YOU DESERVE THE BEST SECURITY

SECURE REMOTE ACCESS OPTIONS: CLOUD-BASED ZTNA VS TRADITIONAL ON-PREMISE VPN FOR REMOTE AND HYBRID WORK ENVIRONMENTS

Securing the Modern Corporate Network

In the current era of public cloud resources and hybrid work environments, legacy VPNs fall short in providing the secure remote access modern businesses require. This leaves organizations vulnerable to security breaches and increases the risk of cyberattacks.

By default, they lack any granular access controls that restrict users to only the specific applications they need. Instead, users within the organization gain access to the entire internal network, resulting in a larger attack surface and increasing an organization's security risk.

Zero trust network access (ZTNA), by comparison, supports companies with segmented user access and seamless scalability to secure resources whether they're on-prem or in the cloud.

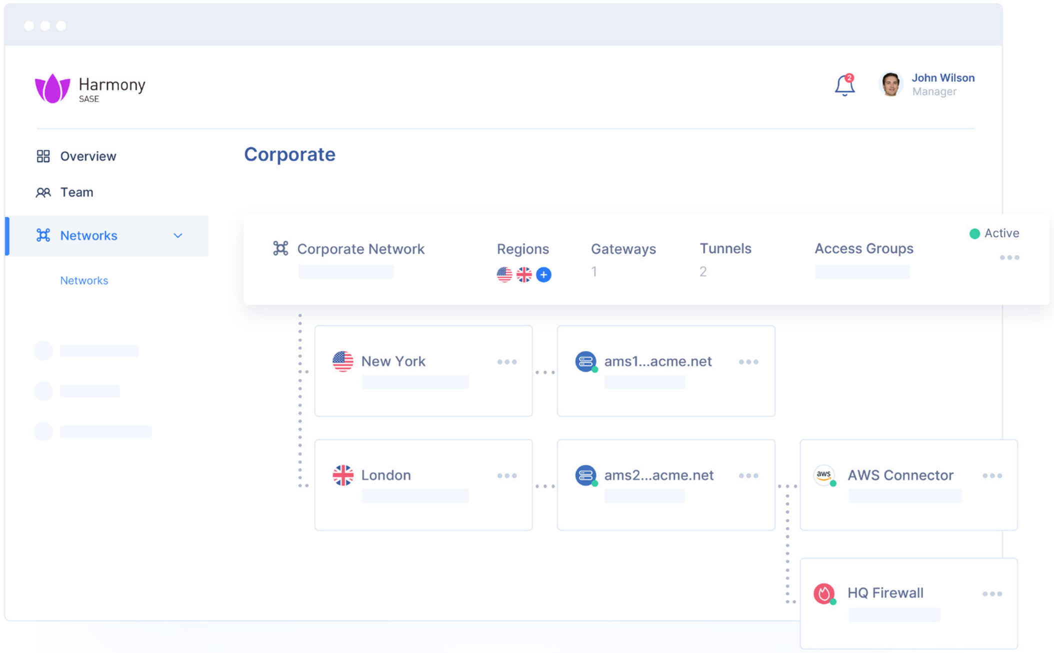
Enterprise-Grade Network Security for All Businesses

The traditional perimeter-focused approach grants implicit trust to any user that enters the network via an approved VPN tunnel. This means that compromised VPN credentials can lead to malicious "authenticated" access by attackers who can move laterally through the network.

Zero trust network access (ZTNA) grants access to corporate resources based on the principles of zero trust, which is an evolution of the principle of least privilege: only specific employees may access specific company applications. In addition, continuous verification using context-based rules ensures that only approved users who meet certain security conditions can access resources.

Strict access control enables ZTNA solutions to narrow an organization's attack surface and helps reduce data breaches and data loss, system and application vulnerabilities, advanced persistent threats (APTs), denial of service attacks, account hijacking, and the impact of malicious insiders.

Ideal ZTNA solutions are delivered from a flexible cloud-based platform that converges the secure connection of a VPN with easily implemented granular access rules for better overall security. Moreover, this all happens inside a single management platform that provides a 360-degree view of network activity.



