RESEARCH
Influence and insight through social media

May 2020

RETHINKING THE NETWORK

in the Post-Pandemic Era

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: POST-PANDEMIC ORGANIZATIONS WILL BE NETWORK CENTRIC

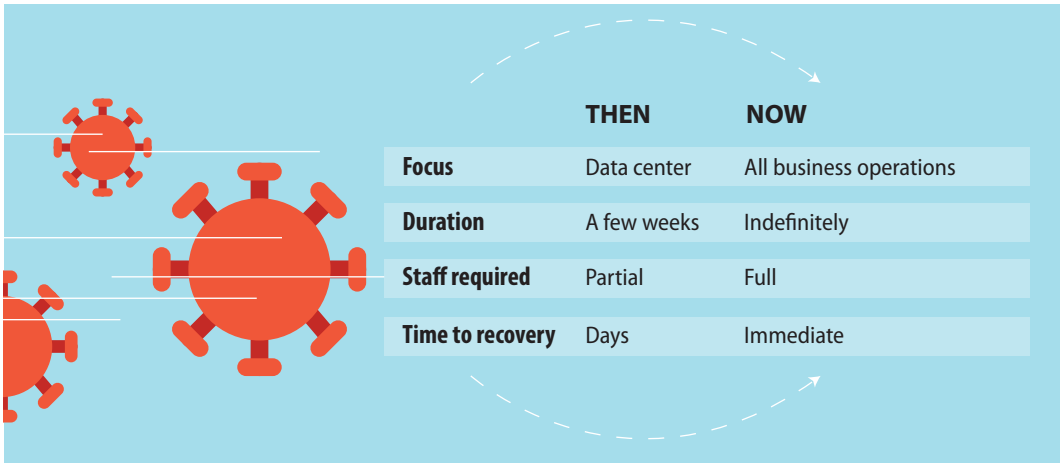
The COVID-19 pandemic hit businesses like a fast-moving hurricane. In a short period of time, organizations had to completely redefine themselves and set people up to work from home. This has had a profound impact on the way companies run, as the definition of business continuity has been redefined (Exhibit 1). Historically, business continuity plans have revolved around keeping an organization running temporarily with a minimal set of services and people. Today, because of the pandemic, it's been redefined as running the entire organization, fully staffed, for an indefinite period of time.

The pandemic-induced work-from-home (WFH) trend is very real and expected to last for quite some time. According to ZK Research, 90% of organizations now have a subset of employees working from home, with many exceeding 95% of the total worker population. Also, 93% of business leaders expect to see a permanent rise in remote working by at least 30% post-COVID-19.

The big unknown with the pandemic is how long it will take for the world to return to "normal." Based on ZK Research interviews with business leaders, it will be at least six months before most workers even begin to return to the office. However, there will be no "big bang" where every worker returns to the office at once. Rather, employees will likely come back departmentally and/or in shifts to limit the number of people in the office at once. Also, business leaders will need to be prepared for a return to WFH if another outbreak occurs.

The uncertainty about what the future of work will look like creates a significant challenge for IT leaders because organizations need to be prepared for any scenario—ranging from everyone working in the office to everyone working from home. This has caused a rise in demand for cloud-based applications, as they can be accessed from anywhere, without virtual private network (VPN) clients, and they provide a consistent user experience regardless of where the worker is located.

Exhibit 1: COVID-19 Has Changed the Definition of Business Continuity



ZK Research, 2020

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

ZK Research predicts that over the next five years, the overall cloud services market will see an incremental growth of more than $15 billion because of the COVID-19 pandemic.

