ROBERT FRANCES GROUP
Business Advisors to IT Executives

Sep. 14, 2020

# Summary Insights: Satisfying Networking Demands of Remote Workers Today and Tomorrow

**RFG Perspective:** Given that Work From Home (WFH) is a factor in business, business executives and IT executives must rethink their networking topologies with consideration towards data management and privacy, identity, and security. No one knows when work-from-home (WFH) for employees will end as a standard work option. But it's quite possible that many employees and companies will become so accustomed to flexible office hours, options and tools that networking and security procedures will never revert to their former state. WFH, or a mixed model for working flexibly from office or home, is likely to persist for some time – and network topologies must adapt to the New Normal.

Six months into the COVID-19 pandemic – and the rapid move for employees to work-from-home (WFH), the impact on networking, data management and security is becoming clear. RFG100 conference attendees discussed the next phase of networking impacts caused by the shift to a combined WFH-plus-office (WFH/office) work environment in a panel on Sept. 2, 2020.

A real-time poll of the RFG100 attendees showed several top takeaways: (See full poll results in the Appendix at the end of this document, below).

- Nearly 80% said some networking modifications are needed
- More than 60% said their organization is including modernization projects in the implementation of their WFH/office transition.
- Nearly 90% said they think that compliance, privacy and security risks are higher in the WFH/office environment – and must be addressed soon.

This document unpacks the content of the RFG100 discussion, which included input from top IT executives from the banking and financial industries. We believe that all firms should quickly address the impacts of this combined WFH/office networking model to minimize the business risks.

## Overview: The Scramble Settles Down

Some IT managers are re-thinking how they will implement security, identity and data privacy in a WFH/office world. They realize that many aspects of the current WFH situation are quickly becoming permanent, or semi-permanent. As a result, they must decide which networking technologies they will keep – and which technologies must go.

The initial scramble to move employees to WFH was mostly about supporting them with VPN (Virtual Private Network) connections and a familiar, secure desktop via

VDI (Virtual Desktop Interface). Many companies accomplished a working model for VPN/VDI deployment within weeks. Now is the time to refine the initial changes made during the rush to support WFH– and choose which ones will stay and which ones will go.

## Identity is the New Perimeter

The COVID-19 era has turned traditional ideas about network security upside-down. Historically, there was a network "perimeter" around the well-protected enterprise data center. The location of the "center," the "perimeter," and the "edge" – all of these have changed in recent years, with the migration to hybrid cloud and multi-cloud deployments.

When the cloud era began, the old notions about the corporate network morphed into a new topology that included enterprise data centers, the hybrid cloud (connecting data centers with the public cloud). Then came the hybrid multi-cloud, with multiple clouds supporting applications and data that have migrated outwards from the data center.

Yet even in the age of COVID-19, people move to multiple locations: office, home and other places. Thus, the innate assumption that anyone inside the corporate network is trusted is no longer an operable assumption. That has been proven by security breaches in which outsiders access corporate networks by using employee credentials in a cybersecurity attack. These incidents are prompting many network managers to reassess older notions of network security – and to look to identity and multi-factor authentication (MFA) to assure safer access to applications and data.

Given the WFH experience, some CIOs and IT managers are now concluding that identity – not location – must be the new recognition determinant. Identity travels with the person, regardless of location or device. The challenge, then, is to adopt a generation of security policies to adapt to these MFA requirements that are independent of physical location or device.

## Unified Security Enforcement

If the employees are working from home and office – and that they are doing so in different geographic locations, then the organization has to acknowledge that data security procedures will vary from geography to geography, and from country to country.

One way to solve that problem is to adopt standards within geographic regions that comply with the local data protection (GDPR in there European Union, CCPA in the U.S.) and data security standards that vary from country to country (e.g., Canada, China, Germany, the U.S.) However, data management should be consistent throughout the global network, applying global policies across the global network and inserting local policies where appropriate.

## Adapting Network Policies

With most WFH employees now "off" or partially off the traditional corporate network, managers must examine their access patterns to applications and data. Given the fluid situation regarding end-user access, it is inevitable that changes will be made to networking policies, including access methods, APIs, and the use of networking protocols.

"Applications are migrating to the public cloud, to colocation sites and to the private cloud (on-premises), one panelist said. "It's hard to control data access when at least 50 percent of users, transports and devices are outside of typical networking controls." In some cases, a new approach to SASE (secure access/service edge) may need to be put in place to address the new network topology.

One unexpected consequence of this is that network control – which was centralized in the data center – may now be enforced from the edge of the cloud, rather than from the center of the corporate network. "I can do bandwidth control from the edge of the network," one panelist said. The most vulnerable resources on the network can be isolated, or accessed only by means of multi-factor authorization.

## Geographic Considerations, Worldwide

Another approach to managing a global corporate network is to manage the systems and data according to the geographic restrictions in each region, or country. On July 16, 2000, the EU-U.S. Privacy Shield Framework was declared invalid. Now, there is no longer a valid mechanism for transferring personal data from the EU to the United States. Initial lawsuits to prevent transfer have already been filed – and many businesses are waiting to see whether fines are imposed on the companies that were sued. Enterprises must act now to address these data and networking challenges before a wave of wider enforcement for PII data privacy begins.

