perimeter 81

CYBERSEC SOLUTIONS

# The WFH Cybersecurity Checklist

perimeter 81

## The Modern Workforce is Predominantly Remote

Providing secure, fast remote access is a top priority as the modern workforce has become predominantly remote. Working from home (WFH) or outside the office was once a choice or a stopgap measure, but today, it's critical for business agility.

**And it is not just about people.**

Devices, technologies, and other network resources are also "remote," with an unstoppable increase in the use of mobile devices and sensitive resources located in the cloud. According to Perimeter 81's recent State of Cybersecurity Report on the decentralized workplace, 87% of companies plan to have employees working remotely in 2022 and beyond, with the overwhelming majority of remote employees working from home two or more days per week.

**Working from home is critical for business agility.**

## The Decentralized Workspace is Here to Stay

During the Covid-19 pandemic, a May 2020 McKinsey survey found that 41% of employees reported they were more productive remotely than in the office. In its analysis of 2,000 tasks and 800 jobs in nine countries, McKinsey concluded that more than 20% of the workforce could work remotely 3-5 days a week as effectively as from an office.

Almost a year later, a May 2021 survey found that 39% of US adults would rather quit their jobs than go back to the office full-time, including 49% of Millenials and Gen-Zs—who comprise more than half the workforce. Although working from home saves only an average of $5,000 in annual expenses, 64% prefer working from home or hybrid work over a $30,000 annual raise.

To say that this has completely redefined the organizational network is an understatement.

Powerful web and video conferencing tools such as Zoom and Microsoft Teams, and instant messaging apps like Slack have enabled remote and hybrid employees to collaborate in real-time across geographic distances, time zones, and organizational boundaries. In addition, a plethora of mobile devices with 24x7 online access keeps them productive wherever and whenever they go.

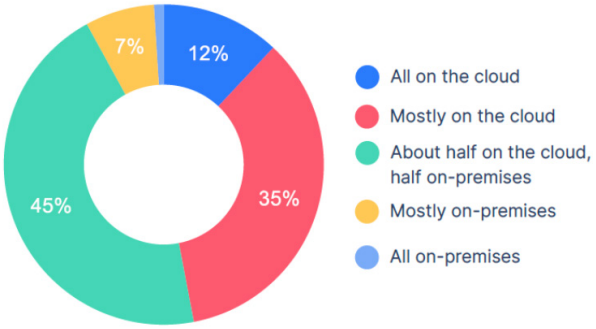
**39% of US adults would rather quit their jobs than go back to the office full-time.**

perimeter 81

Businesses are taking advantage of the unprecedented agility offered by cloud-based environments. Perimeter 81's report reveals that 12% of companies have only cloud resources while 70% are mostly on the cloud or half and half. The good news is that these trends have fueled the modern digital-forward era in which employees can work as efficiently outside the corporate office as in it.

**Perimeter 81's report reveals that 12% of companies have only cloud resources while 70% are mostly on the cloud or half and half.**

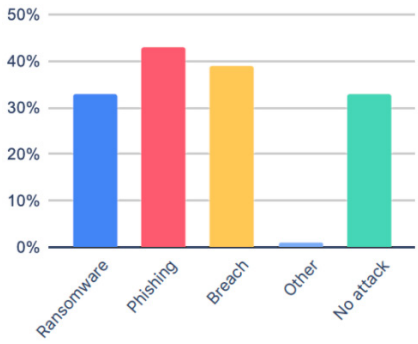
**Where are your computing resources located?**




Unfortunately, there is bad news as well. The accelerated transition to remote and hybrid work has enabled cybercriminals to exploit numerous cybersecurity gaps, with 66% of companies reporting that they experienced a serious cyber incident in 2020-2021.

**66% of companies reporting that they experienced a serious cyber incident in 2020-2021.**

**Has your company experienced any of the following serious cyber incidents in 2020-2021?**




But gaps in security brought on by shifts in the workforce are not insurmountable. The following checklist can help you rapidly deploy secure remote access for your entire workforce—no matter where they are working or which device they are using.

perimeter 81

# The WFH Cybersecurity Checklist

Working from home is a critical factor in accepting a job offer for 70% of job seekers. IT teams can use this checklist to rapidly deliver secure remote access.

## 1. Migrate to the cloud

Migrating to the cloud is usually a no-brainer.  On-prem servers are costly to maintain, operate and keep updated. And they're more frequently targeted in supply chain attacks. Just think of Microsoft Exchange or Kesaya ransomware attack. But migration is a process, and some apps or resources simply can't be moved to the cloud. Use Perimeter 81's Single Sign-On to easily access your cloud-hosted and on-prem applications—with maximum security today.

## 2. Deploy Zero Trust Network Access (ZTNA)

Organizations that grant full network access to anyone with credentials risk their data by default. Permissive access models neglect security gaps when many connections are remote. Zero Trust overcomes this challenge by first reducing the attack surface with authentication based on user ID, device, and other contextual attributes. Network and application access through Perimeter 81 is completely Zero Trust with uninterrupted, continuous monitoring for superior transparency.

