Secure Cloud Networking for the WFH Era

Responding to the COVID-19 crisis with an agile cloud infrastructure

Sponsored by: VERSA NETWORKS

Key Findings

- **Work From Home (WFM) initiatives in response to COVID-19 are causing organizations to rethink their remote networking strategies**. Virtualized networking technology is required to secure, scale, and support remote workers.
- **Challenges include higher remote security needs, reliable SAAS access, cloud-based Virtual Private Networking (VPN), and architectural agility.** Only cloud-based software architectures will meet the needs of a realigned workforce.
- **Platforms that integrate security, agility, and cloud elasticity are needed.** Legacy, hardware-based remote security technologies are cumbersome and not suitable for the current environment.
- **Virtual Private Network as a Service (VPNaaS) will emerge from the current crisis as a key necessity.** Legacy VPN technology lacks a scalable and agile architecture.
- **Software-defined wide-area networking (SD-WAN) as well as Secure Access Service Edge (SASE) technologies will be key contributors**. Virtual technologies with cloud-based and integrated security can solve several WFH problems at once.
- **Versa Networks is well positioned with its Versa Secure Access product.** Versa was already working on a lightweight, flexible remote security product architecture known as Versa Secure Access, which is well suited for WFH.

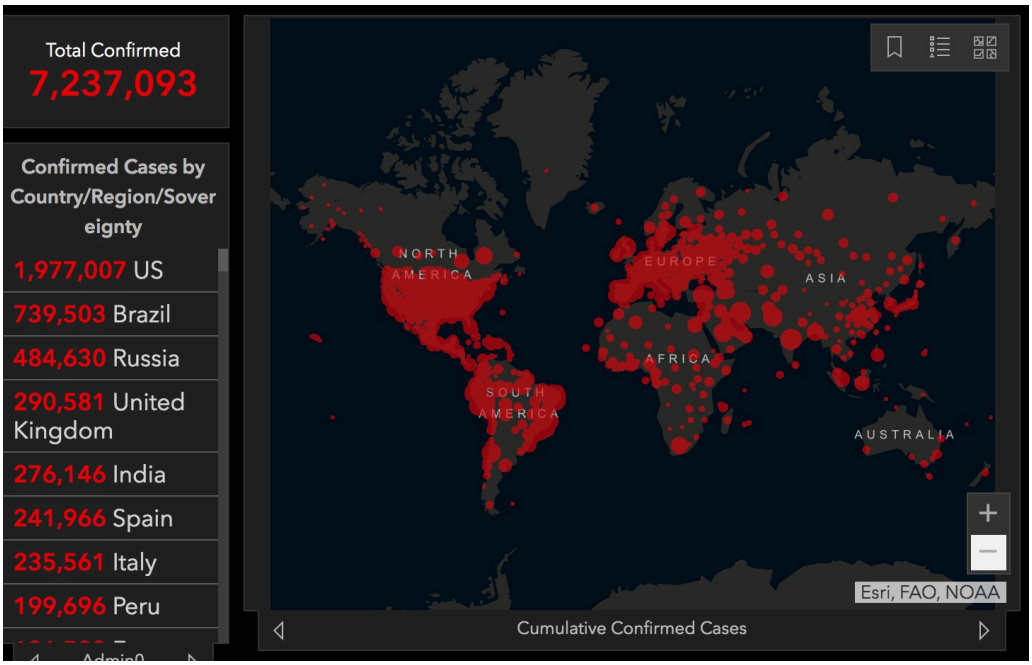
Introduction: How WFH Trends Will Accelerate Demand for Remote Security

The trend toward remote working or Work From Home (WFH) has been accelerated by the COVID-19 crisis and governmental stay-at-home orders. This trend is likely to continue long after the healthcare crisis is resolved, according current trends at leading companies.

These trends are likely to have several impacts on enterprise branch security technology, according to *Futuriom* research. The trends include the following:

- Higher demand for secure, cloud-based networking technology.
- Greater need for automated, scalable encryption and virtual private network (VPN) technology including VPN as-a-service (VPNaaS).
- Requirements to manage business-class networking at the home office, including providing visibility and policy-based networking to home networks.

Futuriom believes the evolving healthcare and economic crisis will accelerate demand for more flexible cloud security and networking solutions to solve the challenges of remote, secure networking at scale.



