Work From Home
Remote Workforce Connectivity

White Paper
September 2020

BACKGROUND: THE "WORK-FROM-HOME" TRANSFORMATION

Almost overnight, COVID-19 forced hundreds of millions of employees worldwide, to work from home.

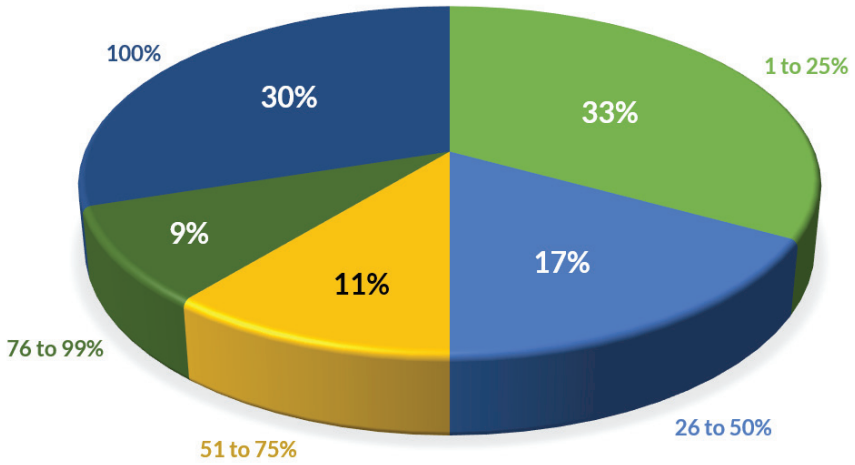
Organizations recovering from the initial shock of shutting down offices are transforming their workforce. New solutions are required to extend company policies to secure employee connectivity and endpoints.

IT departments overwhelmed by digital transformation. Previously, their primary function has been to strike the balance between security, ease of use, and productivity. Now, they find themselves supporting large numbers of remote employees, connecting via unmanageable home networks that are increasingly becoming the principal gateway to the organizations' tools and assets.

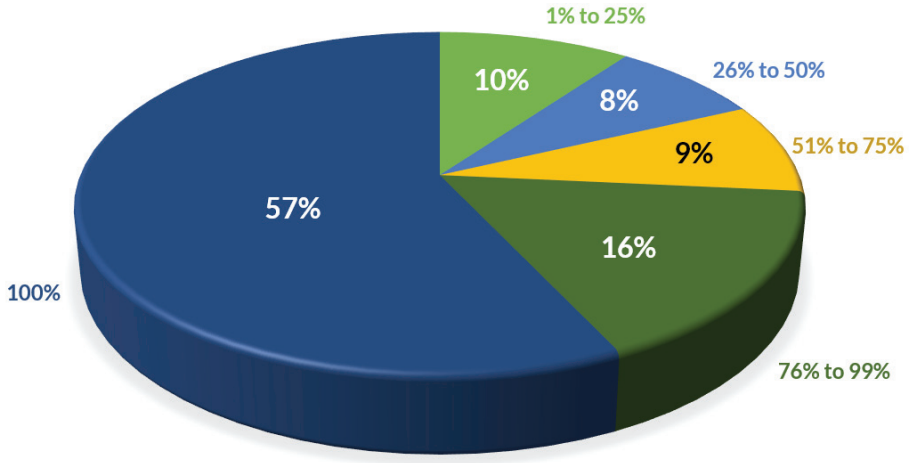
The scale and speed of the shift, the variety and inconsistencies of systems and topologies, and the fact that home networks are simply not designed for remote management, all point to unaddressed and unmanaged risks in both productivity and security.

WHAT PERCENTAGE OF YOUR COMPANY WORKS REMOTELY?

2019



2020



	2019	2020
1% - 25%	33%	10%
26% - 50%	17%	8%
51% - 75%	11%	9%
76% - 99%	9%	16%
100%	30%	57%

Source: State of Remote Report 2019 & 2020 - Buffer

WORK FROM HOME IS HERE TO STAY

Giants like Google, Apple & Facebook have already announced their plans to continue their work from home strategy.

Other companies are quickly following in their footsteps. Some have even made working from home compulsory.

