RESEARCH
Influence and insight through social media

August 2018

The SD-WAN Provides the Fast Path to the

VIRTUAL CLOUD NETWORK

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: DIGITAL TECHNOLOGIES DRIVE NETWORK EVOLUTION

Digital transformation has moved out of the early-adopter phase and into mainstream adoption. According to the ZK Research 2018 IT Priorities Study, 88% of businesses now have digital initiatives underway, up from 84% in 2017. The urgency of IT and business leaders is well warranted, as companies that master being digital will leapfrog the competition and be able to sustain a market-leading position. Those that lag in their digital initiatives will fall farther behind and will struggle to survive.

The key to digital success is having an agile IT foundation that enables businesses to adapt to market transitions faster than the competition. However, there is no single technology called "digital transformation." Rather, it is powered by the following four key enabling technologies:

Mobile computing: Workers want the ability to perform any task from any location, and this has continued to drive the evolution of mobile computing. Based on ongoing research, ZK Research estimates that the number of smartphone users in the United States will reach 250 million by 2020. Mobile devices are already driving internet traffic to new heights. Statista found that in 2017, just over 51% of internet traffic came from smartphones. There's no question that mobility has changed the world and will continue to do so.

Cloud computing: The rise in mobile computing has caused businesses to find new ways of delivering applications. Traditional client/server computing was ideal in an era when the majority of users worked in an office. Cloud computing is tightly coupled with mobility, as data and applications are no longer tied to a single location. The ZK Research 2017 Cloud Forecast shows that by 2019, more workloads will exist in private and public clouds versus traditional on-premises models (Exhibit 1).

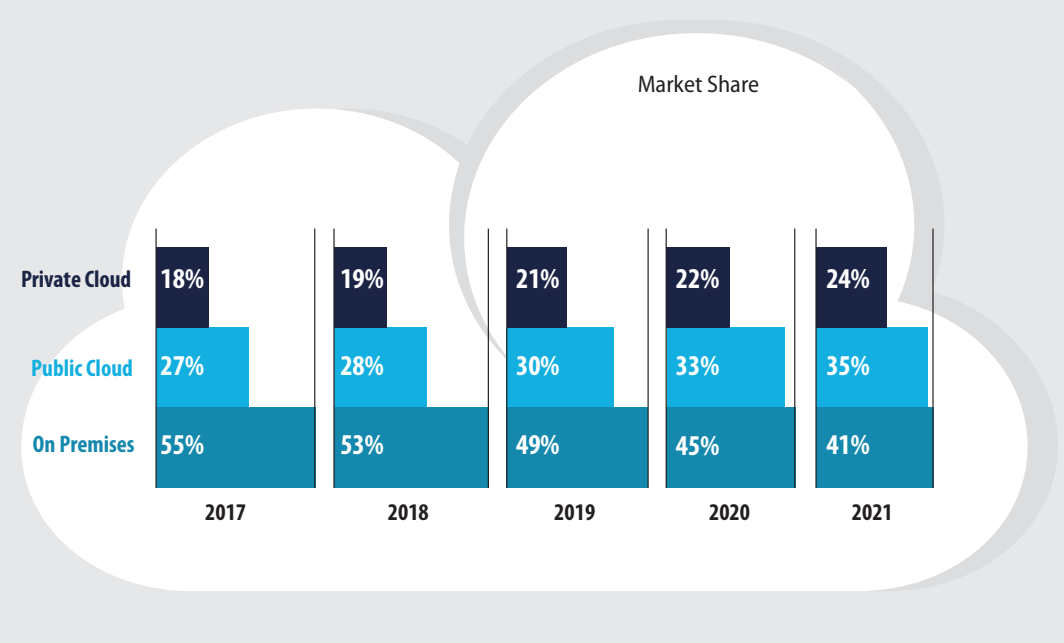
Internet of Things (IoT): Virtually everything is being connected today. Automobiles, lighting systems, appliances, healthcare equipment and anything else one can think of is being connected to company networks. In fact, the ZK Research 2018 IoT Forecast predicts that there will be 80 million connected devices by 2025. IoT creates new experiences and generates massive amounts of data that can be used to gain new insights on how to run the business.

