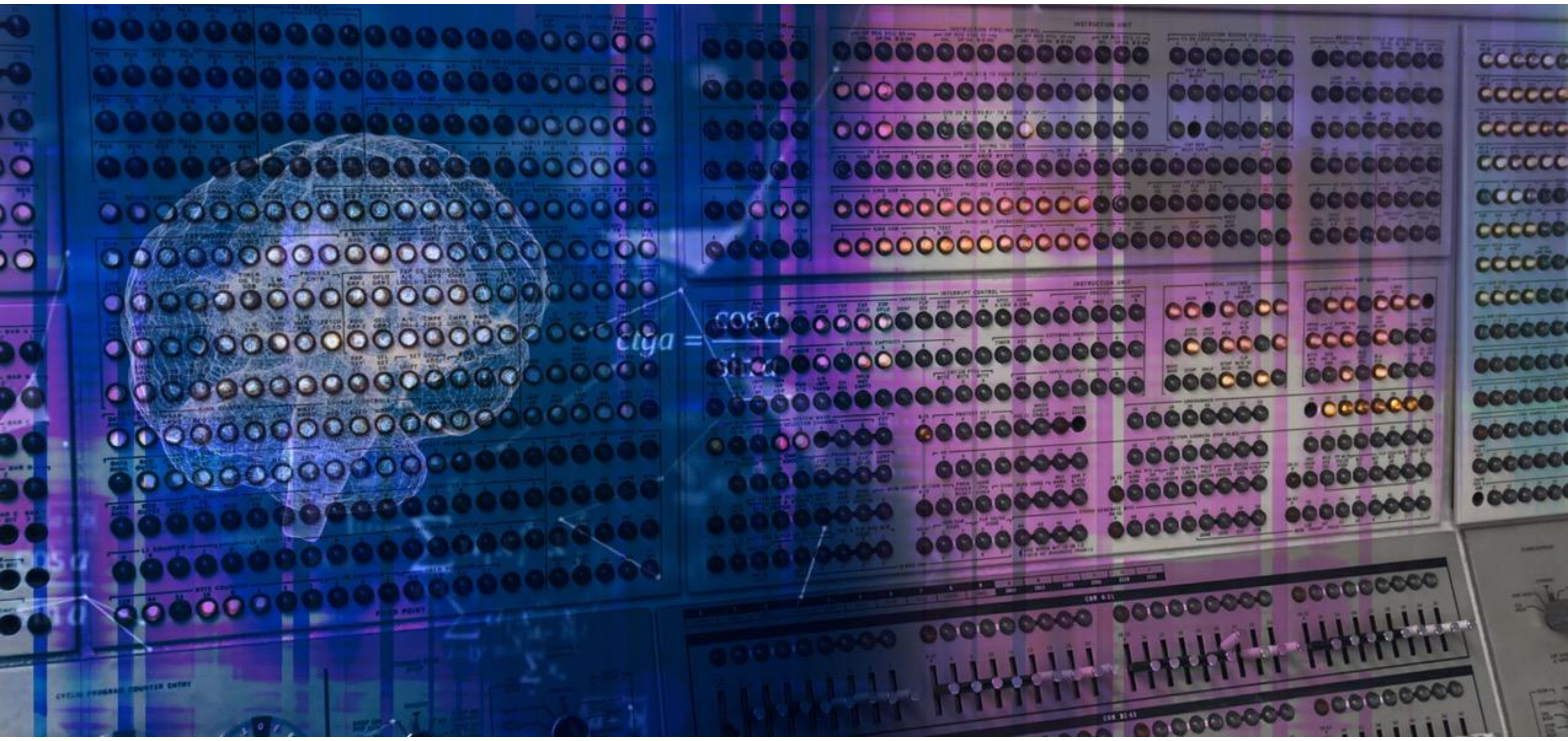


White Paper

Rethinking User Experience on the Edge

The Corporate Network in the Work-from-Home Era

Jason Bloomberg
President, Intellyx

January 2021

The COVID-19 pandemic has driven organizations around the world to shift their employees to work from home (WFH). With this move come complex technology challenges, as these organizations struggle to maintain a high-quality user experience, both for customers as well as employees.

