azure

In the flow description visualized above we can see that traffic, which originated from point A, is located by external users with a client-based, or clientless, VPN. This traffic is terminated in the Harmony Connect for users where all traffic will be inspected and the posture security device will confirm if the remote user can be considered as trusted. If the answer is 'yes', traffic is forwarded to the relevant computing instances (point B) through the Check Point Harmony Connect (ZTNA), peering to the public IaaS data center to access specific services in PaaS (such as app services in point C) or services in the Kubernetes cluster.

FROM	TO
Remote access traffic to cloud data center applications	- **Remote access users ("A") connect to the Harmony Connect ("B") using its public IP address to access all the remote access services in the cloud access gateway.** - **The Check Point SASE connector ("C", acting as a reverse proxy) is located in the cloud data center and has the capability to connect to different applications located in the production vNETs. The reverse proxy also has**

connection t through the egress traffic to the internet ("E") and is connected to the Harmony Connect services ("F").

Public cloud IaaS integrated with a ZTNA framework has many advantages for organizations, the most important of which is how it helps adopters prioritize security, no matter what other tools they're using.

For example, if a business requires a transition from one cloud service provider to another cloud service provider, the SASE platform continues undisrupted due to its platform agnostic. This flexibility also makes it easy for businesses to scale up their security infrastructure as they grow, without having to reconfigure the central architecture or deploy dedicated VPN clusters in the public cloud data center. Such an ability to customize security setting operational needs, enables organizations to create an architecture that meets their current and evolving business needs. It is important to keep in mind the following security and network components of a ZTNA architecture:

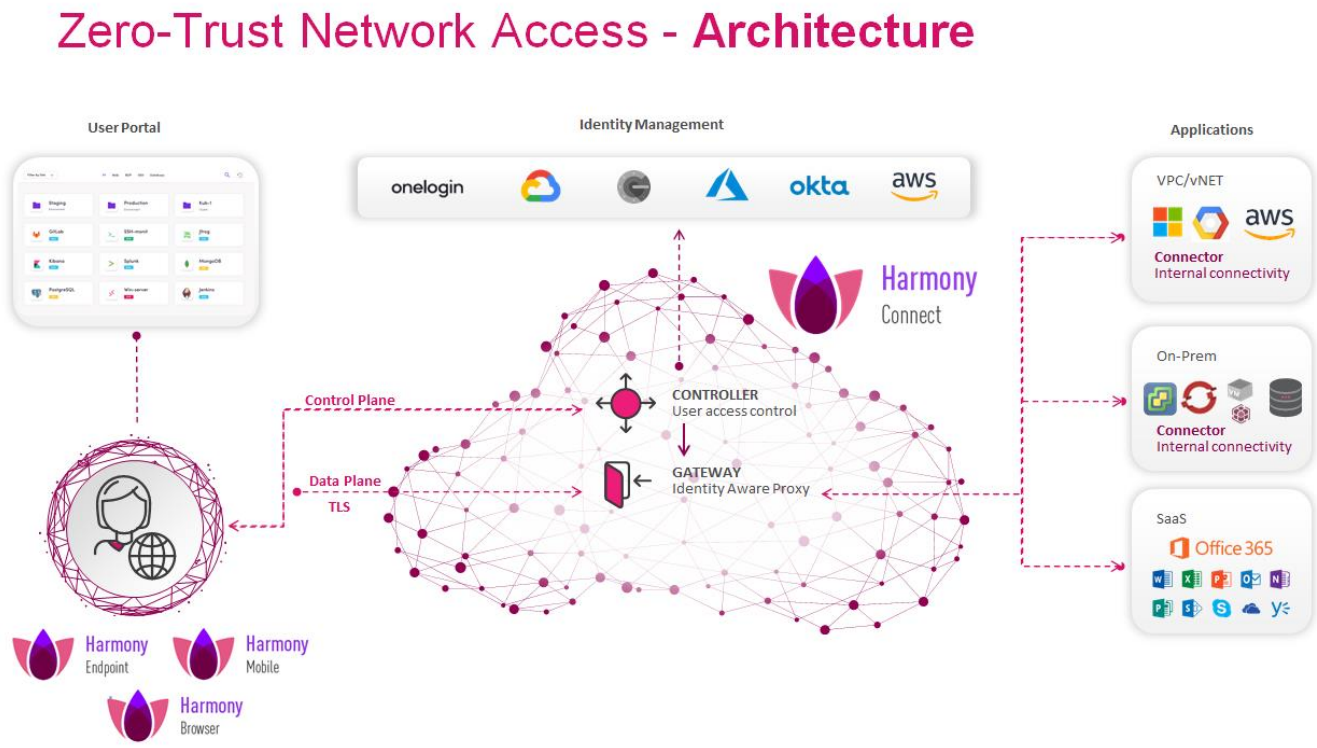


Figure 2: Check Point Harmony Connect - ZTNA Architecture[1]

[1] Check Point Remote Access – URL: https://docs.odo.io/docs/odoaccess-architecture

A similar approach can be seen on the Google Cloud Platform. Following the egress use case described in Google Cloud, the new element here is the ZTNA connector (flow B) that connects to different applications (web, RDP or SSH) located in different VPC's (flow A). Once the reverse proxy is connected to the relevant applications and services are authorized, we can follow the same flow for the egress traffic starting with the Google routes (flow C) and it being processed by Check Point MIG Clusters.