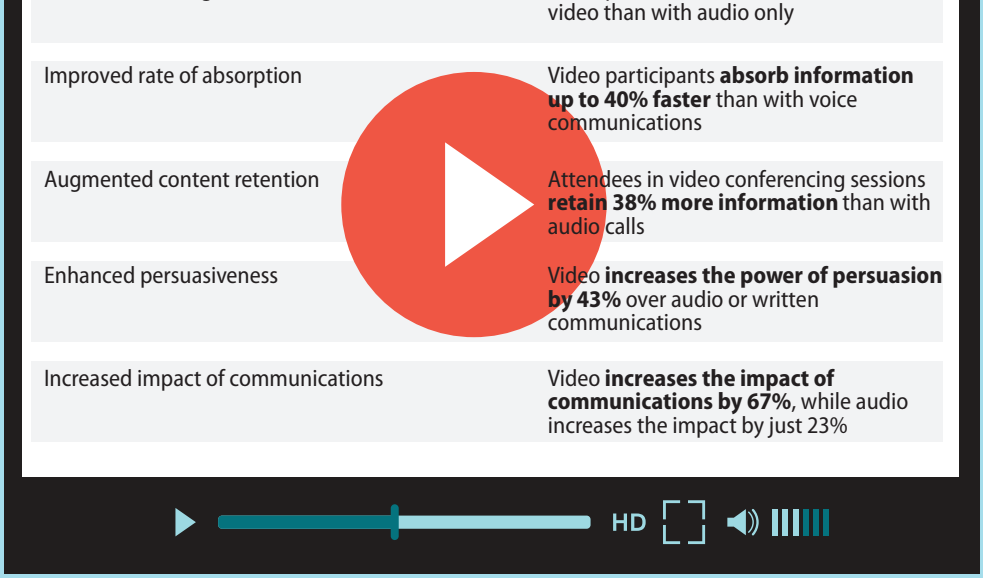
In addition to the cloud, another technology that has seen significant uptake is video-based applications. For example, Zoom, the maker of a video-based meeting application, reported that its daily usage jumped 300% in the month of March. Also, in Vonage's most recent quarter, it announced that its video API saw a 290% increase in utilization. ZK Research recently conducted a number of one-on-one interviews with business leaders about the value of video. Exhibit 2 shows the degree to which comprehension and collaboration improve with the use of video.

Video-based collaboration is here to stay for the foreseeable future, as employees will be partially or fully working remotely for years. However, video is doing more than changing the way people meet and collaborate; it's enabling hospitals to provide telehealth and facilitating court proceedings and depositions in the legal industry, and entertainment is also shifting to a video model. For example, the National Football League (NFL) conducted its recent draft over video, and the individual teams held video-based fan parties. The result was the highest watched draft in NFL history.

The shift to WFH combined with the rise in cloud computing and video services has wreaked havoc on corporate networks. Previously, application traffic was limited to the company network,

Exhibit 2: Video Enables Socially Distant Workers to Maintain High Levels of Collaboration

BENEFIT	RESULT
Increased learning	Participants **learn 200% more** with video than with audio only
Improved rate of absorption	Video participants **absorb information up to 40% faster** than with voice communications
Augmented content retention	Attendees in video conferencing sessions **retain 38% more information** than with audio calls
Enhanced persuasiveness	Video **increases the power of persuasion by 43%** over audio or written communications
Increased impact of communications	Video **increases the impact of communications by 67%**, while audio increases the impact by just 23%



ZK Research, 2020

A complete rethink of the network is required if organizations are to transition their businesses and thrive in the post-pandemic era.

where IT had tight control over performance and security. Today, most application traffic is "off-net," where it leaves the company network. This has increased the attack surface exponentially and created a number of blind spots.

A better solution would be to extend the network to the edge (i.e., small offices/home offices), allowing enterprises to keep all traffic "on-net." In this way, identical policies can be applied whether employees are in the data center, the conference room or their living room.

As companies look ahead at a post-COVID-19 world, the harsh reality is that the "new normal" will not be normal. Businesses must be prepared for the unknown, and that is causing them to adopt a number of network-centric technologies. Historically, the network was considered the "plumbing" of a company and was something few IT and business leaders gave much thought to. In the current and post-COVID-19 environment, the network will be the most strategic technology a company has, as it will connect workers to apps, devices and Internet of Things (IoT) endpoints. The challenge is that most legacy networks are not designed for a world where the majority of workers are accessing corporate resources from the outside in—and in an environment where the majority of components are connected. A complete rethink of the network is required if organizations are to transition their businesses and thrive in the post-pandemic era.

