August 2017

Digital Transformation Success Is Dependent on

NETWORK MODERNIZATION

WHITE PAPER

Prepared by
Zeus Kerravala

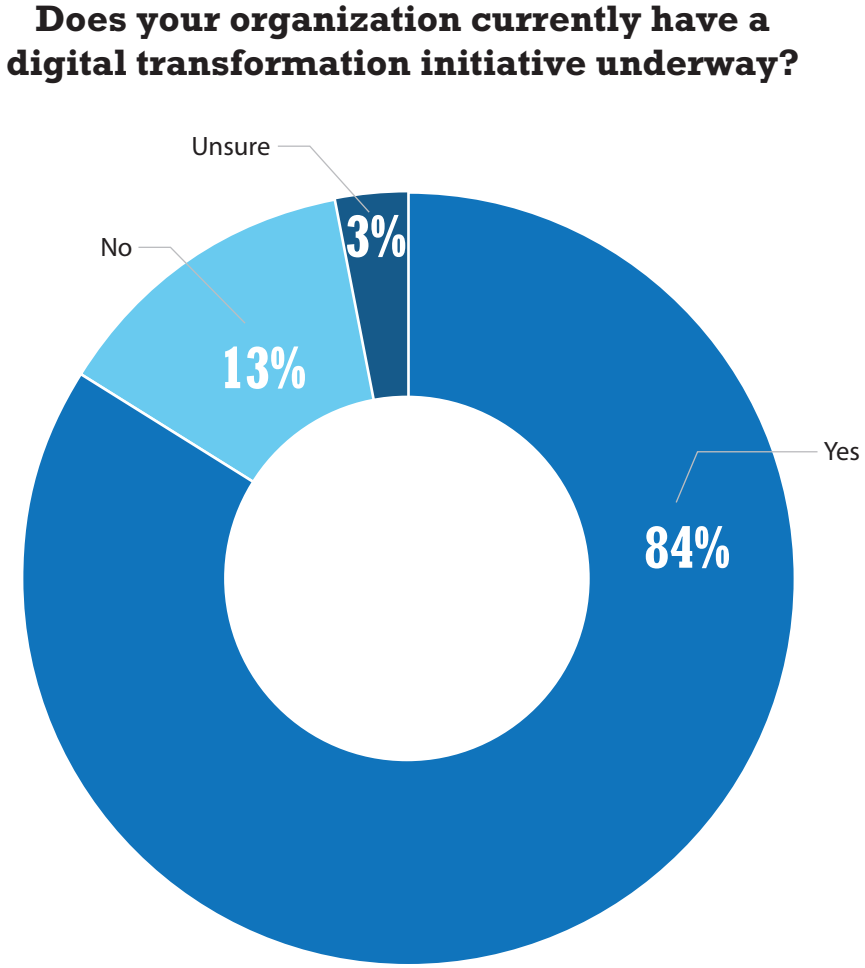
ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: IT'S TIME FOR NETWORK EVOLUTION

Digital transformation has become a top mandate for almost every IT and business leader. The ZK Research 2017 IT Priorities Survey found that 84% of businesses currently have a digital transformation initiative in progress (Exhibit 1). In the digital era, competitive advantage is no longer determined by which company has the best products or even the best people. Market leadership is based on an organization's ability to analyze information, gain insights and make fast decisions to capitalize on market transitions.

One important step in the journey to becoming a digital organization is transforming into an agile business—and it is impossible to do so without having an agile IT infrastructure to enable it. This is why businesses spent more than $14 billion on technology in 2016 to make IT more agile, according to ZK Research.

Exhibit 1: Digital Transformation Is the Norm



ZK Research 2017 IT Priorities Survey

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.

Evolving the network must be a priority for every IT and business leader.

However, one part of IT that has yet to evolve is the network. Evolving the network must be a priority for every IT and business leader because many of the digital building blocks—such as the Internet of Things (IoT), mobility and the cloud—are network centric in nature. Therefore, in many ways, the network is the foundation for a digital business. Also, differentiation for digital businesses will come from the creation of new contextual applications that utilize information such as location and identity that create experiences that delight users.