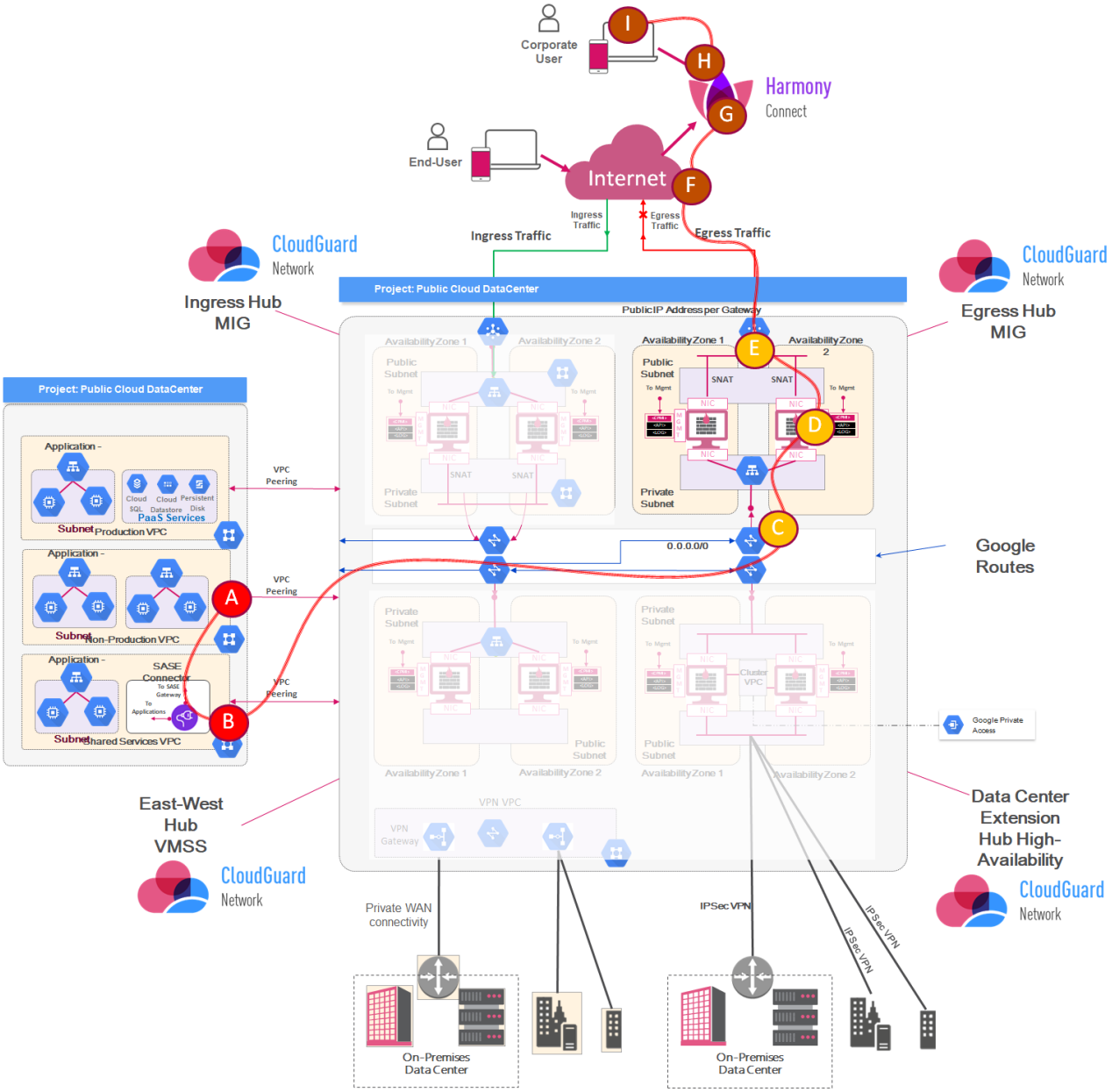


Figure 3: Remote Access Through Check Point SASE – Google Cloud Platform

In AWS, we can integrate the egress and east-west use cases to allow for the connectivity between the SASE connector and Harmony Connect cloud service. The ZTNA connector is located in the SASE and shared services VPC, where it connects to the specific applications located in different VPC's (web applications, remote desktop or SSH), as a reverse-proxy (flow A). The transit gateway then forwards the traffic (flow B) to connect to the applications located in frontend VPC (flow C).

From the user perspective, the clientless VPN first originate the traffic from internet (flow 1), and then connects to the Harmony Connect cloud service (flow 2). Once the user is authenticated, according with their role previously defined in the RBAC policies (flow 3), the reverse proxy uses the egress flow traffic (from A to D, then D to forward the connection from the connector to the Harmony Cloud service.

