perimeter 81

# The Rise of Remote Workers: A Checklist for Securing Your Network

# Introduction

Providing secure, fast remote access is a central concern for organizations in today's modern business environment. The world has changed in several ways, and employees now choose to - or in some cases - are required to work from outside the office. While it may have a positive effect on employee productivity and morale, this reality has complicated the idea of network security significantly, and it lies at the intersection between more powerful technologies such as smartphones, and the increasing sprawl of sensitive resources which now reside both locally and in the cloud.

According to a recent IDC report[1] on worker productivity, "A far greater percentage of employees work remotely or from a home office today, and workgroups often span the globe. Web and video conferencing and tools such as instant messaging and instant meetings let people collaborate in real time across distance, time zones, and organizational boundaries, and mobile devices help them be productive on the go." These devices are connected to numerous vital cloud-hosted applications, which now comprise a majority of organizations' networks.

Such agility allows businesses to quickly build the infrastructure they need to succeed, and it's become so advantageous that over 84%[2] of organizations now host at least one crucial function in the cloud. Of these, 58% utilize a hybrid-cloud model, which makes use of multiple cloud environments alongside local resources. This has contributed heavily to our modern digital-forward era, where employees are able to work as efficiently as if they were at their desks, but from wherever they're most comfortable.

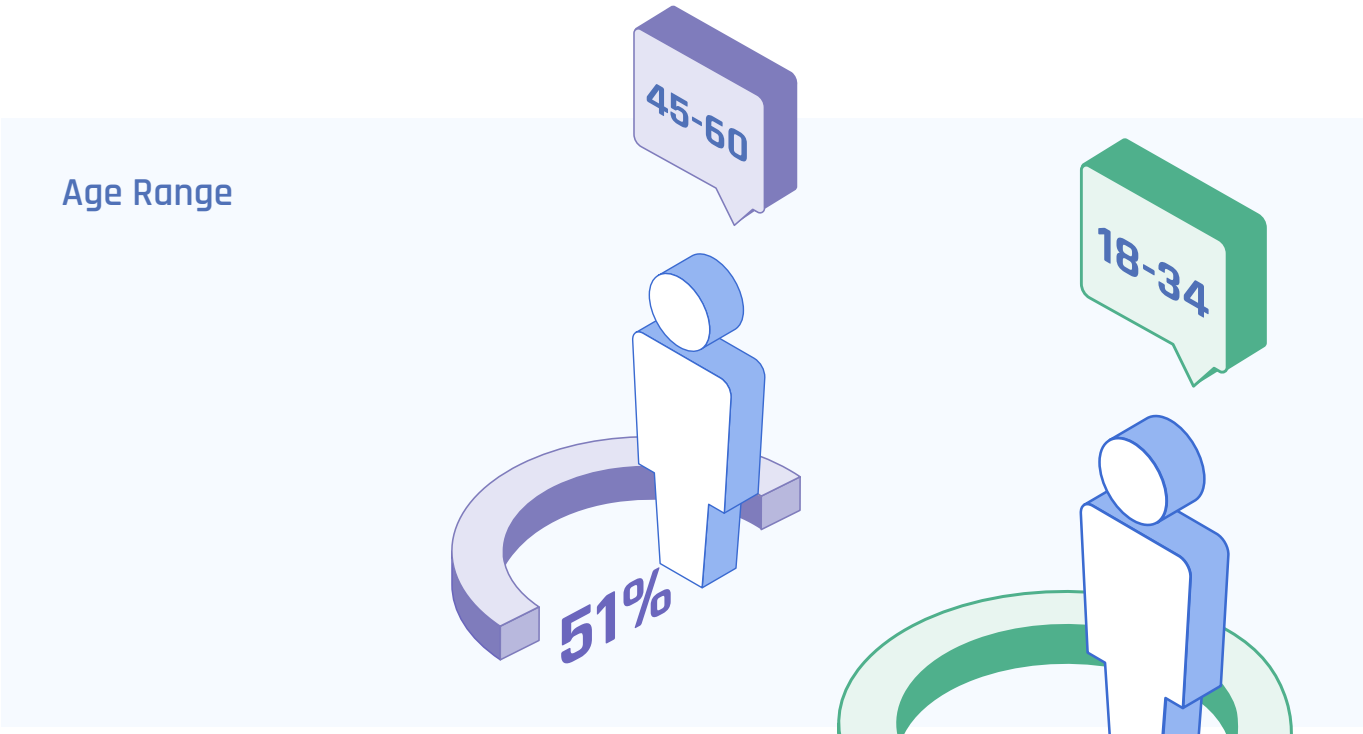
**In places like the UK and USA, the prevalence of flexible work policies runs parallel with employee preferences.[3]**

