2018 Guide to WAN Architecture and Design

Applying SDN and NFV at the WAN Edge

By ***Dr. Jim Metzler, Ashton, Metzler & Associates***
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Steven Taylor, Webtorials
Publisher and Editor-in-Chief
Co-Founder, Webtorials Analyst Division

Sponsored in part by:

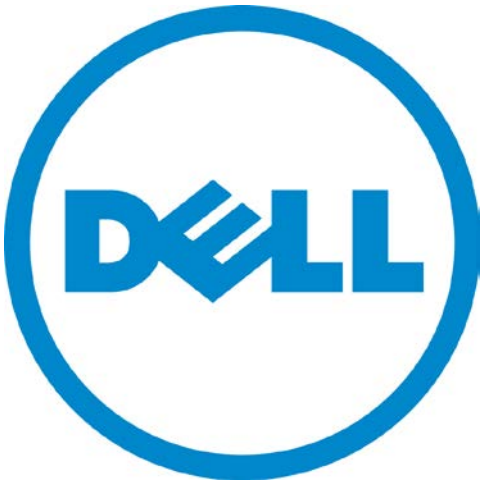


Table of Contents

Introduction

One of the goals of the 2018 Guide to WAN Architecture and Design (The Guide) is to discuss the state of WAN architecture and design with an emphasis on the current SD-WAN solutions. Another goal of The Guide is to provide insight into the emergence of solutions that leverage the key concepts of SDN and NFV to support all components of the WAN edge.

A discussion of wide area networking is extremely timely for two reasons. One reason is that for most of the last fifteen years there has been little investment in the development of new WAN technologies and services. Hence, until the development of Software Defined WANs (SD-WANs) there hadn't been a fundamentally new WAN technology or service introduced into the marketplace since the turn of the century.

A discussion of the WAN edge is also very timely. One reason for that is the burgeoning use of the Internet of Things (IoT). For example, Gartner has forecasted that 8.4 billion connected things will be in use worldwide by the end of 2017, up 31% from 2016, and that there will be 20.4 billion connected things by 2020.

The Guide consists of three chapters which were published in a serial fashion in late 2017 and early 2018. This document is a compilation of the three chapters which are:

- **Chapter 1: State of the WAN**
  This section provides insight into the current state of the WAN, the status of SD-WAN adoption and the status of the branch office. It is based on surveys that were distributed in the March to August 2017 timeframe.

- **Chapter 2: Key Considerations when Choosing new WAN and/or Branch Office Solutions**
  This section discusses a range of considerations that network organizations need to keep in mind as they evaluate alternative SD-WAN and SD-Branch solutions. This discussion is intended to ensure that network organizations choose solutions that meet both their current and their future requirements and which are, to the maximum degree possible, future-proof.

- **Chapter 3: The SD-WAN and the SD-Branch Office Ecosystem**
  This section identifies the ecosystem of vendors who supply SD-WAN and/or SD-Branch Office solutions.

In addition, an executive summary is available.

The State of the WAN

Background

Concerns with WAN Services

Network organizations currently make relatively little use of wired WAN services other than MPLS and the Internet. The concerns that network organizations have with those two WAN services are shown in **Table 1** in descending order of importance.

Table 1: Concerns with WAN Services

Concerns with MPLS	Concerns with the Internet
Cost	Security
Uptime	Uptime
Latency	Latency
Lead time to implement new circuits	Cost
Security	Packet loss
Lead time to increase capacity on existing circuits	Lead time to increase capacity on existing circuits
Packet loss	Lead time to implement new circuits
Jitter	Jitter

Wireline services are not the only WAN services that have limitations. Some of the limitations that are associated with cellular services include:

- Variable signal coverage;
- Link setup latency;
- Constantly evolving specs; e.g., 3G, 4G, LTE, XLTE, 5G;
- Security;
- Effectively supporting multiple carriers at once.

Another concern was highlighted in The 2017 Guide to WAN Architecture and Design. As that document highlighted, only 13% of network organizations have all of the visibility they need to troubleshoot WAN-related performance problems while 20% of network organizations stated that the visibility they have is barely adequate.

State of the WAN

Factors Impacting the WAN

The Survey Respondents were presented with fifteen factors and asked to choose the three factors that would likely have the most impact on their WAN over the next twelve months. The factors that were the most important are shown in **Figure 1**.