Traditional networking technologies aren't up to the task. Modern IT shops must leverage a next generation of tooling to provide the necessary WFH user experience, and to manage and secure it as well.

Shifting to the next generation of technology is only a part of the struggle. Organizations must also move to a new way of thinking about the corporate network, as traditional hub-and-spoke architectures give way to the more powerful and flexible, but more complicated edge computing model.

All of these changes, both organizational and technological, add risk that organizations must assess and manage. Added complexity only amplifies this risk, and organizations must provide strong measurement and responses to issues when they occur.

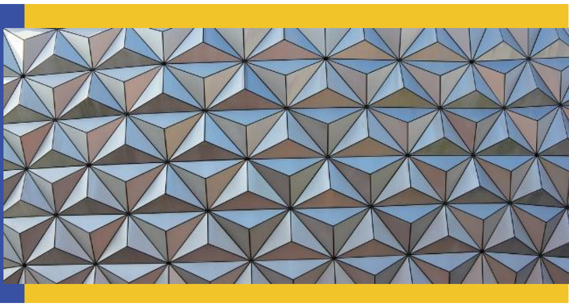
Work-from-Home: Wakeup Call for the Corporate Network

Work from home (WFH) is here to stay.

So say the experts, who point out that even when we're past the pandemic, the office workers of the past won't be in a mad rush to return. There will be reasons to show up in person, of course – but not all day, every day, for almost everyone, as we were so used to before the world changed.

COVID-19 has permanently transformed how we work. Whatever temporary setup you've carved out at home, well, you might as well think of it as permanent.

COVID-19 has permanently transformed how we work. Whatever temporary setup you've carved out at home, well, you might as well think of it as permanent.



That simple, consumer-grade Internet service you've been using, however, is not a permanent connectivity solution for the WFH contingent. Not only does it introduce all measure of security vulnerabilities, but it doesn't have the performance or reliability that enterprises require for their personnel, WFH or otherwise.

For better or worse, there is a regular alphabet soup of technologies that IT managers can bring to bear to address these issues.

There are virtual private networks (VPNs), of course. VPNs provide an encrypted, point-to-point connection between the remote worker and their corporate network. VPNs offer security but don't help with performance. The management overhead for VPN when everybody is WFH can also be unwieldy.

Then there's virtual desktop infrastructure (VDI), which gives users a lightweight client device that accesses all applications and storage over the network. VDI is easy for IT to manage, but prone to bandwidth or latency issues. And, VDI was never intended for an extensive WFH environment.

Other technologies help IT manage and secure wide-area networks (WANs) for connecting corporate networks to remote offices, retail locations, and the like.

Software-defined WAN (SD-WAN) enables IT to remotely manage network equipment in these types of locations, as well as their various connectivity options. Cloud access security brokers (CASBs) help secure remote office access to the cloud. The newer market category secure access service edge (SASE) combines the capabilities of SD-WANs and CASBs.

SD-WAN, CASB, and SASE technologies, unfortunately, center on remote office locations, not WFH individuals, even though the vendors of products in these categories are certainly rolling out WFH-centric options. This entire space is experiencing a period of dynamic innovation, in large part due to the sudden rise of WFH.

Nobody working from home will tolerate a bad user experience to ensure secure interactions with their organization, or vice versa. To survive WFH – and more importantly, to thrive despite it – organizations must ensure both performance and security for every individual in their organization.

Regardless of the mix of technologies a particular organization chooses for its WFH staff, two priorities remain paramount: performance and security. Without adequate performance, personnel cannot get their work done. And without sufficient security, bad actors can take advantage of the WFH situation to compromise the enterprise itself.

Trading off these two priorities isn't an option. Nobody working from home will tolerate a bad user experience to ensure secure interactions with their organization, or vice versa.

To survive WFH – and more importantly, to thrive despite it – organizations must ensure both performance and security for every individual in their organization.