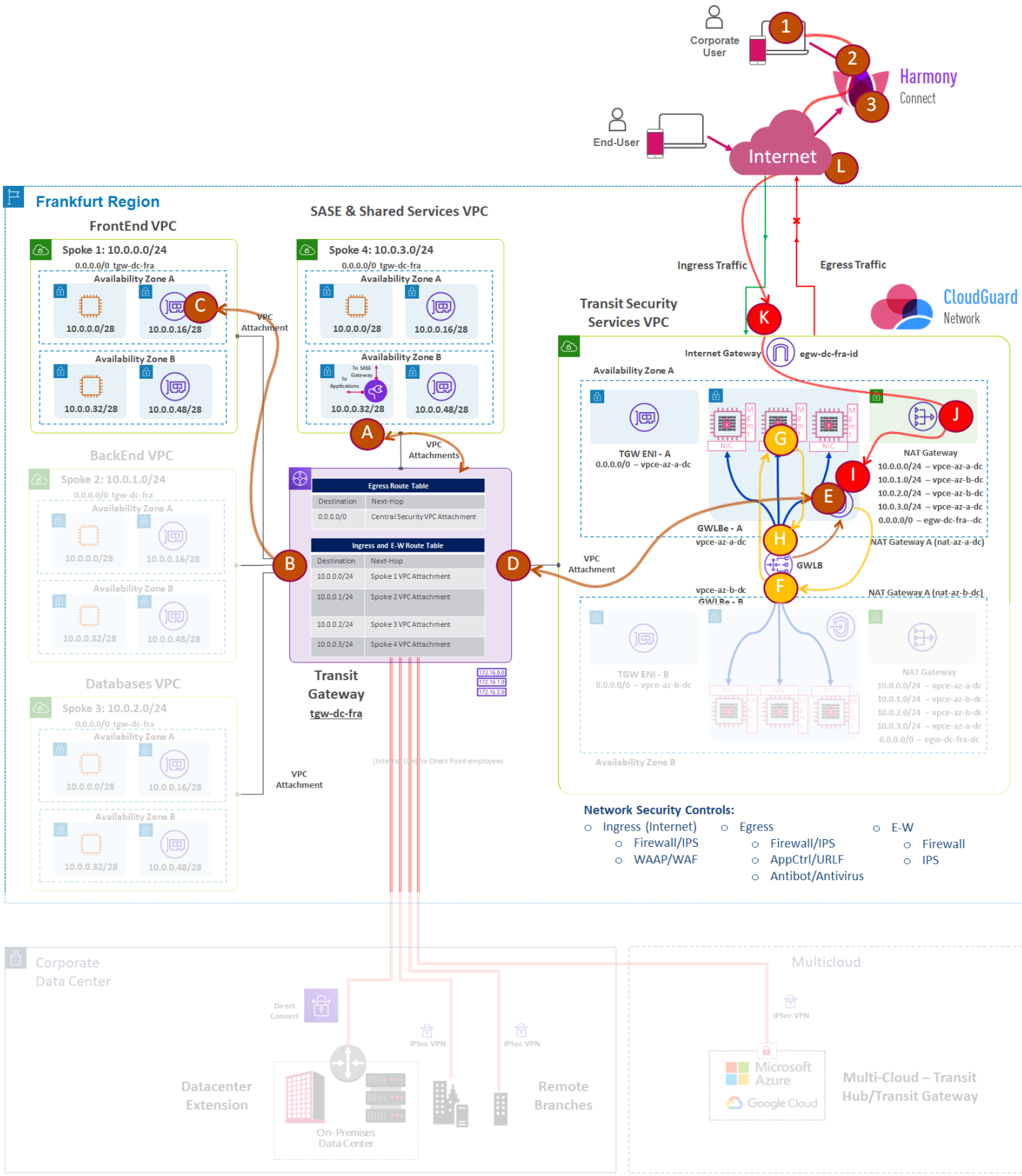


Figure 4: Remote Access Through Check Point SASE – Amazon Web Services

Remote Access and Windows Virtual Desktop (RDP)

Check Point SASE can also enable the Remote working environments with Windows Virtual Desktop or Virtual Desktop Infrastructure as a Service. Windows Virtual Desktop is a comprehensive desktop and app virtualization service running in the cloud. It is the only virtual desktop infrastructure (VDI) that delivers simplified management, multi-sessions on Windows 10, optimizations for Microsoft 365 apps for enterprise, and support for Remote Desktop Services (RDS) environments. Most significantly, you can deploy and scale your Windows desktops and apps on Azure in minutes, and get built-in security and compliance features.

However, one of the major concerns is the latency to deploy ZTNA services located in different data centers worldwide. To provide a more optimized model, Check Point ZTNA can be complemented with virtual desktop infrastructures. In the following diagram, we can gain an overview of how the customer can access their cloud data center services using the WDI (the same approach could be done with VDI).