Artificial intelligence (AI): A massive amount of data is being generated by several different systems. Deciphering the data to gain insights is critical to success in the digital era. Unfortunately, people can no longer analyze the data at the speed it is being generated. However, AI systems are able to "connect the dots" more accurately and faster than people. This is one reason why ZK Research has forecasted that by 2022, 80% of customer interactions will be completed by AI.

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.

Exhibit 1: The Growth of Private and Public Clouds



ZK Research 2017 Cloud Forecast

These four technologies have come together in a "perfect storm" scenario where they act as a single, massive force enabling businesses to make the jump to being digital. These technologies may seem unrelated, but they do have one point of commonality—they are all network centric.

This means that digital transformation success is highly dependent on the network. Unfortunately, most business networks are not ready for the demands of digital transformation. One of the biggest limitations of legacy networks is that they are highly dependent on hardware such as routers and firewalls. Devices such as these typically require configuration updates to be made on a device-by-device basis, meaning a change to the network—even a simple one—can often take months to complete, making the network very brittle. The ZK Research 2018 Network Purchase Intention Study found that the average time for an enterprise to implement a change network wide is four months, which is far too slow for a digital business.

Another issue that plagues existing networks is the lack of centralized visibility. The management tools currently used are device centric. So, for example, a network engineer might have a good idea as to what's happening with a specific router, but an understanding of end-to-end or application performance requires the aggregation of data from all of the devices and then the manual application of analysis. Even the most seasoned network professionals can no longer keep up because of the massive amounts of data being generated by networks today.

Also, legacy networks have no ability to leverage templates or centralized policies that can be applied from a centralized management console. Instead, updates to the network must be ap-

plied manually, leading to high amounts of human error—which is still the top cause of unplanned network downtime.

The network demands of digital businesses are significantly different from a decade ago, and traditional networks can no longer meet their needs. Therefore, it's time for a new type of network. A virtual cloud network is the right network for the digital era.

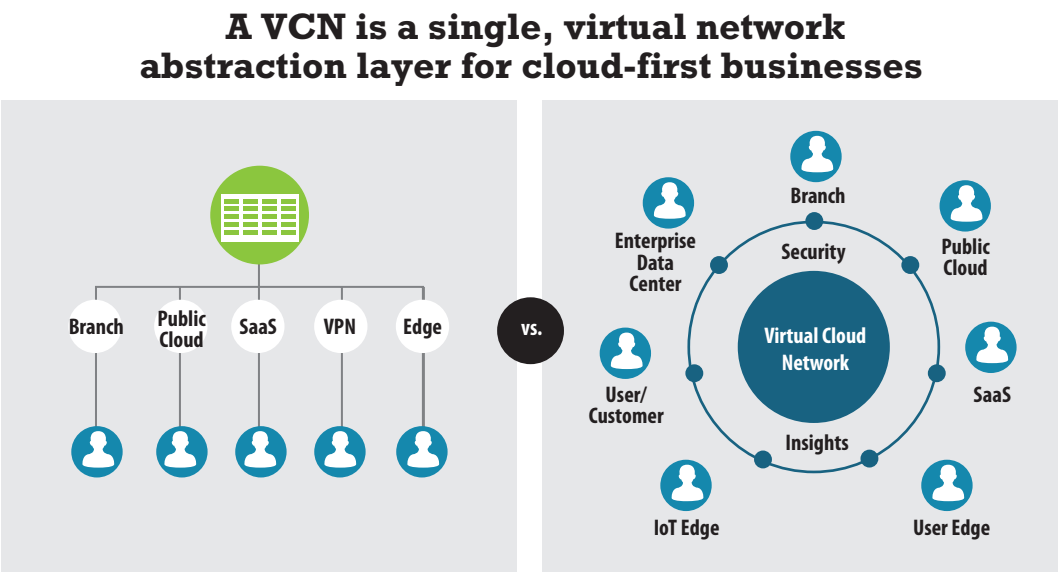
SECTION II: INTRODUCING THE VIRTUAL CLOUD NETWORK

The dynamics of a digital business are driving the need for a different type of network. Historically, a business network was composed of a set of networks that were independently managed. The left side of Exhibit 2 shows how network professionals manage the branch network separately from the network that connects businesses to the public cloud, which is managed independently from software as a service (SaaS), virtual private networks (VPNs) and edge networks.