Bringing the Network to the Edge

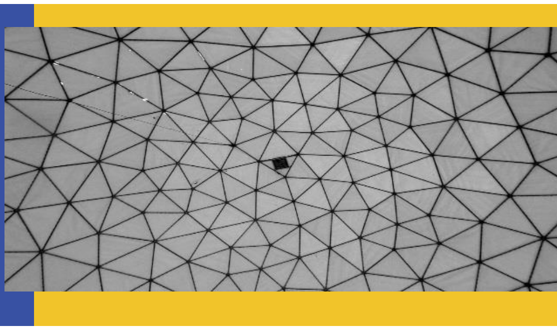
The rise of WFH is both emphasizing and accelerating an important trend: in order for organizations to provide adequate security and management to remote workers – in essence, to provide them with the best user experience – those organizations must rethink the nature of the corporate network.

It is no longer sufficient to think of the corporate network in hub-and-spoke terms, with the corporate LAN as the hub and remote locations and individual workers as the spokes.

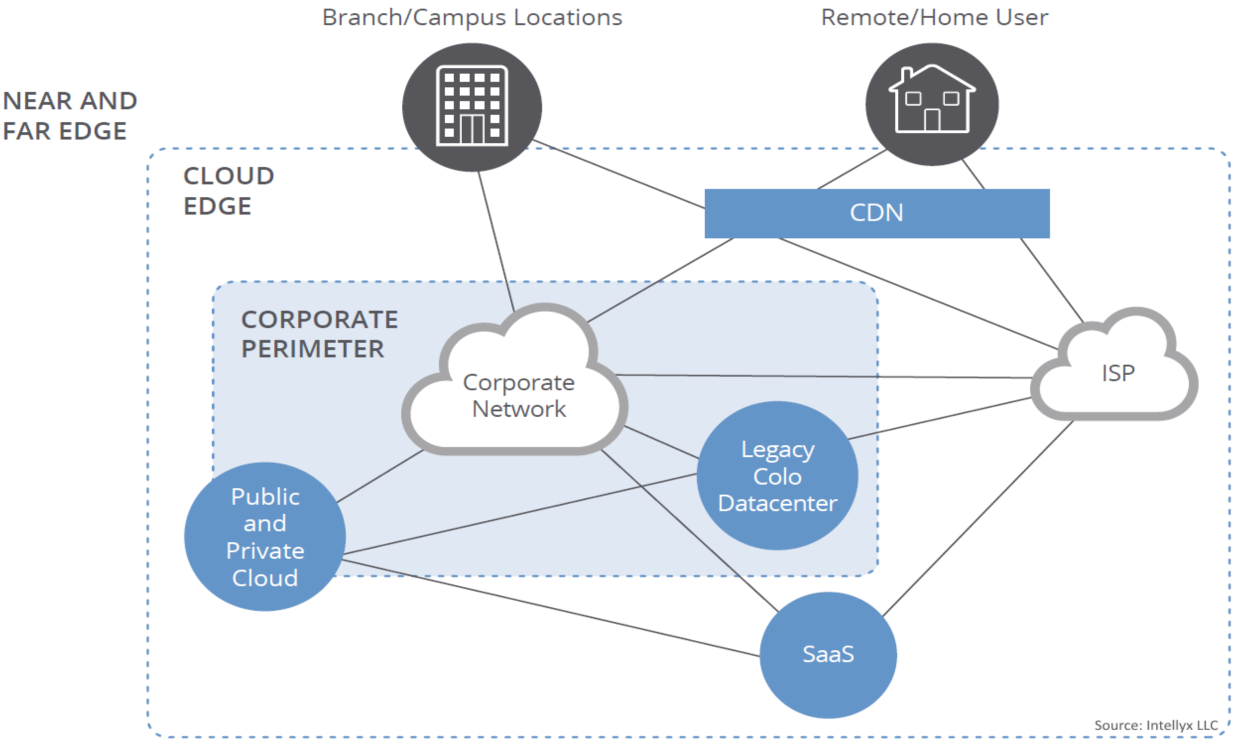
Instead, technologies like VPN, VDI, SD-WAN, CASB, and SASE are transforming to meet a new vision for global corporate networking: *edge computing*.

Edge computing provides a common abstraction across a range of local and remote IT assets in order to support next-generation security and management technology. On the downside, the edge is more complicated than traditional approaches to corporate networking.

Edge computing provides a common abstraction across a range of local and remote IT assets in order to support next-generation security and management technology.