Mark Zukerberg
CEO, Facebook

"We're going to be the most forward-leaning company on remote work at our scale… I think that it's possible that over the next five to ten years — maybe closer to ten than five, but somewhere in that range — I think we could get to about half of the company working remotely, permanently."

A recent study by Gartner supports the claim that WFH will be here long after the COVID-19 pandemic has gone.

"... a recent study of CFOs nationwide, 74% intend to shift some employees to remote work permanently, and that 41% of employees are likely to work remotely at least some of the time post Coronavirus pandemic."

Source:The Verge

WORK FROM HOME - THE RISKS & BENEFITS

COVID-19 forced corporations to send their workers home - a move that was challenging for both companies and employees. Fortunately it turned out that there was a huge benefit to this decision - cost saving.

There are many ways that remote working can offer businesses cost savings. Many established businesses have already enjoyed savings due to WFH. Sun Microsystems identified savings of $68 million a year in its real estate costs. Dow Chemical and Nortel have each saved over 30% on non-real estate costs.

According to Global Workplace Analytics, almost 6 out of 10 employers identify the following cost savings as a major benefit of WFH.

- Rent and utilities
- Cleaning services
- Food
- Taxes

Companies who manage to quickly adapt to the "new normal" while providing their employees with the proper tools to perform their work from home, will contribute to a more productive work environment while, at the same time, boosting employee morale.

Alongside the meaningful benefits, companies that don't manage to adapt to the new normal, by failing to plan for the future of WFH, will run into a variety of hurdles and pitfalls. These will occur both at the employee personal level and also as a result of security risks due to a remote workforce.

Prior to COVID-19 most companies needed only to support a small percentage of their workforce that was working from home. COVID-19 sent most of the workforce home and turned the situation on its head. Companies found themselves in an almost impossible position, unable to support the transition of most of their workforce to remote working.

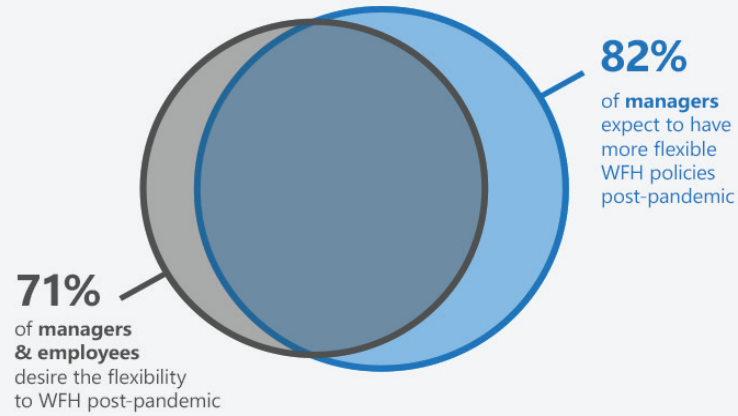
Issues arise in every direction: human resources, remote management & reporting, employee discipline, supporting a large number of remote workers, and facing new cyber security threats. Corporate managers understand that WFH is here to stay. Both managers and employees are showing a desire to keep the WFH policy *(shown below in a recent study by Microsoft)* and they must take immediate action to solve all the issues while planning for the inevitable future of a long-term remote workforce.

Microsoft 365

Managers and employees agree: working from home must be an option long-term

Source: Harris Poll survey commissioned by Microsoft on May 26-30, 2020, among 2,285 total adults ages 18+ who are currently working remotely across the US, UK, Germany, Italy, Mexico and China.

Work from home opportunities post-pandemic



Every business will need to evaluate the benefits and drawbacks as they apply to that specific operation before making decisions. It is worth considering however, that the COVID-19 pandemic has brought remote working to the forefront of employee's interest. It is therefore beneficial for businesses to start the process of determining whether it is feasible to continue to WFH policy after the current crisis has ended.

This paper focuses on the roadmap for remote workers' connectivity, specifically where most of the remote workforce are connecting to the internet via managed routers and internet lines.