SECTION II: NETWORK CONSIDERATIONS FOR A WORLD WHERE THE "NEW NORMAL" IS CHANGE

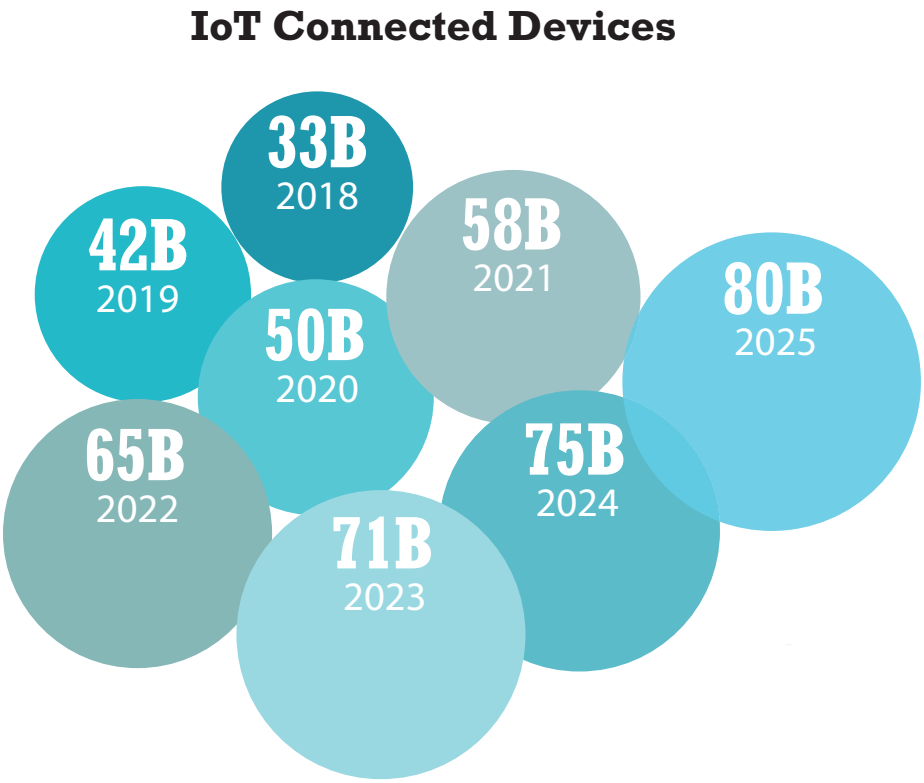
Even prior to the COVID-19 pandemic, the value of the network had started to increase. All of the building blocks of digital transformation—including cloud, mobility, artificial intelligence (AI), and IoT—are network centric, meaning digital transformation is also network centric. In fact, IoT alone will add billions more connected devices over the next five years (Exhibit 3). Network engineers are already overwhelmed by the number of connected endpoints, and the rise of IoT will make a challenging situation untenable.

The COVID-19 pandemic has accelerated the digital transformation plans of most companies. For example, at the end of April, Microsoft CEO Satya Nadella stated that the company has seen "two years' worth of digital transformation in two months" of its third quarter. This has elevated network evolution from important to business critical. In fact, one could argue that evolving the network is the most important initiative a business can implement to protect revenue both today and into the future.

As IT and business leaders plan the next phase of the network, ZK Research has identified the following key network attributes to keep in mind:

Simplified remote access: Most companies are using legacy VPNs to connect remote workers. Although VPNs work, they are an expensive way of providing remote access because the number of user licenses must be expanded and often the firewall or VPN concentrator to which users connect must be upgraded to accommodate the increase in remote workers. Also, remotely configuring VPN software requires significant amounts of IT time. There are better connectivity

Exhibit 3: The IoT Era Has Arrived



ZK Research, 2020

options, such as using cloud-configured routers, switches and remote access points that will make the worker's home setup look like a company location to both the user and the IT department. This architecture enables IT to enforce corporate security standards and communication policies, and it lets IT extend applications to the new edge—all but eliminating "off-net" corporate traffic.