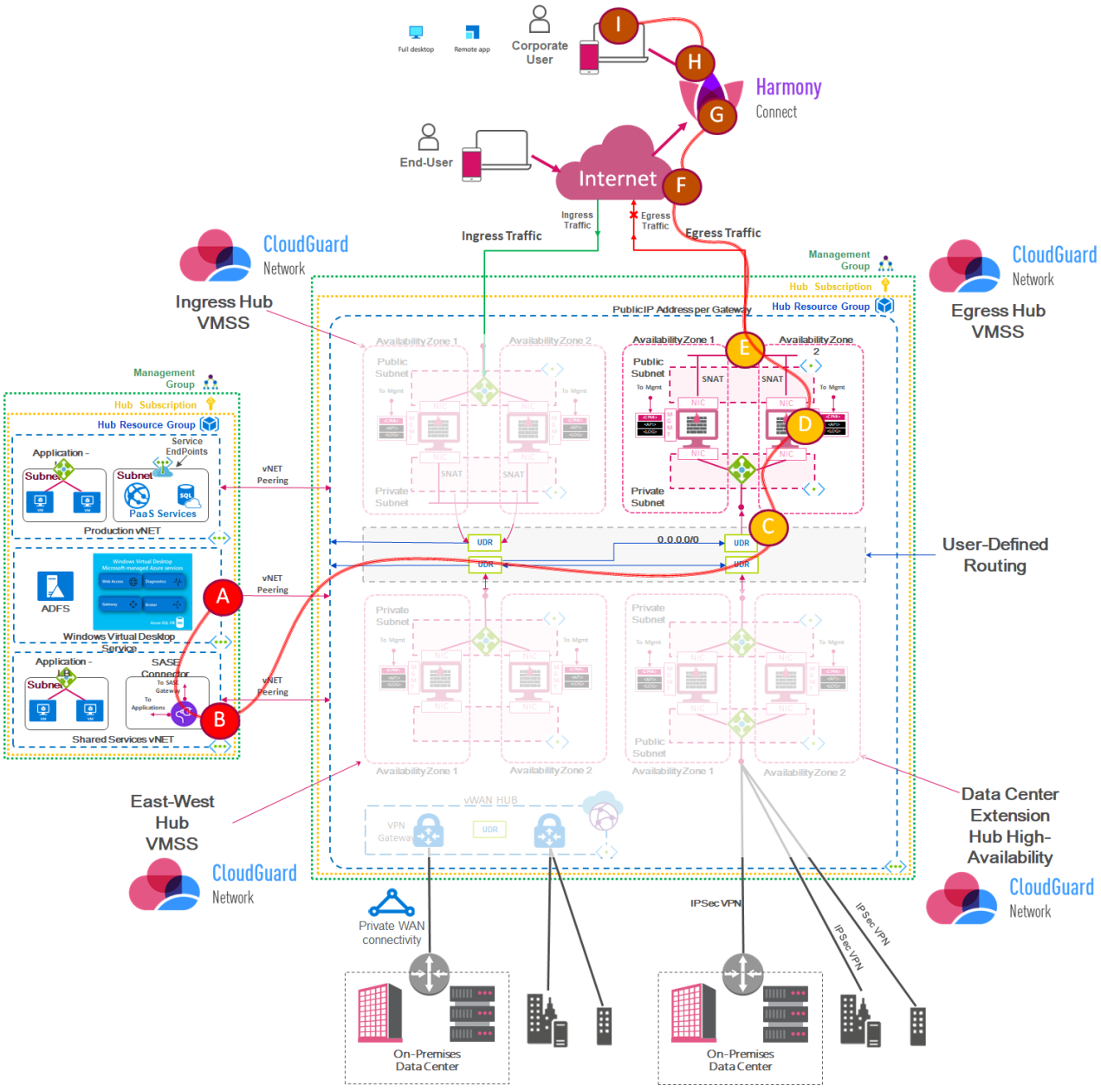


Figure 5: Secure Remote Access With SASE and WDI to the Cloud Data Center

FROM	TO
Remote access traffic to cloud data center applications through Windows Desktop Infrastructure	- **Remote access users ("A") connect to Harmony Connect for users ("B"), using its public IP address. Check Point ZTNA service inspects the traffic and sends it to the internet or to the peering communications ("C"). This provides communication into the virtual network to access Windows Desktop Infrastructure (or another similar solution in "D"). Then, according to policies, remote users ("E") can access one specific application using the service portal or full desktop. Under this approach computing execution is done in the user virtual environment. This saves on bandwidth and latency to access applications installed in the computing instances, PaaS web applications, or container applications.** - **In this scenario, the routing is more simple and flexible. This is due to returning packets being managed internally between the WDI managed services and the peering to the functional vNETs. The only returning packets to warranty are the routes back to the gateway through the use of User Defined Routes (UDR) for the thin client, and the WDI managed service.** - **The reverse-proxy also has connection to the internet through the egress traffic to internet ("F") and is connected to the Harmony Connect services ("G").**

For more details about Security Architecture Reference Guide for Public Cloud IaaS, please refer to the whitepaper at https://www.checkpoint.com/downloads/products/cloudguard-iaas-architecture-reference-and-best-practices.pdf

Data Loss Prevention (DLP)

When data is in motion, APIs allow inspection and potential leakage of data for corporate applications using the Harmony WAAP product and for SaaS applications, Harmony Email & Office.

However, when corporate data residing on the endpoint itself is at rest, it needs protection as well.

This is why a full endpoint agent on the roaming users' machines still makes sense as certain features cannot be enforced in the cloud (i.e. Full Disk Encryption). The same challenge arises when the machine is not connected to the internet. It can still be vulnerable in that scenario: removable media could potentially contain malware and harm the machine even offline. Having a full endpoint solution on the machine ensures it is always protected, regardless. In the future, the lightweight agent to connect to Harmony Connect will become part of Check Point's full End Point Suite.

Harmony Email & Office security

The ability to access SaaS applications *directly* in a secure fashion combined with satisfying user experience (without the additional latency caused by backhauling traffic through a Data Center) is a core business driver for adopting the SASE model.

Email Security

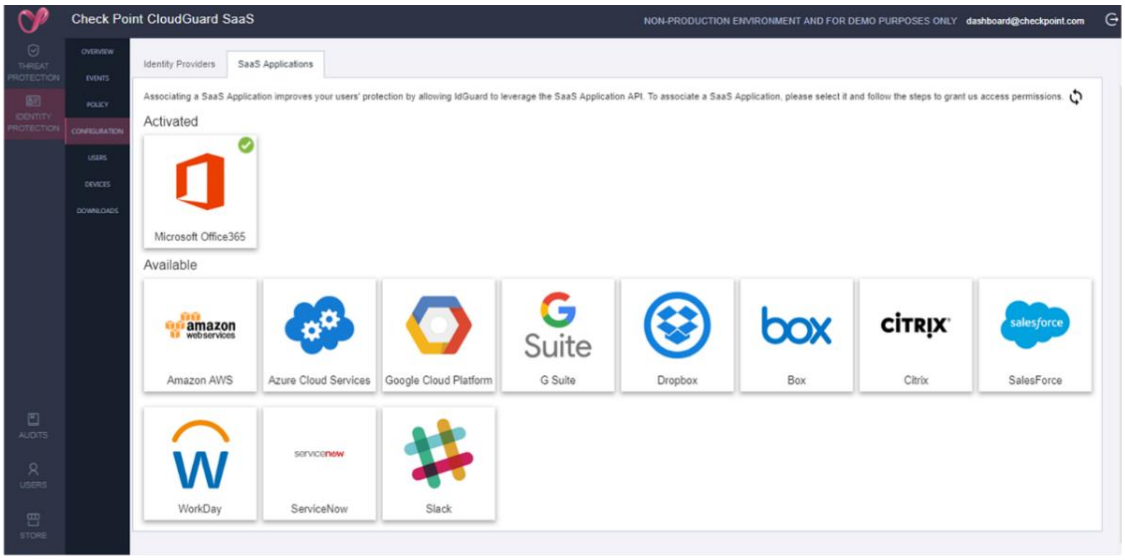
Many organizations have moved or are in the process of moving towards cloud-based email services such as Office 365 or G-Suite, for obvious reasons. However, when doing so, it is important to re-evaluate the email security, as attack vectors shift.