A virtual cloud network (VCN) is the next big evolutionary step of the network, and it is optimized for cloud-first organizations. A VCN is a single network abstraction that creates operational consistency regardless of the underlying hardware or services and connects everything from the branch to the cloud to the data center. It provides pervasive connectivity for users to apps and for businesses to data, as well as intrinsic security, regardless of location. A VCN enables the vision of connecting any user to any application in any location to finally become a reality.

With a VCN, the branch, public cloud, SaaS, user edge, IoT edge and data center all run on a single, common network with a consistent set of services (as shown on the right side of Exhibit 2). This is possible because a VCN is built on the same principles that underlie the cloud. Consequent-

Exhibit 2: The Evolution of Branch Network Management



ZK Research, 2018

A VCN can meet the needs of everything from the smallest companies to the largest cloud-scale organizations equally.

ly, a VCN can meet the needs of everything from the smallest companies to the largest cloud-scale organizations equally.

The key characteristics of a VCN are as follows:

Automated: The provisioning, deployment and management of network and security services across the enterprise have historically been done manually, leading to high amounts of human error and slow deployment cycles. Automation can significantly speed this up and reduce unplanned downtime to zero. Also, automation will free up valuable engineering time, enabling those resources to focus on innovation and strategic initiatives.

Programmable: Application development and network operations are coming together, and programmers need the ability to access network services in order to build differentiated applications that create competitive advantage.

API accessible: The days of configuring the network and accessing information through a command line interface (CLI) have come to an end. Obviously, application developers will prefer to interface with the network via application programming interfaces (APIs), but so should network engineers who can manage the network through the same interfaces. This can greatly reduce the complexity associated with network operations.

Elastic: The cloud enables businesses to add compute and application resources on demand and then scale up capacity quickly. The network requires the same level of elasticity to ensure applications are performing optimally regardless of where workers, applications and data are located.

End to end: Network operations teams have historically treated the network as a set of discrete places, such as the campus, branch, data center and edge. Applications, of course, traverse all of these and require consistency in the areas of performance and security. A virtual cloud network considers the network in its entirety and removes these silos.

Autonomous: Over time, a virtual cloud network will be autonomous and dynamically reconfigure as the business environment changes as dictated by business policy. For example, if an organization decides that it's safest to put all IoT devices in a single, secure zone, and then something is moved out of the zone, the network should adapt to extend that segment.

Machine learning based: The network is generating massive amounts of network data—far too much for even the most experienced engineer to connect the dots to understand what is happening. Machine learning can be used to recognize breaches, spot congestion points that might be

impairing application performance and even predict when issues will occur so corrective action can be taken before they impact the business.

Application centric: Legacy networks are designed without considering what types of applications are currently running on them and what kinds of services and resources are required. A virtual cloud network is built with the needs of all types of applications—both cloud and on premises—in mind.

Consistent operations from data center to branch: With a VCN, networks will have operational consistency in every part of the network. This will significantly reduce the requirement to have high-level engineers dedicate huge chunks of time to performing repetitive tasks.

It's unlikely that any organization, no matter how technically astute, will be able to migrate its entire network to a VCN overnight.

It's important to understand that with a VCN, architecture matters. Without the necessary building blocks that utilize software-defined networking (SDN) principles and are virtual, flexible, scalable and cloud based, a true VCN can't happen. VCNs must have all of these characteristics for a seamless, integrated model to work. Without it, the entire structure falls apart.

It's unlikely that any organization, no matter how technically astute, will be able to migrate its entire network to a VCN overnight. This raises the question of where the shift to a VCN should begin. For many businesses, a software-defined WAN is the best starting point.

SECTION III: SD-WANS ARE THE BEST STARTING POINT FOR A VCN

Software-defined WANs (SD-WANs) are an entirely new way to think about wide-area networks. SD-WANs represent a shift away from the traditional hub-and-spoke architecture that has been in place for the better part of 30 years. This legacy model was ideally suited for client/server computing. But as businesses have become more dynamic, distributed and cloud centric, traditional WANs are proving to be far too brittle and operationally intensive.

The technical definition of an SD-WAN is a WAN in which the control and data planes have been decoupled, enabling the network to be managed centrally through software. From a business perspective, an SD-WAN is a network that can be defined by IT policies, which are defined by business objectives. Unlike a legacy WAN, in which network operations are isolated from the organization's objectives, an SD-WAN is tightly coupled with business priorities. The IT policies can then automate the configuration of changes or move traffic flows to ensure the network is meeting the needs of the business, making the network more agile.