Source: Johns Hopkins University

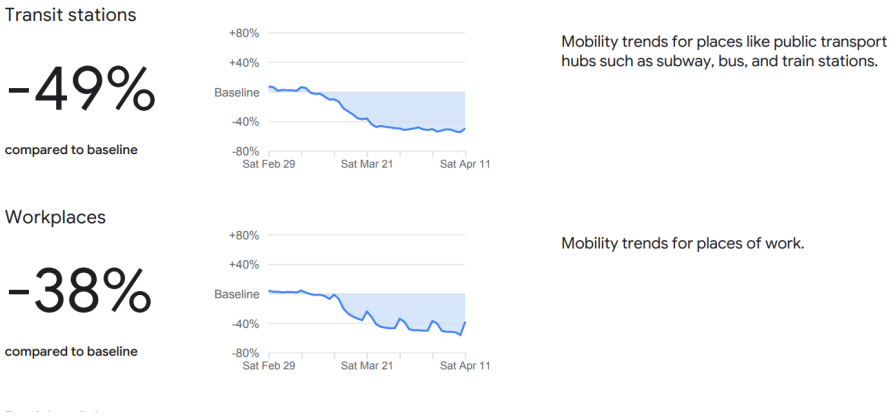
How COVID Triggered the Trend

The COVID-19 virus has hit the world economy and health systems with full force. Originating in China, the virus has spread throughout the world with an alarming speed that has left many world governments and businesses off guard. The financial implications have yet to be determined, but it has resulted in rapid, real-time re-alignment of organizations and workforces.

As of April 21, there were 2.5 million cases of COVID-19 worldwide, with 800,000 in the United States alone. More than 170,000 deaths have been reported as a result of the virus. Airlines have cut as much as 90% in travel capacity, governments worldwide have instituted stay-at-home or social distancing guidelines, and many major corporations have instituted WFH policies for a large percentage of the workforce.

Google has implemented a data tracking system known as COVID-19 Community Mobility Reports, which is using aggregated, anonymized data showing how busy certain types of places are — helping identify business tends.

As of April 21, the Google Mobility reports showed retail activity in the United States down 45%, transit station traffic down 49%, and workplace activity down 49%. In Germany, retail activity was down 57%, transit stations were down 48%, and workplaces were down 29%. In Japan, transit station activity was down 48% and workplaces declined by 22% as compared to the baseline. Globally, work and transit mobility is down 25-50%.



Source: Google Mobility Reports

Large firms worldwide put into place remote work policies, which required new systems to support remote workers. Large tech companies including Amazon, Microsoft, and Google advised workers to stop coming into the office in late February. In manufacturing, many operations have been suspended. For example, Boeing suspended production at its giant manufacturing plants for two weeks starting March 25 and increased its remote workforce. In Italy, one of the countries hit the earliest and hardest by COVID-19, Ferrari has shuttered production but has plans to get employees back to work with an aggressive testing program.

Global Workplace Analytics estimates that 45% to 50%, or 60 million to 70 million Americans, may resort to telecommuting during the coronavirus emergency. There are also benefits to this: Companies will save money from remote working, a fact that may be highlighted in the current crisis. A typical company saves about $11,000 per half-time telecommuter per year, according to Global Workplace Analytics.

It's clear from the data as well as our daily experiences that most people are staying at home and working from home. This is likely to continue for several months. But even when the workforce returns, the pattern may not revert to previous norms. Many experts say that more people than before may continue to work from home -- and that companies have realized that they need more comprehensive support policies, including technology, to help their workforces work from remote locations or at home.

Matt Mullenweg, chief executive of WordPress and Tumblr owner Automattic, told The Guardian that new work policies are likely to shift attitudes toward remote working by both employees and employers. He predicts the changes will result in a shift in culture.

"Millions of people will get the chance to experience days without long commutes, or the harsh inflexibility of not being able to stay close to home when a family member is sick... This might be a chance for a great reset in terms of how we work," he told The Guardian.

"I think a takeaway from this pandemic will be more people recognizing the value in remote work," Liz Ahmed, the executive vice president of people and communications at Unum, recently told CNBC. "It helps with business resiliency in unforeseen circumstances and also gives people more choice in when, where and how they work — and a lot of people value that."

New Requirements for the Secure Home

Prior to the COVID-19 crisis, remote working was already a growing trend. Gallup's State of the American Workplace 2017 study found that 43% of employees work remotely with some frequency.

Make no mistake about it -- COVID-19 has turned all attention to connecting to the cloud. This must be done in an efficient and secure way possible, while adhering to enterprise standards. The "cloud crush" is on. Amazon has been forced to hire thousands of people to meet customer demand. Traffic on consumer services such as Facebook and YouTube has soared. And Zoom has topped the charts in app downloads as teleconferencing systems have become indispensable tools.

The WFH trend and increased demand for cloud resources means home workers need secure and efficient access to software as-a-service (SAAS) or enterprise network resources. The crisis is likely to accelerate demand for cloud technologies, especially those that can enable more efficient and secure management of remote work environments.

Fortunately, a range of new virtualized remote access technologies play right into this trend. SD-WAN technology can be used to help enterprises adapt to remote work because it solves several problems at once: It can be used to automate the installation and management of

remote and branch work environments, improve the performance of broadband links and access to cloud applications, and increase the security of remote connections.

This evolution to Secure SD-WAN, also being referred to as the Secure Access Service Edge (SASE), combines the functionality of SD-WAN products as well as cloud security and VPN. The current healthcare crisis is accelerating demand. A key element needed for remote workers is providing default security such as VPN delivered as-a-service, so that it can be rolled out on demand.