## 3. Ditch your old-fashioned VPN

Using old VPN technology to secure and provide remote network access is simply asking for trouble. Just check out what happened to Colonial Pipeline. A frequent problem with VPNs is their inability to segment the network. This means that once bad guys hack a VPN, they get free access across the entire network. Perimeter 81's Firewall as a Service (FWaaS) answers this by incorporating critical features like precise user segmentation, device posture check, and more.

perimeter 81

## 4. Block access to and from dangerous websites

With employees working from anywhere on any device, web filtering and user-centric rules that allow, warn, or block access to and from dangerous websites are essential. Perimeter 81 Secure Web Gateway adds web security to daily browsing and protects users and the network from malware, ransomware, phishing attacks, and viruses.

## 5. Secure the edge with low-latency connectivity

Your users are no longer located at the office, and forcing them to access the cloud through your old location often results in high latency that frustrates users and lowers productivity. Perimeter 81's 40+ data centers on four continents deliver low-latency connectivity to your users wherever they work, whether they're in the office, at home, or even in another country on a "workcation.

## 6. Enforce multifactor authentication

Requiring employees to authenticate themselves in more than one way is a must-have in today's world of cyber risk. This very easy to install safety net ties network access to the proper credentials and employees' personal mobile devices. Perimeter 81 multifactor authentication (MFA) support includes policy-based access integrated with LDAP, Google Suite, Azure, OKTA, and more, ensuring authorized and secure remote access that is easy to deploy and convenient to use.

perimeter 81

## 7. Provide secure agentless connectivity for authorized contractors and partners

You need to prevent network security gaps from sources external to your business but can't possibly run a profitable business in a hermetically sealed bubble! Contractors, vendors, and partners are a part of your operation. The simplicity of agentless access makes it one of the most robust and lightweight building blocks of a secure network. By enabling agentless access for employees and third-party workers, you can stay safe and stay profitable. Perimeter 81 has built-in agentless Zero Trust Application Access (ZTAA) to isolate third-party connections.

## 8. Check the security of every device

Device Posture Security ensures that only authenticated devices that comply with specific security policies can connect to the network. When devices are authenticated through installed files, certificates, or registry keys, the corporate network is protected from phishing attacks that

rely on stolen usernames and passwords. Perimeter 81's Device Posture Check (DPC) ensures devices cannot connect to your network unless they meet your policies for the presence of anti-virus software, Windows Registry keys, disk encryption, certificates, and specific files or processes.

## 9. Onboard new users quickly and easily

If you can't instantly onboard and deliver immediate protection for the entire organization, you are already behind schedule. To succeed in today's dynamic workplace, both your business and network must have unprecedented agility. Perimeter 81's Cybersecurity Experience Platform (CSX) makes it radically simple to immediately deliver secure networking to your remote and hybrid workforce, whether for five users or 50,000.

perimeter 81

### 10. Monitor, monitor, monitor

In a changing and evolving threat landscape, you need to have visibility into your network and detect anomalies or attacks before significant damage occurs.  Perimeter 81's Monitoring Dashboard gives you a minute-to-minute view of your network usage, including active sessions, licenses, gateways, and more. Its beautiful, simple graphs allow you to drill down for more precise information as needed.

## A Quick Win with Perimeter 81's Cybersecurity  Experience Platform

At Perimeter 81, we believe that the best way to prevent cyber attacks is to radically simplify your cybersecurity. Perimeter 81, the world's first Cybersecurity Experience (CSX) Platform,  allows organizations companies of all sizes to meet the immediate needs of their remote workforce while granting IT teams the robust tools they need to manage it all safely.

**The best way to prevent cyber attacks is to radically simplify your cybersecurity.**

Our holistic, cloud-based solution embraces the principles of Instant Deployment, Unified Management, Full Visibility, and Integrated Security. To allow users to secure zero-trust access on-prem, in the cloud, or anywhere in between—in just a few clicks.

Too simple to be true? Check it out. Contact us to book a demo.

perimeter 81

# About Perimeter 81

Perimeter 81 radically simplifies cybersecurity with the world's first Cybersecurity Experience (CSX) Platform. As a holistic, cloud-based solution, Perimeter 81 allows organizations of all industries and sizes to easily support the decentralized, hybrid workplace while avoiding the cyber complexity that hurts IT's ability to defend corporate cloud and on-prem networks. Backed by Tier 1 Investors such as Insight Partners, Toba Capital, and others, Perimeter 81 is headquartered in Tel Aviv, the heart of the startup nation, and has US offices in New York and Los Angeles. Our 2,100 customers range from SMBs to Fortune 500s across a wide range of industries, and our partners are among the world's leading integrators, managed service providers, and channel resellers.


**Contact Cybersec Solutions**

Tel: 01494 936696 | Email: info@cybersec.solutions | Web: www.cybersec.solutions