



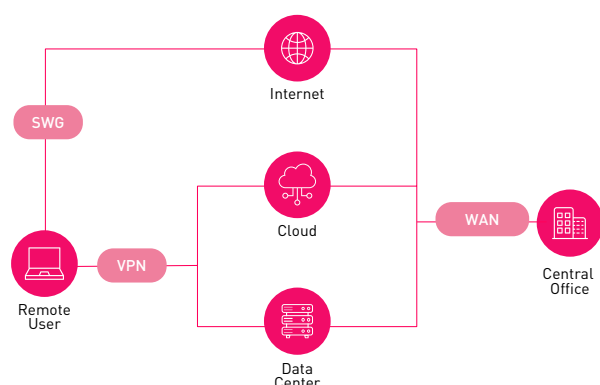
HARMONY SASE FOR BRANCH OFFICE SECURITY



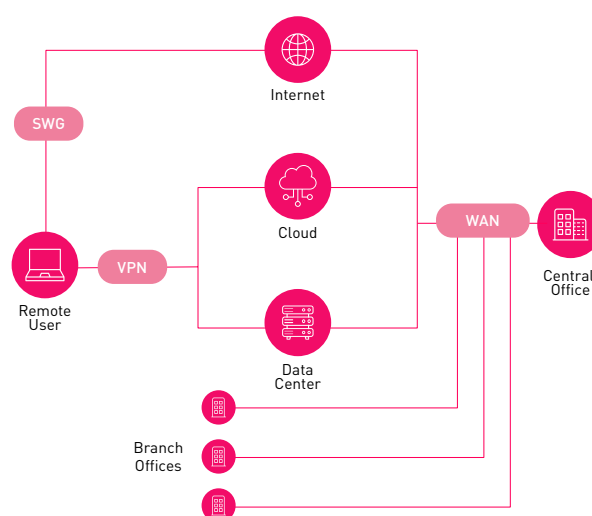
Businesses that operate networks of branch locations have networking and security requirements that typically differ from other types of organizations.

While a corporate office has a clearly defined and easy-to-visualize network, retailers, restaurant chains, financial institutions – among other types of businesses – may have dozens or hundreds of branch sites, with a variety of local factors and challenges to consider.

Simplified network architecture:
Business with a central office



Simplified network architecture:
Business with multiple branch offices



Regardless of where each branch is located and what services are locally available, branch users need easy access to centralized datacenters, on-prem and hosted applications, and internet sites. With the majority of business workloads running in the cloud, they also need seamless connectivity to SaaS applications to handle daily activities such as:

- Sales and customer relationship management
- Inventory management
- Employee management and scheduling
- Document management
- Industry-specific systems, such as reservation software for a hotel chain or a loan processing application for a bank

Network administrators, whether they're working from the corporate headquarters, from home, or from any other location, occasionally need to connect to resources at branch locations. For example, a user might need remote support with an application or a device in the branch may require maintenance. As the branch locations increase in number and across geographies, this becomes exponentially more challenging for the IT team.

Setting Up the Networking and Security Architecture

Establishing and maintaining a network architecture that combines both virtual and physical assets can be challenging. The architect has to consider factors such as bandwidth constraints, scalability, network performance, maintenance and upgrades, among others.

Of course, branch locations need more than just network connectivity. Just like the corporate headquarters, branch offices require robust security such as firewalls, malware prevention, granular access controls, and content filtering.

Traditional Approaches

Some organizations have set up connections to their branch offices using expensive MPLS connections, which require dedicated leased lines between sites. These connections are fast but not inherently secure, necessitating additional security tools.

Alternatively, other orgs rely on traditional VPN connections, which encrypt traffic but suffer from bandwidth constraints and latency due to backhauling. Such setups diminish productivity, frustrate branch users, and make it impractical to use high bandwidth applications such as videoconferencing.

Check Point SASE for Branch Locations

Any-to-Any Connectivity

The Check Point SASE full mesh network is underpinned by more than 75 points of presence globally, providing fast, seamless connectivity to any endpoint, cloud service, data center or SaaS application. And the IT team can easily connect to devices at the branch level, saving time and improving productivity.