The lack of network agility is the most obvious problem solved by an SD-WAN. The network cannot be agile if each remote location has independent functions on a standalone hardware appliance. An SD-WAN enables network services to be delivered to the remote office without the complexity of having a wide range of hardware deployed locally.

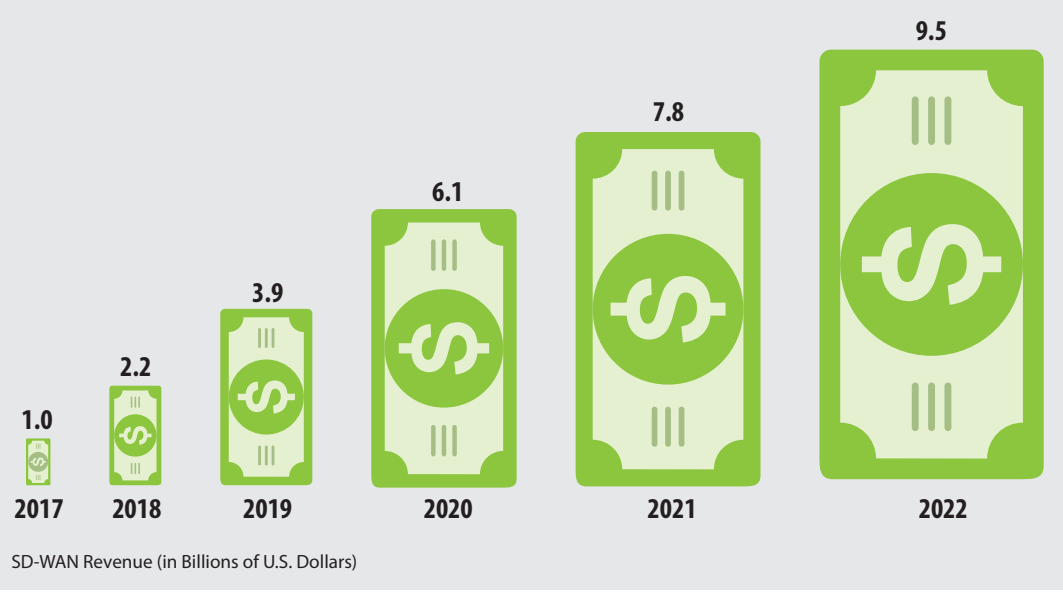
With legacy WANs, the policies are determined by network parameters such as IP address, port and media access control (MAC) address level. With SD-WANs, applications, identity and network functions determine policies. For example, a business policy may require a change in security policy, and this can be configured centrally and pushed out to every device in the network simultaneously, obviating the need to log in and reconfigure every box. The ability to centralize control functions to orchestrate the management of the network will greatly simplify and speed up network operations.

The rigidity of legacy hardware is one reason the branch router market is currently in decline. In contrast, the SD-WAN market is one of the fastest growing areas of IT spending. The ZK Research 2018 SD-WAN Forecast projects that SD-WAN revenue will grow from $1 billion in 2017 to $9.5 billion in 2022 (Exhibit 3).

Another benefit that SD-WAN brings compared to traditional WANs is the efficiency gained by leveraging broadband. Businesses can mix and match broadband and Multiprotocol Label Switching (MPLS) in any configuration to design the network to best meet their needs. This provides the following benefits:

Transport-independent network: Legacy networks use expensive MPLS as a primary connection and then an equally expensive network as the backup link. A hybrid WAN can leverage any combination of different network connections including MPLS, broadband internet or some form of wireless networks. This not only significantly reduces costs but also provides greater media redundancy; broadband and MPLS are often carried over different wires, while the wireless connections are conducted over the air.