Traditional networks were designed for an era of best-effort services to deliver non-mission-critical services. Today, most companies can survive without the network, but the following limitations must be overcome:

Traditional network management is done "box by box." Historically, network managers have had to network devices on a box-by-box basis through a highly manual, repetitive process. This means that even the most basic network changes can take weeks or even months to complete. Additionally, because there are so many types of devices and network operating systems, the syntax required to make a configuration change could be quite different from platform to platform—making the task even more challenging.

Lack of automation keeps the total cost of ownership (TCO) high. With respect to the TCO of the network, almost 68% comes from operational costs associated with running the network. These costs are high due to the manual nature of configuring, updating and maintaining network devices. Some organizations have attempted to lower the TCO by purchasing less expensive network devices, but hardware only accounts for less than a third of network TCO. The only way to significantly lower the TCO of the network is to reduce the operational costs associated with running it—and doing so requires more processes to be automated.

The network has no ability to interface with applications. Application development has shifted to a highly agile model called DevOps, which is based on the idea of continuous innovation. DevOps has a profound impact on network infrastructure for multiple reasons. Network operations needs to be able to move with speed and make changes at the pace that DevOps operates. The manual processes that plague traditional networks are far too slow. Also, applications ideally should have the ability to access network resources, so the network must become more programmable.

Network operations lives in a silo. Historically, application development and the infrastructure teams have operated independently. This leads to finger pointing and a lack of ownership of problems that can impair the company's performance. Adding to the problem is the fact that the subdomains of IT—such as network, server, security and storage operations—function in their own silos, leading to fractured IT strategies. The network connects IT resources to the applications and must be tightly aligned with the other groups in IT and the application team.

If businesses are to become agile businesses that can move with speed and keep up with their digital peers, the network must evolve.

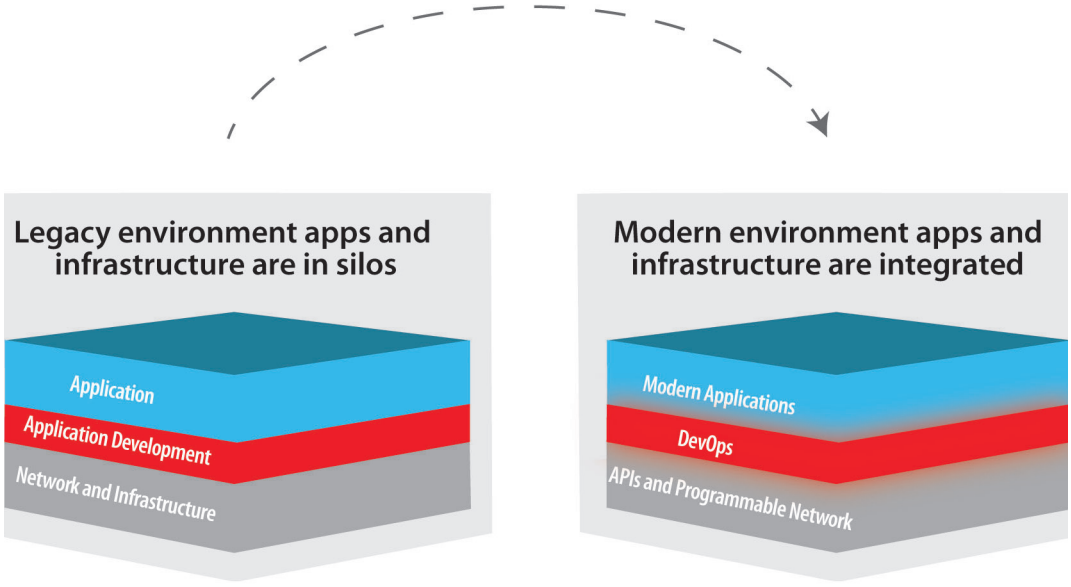
SECTION II: THE NEED FOR NETWORK MODERNIZATION

The current architecture used to build and operate networks has been in place now since the birth of the internet. It was designed in an era when the majority of company workers and data was located on premises and there was very little that was unknown to network operations. Today, that has all changed. Workers are scattered all over the globe, data is in the cloud and non-IT devices are connecting to the network at a rate never seen before. As the world becomes more connected, dynamic and distributed, the network will continue to grow in importance.