**As you can see above, the trend towards remote access is becoming the status quo, but when the need for remote access is more rapid, networks may experience strain and expose themselves to data breaches if not properly secured. For organizations currently grappling with this notion, the following checklist allows them to prepare, and provide speedy, safe access to any number of remote employees no matter where they're working from.**

1 https://warekennis.nl/wp-content/uploads/2013/11/bridging-the-information-worker-productivity-gap.pdf
2 https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/
3 http://assets.regus.com/pdfs/iwg-workplace-survey/iwg-workplace-survey-2019.pdf

# Why Remote Work is Inevitable for Organizations

As younger workers replace older employees, their preferences for work come along as well. However, the introduction of remote or flexible work policies is proven to suit all age groups, with over 68% of employees indicating that the trend benefits their work-life balance. It then makes sense that while over 70% of 18 to 34-year-olds take advantage of the freedom to work anywhere, more than half of workers up to age 60 do as well.




Those taking advantage of flexible work policies are the statistical majority in all age groups.[4]

4 https://www.polycom.com/content/dam/polycom/common/documents/whitepapers/changing-needs-of-the-workplace-whitepaper-enus.pdf

# Checklist: Preparing for an Inundation of Remote Workers

With 70% of potential hires considering remote work a key factor in whether or not to take a new position, IT teams need to be ready for an influx of remote workers requesting access to a wider array of resources, via a plethora of devices, and over potentially unsafe Wi-Fi connections. Accordingly, several things must be considered before being able to say that their network is secure:

## Transition from Perimeter-Centric to User-Centric

It's challenging to apply the perimeter-centric security approach to a network that is constantly changing shape. Organizations that grant full network access to anyone with credentials risk their data by default, as a permissive access model neglects gaps in security that occur when numerous connections are remote. **Zero Trust** is the solution because it reduces the attack surface with authentication occurring first based on user ID, their device, and other contextual attributes.

## Transition from Perimeter-Centric to User-Centric

Virtual Private Networks (VPNs) are an essential part of safe networking, as they require employees to first log into a mobile, web, or desktop application that then creates an encrypted tunnel between their device and the resources they need to do their jobs. Wireguard and IPsec tunneling make it easy for IT teams to track how people move through the network, and to stay aware of their activity. NaaS (Network as a Service) is the evolution of this idea and incorporates additional critical features such as more precise user segmentation, Secure Web Gateway, and others.

## A Cloud-Friendly Approach

Given the near universality of hybrid-cloud networks, security solutions must be cloud agnostic and able to seamlessly integrate into whichever SaaS or cloud-hosted resources the organization uses on a daily basis. Local resources are also included in this idea, so that no matter which applications, data and file storage sources, or systems the employee is using, they're all part of the same secure environment. This also eases the burden on IT, who must otherwise manually configure many systems to work together in tandem.

## Defense Against Unsecured Wi-Fi

One of the biggest gaps in security that occurs when remoteness becomes a central theme in network access is public Wi-Fi, or simply unsecured Wi-Fi. Many employees will work from home, cafes, or places where the internet connection is less secure than if they were at the office, so the **Wi-Fi security approach** taken by organizations must account for this glaring threat and act accordingly. Surveys show that over 60% of people believe their connections are safe when connected to public Wi-Fi, despite heavy evidence to the contrary.

## Geographically Diverse Data Solutions

Concentrating a virtual private network and security solution in one physical location will not suffice for larger organizations with many remote employees, who likely live far and wide of the office or their local branch. It's therefore vital to find a provider with multiple data centers across the world, as employees can then connect to the most proximate server for the resources they need, which reduces latency and increases productivity for the entire organization.

## 2+ Layers of Authentication

Requiring employees to authenticate themselves more than once is some of the lowest-hanging fruit for comprehensive network security, as it ties network access to the proper credentials but also the employee's personal mobile device. This is a very easy safety net to install, and at the very least, the network security model employed should include Google Authenticator via application or SMS.

## Bring Your Own Device (BYOD) Accountability

Most modern devices are capable of connecting to a remote network and being used for work, and with employees using a wide selection of smartphones, tablets, and laptops, it doesn't pay to be narrow-minded when it comes to security. In fact, it literally pays to be pro-BYOD, with employees generating an additional $350 per capita[6] in value when allowed to use their own devices for work. The best network security solutions are dynamic and consider users and their chosen devices on an individual basis, covering all endpoints with the same efficiency and agility.