NETWORK SECURITY BUSINESS PRACTICE - CISO

One of the CISO and his team's responsibilities is to control and oversee the full length of the corporate network's security - from end point through to backend and cloud. Secure management of the internet pipe is required to allow a safe, reliable and fast network, helping the company and its employees retain their edge in the market.

Today, as security threats increase, this is becoming more and more of a challenge. Fortunately, guarding the corporate environment is not a new concept and multiple companies are offering solutions. In recent years we have seen a shift from the traditional monolithic network architecture to a cloud architecture. Here too, there are multiple available solutions built to assist the CISO in accomplishing his goals.

Unfortunately, COVID-19 forced businesses to completely rethink their existing network topology in order to cope with the new normal.

The new and immediate challenge that all businesses with a remote workforce are now facing, is to provide a reliable service that meets their existing corporate standards while retaining robust security over their infrastructure.

Research from Neustar and many other groups has shown that most businesses are simply not prepared to meet this challenge due to the unmanagement endpoints (routers) that the remote workforce are using to connect to the internet.

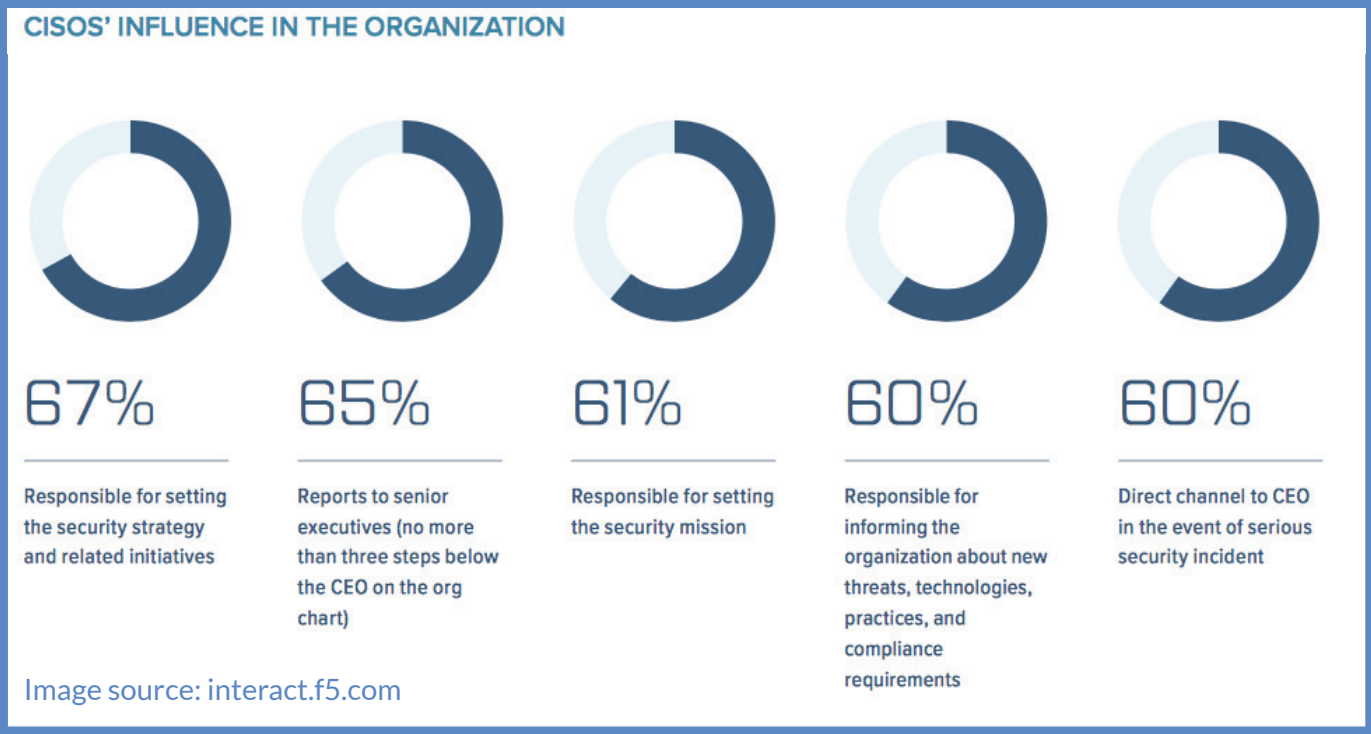


Image source: interact.f5.com

In a recent study, released by the Neustar International Security Council (NISC), a survey of cyber security professionals based across Europe and the United States, found that:

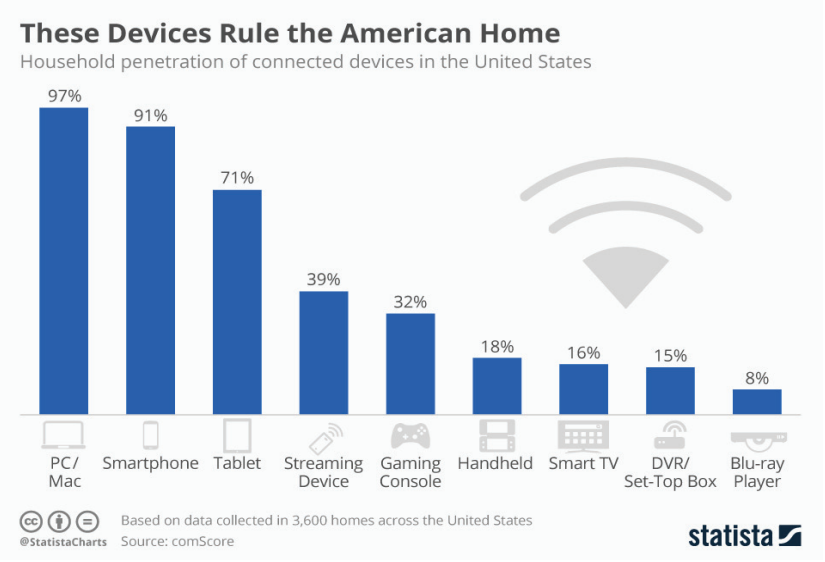
64% of companies have experienced disruption to network security business practices while working from home. While this disruption to network security felt by two thirds of businesses was said to be at least moderate, 23% of participants in the Neustar study declared major disruption.

NETWORK SECURITY BUSINESS PRACTICE - THE ENDPOINT

Whether organizations use traditional remote access tools like VPNs, or implement the latest cloud technologies and policies, the Achilles heel of remote connectivity are the endpoints - the employees' home networks and routers.

A recent study conducted by Germany's Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) called Home Router Security Report 2020. Tested 127 router models from ASUS, AVM, D-Link, Linksys, Netgear, TP-Link and Zyxel. Found: That there is not a single device without known critical vulnerabilities!!!

In addition, "Many routers are affected by hundreds of known vulnerabilities. Even if the routers got recent updates, many of these known vulnerabilities were not fixed. What makes matters even worse is that exploit mitigation techniques are used rarely," … "the issues don't stop with vulnerabilities that are hardly ever patched. Some routers have easily crackable or even well-known passwords that cannot be changed by the user," reads the study. More precisely, 50 routers came with hardcoded admin credentials, including 16 with well-known or easy-to-guess login details."



Employee endpoints are now beyond the control and management of IT departments. The spike in the numbers of remote workers is having a huge impact on both productivity and security. Productivity is hampered by traditional tools' bandwidth constraints, and security is impacted.

Corporates must not make the critical error of confusing home routers with business routers. There is a huge chasm between the two technologies. The same applies to the gap between Basic-level SLA (Service Level Agreement) that covers most standard home internet connections, and Corporate-level SLA.

IT departments

- can't address home workers' connectivity issues.
- can't manage the remote networks
- can't access home workers' routers
- can't apply corporate policies on home networks & routers

According to Franhofer Research, 90% of employees answer "No" or "Never" to each of the following questions:

When was the last time you changed their WiFi access password?
Have you ever changed your router's default username or password?
Have you ever updated the firmware on your router?
Have you ever upgraded your router to the newest version with the latest security patches?

Moreover, home networks are routinely accessed by employees' families and guests, oblivious to the potential harm to their home network and ultimately exposing organizations to various attack vectors.