- Over 90% of cyber-attacks on organizations start from a malicious email.
- Business Email Compromise (BEC) attacks alone cost $300 million a month to organizations.
- Phishing schemes are getting more sophisticated by the day.
- Platform-provided security solutions miss about 30% of malicious emails

Harmony Email & Office is a cutting-edge email and office-suite security solution that is trained to catch what other solutions miss. Harmony Email & Office deploys in minutes and provides organizations with a simple management platform and an invisible architecture that will not expose you to cybercriminals.

Harmony Email & Office Apps

A brief overview of some of the applications that can be accessed safely are listed below (the list is not exhaustive):

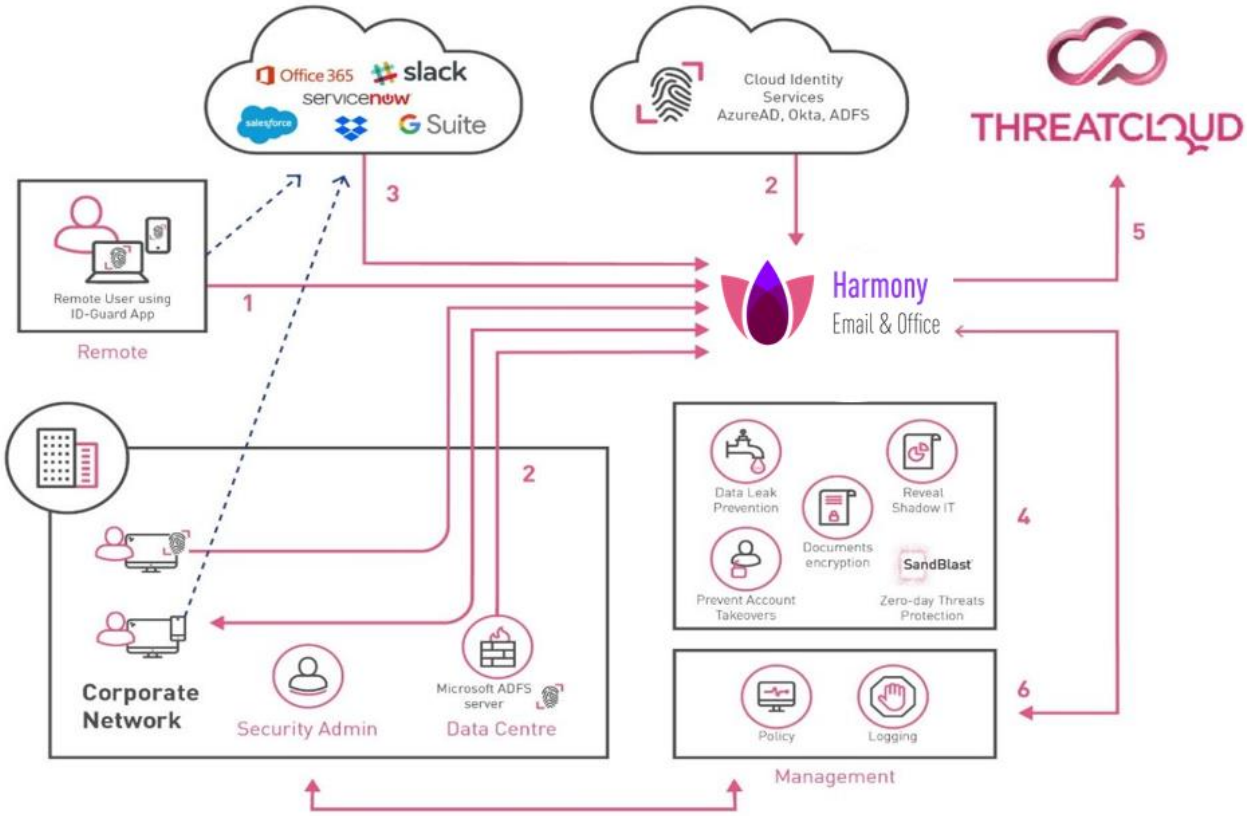


Harmony Email & Office Architecture

Harmony Email & Office is a cloud-only, API-driven, Threat Prevention and Identity Protection platform leveraging several components to perform SaaS application security. This section breaks down the architecture to ensure the correct configuration is achieved.

The security services offered by Check Point SaaS can be split into two categories: Threat Prevention and Identity Protection. Upon configuration, all these services are available from the Check Point Portal.

The following graphic outlines the key components and their relationships:



This graphic shows how the Harmony Email & Office integrates with the cloud and device ID services

- **Agent** or **Agentless** connections options:

  Agent-mode is a lightweight agent installed on all Windows machines allowing user-identity and connection-context to be shared with the Harmony Email & Office platform. The Harmony Email & Office is called ID-Guard and is mandatory if identity protection is required.

  In agentless-mode**,** one-time passwords are sent to either the Check Point Sandblast mobile application or by SMS, used to identify users. Agentless-mode also makes use of the connection context, such as source IP, time of connection, etc. to relay information to the platform.

- **Identity Providers**

  Harmony Email & Office integrates with ADFS using a Check Point agent installed on the ADFS server. Harmony Email & Office can also use cloud-based identity providers such as AzureAD.

- **Service Provider**

  Harmony Email & Office essentially acts as the mediator between the Identity Provider and Service Provider. It is a service required by users.

- **Harmony Security Services**

  These Check Point services are available to the administrator once the SaaS application has authorized Harmony Email & Office access.