5 https://www.nortonlifelock.com/content/dam/nortonlifelock/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf

6 https://techjury.net/stats-about/byod/#gref

## Effortless Onboarding for IT

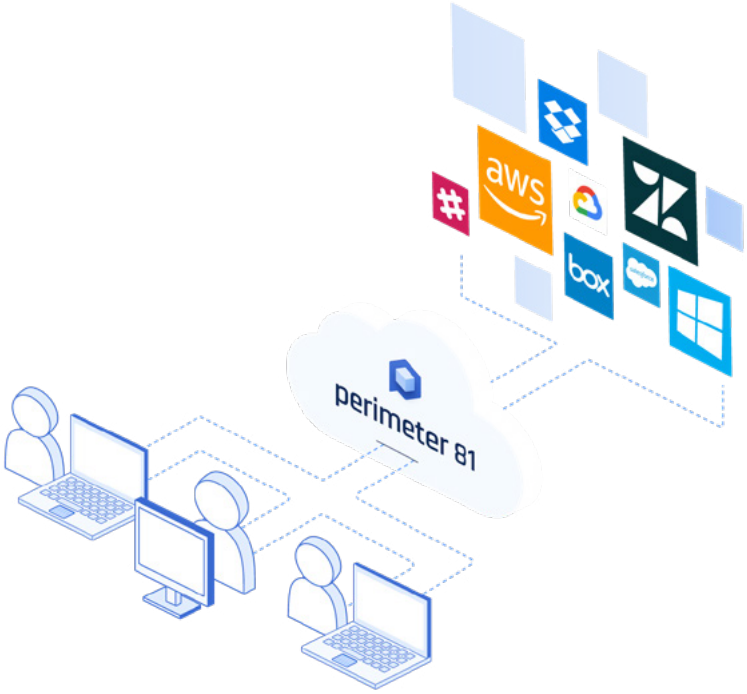
Proper network security models allow IT teams to seamlessly onboard new users into the system, assign them a profile or segment which grants access consistent with their role, and specific rules as to how their device connects. If the IT team is given this capability then they'll be more likely to respond efficiently when the need for remote access spikes across the organization.

## Seamless Logins

Almost like a digital ID card, user-friendly features like Single Sign-On (SSO) are key to a user-centric security model and help reduce organizational liability for storing credentials. It's especially powerful when combined with user segmentation features, and should be prioritized for companies that put a premium on productivity, reducing help desk costs, and streamlining the login process.

## Agentless Remote Desktop

For in-browser access to data in the cloud, Remote Desktop Protocol (RDP) is a much appreciated addition to any network security apparatus, and tends to benefit particularly distributed workforces. The simplicity and agentless nature of RDP makes it one of the strongest and most lightweight building blocks of a secure network, but also one that maintains its accessibility to remote employees.



# A Quick Win with Perimeter 81 Secure Remote Access

Unlike traditional hardware-based network security providers, Perimeter 81 provides greater network visibility, seamless onboarding, and automatic integration with all the major cloud providers, giving companies of all industries and sizes the power to be securely mobile and cloud-confident. When remote access is a dire need, the Perimeter 81 Zero Trust Secure Network as a Service is the unified solution enabling organizations to serve employees efficiently.

### Zero Trust Access

Network and application access through Perimeter 81 is completely Zero Trust, with continual monitoring for superior transparency.

### Remote Access VPN

Perimeter 81 deploys a Software Defined Perimeter around your organization's network, and IPsec tunneling for encrypted remote access.

### Cloud Agnostic

Integrate Perimeter 81 with any and all cloud-hosted SaaS applications or resources, as well as your local environment.

### Automatic Wi-Fi Security

Our automatic Wi-Fi security feature instantly routes remote employees through a secure server if their connection is unsecured.

### Remote Desktop

Grant employees easy connectivity to virtual PCs via Remote Desktop Protocol (RDP), for easy access to resources crucial for their role.

### 30+ Data Centers

Low latency for remote workers is expected with Perimeter 81, as we operate many global data centers closer to those requesting access.

### Multi-Factor Authentication

Ensure authorized and secure remote access with support for multiple forms of 2-factor authentication, including via Google.

### Endpoint-to-Endpoint

Extend your comprehensive security policy across all devices connecting to the network, whether laptops, tablets, or smartphones.

### Instant Onboarding

Immediate protection for the entire organization, with or without an agent. IT teams can quickly add new users and rules according to policy.

### Single Sign-On

Reduce password fatigue and simplify username and password management with built-in SSO utility.

# About Perimeter 81

Perimeter 81 has taken the outdated, complex and hardware-based traditional network security technologies, and transformed them into a user-friendly and easy-to-use software solution — simplifying network security for the modern and distributed workforce. Based in Tel Aviv, the heart of the startup nation and a global hub for innovative technology development, and with offices in New York and employees around the globe, our team of security as a service experts comes together every day to deliver a truly innovative, world-class network security service. Our clients include Fortune 500 businesses and industry leaders across a wide range of sectors, and our partners are among the world's foremost integrators, managed service providers and channel resellers.

**To learn more about achieving seamless and efficient remote access for your employees with a Zero Trust Secure Network as a Service platform, visit Perimeter 81 or schedule a demo.**

## Contact Us

www.perimeter81.com

1-917-994-8659

Request a Free Demo




Blog

perimeter 81