Also, DevOps has accelerated the pace of innovation and software development. Instead of rolling out one or two major software releases per year, companies have shifted to a continuous innovation model where new software is released daily or faster. ZK Research estimates that more than 100 billion lines of new code were created in 2016, meaning software is now dominating the world.

The rise of applications is changing the very nature of the network and infrastructure. In the past, application developers could not gain any information from closed hardware systems; but now, programmable infrastructure exposes key information via open APIs, enabling modern applications to leverage a programmable network (Exhibit 2). The advancements in both APIs and programmable infrastructure are creating amazing opportunities for developers to not just build apps that run on top of the network, but to also enable them to derive and benefit directly from the network.

Exhibit 2: Apps and Infrastructure Have Come Together



ZK Research, 2017

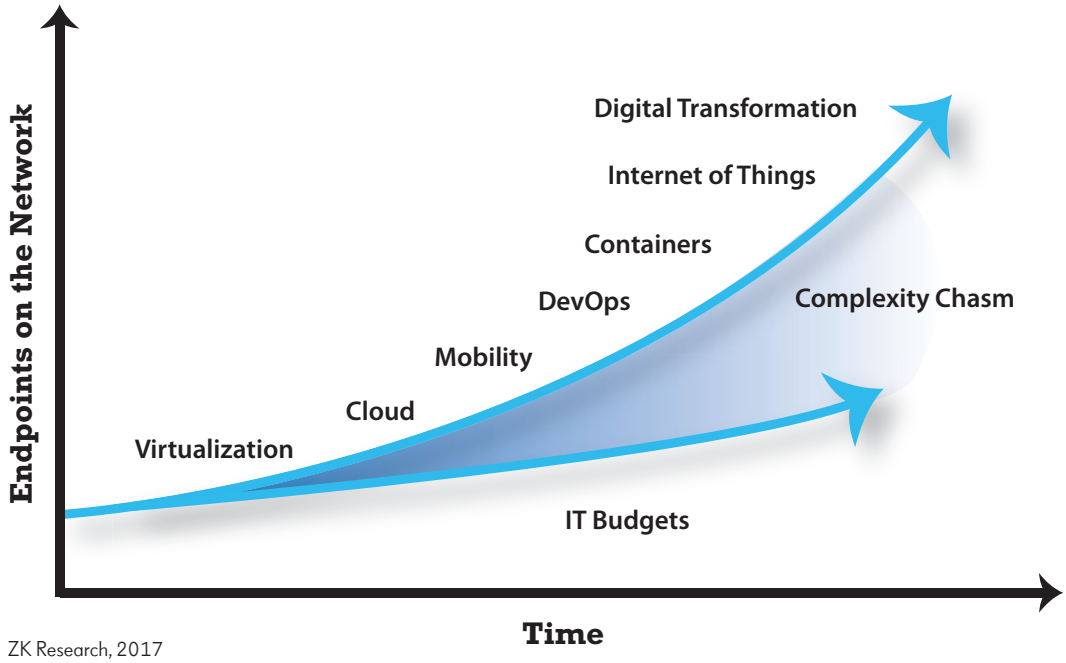
In addition, IT is able to create "as a service" type catalogs for applications and tools that developers need to build modernized apps without even thinking about the network and its various functions and protocols. This masks the complexity of the network from developers but still enables them to work with network service.