Another challenge is segmenting traffic in the home office. When corporate applications and data are co-mingled on the home network, IT and network managers need control and

visibility into these networks. An enterprise with a large workforce being redeployed to home may need to re-allocate cloud instances that were going to enable branch offices to service the WFH end users. In a hardware-based model, this is difficult to manage and scale, as the location of the workers is changing in real-time. But a cloud-based architecture can simply spin up new instances of the remote security and Secure SD-WAN platform in the cloud, being deployed in locations that are needed.

Another common challenge is the limitations of legacy-based hardware implementations such as VPN concentrators, which are difficult to scale and re-deploy. By moving VPN and other security services to a software-based architecture, cloud-based resources can be re-allocated on the fly to support the mobile workforce.

These are just some of the most common challenges we are hearing about in the market. The chart below shows some of the challenges and potential solutions in the current environment.

WFH Challenge	New Era Trend	Required Solution
Remote security	Software-defined security architecture	Cloud-based Secure SD-WAN or SASE
Home and work network cohabitation	Network segmentation by application	Policy-based application networking in the home.
Real-time network management and VPN scalability requirements	Cloud elasticity	Secure SD-WAN and SASE implemented as cloud instances
Increased SAAS applications and bandwidth use	Policy-based network prioritization and SAAS connectivity.	Cloud-based Secure SD-WAN routing capabilities.

The paradigm has changed: The home is now part of the office. Moving forward, it's likely that IT and network managers will put more systems into place to support agile and scalable remote operations to support users shifting between home and the office, using their residence as a virtual branch.

"The home is now the branch, with a single user," says Kelly Ahuja, the CEO of Versa Networks, a leading Secure SD-WAN and SASE provider. Getting the solution right means IT managers must have visibility and control of user experience directly to the home, but with a legacy VPN they don't have that visibility."

Agile VPNaaS to the Rescue

Given the rising complexity and demands of managing a large number of remote workers, big changes are needed for VPN technology. The current crisis is highlighting this change in trend.

Legacy VPN technologies are hardware-based, making them inherently non-scalable. For example, let's say a number of enterprise users need to connect to a VPN hub, typically deployed using VPN concentrators. Imagine that suddenly, there is a surge in the number of users at the same time as a shift in geographic distribution. Instantly, the network requirements may change due to an exogenous event such as COVID-19. VPN concentrators based on hardware architectures are difficult to shift and scale based on the changing requirements of the organizations. In order to support the dynamic needs of organizations, VPNs need to move to a cloud-model and be available as-a-service.

VPNs should be fully integrated with the existing enterprise network. This can be done with a modern cloud architecture with integrated next-generation firewall, IPsec functionality, and integration authentication approach such as Active Directory (AD) and RADIUS.

Secure	Connectivity

• Certificate-based authentication ensures no actions performed until requester's identity is determined
• Perfect Forward Secrecy
• Assured secrecy and integrity of data by ensuring non-duplication of keys and session expiration
• Supports EAP
• Strong Cyphers, Large Key sizes (256bit or higher)
• Trusted for Government, NGO, and Civilian use
	• Standards based IKEv2 IPSec VPN
	• Constant, Always-On, Stable Connection
	• Auto-recovery after lost connection
	• Fast speed & Low Latency
	  ○ Effective request, response mechanism
	  ○ Much faster than PPTP or L2TP
	• Supported OS
	  ○ Windows, MacOS, iOS, Linux and more

The modern VPN also has a diverse number of needs, including authentication capabilities, supported OSes, and encryption capabilities. In the table below, Versa Networks shows how comprehensive VPNaaS capabilities can be integrated with a full-service cloud-based SD-

WAN platform, yielding Secure SD-WAN. There is functionality available in the Versa Secure Access product.

The modern VPNaaS can be built as a cloud instance available at a point-of-presence that provides additional cloud security and SD-WAN functions. These services can be spun up on demand, providing multi-tenant and multi-function gateways that deliver capabilities such as VPN concentration, routing, and cloud security. In addition to providing scalable security, this model can also improve network performance by providing direct connections to other SAAS and cloud applications.

Conclusion: Remote Work Changed Forever

As global governments, organizations, and businesses deal with the ongoing progress of the COVID-19 virus and what it means for global citizens, one thing is certain – major changes will become permanent.

A key takeaway from the development of the crisis is that all organizations, ranging from government to individual households, could use more resilient technology systems to adapt to *any* crisis environment. Fortunately, the advent of many cloud-based technologies, including Secure SD-WAN and SASE, have been in development to help with these exact challenges.

As the world works to develop treatments and vaccines for COVID-19, get people back to work, and restore society and business to relative normalcy, the natural agility and scalability will help deploy technology resources where they need to be, in real-time.

Going forward, enterprises will seek to implement highly elastic, secure, and scalable solutions that can be deployed, re-configured, and managed on the fly with modern software-defined techniques.