There are actually several flavors of edge computing. Where before, we could consider the transitions from LAN to WAN and WAN to the cloud to be the edges of the respective networks, we now add the notions of the *near edge* and the *far edge* to the *cloud edge*, as the figure on the next page illustrates.



Source: Intellyx LLC

Edge Computing and the Corporate Perimeter

The *cloud edge* is where the content delivery networks (CDNs) and colocation providers (colos) play. CDNs will locate web servers close to end-users in order to distribute traffic and reduce latency, while colos extend the reach of corporate data centers to third-party facilities to locations around the globe.

The near edge mainly consists of servers or other equipment at customer premises, which might be anything from a phone closet at a retail branch location to the server room in an office building.

The near edge may also represent a facility that hosts Internet of Things (IoT) gateways, perhaps at a factory, in a city's traffic switching office, or in the security command center of a large building (or campus) like a stadium, airport, or office building.

As telecommunications providers ramp up their 5G infrastructure buildout, a third example of the near edge is becoming increasingly important: networking equipment located at cell towers or local telco points of presence.

Such locations are typically well-suited to host small data centers with all the essential trimmings – power, cooling, racks of equipment, and sometimes a barebones staff.

Given the complexity of the near edge, the far edge is more straightforward. It consists of the user devices themselves – PCs as well as either handheld smartphones or similar, as well as IoT sensors and actuators.

Remote workers, therefore, live and work at the far edge, while we can consider their network equipment to reside at the near edge, even if it resides next to the family television. In any case, we've blown up the notion of the corporate network by considering it to be part of the edge.

The technologies that support the remote worker – VPNs, VDI, SD-WAN, CASB, and SASE – are now part of the fabric of technology that implements, manages, and secures the entire edge.

Regardless of what combination of these technologies (or other, similar products) a particular organization deploys, it must nevertheless provide a single, unified management and security control plane that supports the changing needs of the remote worker as well as the organization – without sacrificing the user experience.

The Importance of User Experience in the WFH Era

Customer experience is unquestionably important, especially when an organization's customers are consumers. Give them a poor experience, and they'll simply jump to a competitor.

Employee experience, on the other hand, is often taken for granted. When employees are office workers, they have the luxury of company-issued equipment, software, and Internet connectivity. Maintaining the experience using such technology is simply routine IT management.

WFH is changing this equation. Not only do IT organizations need to bridge the gap between the in-office and WFH experiences, but organizations must also provide additional support for WFH personnel to facilitate communication and collaboration – tasks that simple proximity would promote in the office setting, but are now under strain.

WFH also introduces a shift in the type of worker who might be WFH. Pre-pandemic, WFH personnel tended to be customer-facing, particularly in B2B organizations. In other words, they are the individuals responsible for representing their organizations with customers, partners, and others, whether they be contact center agents, salespeople, or support personnel

In the WFH era, organizations are adding 'back office' workers to their WFH cadres who are perhaps less comfortable with WFH arrangements than 'front office' personnel who routinely work away from the office.

True, WFH has impacted their lives as well, as meetings are now remote, but the back-office data entry clerk may have never needed to worry about using a work laptop at home before.

> In the WFH era, organizations are adding 'back office' workers to their WFH cadres who are perhaps less comfortable with WFH arrangements than 'front office' personnel who routinely work away from the office. WFH has impacted their lives as well, as meetings are now remote, but the back-office data entry clerk may have never needed to worry about using a work laptop at home before.

Of course, these points are mere generalizations – there is in fact a great variety of different individuals with different roles within any large organization, and WFH may impact them all differently.

This variety, in fact, exacerbates the user experience challenge, and with it, the difficulties with managing and securing the corporate network, now that it's part of the edge.

Managing and Securing the Network in the WFH Era

True, many applications have moved to the cloud – but there remain many back-office applications that require users to access services through a VPN gateway. In addition, many organizations have implemented VDI to simplify the work of IT while delivering a familiar digital experience to the user.

Regardless of the combination of underlying technologies, however, IT requires comprehensive visibility into the services that they deliver via any such products in order to adequately manage and secure them.

Metrics that expose the user experience, enabling operators to quickly analyze and address availability and reliability issues, is particularly important in an edge computing environment. In fact, such operators require visibility into the actual activity of WFH personnel and how application dependencies deliver services to both employees and customers.