Figure 1: Top Five Factors impacting WAN

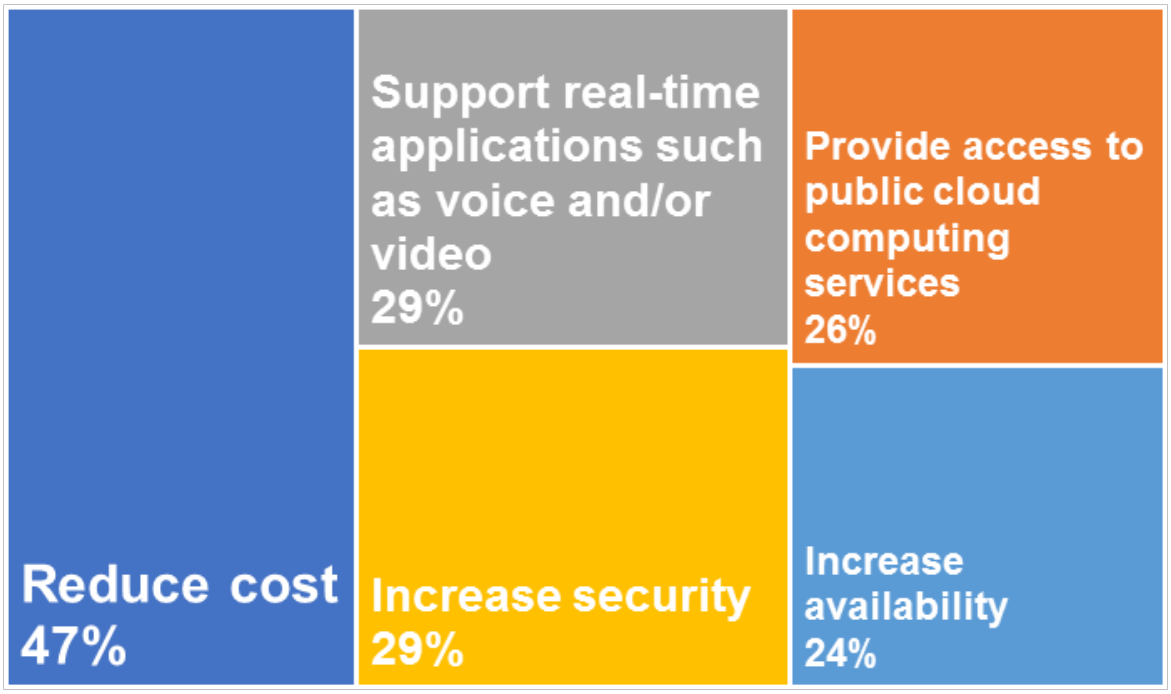


Figure 1 highlights the fact that WAN use cases have changed significantly since MPLS-based branch office WANs were first deployed roughly fifteen years ago. For example, fifteen years ago providing access to public cloud computing services was not a concern when architecting a WAN. Today it is one of the top concerns.

