

Smarter Connectivity for Remote Employees

A Teridion White Paper

JANUARY 2024

How We Work Has Permanently Changed



In the leadup to March 2020, only 6% of Americans and 5% of Europeans worked primarily from home. Covid-19 changed that within days, and even as late as May 2021, 70% of white-collar employees were still remote. Fast forward to December 2023. Though the shift back to the office has seen some dramatic twists and turns, it's safe to say that the percentage of global hybrid workers will never go back to the single-digit numbers we knew before the pandemic. Gartner has even forecasted that 39% of global knowledge workers will be hybrid by the end of this year.

However, internet connectivity for remote work remains a real challenge. Video conference calls and cloud apps require high-bandwidth connectivity and enterprise-grade SLAs to ensure uninterrupted communications. Quality of service (QoS), one of the keystones of office connectivity, isn't generally available for home connections.

What does all this mean for the future of global networks?

The patchwork solutions that enabled connectivity for remote and work-from-home employees must now be upgraded and adapted. Tools and solutions like VPN, ZTNA, SD-WAN, and SASE need to be reconsidered in the context of this new work paradigm, where network resilience, particularly along the mile, is more critical than ever.

Pros and Cons of Common Solutions

To this point, organizations have relied on one of three solutions. Each solution has its own benefits and drawbacks for employees and organizations.

Home or public internet connection

Many businesses are relying on their employee's home internet to access the internet. They hope that home and public internet connectivity will be enough.

While this approach does enable employee connectivity to business-critical information, it presents a number of drawbacks for the organization. For starters, home and public internet connections don't offer a corporate-level SLA. Line stability and connection speeds can change throughout the day, and companies have zero visibility into their network. When things go wrong, a company's IT specialist can't support their employees or get them reconnected. Furthermore, these connections are not secured, and employees can unwittingly expose critical data on the public web.

Virtual Private Networks (VPN)

VPN services are frequently used by organizations to securely connect their employees to corporate resources and systems. A Netmotion survey of 750 IT leaders from around the world found that 54% of their organizations were relying on VPNs in 2020. While VPNs are a common tool that has provided secure connectivity to remote works for years, it doesn't solve the quality of service (QoS) issues since it keeps employees reliant on consumer-grade - rather than corporate-grade - SLA connectivity. The level of service is 'best effort' which simply isn't good enough., VPNs can actually slow down connectivity as multiple users try to access the same resources, leading to latency issues and interfering with productivity.

Furthermore, VPNs aren't well suited for dynamic workforces, as they require constant management, hardware installations, and don't adjust easily to changes in networks. They make it increasingly difficult for IT teams to effectively manage hybrid and cloud-based computing architectures.

VPNs often introduce a single point of failure. In such cases, if the VPN server is down, all users are impacted, leading to productivity drops across the company.

VPN-as-a-Service(VPNaaS)

Similar to VPN, VPNaaS allows users to access a private network securely from anywhere in the world, promoting remote work and enhancing accessibility. VPNaaS services are also often scalable, accommodating the changing needs of businesses. They can easily adapt to an organization's growth or fluctuations in demand. For many

businesses, outsourcing VPN services can be more cost-effective than establishing and maintaining an in-house VPN infrastructure.

However, depending on the service and infrastructure, VPNs may experience latency issues, affecting the performance of real-time applications. For certain industries and regulatory requirements, using a third-party VPN service may also introduce compliance challenges that need to be carefully addressed. Moreover, external factors such as server outages or maintenance on the provider's side may lead to service disruptions, impacting the availability of the VPN.

Solutions with corporate-grade SLAs are the only ones that are ideally positioned to serve the needs of organizations with remote and hybrid employees.

Zero Trust Network Access (ZTNA)

ZTNA is another frequently used security tool for remote connections. In terms of security, ZTNA is excellent, providing users with access to services for which they have been authorized.