The network has struggled to keep up with changes in the application development process and consequently has put the success of digital initiatives at risk. For example, ZK Research recently interviewed a U.S.-based hospital that was using the network to deliver messages from patient-monitoring equipment to clinicians' mobile devices. The hospital spent millions on a custom application and on new devices in an effort to improve patient care. However, the network was not modernized as part of the project, and the result was a system with so much latency that it often took five minutes or more for clinicians to receive alarms—many of which had life-saving implications. In this case, an investment in the network would have delivered a much better return.

Digital applications require a network that is resilient, secure and automated for the best possible performance. Unfortunately, the network has become increasingly complicated, creating a complexity chasm that is widening exponentially (Exhibit 3). Relatedly, human errors now account for 34% of network downtime—by far, the largest cause—according to the ZK Research 2017 Network Purchase Intention Study.

Shifting to a software-defined network (SDN) is the first step in the network modernization process. With SDNs, the control and data-forwarding planes have been decoupled, enabling network management to be abstracted away from the physical device and centralized in an SDN controller.

Exhibit 3: The Network Complexity Chasm Continues to Grow



ZK Research, 2017

SDNs are highly automated, so network managers no longer need to perform the highly repetitive, mundane tasks that are required with traditional networks.

SDNs bring many benefits to the network, including the following:

Faster configuration changes and updates: Network administrators can make configuration updates at the controller level and push the changes out to the entire network at once. This can shorten the time it takes to make network-wide changes from months to minutes.

Improved security: SDNs can be used to "micro-segment" the network. Traditional networks use virtual LANs (VLANs) and access control lists (ACLs) for coarse-grained segmentation. SDNs enable the network to be partitioned at a much more granular, or fine-grained, level. Also, because the segmentation is done in a virtual network that runs above the physical network, devices can be dynamically assigned to segments by policy. When the devices move, the policies will follow without any reprogramming of the network. This is critical for securing IoT endpoints.

Programmable network: SDN controllers expose APIs that application developers can use to interface with the network. For example, a video application could dynamically reserve bandwidth for the duration of the call and then release it when the call ends. Without APIs, developers would need to use vendor-specific scripts that invoke command line interface (CLI) commands, which requires a deep understanding of that vendor's network commands—something that most application developers do not have. Developers can access the programmable network directly via APIs or via automation by their cloud tools.

Hardware agnostic: Because an SDN runs as an overlay, the underlying network is transparent to it. This creates the widest range of choice for the business, as it can leverage the network that is currently in place. SDNs also enable companies to benefit from the cost advantages of commodity, white box switches, whose prices can equate to a savings of 50% or more compared to the cost of traditional network devices.

Lower cost of operations: SDNs are highly automated, so network managers no longer need to perform the highly repetitive, mundane tasks that are required with traditional networks. By offloading these tasks, network engineers can spend more time working on strategic initiatives instead of just "keeping the lights on."

Alignment of IT and application teams: A programmable, software-defined network shifts the network from hardware centric to software centric and enables network operations, the rest of IT and application development to operate at the same pace and align their goals. The only way to bring these resources together is with a programmable network.