NETWORK SECURITY BUSINESS PRACTICE - CLOUD NATIVE

To overcome the challenges of multiple unmanaged endpoints over unmanaged internet connections, a new kind of device and service is required. Employees will be able to use a private router irrespective of their location - home, park, coffeeshop or even on vacation. To solve this need, a solution is required that:

- ensures that only approved employee devices are allowed to connect via the personal router.
- is cellular based, allowing the user to access the internet from anywhere.
- is small enough to enable it to fit comfortably in the user's pocket.

However, being mobile, private and pocket-sized is not sufficient to be a complete corporate-level solution. The new device also needs to provide a full suite of management and control solutions. The IT team must be able to mirror the existing company policies - retaining control over connectivity and authentication, thus protecting the corporate infrastructure.

It is vital to find a solution that is cloud native.

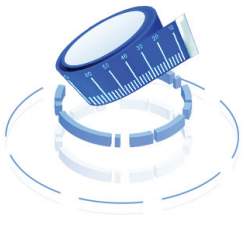
The infrastructure is transferred to the cloud with a core central management, pre-provision and FOTA capabilities. No installation nor technician is required, allowing the device to be shipped directly from the service provider to the employee without the device passing through the hands of any corporate personnel. The solution should offer business grade SLA with 24/7 customer support to facilitate every need.

CLOUD MANAGED

PRIVATE & SECURE

POCKET-SIZED & PERSONAL

CELLULAR ROUTER



TAILORED

STRATUSX

CONNECTIVITY ON YOUR TERMS™

StratusX - Solution for the Remote Worker

StratusX is a cloud native architecture, designed from the ground up to provide managed service for large deployment of cellular devices.

> Its award winning & worldwide patented Virtual SIM technology makes StratusX the best available solution for the remote workforce.

StratusX Cloud

StratusX cloud can be hosted on both Google and AWS using the latest technology based on flexible micro services that can cope with heavy load and load changes. Our solution was created, designed, programmed and implemented to be cloud native.

Under the hood StratusX holds powerful microservices each of them responsible of service delivery of different aspect in the system:

Authentication and authorization	Each element of the cloud as an independent user access control
User management	Manage the access rights of users and groups of users to the user
Device management	Manage the access rights of a device and/or groups of devices
Service plan management	Responsible for the specific service plan assigned to a user or group of users
SIM access management	Core connectivity capabilities, choosing the most appropriate SIM for the desired connectivity
Usage and reporting	Sophisticated billing system to provides billing information from personal user to group of users, including statistics and compute data for data analytics
Business administration	API for business integration Web based management portal
CARLOS - Automated QoS tests.	Cyclic Automatic Reporter & Logger of Statistics

StratusX Portable Router

StratusX is a Cloud Managed, Private, Pocket-Sized, Cellular Router, specifically designed for remote workers, offering its users a private connection. It incorporates cellular connectivity with cloud SIM functionality for guaranteed performance into one compact, remotely managed device.

The StratusX router is based on the Qualcomm chipset, running on Android OS making it very flexible when it comes to integration with 3rd party services and applications.

StratusX is the only solution that ensures high quality, risk-free, and managed connectivity for all your remote workers.

1. Portable and easily managed remote router
2. Highest SLA – 24/7 online support
3. Cellular LTE CAT4 internet speed
4. Remotely switch mobile operator to the best/cheapest available network
5. Limit access to only your remote workers and approved devices - perfect for companies operating a BYOD scheme
6. Company policies are mirrored to the device
7. Authentication first methodology - even in VPN environment
8. Portability and flexibility - connect from anywhere
9. Battery operated, supplying up to 10 hours of continuous charge

And that's just the beginning!

Post-pandemic, organizations will continue to offer their workforces the freedom and flexibility to choose how and where they work. Remote workers will outweigh the number of office-based workers for many organizations.

Today more than 45 million people are working from home - compared to less than 10 million prior to COVID-19. Research estimates that post COVID-19, at least 30% of the workforce will continue to work from home a few times per week.

Contact StratusX today to arrange a free trial and see what we can do for you.

CONTACT

info@StratusX.com

1220 Broadway, New York
NY 10001, USA

www.StratusX.com

STRATUSX
CONNECTIVITY ON YOUR TERMS