The ZTNA Adoption Pipeline

ZTNA isn't a switch you flip. Instead, it's a strategy that employs a set of technologies to identify, authenticate, and verify each company user in order to access company applications and resources.

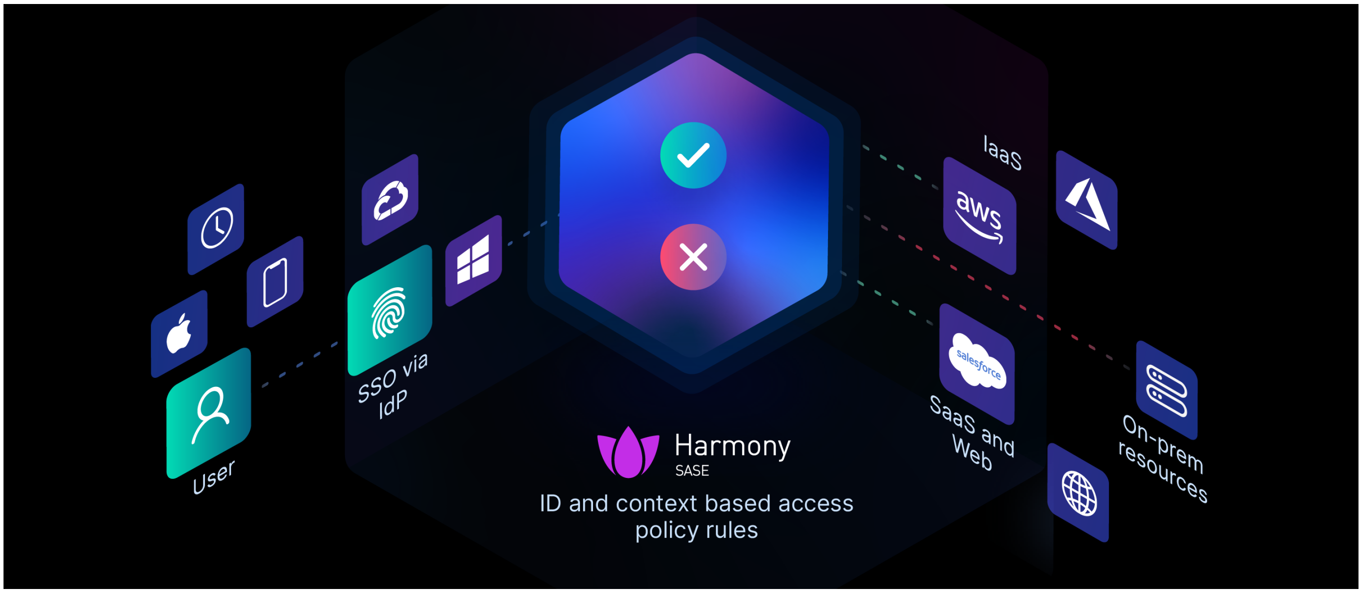
- ZTNA starts by identifying users through integration with a company's Identity Provider that ideally supports Single Sign-on (SSO) and Multi-Factor Authentication (MFA).
- Access is either blocked or permitted based on the user identity, context, device security posture, and access rules required for each resource.
- Thus, a malicious actor with stolen credentials (assuming they could also defeat the SSO and MFA steps) will have their access limited to specific areas and will not be able to fully traverse the network. This significantly reduces the level of exposure and potential damage to the company network.

To limit the attack surface and decrease the chances of online threats, ZTNA adoption in place of on-prem solutions has rapidly become the norm.