- **Check Point Security Services Including Threat Cloud**

  Harmony Email & Office is deployed into Check Point data centers (currently in the EMEA and USA), offering the same security services as Harmony Connect.

- **Harmony Email & Office Portal**
  All admin is done using a web portal, including setting up the policy, logging, etc., and downloading the required agents.

Putting identity at the core of SaaS application security

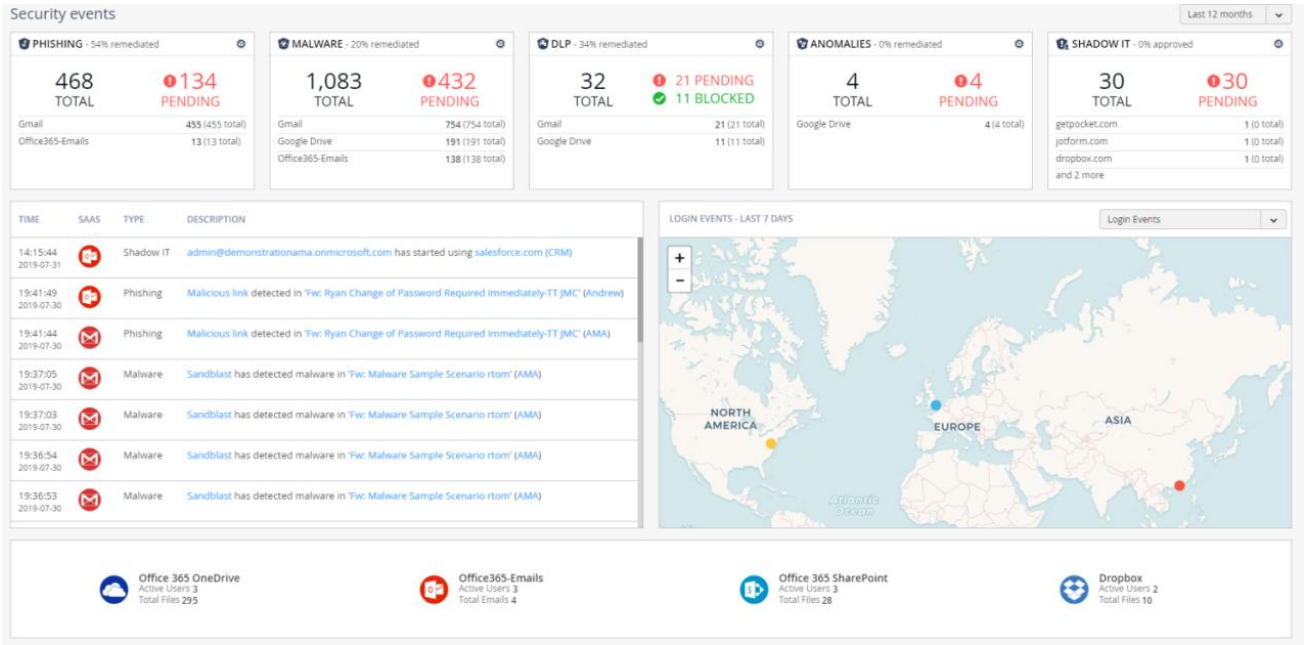
A key component of a modern security approach is the incorporation of user-identity into the security policy, security platform, and security posture. Label-based or identity-based security is more effective where mobility and agility are business requirements. Check Point has developed a unique Identity Protection engine, which integrates with any Identity Provider and SaaS Provider that supports the SAML 2.0 protocol.

MANAGEMENT AND REPORTING

Harmony Email & Office Management

The management interface of the platform allows administrators to build the required security policy, download the various Harmony Email & Office agents, and configure identity protection policies. Once configured, the SaaS portal can display logs and heat-maps to help identify the use of shadow IT. Currently, the management interface is cloud-only. In the future, the SaaS management interface will be merged with the Harmony Connect and Edge Management interface.

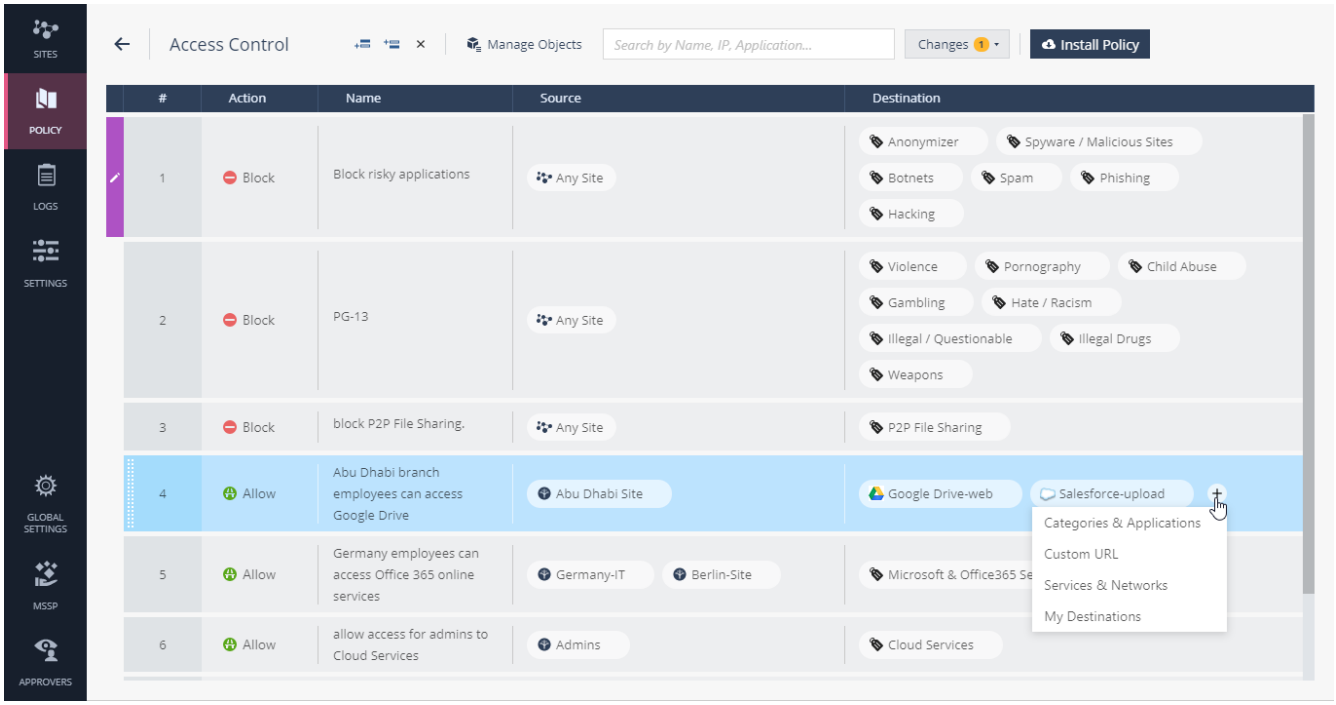
The screenshot below shows the Cloud Guard SaaS management portal. Please refer to the user manual for more details.