Exhibit 3: SD-WAN Revenue Skyrockets Through 2022



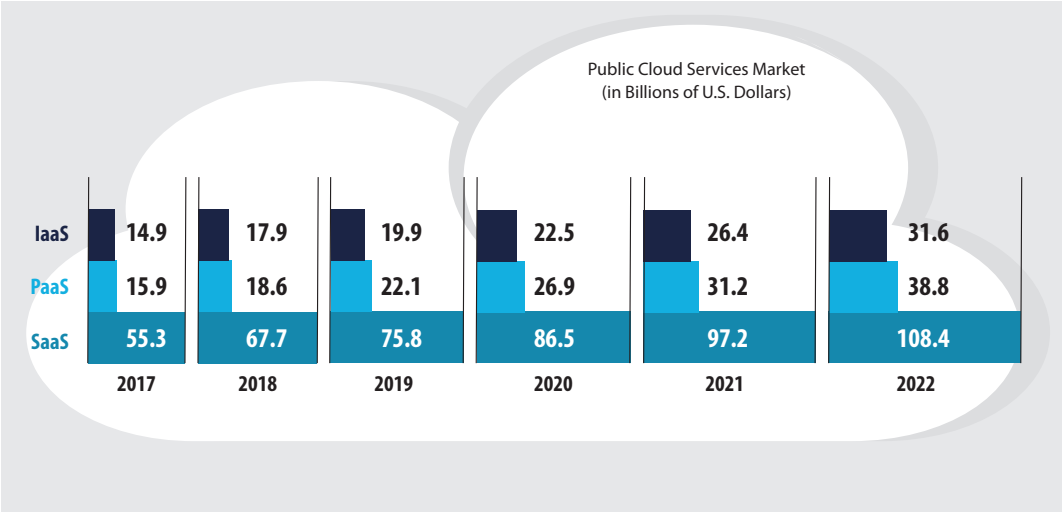
ZK Research 2018 SD-WAN Forecast

Active–active architecture: The active–passive architecture of legacy networks uses bandwidth highly inefficiently. With a hybrid network, all connections are active, creating greater agility regarding how the traffic flows. For example, a business may decide that mission-critical traffic flows over the MPLS connection and all other traffic connects over an internet-based VPN. The active–active architecture enables businesses to implement intelligent path selection, flow symmetry and traffic isolation with granularity down to the individual session level within each application.

Optimized for the cloud-computing era: Legacy WANs are ineffective for the cloud, as all internet traffic goes through a single choke point and then is distributed over the WAN to the remote location. A hybrid WAN offers secure, direct internet access so that cloud and mobile applications can directly use the entire network more efficiently. Optimizing the network for the cloud becomes increasingly important as the cloud continues to grow. Exhibit 4 highlights the importance of aligning the network with the cloud, as public cloud services will grow from $86.1 billion in 2017 to $178.8 billion in 2022. The cloud drives significantly different traffic patterns compared to client/server applications.

The growth of SD-WANs is tightly coupled with the growth of the cloud, making it a core component of a VCN. For most businesses, SD-WANs will provide the ideal starting point for a longer evolutionary transition to a VCN. Of all the "software-defined" segments, SD-WANs provide the fastest ROI, as the WAN is the biggest network for most companies and the most expensive to run. The transition from MPLS alone to broadband can often knock 40% or more off of a WAN budget.

Exhibit 4: The Growth of the Cloud Drives WAN Evolution



ZK Research 2018 Cloud Computing Forecast

The ease of deployment combined with the fast payback means the shift from a legacy network to an SD-WAN is a low-risk venture for most companies.

The additional budget returned from an SD-WAN can be used to facilitate the transition to a VCN in the data center, network edge or other part of the network.

Also, SD-WANs are relatively easy to deploy. They have been designed to be non-intrusive to branch operations. A business can transition to an SD-WAN by implementing a small, low-cost, zero-touch provisioning device in each location. The underlying hardware remains the same, and the SD-WAN infrastructure creates a highly dynamic and secure overlay. As the existing hardware comes to the end of its useful life, the network services can be moved to the SD-WAN appliance or the cloud.

For example, every branch office has a branch router, which can typically cost $5,000 or more per location. An SD-WAN appliance can be deployed alongside the router, where it provides SD-WAN–related services, and the router continues to route traffic. In a few years, the router will reach its end of life, and the routing can be moved to either the SD-WAN appliance or the cloud.

The ease of deployment combined with the fast payback means the shift from a legacy network to an SD-WAN is a low-risk venture for most companies. Another advantage is that services can easily be extended everywhere. SD-WANs are cloud managed, which follows the architectural principles of a VCN, and that management paradigm can be used across the end-to-end network—from the data center to the cloud and the branch.