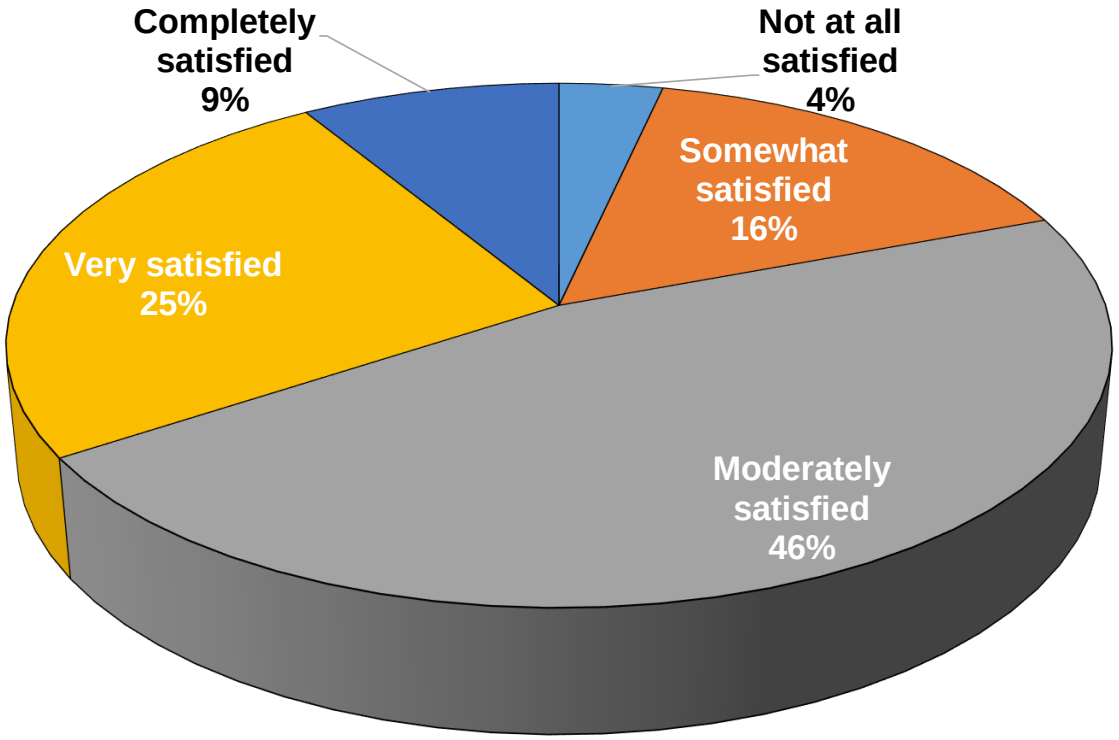
In addition, while not shown in **Figure 1**, thirteen percent of The Survey Respondents also indicated that supporting mobile users is one of the top factors impacting their WAN and twelve percent of The Survey Respondents indicated that supporting the IoT was one of the top factors impacting their WAN. These concerns were of little if any importance as recently as a few years ago.

Why is this important?	Given the pressure to support these new use cases, network organizations should evaluate WAN architectures in large part based on their ability to effectively provide access to public cloud computing services, support mobile workers and support the IoT.

Satisfaction with the Current WAN Architecture

The Survey Respondents were asked to indicate how satisfied their organization was with their current WAN architecture. Their responses are shown in **Figure 2**.

Figure 2: Satisfaction with Current WAN Architecture



Why is this important?	The fact that two thirds of network organizations are at best only moderately satisfied with their current WAN architecture indicates that a large portion of the WAN marketplace would likely be receptive to alternative WAN architectures.

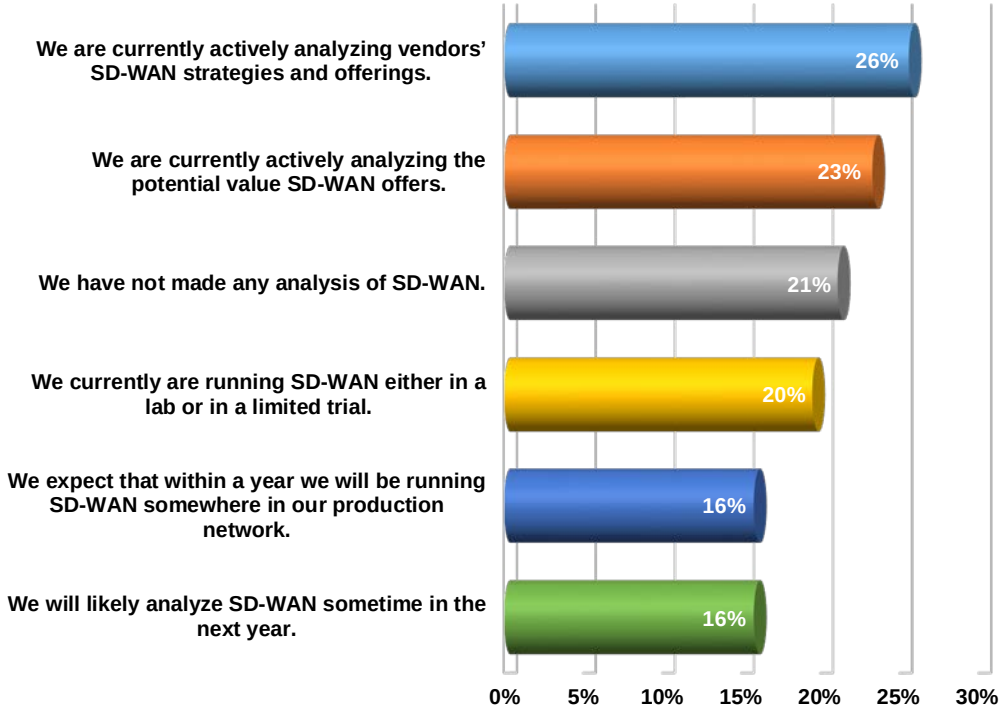
Software Defined WANs (SD-WANs)