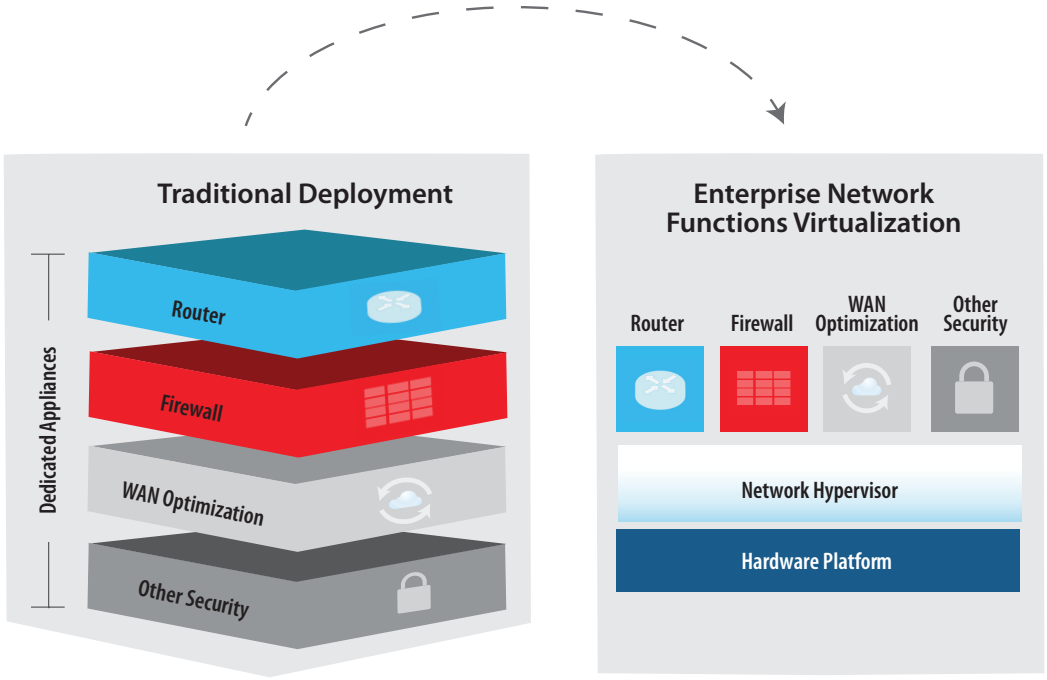
A software-defined network is an important step on the path to network modernization, but it doesn't solve all problems because network services are still tied to the underlying hardware. Functions such as security services, routing and WAN optimization are often tied to a dedicated appliance.

Network functions virtualization (NFV) changes this paradigm by decoupling the network functions from the underlying hardware platforms. The shift to NFV is similar to the transition that the compute industry experienced when server virtualization went mainstream. With server virtualization, applications ran as virtual workloads in software. Server virtualization consolidated hardware, lowered costs and improved compute utilization from approximately 25% to more than 75%. The benefits of server virtualization can now be applied to the enterprise network. NFV enables network services such as security functions, routing and optimization features to be run as a virtual workload in software (Exhibit 4).

To date, NFV has been used primarily by service providers, but recently it has become a priority for digital organizations. This is one reason why 61% of organizations are investigating or have deployed NFV, according to the ZK Research 2017 Network Purchase Intention Study (Exhibit 5).