Cloud-optimized networks: Legacy networks were tuned for client/server traffic, where the assumption was that all traffic was clean. Cloud traffic comes via the internet, and the assumption should be that it poses a risk. Organizations should use tools such as split tunnels and network segmentation to isolate traffic so if a breach occurs, it will not impact the entire company.

Agile management tools: There's currently a debate as to whether network management tools should be located on premises or in the cloud. The fact is, neither is better, per se. Rather, the cloud makes sense in highly distributed organizations or when IT personnel are remote, while on premises might be a better model when the majority of employees are based in a few locations. The key is to implement a management model that supports moving between the two.

As the COVID-19 pandemic rages on, network managers will be called on to make more changes even faster.

Advanced visibility and analytics: There's an axiom with networking that "you can't manage what you can't see." Network professionals need visibility and analytics tools to understand how applications are performing. These tools must extend to the cloud and be automated to see new devices as they connect to the network. Also, machine learning (ML) must be used to analyze the massive amounts of data that networks generate today.

Intrinsic security: Legacy security architecture is built on an overlay model in which much of the protection was implemented at the endpoints. Businesses no longer have tight control over the endpoints, and security software changes too fast to require continual updates to endpoints. Security must be embedded in the network to quickly identify threats. ZK Research found that the average time to locate a breach in a traditional endpoint security model is 103 days, which is far too long to be effective. Network analytics can notice the smallest anomalies and detect possible breaches almost immediately.

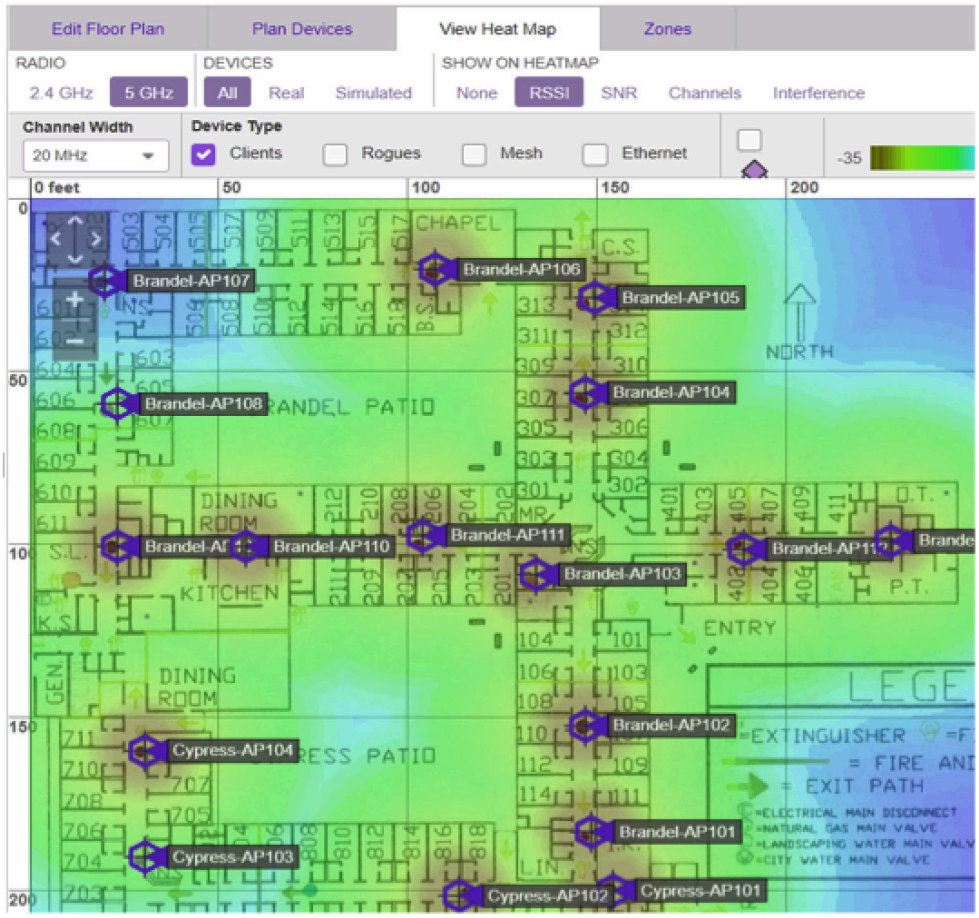
Automated operations: The ZK Research 2019 Network Purchase Intention Study found that it takes enterprise-class companies an average of four months to implement a change network wide. This long lead time for changes results from the manual nature of network operations. As the COVID-19 pandemic rages on, network managers will be called on to make more changes even faster. However, people can't work at digital speeds. By automating configuration changes, businesses can implement them quickly and accurately.