Plans for Evaluating and Implementing SD-WANs

Figure 3 shows the six primary ways that network organizations are approaching SD-WAN adoption. The topic of how network organizations are approaching SD-WAN adoption was also analyzed in *The 2017 Guide to WAN Architecture and Design*. While the order has changed somewhat, the approaches shown in Figure 3 are the same approaches that bubbled to the top last year. In addition to the order, the relative popularity of each approach has also changed somewhat. Last year 17% of the respondents indicated that their organization was actively analyzing vendors's SD-WAN strategies and offerings. This year that rose to 26%. Last year, 10% of respondents indicated that they expected that within a year that their organization would be running SD-WAN somewhere in their production network. This year that rose to 16%.

One of the most interesting changes in the year-over-year data doesn't show up in **Figure 3**. Last year, 5% of the respondents indicated that they were running SD-WAN functionality in their production network. This year that rose to 9%.

Figure 3: Primary SD-WAN Evaluation and Implementation Plans



Why is this important?

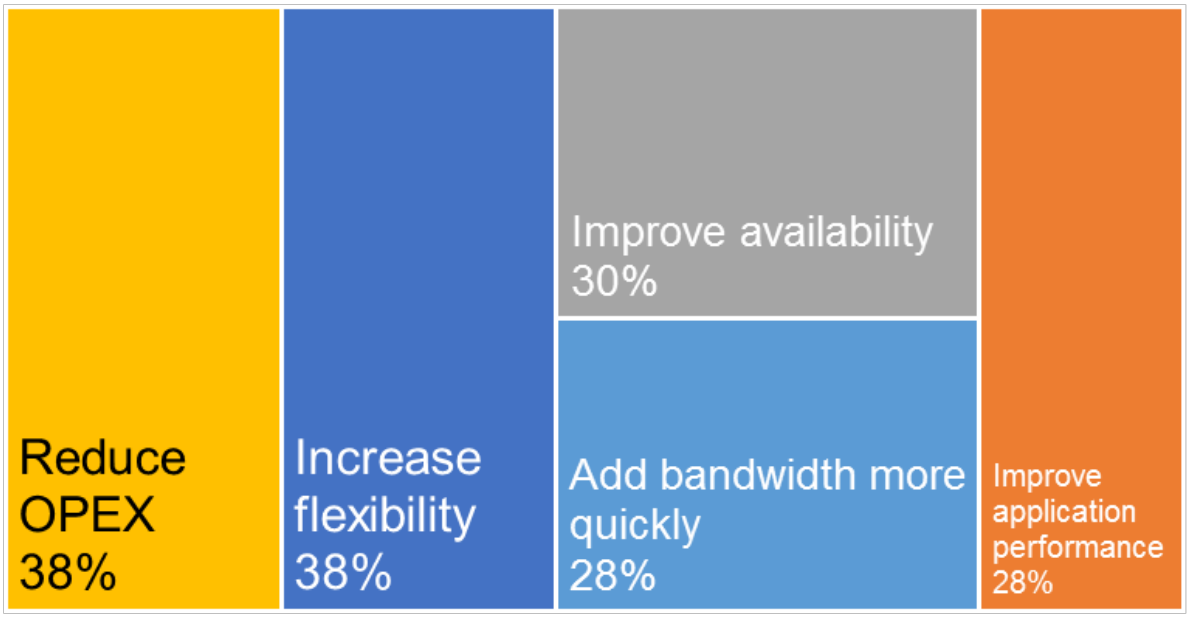
The combination of the fact that year-over-year more organizations are running SD-WAN functionality in production, that more expect to put it into production within the next year and that more are actively analyzing vendor's SD-WAN strategies and offerings suggests that the adoption of SD-WANs will increase significantly over the next year.