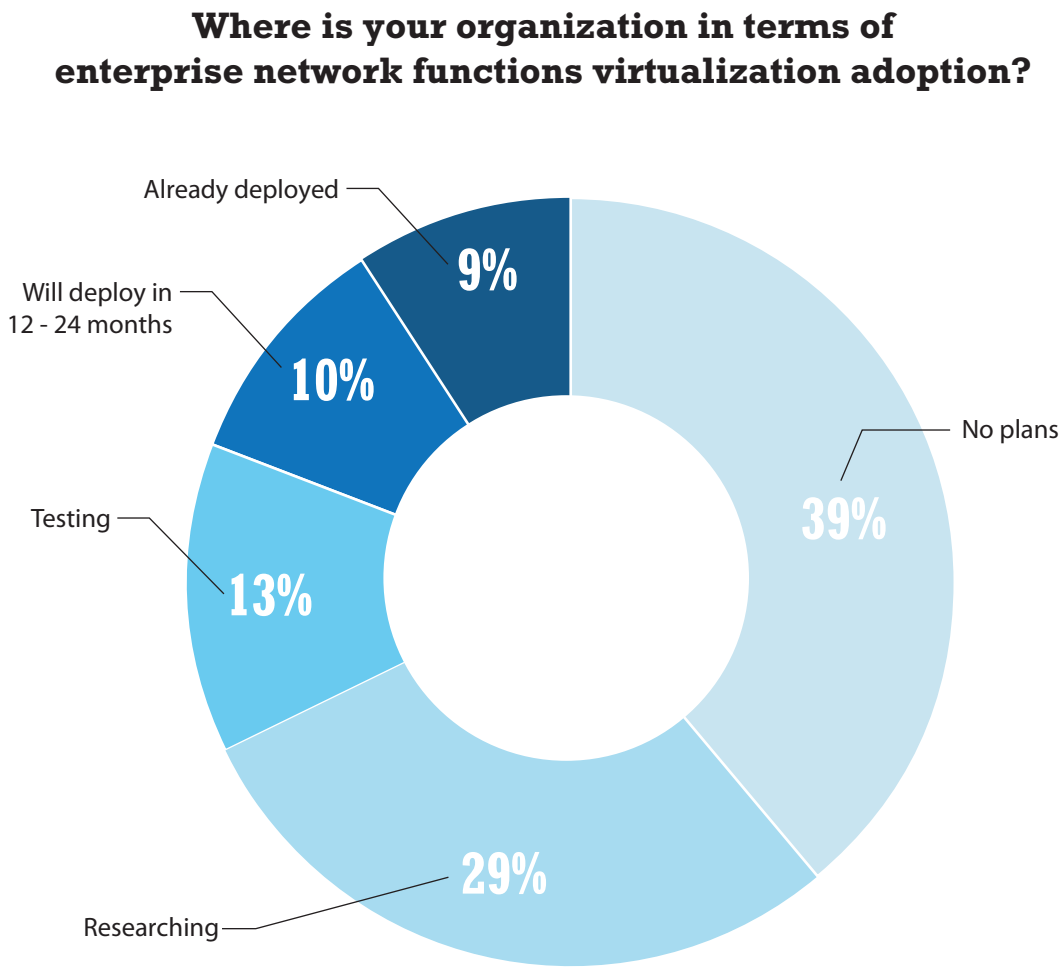
However, there is one significant difference between server virtualization and NFV. Server virtualization has primarily been used to consolidate servers in the data center. And while NFV has

Exhibit 4: NFV Brings Agility to Network Functions



ZK Research, 2017

Exhibit 5: NFV Is Seeing Strong Enterprise Adoption



ZK Research 2017 Network Purchase Intention Study

tremendous value in the data center, it can also bring value to other points in the network including the campus, branch offices and even the cloud.

Digital trends are rapidly changing the business landscape, and therefore organizations must think differently about the network. The network needs to become an enabler of business innovation instead of something that's holding the company back.

SECTION III: KEY ATTRIBUTES OF A MODERNIZED NETWORK

Network modernization must be at the top of every IT and business leader's priority list, as it is a critical component of digital transformation. However, solutions can vary greatly from vendor to vendor. It's critical that decision makers do not choose a vendor based on incumbency or market share. Rather, they should choose a vendor that can deliver a secure, agile and programmable network.

Businesses that embrace DevOps are highly agile, and the network must be equally flexible and dynamic.

The following list summarizes characteristics that companies should consider when selecting a strategic network vendor that will provide the platform for digital transformation:

Operates as a software overlay: The network solution should operate as an overlay to the physical network. This provides flexibility in deployment and investment protection, as the underlay network does not need to go through a "forklift upgrade"—leading to significant speed and cost advantages over a network composed of independent physical systems.

Provides network services and information delivered as APIs: Application developers need to access network services such as VPNs, single sign-on (SSO), network address translation (NAT) and quality of service (QoS) to secure and optimize application traffic. These services should be made available via RESTful APIs so that application developers can leverage them without requiring the assistance of a high-level network engineer.

Delivers a complete set of network services: Not all SDN solutions are created equal; some offer only a small set of network features. Therefore, ensure the solution includes all the key features required to operate a network such as switching, routing, firewalls, load balancing, VPN, cloud management and support for orchestration systems. These should be made available as NFV-based services.

Integrates with cloud management tools: A modern network addresses the challenge of long network provisioning times, labor-intensive tasks and human errors. The solution should offer native integration with leading cloud management platforms such as OpenStack and VMware vRealize.

Offers enhanced security: The solution should enable the business to segment the network into distinct security segments down to individual workload, regardless of the workload's subnet or VLAN. The network or other IT teams should have the ability to define policies and controls at an individual workload level. This helps stop breaches from spreading across the data center and to the rest of the enterprise network.