One such service that is useful to encompass the entirety of the network is segmentation. IP networks are based on the concept that every device can communicate with every other device. This creates some obvious security challenges, as a single breached endpoint can affect every device on the company network. Segmentation enables virtual partitions to be created as an overlay to the physical network, limiting the access devices have to one another. For example, in a hospital, a policy can be created to dictate that all medical devices are in their own network segment. Similarly, a network segment can be created to ensure all guests are placed in a discrete segment. Because segmentation operates as an overlay to the physical network, the segments operate dynamically so the network can automatically adapt to changes.

Consider the case where medical devices are in a secure segment. Prior to SDNs, if a device moved, a network engineer would need to reprogram the network. With SDNs, the policies follow the devices, so the intent of the segmentation policy is always being met. SD-WANs enable organizations to create network segments across the wide-area network, which can then be extended to other areas as companies shift to a VCN.

This is true for other management and security policies and is a key step in migrating to a zero-trust environment, where no device can communicate with any other without being explicitly allowed. The concept of zero trust minimizes security risk, as it protects high-value assets from being infected by a breached low-value endpoint.

Also, analytics and visibility can be extended across the entire network. Most SD-WAN vendors have the capability to capture real-time application and network data. This data can be analyzed to understand the state of the network, where problems are currently occurring, and even predict when

Businesses that want to transition to a VCN have a choice of many solutions.

they might occur so corrective action can proactively be taken. Companies can implement this on their WAN with an SD-WAN and then expand it as other parts of the network migrate to a VCN.

SECTION IV: WHAT TO LOOK FOR IN A SOLUTION PROVIDER

Businesses that want to transition to a VCN have a choice of many solutions. ZK Research has identified the following key criteria to consider when making this decision:

Software based and cloud centric: A VCN should abstract the network services from the underlying hardware and be entirely software based. Also, the architecture should follow the principles of the cloud so it can be extended dynamically with no disruption to the business.

Hardware independent: Most SD-WANs are available on dedicated hardware, but they should also run on other types of hardware as well as software platforms such as virtual machines, the cloud and containers. This should also be true for the data center, IoT and other parts of the network.

Consistent operational model: Because a VCN operates as an overlay to the underlying hardware, it can be run from a single management console. The consistent operational model of the end-to-end network should be a key attribute of a VCN vendor.

Best-in-class SD-WAN: Since the starting point for a VCN will likely be an SD-WAN for many companies, the vendor should have a best-in-class SD-WAN. And while all vendors may claim this, customers should also look for a vendor that has a large customer base and is a leader in market share.

Integrated security: Security is a top priority for businesses, and IT leaders don't want their company to be the latest organization to make the news for being hacked. A virtual cloud network should include integrated security that is consistent with and naturally integrated across the entire solution.

Programmable infrastructure with rich APIs: A virtual cloud network should have a suite of programmable APIs that facilitate connections with a wide variety of applications. Also, the VCN should be programmable so that it can respond to traffic trends.

Automatable infrastructure: A VCN should have automation capabilities that make the network run autonomously or with minimal human interaction. Automation enables network professionals to offload repetitive tasks and find more time for strategic initiatives.

SECTION V: CONCLUSION AND RECOMMENDATIONS

Digital businesses are hyper-connected entities. Legacy networks were designed for a compute era that has been on the decline for decades. Businesses now need a different approach to the network—one that is aligned with the principles of the cloud.

A virtual cloud network can make the network a dynamic, agile and security IT asset capable of enabling the shift to a digital business. The move to a VCN must be a top priority for companies of all sizes. ZK Research offers the following recommendations to help businesses transition to a VCN:

Chart a path to a VCN to modernize the network. A VCN is a software-based, cloud-centric and hardware-independent network that follows the architectural principles of the cloud. The cloud, IoT, AI and mobility are driving the need for a different type of network—one designed to specifically meet the needs of a digital business—and a VCN delivers this.

Start the VCN journey with an SD-WAN. The ultimate goal of a VCN is to transform the entire network—from the core of the data center to the IoT and the user edge. However, it's unrealistic to change the whole network at one time, as that would be highly disruptive to the business. An SD-WAN is a low-risk starting point because it offers a quick payback and is fast to implement.

Compare vendors based on criteria unique to SD-WANs. In the past, technology vendors typically were compared using technical metrics such as the speed of the boxes and port density. SD-WAN vendors should be measured on factors critical to the success of an SD-WAN, including the following:

- Application performance improvements
- Speed of deployment
- Reduction in operational expenses
- Speed of configuration
- Policy-based control versus command-line interface

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314