The Drivers of SD-WAN Adoption

The Survey Respondents were asked to indicate the three primary factors that would drive their company to implement an SD-WAN. The top five factors are shown in **Figure 4**.

The drivers and inhibitors of SD-WAN adoption were also analyzed in *The 2017 Guide to WAN Architecture and Design*. As shown in Figure 4, reducing OPEX and increasing flexibility are the two top factors currently driving SD-WAN adoption and these were the top two factors in last year's report. The biggest change in the top five factors year-over-year is that improve availability, which came in sixth last year, jumped up to third place in this year's survey and improve security, which came in fifth last year, dropped down to seventh.

Figure 4: Top five advantages driving SD-WAN adoption



Why is this important?	The fact that the perceived advantages of SD-WAN adoption match up so well with the primary factors currently impacting the WAN (**Figure 1**) indicates that at least at the conceptual level, SD-WANs are a very appropriate solution for most of the current and emerging WAN-related requirements.

The Inhibitors to SD-WAN Adoption

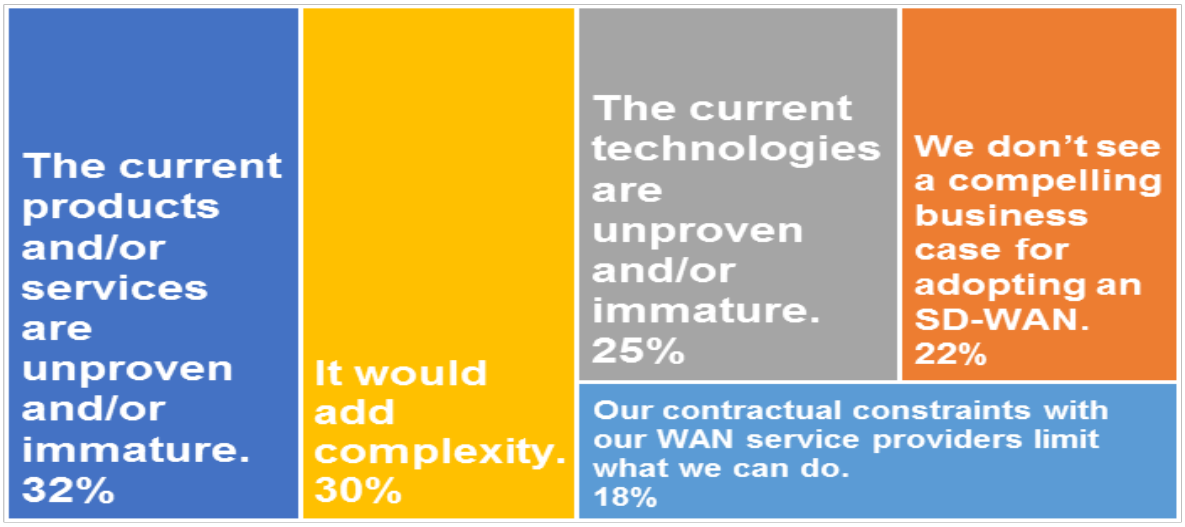
In *The 2017 Guide to WAN Architecture and Design*, the top two inhibitors to SD-WAN deployment were that the current ***technologies*** are unproven and/or immature and that it would add complexity. These were followed by:

- We don't see a compelling business case for adopting an SD-WAN
- The current ***products and/or services*** are unproven and/or immature;
- It would increase CAPEX.

As shown in **Figure 5**, the top four inhibitors last year are the same at the top four inhibitors this year. One minor difference year-over-year in terms of the inhibitors is that concerns that an SD-WAN would increase CAPEX dropped out of fifth place and was replaced by concerns over contractual constraints.

A major difference year-over-year relative to the inhibitors to implementing an SD-WAN is that each of the inhibitors is less important this year than it was last year. For example, last year 37% of the respondents indicated that they didn't see a compelling business case for adopting an SD-WAN. This year that dropped to 22%.

Figure 5: Top 5 inhibitors to implementing an SD-WAN



Why is this important?

The fact that each of the inhibitors to implementing an SD-WAN solution is less impactful than it was last year is an indicator that SD-WANs will soon be broadly adopted. However, if not resolved, the issue of complexity, which is raised again later in this document, could significantly hinder that adoption.