Harmony Connect Management

Harmony Connect is managed via the Infinity Portal and with an R80.20 or the SmartCenter above.

The following is a screenshot of the Infinity Portal:

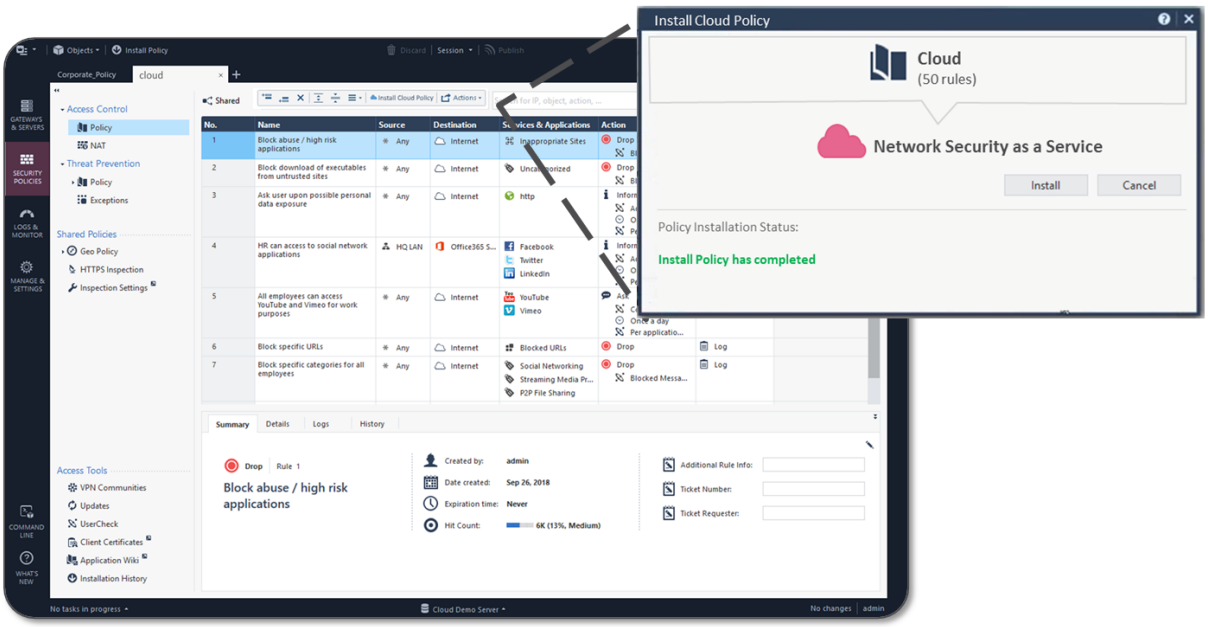


Benefits for managing Internet policy within the Infinity Portal:

- The destination column consolidates applications, custom IPs, and custom URLs
- A single, unified policy for all branch offices ensures central management
- The first three predefined security policy rules in the security portal are out-of-the-box-defaults which secure branch offices with zero customization.