## Move the Laptop, Move the "Dock"

When it comes to WFH, everything is "local" for the end-users. The employees want their work environment at-home to replicate the one they knew in the office. This can be done in at least two ways: replicating the platforms and software they used in the office – and bringing that environment home. Another approach uses virtual desktops (VDI) to support end-user access to centrally secured data.

Laptops are mobile, by design. That's why Network managers need to decide whether to move beyond the traditional network "perimeters" as they work to secure users' devices. The reality of WFH/office is that changes will have to be made in any case – due to concerns about cybersecurity, ransomware and malware attacks – although the specific changes will vary from company to company.

One solution: Some financial institutions have found that WFH means physically moving their two-screen setups from the office to the home. This move supports network security and data integrity. But having a dedicated line brings greater security to the employee's set-up – and greater end-to-end security to the business, because the line is no longer shared between business and personal uses.

For those employees who will continue to primarily be using the WFH option, employers should consider paying for a second, dedicated line into the home – a deployment that was once considered to be a "perk" reserved for top managers and company executives. WFH may require it either for redundancy or to provide the needed bandwidth and latency as others in the household may be consuming too much of the existing "personal" Internet connection.

## Moving to a Zero-Trust Environment

Finding a way to implement a zero-trust environment, with all potential users challenged before being granted access, is an achievable goal. But IT organizations and network managers must identify the sign-posts of a zero-trust environment. Interim steps must be taken to "change gears" on the way to establishing it.

Zero-trust is already gaining popularity for distributed computing in general, due to the need to prevent cyber-security attacks, malware intrusions, and spoofing (in which external parties masquerade as internal employees). If all end-users need to present their security credentials before gaining access – hence the name zero-trust, then the instances of hacking, phishing and other type of attacks will be reduced.

Some have suggested using a portable ID and ID transference as a way to assure identity that does not depend upon a central authority (e.g., an active directory or registry) for recognition. It allows the individual to use the ID in multiple places and/or countries. However, with this approach, the user does need to have their identity verified by some trusted source (like a bank or credit agency).

Most importantly, the over-dependence on user passwords must "go." IN place of the passwords – which are often hacked, allowing entry to private networks RFG100 attendees said biometric, QR codes and multi-factor authentification (MFA) would be preferable.

## Creating a Cloud-First Networking Topology

The waves of cloud migration over the last 10 years suggest it may be time to implement a "cloud-first" network topology that recognizes that most applications reside in the cloud – whether they are cloud-native, or not.

With the shift to a WFH/office paradigm, companies should re-evaluate their networking topology, especially if the message transport logic forces all transactions to be routed through the data center, even if no other local processing is performed there. The switch to a cloud-first network topology could reduce latency and costs.

Companies could implement these changes themselves and continue to provide the ongoing networking support – or they could enlist the services of cloud services providers (CSPs), MSPs, system integrators (SIs) or channel partners to get the work done.

## Too Many Collaboration Tools

Then, there is the matter of collaboration with other employees, to get their daily work accomplished. The collaboration is an inherent part of the employee's everyday work environment. But the RFG100 panel acknowledged that most large companies already support multiple collaboration tools.

RFG100 attendees agreed that WFH is causing a proliferation of collaborative software tools on employees' desktops. A small sampling would include: Cisco WebEx; Citrix; Google Docs; Microsoft Office 365; Microsoft Teams; Slack; Zoom and other software platforms. The sheer variety of collaborative tools is admirable, but it is often complex to manage.

Employees have preferences, also, using a mix of collaborative software tools during their working hours. Organizations are finding that the rapid rise in multiple collaborative platforms is challenging their goal of adopting collaboration software standards that can be supported in a consistent way across the corporate network.

Further, this mixed environment can impair employee productivity, depending on what software is deployed – and the end-user's customer experience may suffer. While there is no single "correct" answer to selecting the perfect collaborative tools, this is a key issue identified by the RFG100 panel. That's why organizations should consider how many collaboration tools they want to deploy, maintain and support over the next decade.

Sep. 14, 2020

## SUMMARY

The patchwork upgrades that large enterprises adopted to deal with the sudden adoption of work-from-home (WFH) environments required many technical compromises, due to the speed of implementation in the March/April 2020 timeframe, in the wake of the COVID-19 pandemic. In the short term, many enterprises succeeded in deploying network configurations that combine WFH networking support with office configurations, but these stop-gap networking environments must now morph into long-term stable solutions that are secure, available and efficient.

**RFG POV: The compromises and concessions created during the creation of the WFH environment must now be rectified. IT executives will need to work closely with business teams and security teams to achieve the benefits of having a networking infrastructure that will ensure long-term business productivity and certified risk compliance during the transition from the traditional office network topology to a new IT model that supports both WFH- and office-based employees.**

*Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research. Jean S. Bozman, President of Cloud Architects Advisors LLC, co-authored this report.*

-----------------------------------------------------------------------------------------

# APPENDIX 1: RFG100 Survey Results

Questions to the RFG100 attendees, followed by the poll results (shown as percentages of total):

- 1. Do you believe your organization requires no networking or topology changes in order to make the shift to the new WFH/office environment
    - No, a few modifications needed 79%
    - Yes, new same as old 7%
    - Yes, changes made and complete 7%
    - No, no major tasks to do 7%
- Is your organization including some modernization projects in this WFH/office transition effort?
    - Yes 64%
    - No 36%
- Do you believe the compliance, privacy, security risks will increase in the WFH/office environment?
    - Yes 86%
    - No 14%

-----------------------------------------------------------------------------------------------