Safe mobility: Providing a safe working environment must be top of mind for IT and business leaders. One way to do so is by providing "safe mobility." Modern Wi-Fi systems have analytics tools that understand where workers are going, whether there are unnecessarily large clusters of people, and with whom people come into contact. The data from Wi-Fi systems can be imported into contact-tracing solutions to provide further granularity. Safe mobility is now mandatory for a safe workplace. Exhibit 4, from Extreme Networks, shows how location, presence and proximity can be seen from Wi-Fi data.

IoT support: The pandemic will accelerate the deployment of several new connected devices such as thermal scanners, security cameras, cleaning robots and autonomous vehicles. Many of these will be connected via a wireless network that needs to support all the various wireless standards. In addition, the network can track devices to ensure they've gone through the proper sanitizing protocol before they are put back in the workplace.

Wi-Fi 6: The rise of video, IoT and cloud services could double or even triple demands on older Wi-Fi solutions that are designed to augment wired and cellular-first use cases. Wi-Fi 6 is the first standard designed for an environment that is predominantly Wi-Fi based. ZK Research

Exhibit 4: Wi-Fi Data Ensures Campus Safety



Extreme Networks, 2020

recommends that any customer running Wi-Fi 4 or older should make upgrading to Wi-Fi 6 a priority. Wi-Fi 5 customers are likely fine for the short term, but a plan should be put in place to upgrade to Wi-Fi 6 within 24 months.

Resilient network: With application components scattered everywhere, the network has effectively become the new computer. That means any weakness in any part of the network could make mission-critical applications unavailable or perform poorly. The network needs to be highly resilient and "always on" to support an increasingly dynamic and distributed workforce.

SECTION III: WHAT TO LOOK FOR IN A NETWORK SOLUTION PROVIDER

The COVID-19 pandemic has changed the world and made businesses network centric. A company's choice of network provider is among the most important decisions it will make in the next decade. These are some key attributes to look for in a network provider:

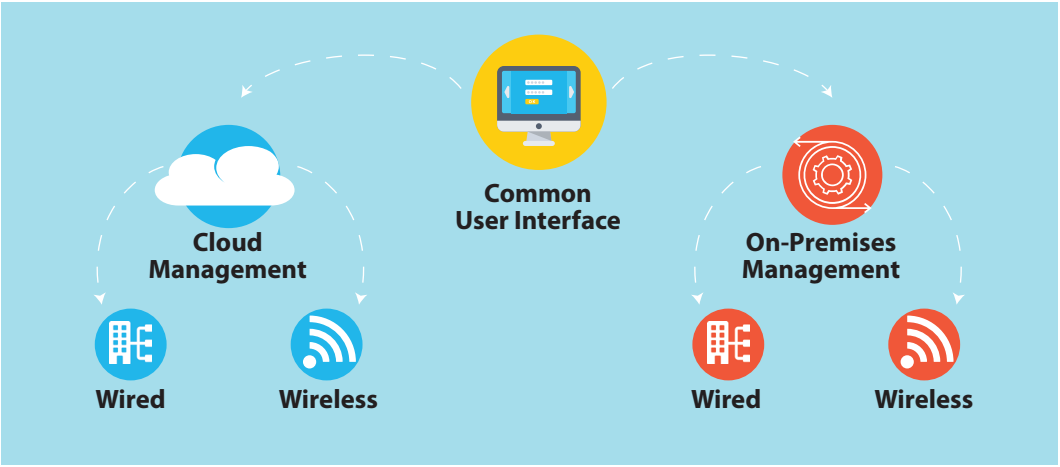
Trusted advisor: The network vendor should have a culture of innovation and offer the highest level of customer service that's insourced, as it makes the provider directly responsible for customer success. The following are good questions to ask: What percentage of the Fortune 50 are served, and where does the vendor's customer service rank? These details can help customers find a network vendor that puts its reputation on the line with every customer deployment.

End-to-end portfolio: The network is often perceived to be broken up into segments—the wireless network or the data center network, for example. In fact, there is one network that delivers applications and experiences, and the vendor should have a portfolio of products that reflects that.

Management flexibility: Vendors often have different configuration tools for different product lines. This can happen when acquisitions are used to fuel innovation or when product teams operate in silos. Management tools should work across all products, regardless of whether the management is handled in the cloud or on premises, or whether the network being configured is wired or wireless (Exhibit 5). This arrangement also ensures that policies are consistent across the wired and wireless networks. Customers should have the option of moving between these two models as necessary.

Advanced Wi-Fi 6 capabilities: Wi-Fi is no longer a network of convenience. One could argue that the quality of Wi-Fi will be the factor that ensures the success (or failure) of digital projects. The vendor should have a broad range of Wi-Fi access points (APs), including indoor and outdoor, and innovative APs such as wall plates. Also, the Wi-Fi should support other wire-

Exhibit 5: Management Flexibility Creates Network Consistency



ZK Research, 2020

less standards such as Bluetooth for IoT connectivity. Advanced capabilities are delivered via ML for automated operations and proactive remediation.

Contact-tracing support: No network vendor can offer a full contact-tracing solution, but vendors should provide features that support tasks such as occupancy management, which is considered a "light" version of contact tracing.

SECTION IV: CONCLUSION AND RECOMMENDATIONS

Businesses will start planning to come out of the COVID-19 pandemic soon, but the impact will be felt for years. The pandemic has ushered in the digital era faster than most organizations were prepared to handle.

Today, competitive advantage is based on an organization's ability to be agile, adapt to changes and make rapid shifts to capture market transitions. Several digital-enabling technologies—such as IoT, cloud and mobility—have been introduced into businesses in the past several years, and they are all network centric. If the business is to harness the full potential of these technologies, the network must evolve.

To help businesses get started with their network evolution, ZK Research makes the following recommendations:

Focus on transforming the network. For most businesses, the network is the business. The COVID-19 pandemic is forcing organizations to find new ways to service customers and employees. This includes the increased use of video, a shift to mobile applications and the utilization of virtual reality. The network must be transformed to handle these new types of traffic and the increased load, and network transformation must happen now.

Automate as much as possible. Automation is not the enemy of the network engineer; rather, it should be viewed as a strategic tool that can eliminate many mundane tasks, such as Wi-Fi troubleshooting, that network professionals are burdened with today. Businesses should use AI- and ML-based automation tools to streamline network operations and move to a predictive management model that is self-healing and offers better security.

Evaluate a wide range of vendors. When refreshing the network, it's easy to choose the incumbent provider or the market leader. However, at moments of market transition, the market leaders are often hesitant to move the industry in a new direction because it disrupts their own businesses. Therefore, companies should evaluate at least three vendors as part of their evaluation process.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314