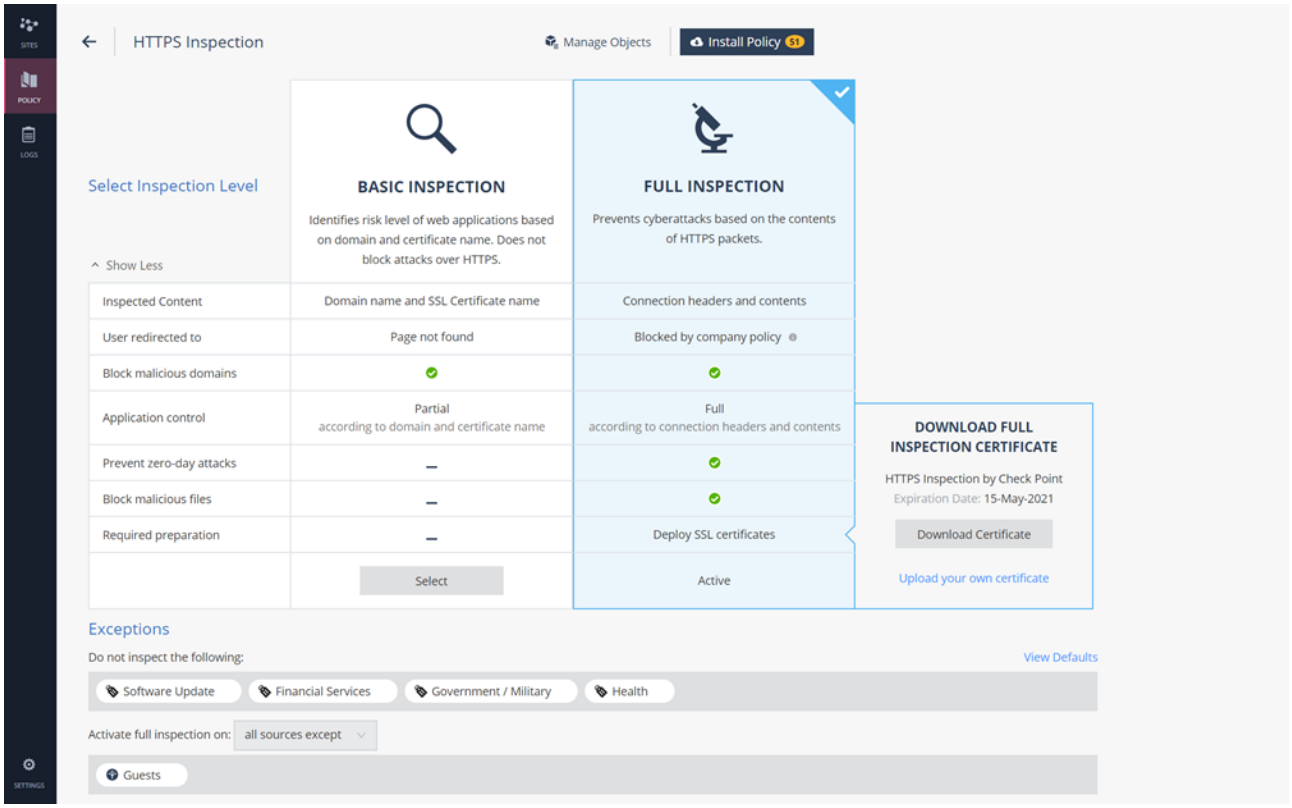
Another option is to manage the SD-WAN policy using an >R80.20 management station.

This method is supported by both Quantum Edge and Harmony Connect.



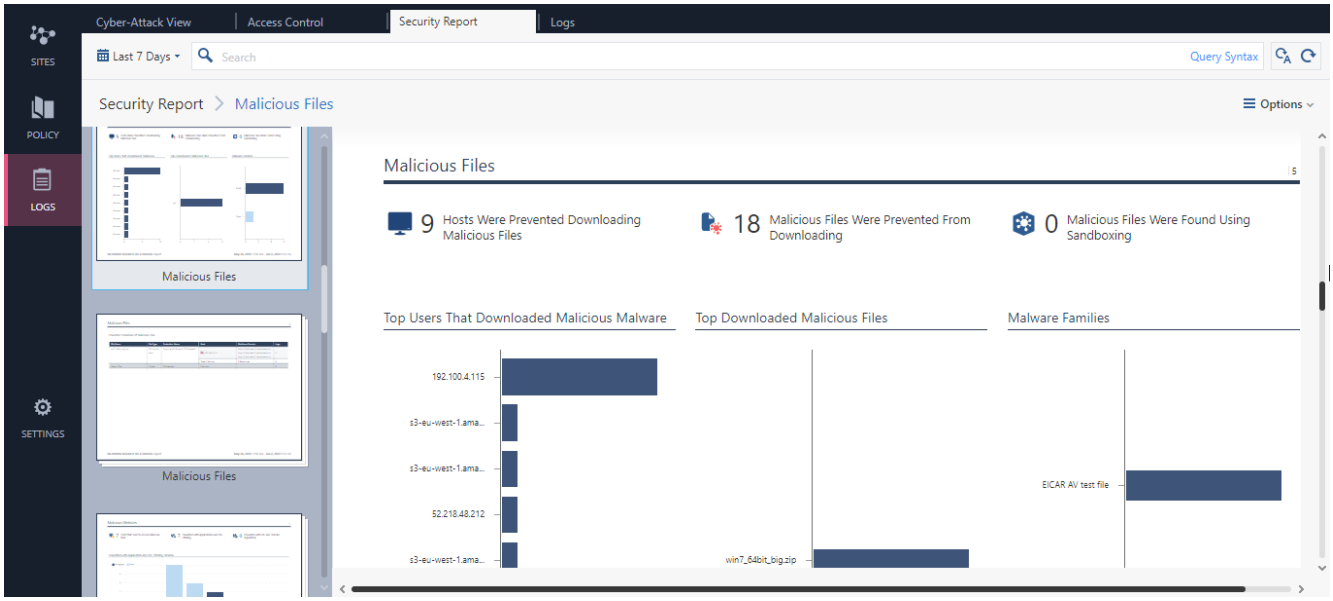
As Quantum Edge VNF is a gateway SMB image, it can be managed by the local web, SMP cloud web management, or by SmartConsole of any version that supports Check Point's Large-Scale Management (LSM), which is essentially any version except for R80.10.

Full HTTPS inspection is also supported:



As can be seen at the bottom of the screenshot, HTTPS inspection can be bypassed for traffic originating from specific sources at the branch office.

Examples of a weekly threat report and logs:



CONCLUSION

SASE allows organizations to easily migrate from expensive on-premise, bare-metal-based networks to an OPEX-based and cloud-centric security architecture that is far more agile, cost-effective, and secure.

Check Point believes that SASE technology will gradually become more widely used and accepted and that eventually, most on-premise appliance-based security controls will be replaced with cloud-based alternatives.

SASE helps support SD-WAN technology, secure access to SaaS applications, and protect roaming users - while meeting the specific needs of each business and their unique infrastructure. All products discussed in this paper are part of the Check Point Infinity architecture and can be managed from a single pane of glass; the Infinity portal.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com