However, like VPN and VPNaaS, ZTNA doesn't address quality of service issues. Users continue to struggle with connectivity issues, including latency and slow file transfers, leading to a poor-quality experience.

The Missing Component

Poor connectivity hampers remote work. It disrupts video conferences, delays work and frustrates employees who are trying to connect to cloud-based or remote servers and applications. The ultimate remote access experience begins with high-speed broadband solutions that is stable, with low latency and backed by SLA for the end user.

SD-WAN network architecture solves many of the network challenges and quality-of-service issues enterprises are facing. It improves connectivity, agility and network flexibility as it provides employees with an online working environment that is similar to the office experience.

However, SD-WAN doesn't quite go far enough to support remote users. It lacks a guaranteed SLA, and doesn't necessarily resolve issues in highly-regulated countries, like China or Russia.

As companies continue to rely on SaaS applications and utilize high-bandwidth video conferencing, they need guaranteed, high-speed connectivity. Only solutions with corporate-grade SLAs are ideally positioned to best serve the needs of organizations with remote and hybrid employees.

Teridion's AnyPlace Solution

Teridion AnyPlace is a secure, remote connectivity service that was designed from the ground up for today's remote workforce. Based on Teridion's renowned overlay network that sits on 25 different cloud providers with over 500 points of presence (PoPs), AnyPlace uses AI to monitor the network and determine the fastest route.

AnyPlace is a reliably fast, global WAN-as-a-Service that improves enterprise connectivity and guarantees consistently good internet performance. AnyPlace is ideal for inter-site activity, remote users, and site-to-SaaS connectivity.

Users can connect to AnyPlace through any edge device. It is a clintless deployment that prevents compatibility or managment issues, and simplifies the user experince for both IT administrators and end users.

Designed to meet remote work's biggest challenges

Teridion AnyPlace provides enterprises and end users with the SLAs they need to remain productive.

Superior internet connectivity

Teridion AnyPlace offers a service-provider-grade SLA, guaranteeing high-speed connectivity for all employees, regardless of their location. The service includes 24/7 support, as well as monitoring and reporting tools so your IT team has full visibility into the service.

Accelerated application access

AnyPlace provides the SLA-driven connectivity that accelerates connectivity to your corporate sites, clouds, and SAAS application whether you use your home or public internet connection with or without tools like ZTNA, VPN, or VPNaaS.

Fast, stable, and reliable

Teridion AnyPlace constantly monitors the internet, looking for the best route to deliver data. It quickly adapts to changes on the internet, delivering a seamless experience for the user.

Meets regulations and industry standards

AnyPlace optimizes connectivity in highly regulated countries, including China and Russia. It is fully compliant with regulations in those places and uses its unique architecture and 500 PoPs to continually deliver high-speed connectivity to its users.