Comparing ZTNA vs On-Prem VPN

	Zero Trust Network Access	On-Premises VPN
Device Security Posture Enforcement	Devices are checked for security posture before gaining access and at regular intervals.	Devices do not undergo a posture check.
Cost Reduction	Cloud-based ZTNA reduces configuration complexity and onboarding time. Plus, it eliminates the need for hardware maintenance and upgrades.	Hardware requires manual installation, configuration, physical storage space, cooling, ongoing maintenance, and trained personnel to install and maintain. VPN upgrades via concentrators can be very costly and complex to manage.
Unified Management	Networks and users are easily managed from a single dashboard.	Each on-prem appliance is individually managed often with complex interfaces and spread across multiple offices.
Improved Network Performance	Direct to cloud access enables faster connections, and better network performance.	Traffic backhauling to the corporate physical location means the user experiences high latency, and a less efficient workflow.

	Zero Trust Network Access	On-Premises VPN
Simpler and More Secure User Authentication	Centralized management of user access with identification and multi-factor authentication. Wide support of IdPs, for easy single sign-on (SSO).	User identities managed across multiple firewalls. Only some IDPs are supported.
Support for Unmanaged and Third-Party devices	Clientless access to apps for unmanaged devices, without exposing those users to the whole network.	Not supported.
Easy and Fast User Onboarding	Adding users and expanding networks can be done in minutes.	Scaling is often a complicated and manual process.
Full Network Visibility	Single interface for entire network visibility.	Network visibility is fragmented across different locations.
Traffic Encryption	All traffic is end-to-end encrypted.	Only from the client to the VPN appliance.
Secure Granular Access Control	Segmented user access across network resources.	Segmenting user access can be complicated, and performance may be hindered.
Converged Advanced Security Capabilities	Secure internet features such as web filtering and malware protection should be integrated alongside ZTNA to maximize network security.	Firewall capabilities extend to anti-malware and intrusion prevention systems.



Check Point Harmony SASE Private Access

The Check Point Harmony SASE platform includes a powerful cloud-based ZTNA solution called Private Access.

- Private Access ensures that users access cloud resources via encrypted tunnels directly from the Harmony SASE network, with granular access rules for network resources and application access.
- The Check Point Harmony SASE network is global with over 75 PoPs located across the world, ensuring minimal latency and a faster user experience to any user anywhere in the world.
- Check Point Harmony SASE Internet Access with robust web filtering and malware protection adds another layer of defense to ensure users are secure while interacting with the open internet.
- Private Access secures access to any network resource: on-prem data centers, public cloud (AWS, Azure, GCP), or private cloud, via IPsec or more advanced Wireguard tunnels.
- Private Access supports an array of ports and protocols, including non-web applications like VoIP.
- Check Point Harmony SASE's global backbone uses dual Tier-1 carrier networks and peering agreements with all the major cloud providers with reserved bandwidth for optimized delivery.
- Private Access includes agentless access and supports a wide range of protocols: SSH, RDP, VNC, Telnet.
- SD-WAN with Check Point ThreatCloud integration optimizes steering for more than 10,000 business applications and adds an extra layer of site security.

Check Point Harmony SASE is the right solution for a network environment of increasing complexity, which is the single greatest obstacle to effective network security.

Fast Deployment: Check Point Harmony SASE allows you to purchase, provision, and enable secure zero-trust access on-prem, in the cloud, and anywhere in between. Easy scalability and transparent pricing allow you to easily grow, backed by our 24/7 Customer Success engineers.

Unified Management: Effortlessly manage and onboard employees, deploy a multi-regional network in less than an hour, and install our cross-platform agent across all endpoints within a single dashboard.

Full Visibility: Effectively monitor network health, view employee resource access, integrate with leading SIEM providers, and identify any suspicious activity for a unified view of your network security.

Converged Security: Avoid the complexity of using multiple cybersecurity solutions in favor of a single platform that makes it easy to configure your network, implement security policies, detect attacks, and defend against data breaches. In addition, Check Point Harmony SASE is integrated with Check Point's Infinity Portal, a unified management security platform that encompasses the data center, network, and cloud, in addition to the branch office and remote users.

Meet Check Point 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 Harmony 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.

Combining innovative on-device and cloud-delivered network protections, Check Point Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties.
Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

Check Point Harmony 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 you covered 24/7.

Harmony
SASE

CHECK POINT™