In this context, it rapidly becomes clear that both VPN and VDI are earlier-generation technologies that are not particularly well-suited for the WFH era.

In particular, the VPN concentrator has become a new favorite target of DDoS attacks. Bad actors know they can impact an organization by launching a relatively small DDoS state exhaustion attack against VPN concentrators already running at or near connection capacity.

Filling these VPN concentrators with illegitimate connections denies connections to a legitimate WFH workforce, essentially ceasing their productivity.

Not only do end-users generally dislike VPNs and VDI, but the sudden move to WFH has led many IT shops to expand the number of simultaneous VPN connections dramatically, requiring a scramble for new resources. Furthermore, VDI in particular is exceptionally sensitive to network performance, thus raising the bar for IT.

The broader context for these issues with older VPN and VDI technologies is the extension of software-defined approaches to remote endpoints – now including WFH personnel's devices in the mix. This edge computing trend calls upon SD-WAN technologies and SASE to evolve to encompass VPN use cases.

Managing and securing the network must begin at its most atomic level: the TCP/IP packet itself. Building upon this packet-level visibility, Network Traffic Analysis (NTA) is able to manage the user experience across complex combinations of networking technologies.

Given this mélange of different technologies, managing and securing the network must begin at its most atomic level: the TCP/IP packet itself. Building upon this packet-level visibility, Network Traffic Analysis (NTA) is able to manage the user experience across such complex combinations of networking technologies. Adding synthetic transactions to the NTA perspective extends IT's ability to isolate problems, for example, whether the home network or the ISP is responsible fora performance degradation.

Additionally, the continuous testing of services can alert IT to a problem before it significantly impacts users. While it may not be practical to provide testing from all users' perspectives, representative samples combined with actual traffic can provide significant insight into the user experience.

To this end, NETSCOUT leverages NTA and synthetic tests to provide real-time monitoring and measurement of user experience, even in complex, dynamic networks. NETSCOUT can then resolve and identify the root cause of issues when they occur.

Operators can deploy NETSCOUT technology on any infrastructure platform, including edge computing platforms, public and private clouds, and legacy network environments. Such deployment can take place at the near or cloud edge, in front of essential devices such as VPN concentrators, firewalls, and load balancers to protect them and the services behind them from DDoS attacks.

NETSCOUT delivers analytics based on the packets themselves, providing visibility into all user and application traffic, correlating the resulting information in order to give operators the insights they require in order to adequately secure and manage the user experience for anyone, WFH or otherwise.

The Intellyx Take

It's easy to think of the pandemic-driven WFH phenomenon as a temporary aberration, representing little more than people working from here rather than there.

The underlying reality, however, is far more disruptive. Not only is WFH here to stay in one form or another (as yet undetermined), but it also represents a new working reality for untold millions of office workers and others.

In any case, the reality for IT has permanently changed. Traditional ways of looking at corporate networks are now dangerously obsolete. Edge computing architectures coupled with next-generation security and management technologies are now absolutely essential for maintaining the user experience both employees and customers expect.

It's true that many IT shops aren't ready to make such a move yet – but even the most conservative of IT shops should be planning ahead for how to transition existing VPN and VDI technologies to the next generation.

Visibility into user activity, network performance, and application dependencies is essential for getting a handle on today's WFH needs as well as for putting together a roadmap to edge computing that offers greater flexibility, performance, security, as well as an improved user experience, today and into the future.

About the Author: Jason Bloomberg

Jason Bloomberg is a leading IT industry analyst, author, keynote speaker, and globally recognized expert on multiple disruptive trends in enterprise technology and digital transformation.

He is founder and president of Digital Transformation analyst firm Intellyx. He is ranked #5 on Thinkers360's Top 50 Global Thought Leaders and Influencers on Cloud Computing for 2020, among the top low-code analysts on the Influencer50 Low-Code50 Study for 2019, #5 on Onalytica's list of top Digital Transformation influencers for 2018, and #15 on Jax's list of top DevOps influencers for 2017.

Mr. Bloomberg is the author or coauthor of five books, including *Low-Code for Dummies*, published in October 2019.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius™ service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.