Secure Access to SaaS and Cloud Platforms

Each Check Point SASE customer enjoys their own static IP, enabling you to allow only traffic coming from that address to access your cloud environment. Organizations with compliance requirements or that simply prefer an additional layer of security can establish encrypted tunnels between their SASE gateway and cloud resources.

Bandwidth Hungry Apps

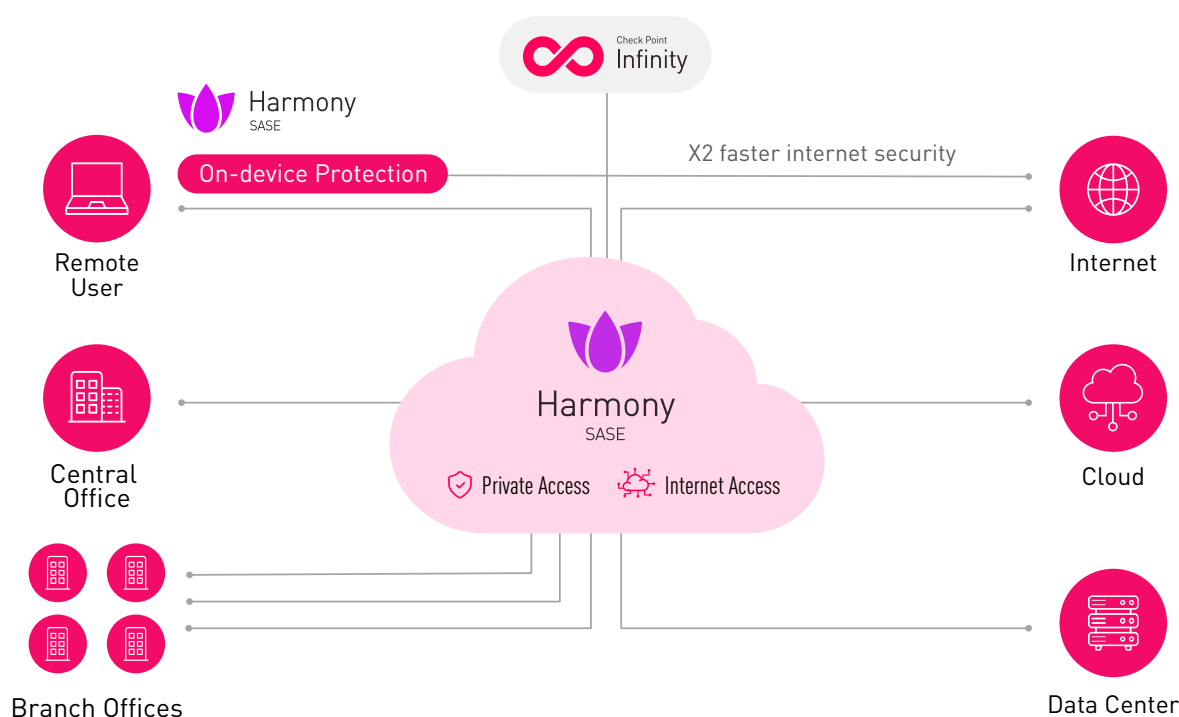
Split tunneling lets your branch team use videoconferencing and other high bandwidth applications with confidence.

Advanced Web Protection

Harmony SASE lets users establish direct, secure connections to the internet. This includes advanced capabilities such as anti-bot, threat emulation, and zero phishing.

Scalability

Bringing new branch offices online is a matter of a few clicks within the Check Point SASE unified management platform. Within minutes, administrators can set up and test the new connection, then get back to their other priorities.



Check Point SASE delivers robust, zero trust connectivity between branch offices and corporate resources, wherever they are located

Meet Harmony SASE

2x Faster Internet Security | Full Mesh Private Access | Secure SD-WAN

The internet is the new corporate network, leading organizations to transition to SASE. However current solutions break the user experience with slow connections and complex management.

Check Point SASE is a game-changing alternative that delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Check Point SASE enables any business to build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has

To learn more, visit <https://www.checkpoint.com/harmony/sase/> or [schedule a demo](#).