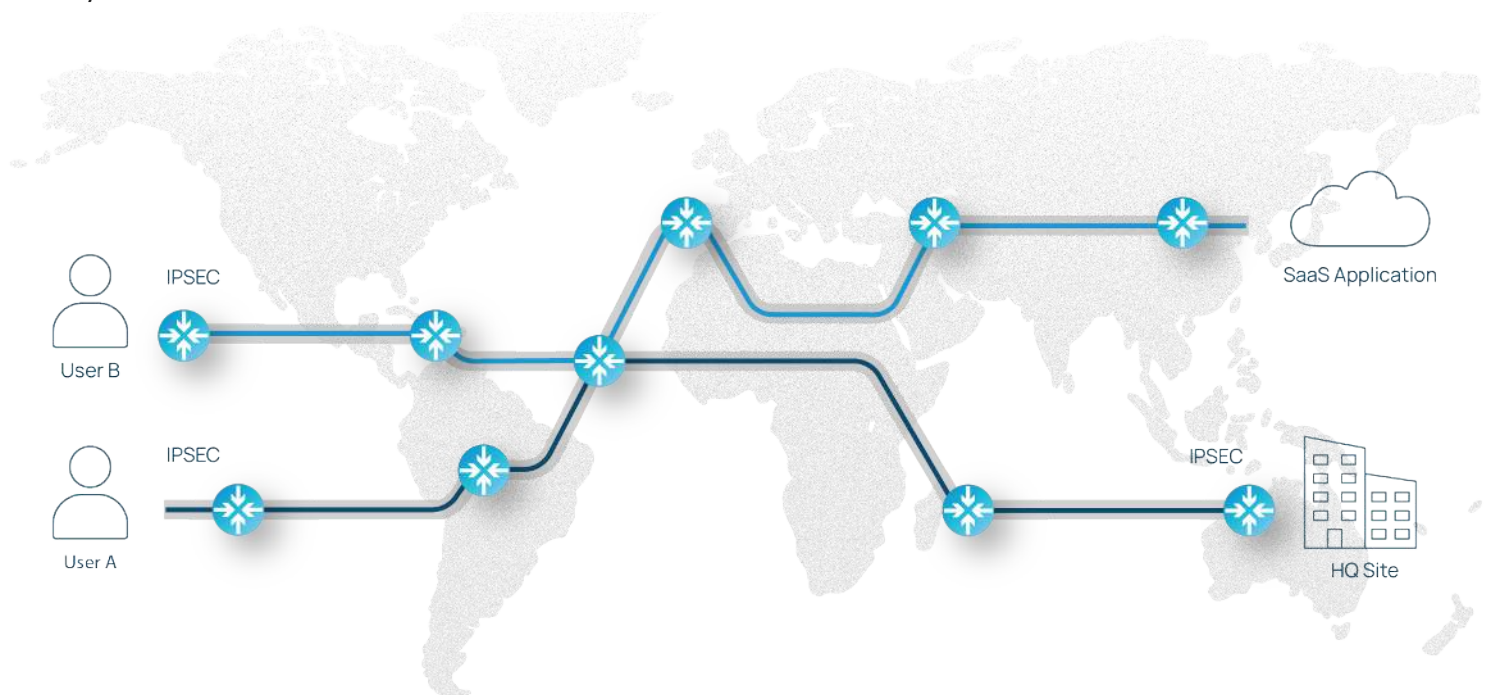
AnyPlace meets all the major regulatory standards, including SOC2 Type 2 compliance, NOC 24/7/365 inspection, OWASP Top-10 2021 Defense Updates, and NGFW implementations, and is GDPR compliant.

Hassle free for end-users and IT teams

Designed with end-user simplicity in mind, Anyplace provides the simple, secure remote experience your team requires. The clientless deployment eliminates the need to add additional hardware or software onto employee devices, as well as any related compatibility, maintenance, or dependencies issues.

AnyPlace can be managed from a central, cloud-based portal, allowing IT admins to securely manage certificates for client authentication from anywhere while meeting the industry's highest security standards.

AnyPlace solution



About Teridion

Teridion sets a new standard for WAN connectivity through AI-powered route detection. Our Network as a Service uses a flexible, plug-and-play platform to deliver fast, reliable internet performance to any location and edge device. It's now easier than ever for enterprises to support digital transformation with global teams working together as though in the same room.

-
1. https://www.nccci.com/SecureDocuments/QEB/QEB_Q4_2020_RemoteWork.html
 2. <https://www.weforum.org/agenda/2021/05/europeans-work-from-home-remote-covid-coronavirus-pandemic-europe-eu/>
 3. <https://news.gallup.com/poll/348743/seven-u.s.-white-collar-workers-still-working-remotely.aspx>
 4. <https://www.gartner.com/en/newsroom/press-releases/2023-03-01-gartner-forecasts-39-percent-of-global-knowledge-workers-will-work-hybrid-by-the-end-of-2023>
-

Get Started

Ready to connect enterprise sites at the highest performance?
Contact us for any further questions.

Teridion Ltd: 34 Jerusalem st, Raanana, 4350110, Israel
www.teridion.com | +1 (415) 940-7040 