Aligns with DevOps: Businesses that embrace DevOps are highly agile, and the network must be equally flexible and dynamic. IT operations needs the ability to quickly spin services up and down to make changes that can keep up with the speed of application development.

Provides application continuity: Because SDNs abstract network control from the underlying hardware, security and network policies can be bound to workloads. Companies can quickly and easily replicate entire application environments for development or disaster recovery capabilities, which can be an important step in moving to a hybrid cloud.

It's crucial for businesses to embrace the concept of network modernization—and to start now.

SECTION IV: A 10-STEP PLAN TO A MODERN NETWORK

It's crucial for businesses to embrace the concept of network modernization—and to start now. However, the path to achieving a modern network may not be obvious. Therefore, ZK Research has outlined the following steps to help companies get started:

1. **Start the educational process now.** A new, modern network is quite different from a traditional network, and understanding this difference requires a mind-shift change across the company—starting with education by learning from peers and other organizations that have made the transition.

2. **Reskill network operations.** The skills needed to run a software-defined network are different from the ones needed today. A wide range of new skills are needed, such as programming, data analytics and scripting. It's critical for the longevity of network engineers that they become comfortable working with software, as that is becoming the norm across networking.

3. **Make decisions based on the need to automate, secure and improve resiliency.** Historically, network refresh was driven by the age of equipment, port speed and other technical features. Network purchase decisions should be made with digital success in mind and not technology.

4. **Align infrastructure operations and DevOps.** Digital transformation requires DevOps and infrastructure to be in lockstep. If these groups exist in silos, finger pointing and long delays in delivering applications to the workers or customers could result. These delays could be the difference between being a market leader and rapidly falling behind competitors.

5. **Once DevOps and infrastructure are aligned, set their goals at a business outcome level.** This means both groups should be measured on the success of specific business initiatives such as the quality of a mobile application, IoT deployments and data center modernization.

6. **Embrace software-defined networking as the first step in network modernization.** Get some quick wins by using SDN to automate repetitive, manually intensive tasks. This will free up valuable engineer time, cut down on downtime caused by human error and lower the operation costs required to run the network. The cost savings can be re-invested into the network to fund further advances.

7. **Leverage network functions virtualization.** NFV should be used to bring agility across the end-to-end network. For example, NFV can be used to quickly add a stateful firewall to a branch office that requires direct internet access.

8. **Implement micro-segmentation.** Once SDN and NFV are in place, the network should be segmented down to the workload level. This is particularly important for IoT deployments or in data centers where there is a large amount of lateral, or east–west, traffic. Micro-segmentation can contain threats by effectively containing the "blast radius."

9. **Consider using white-/brite-box switches.** Once the software overlay is in place, consider using white- or brite-box switches as a way to cut hardware costs. White boxes have basic operating systems and require the business to write software for more advanced features. For businesses that find this daunting, a brite box is similar to a white box but offers a more robust operating system and vendor support.

10. **Automate everything.** The utopian state for IT operations is to have a fully automated environment that is self-sustaining and managed through intent. Although this vision may never be achieved, businesses should aim to automate as many functions as possible. Start with the most repetitive tasks, which cause the highest amount of unplanned downtime and network problems.

SECTION V: CONCLUSION

The era of the digital business is here to stay. Today, competitive advantage is based on an organization's ability to be agile, adapt to changes and make rapid shifts to capture market transitions. Virtualization and the cloud enable businesses to have compute agility. However, the network remains relatively inflexible. The long lead times required to deploy, change and optimize the network can be considered the hidden killer of companies, as the true cost of staying with a legacy network is missed business opportunities. At best, these missed opportunities will result in a loss of market share and revenue; at worst, they could be the death knell of an organization. IT and business leaders must make a modernized network a top priority because doing so can align a company's network with its business goals by delivering a highly agile, dynamic network that can power any digital initiative.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314