Preferred Location of WAN Functionality

In contrast to traditional WAN architectures in which most of the underlying functionality is hosted on premise, in the emerging WAN architectures there are several places to host functionality such as orchestration, control and security. Those locations include:

- At the customer's branch offices;
- In a service provider's central office;
- At the customer's regional office or data centers;
- At a co-location facility;
- At a public cloud provider's facility.

The Survey Respondents were asked to indicate where their organization thinks that WAN functionality such as control, optimization and security should be located. Their responses are shown in **Figure 6**.

Figure 6: Location of WAN Functionality

Why is this important?

There is a shift underway in terms of how network organizations are thinking about WAN architecture. One characteristic of that shift is that the interest in housing all WAN functionality onsite is relatively low. Another characteristic is that the interest in housing at least some WAN functionality in the cloud is very high.

Choice of Implementation Options

When network organizations evaluate new WAN solutions they have a variety of implementation options to consider. This includes:

- Do-it-Yourself (DIY)

  In this option, network organizations perform all facets of the lifecycle of a WAN solution; i.e., the planning, designing, implementing and ongoing management of the solution.

- Managed Service

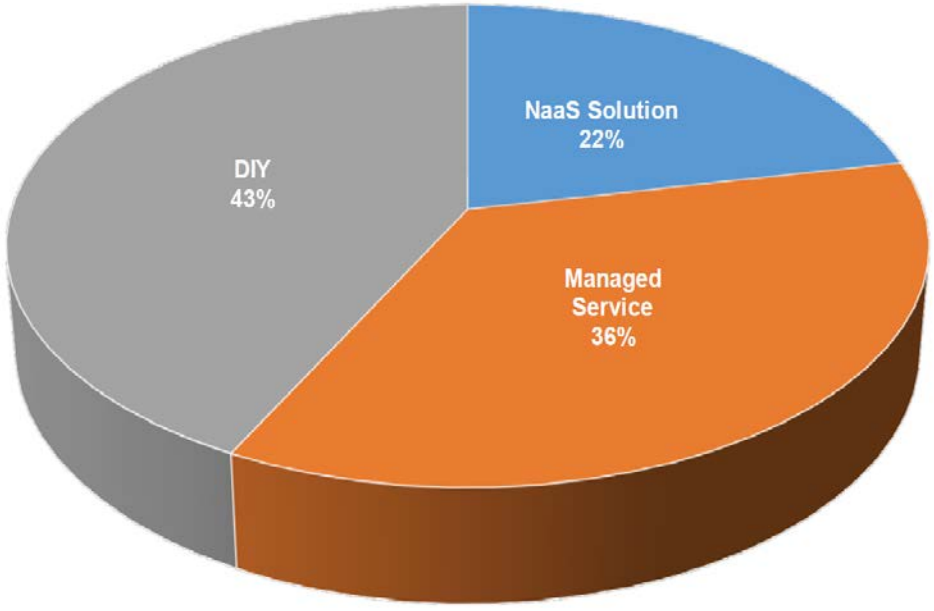
  In this option a 3rd party takes on the responsibility for all facets of the lifecycle of a WAN solution.

- Network-as-a-Service (NaaS)

  Numerous Communications Service Providers (CSPs) have either already launched or have announced their intention to launch a NaaS offering based on SDN and/or NFV.

The Survey Respondents were asked to indicate which implementation option their organization was most likely to implement. Their choices are shown in **Figure 7**.

Figure 7: Location of WAN Functionality



Why is this important?

One way to look at the survey results is to conclude that the DIY option is the preferred option. Another way to look at the survey results is to observe that a solution provided by a 3rd party, whether that is a managed service provider or a NaaS provider, is preferred over the DIY option by a wide margin.

Choice of Vendors

After more than a decade with little change in the available WAN products and services, the last few years has seen the emergence of a broad range of new WAN-related products and services from tens of vendors, many of them new to the WAN market. Whenever there is a transition point in IT, such as the one that exists now in the WAN market, there is the potential that some vendors will gain market share and that some will lose market share.

The Survey Respondents were asked to indicate how their organization would likely approach the selection of a WAN vendor. Their responses are shown in **Figure 8**.

Figure 8: Interest in Looking for New Vendors

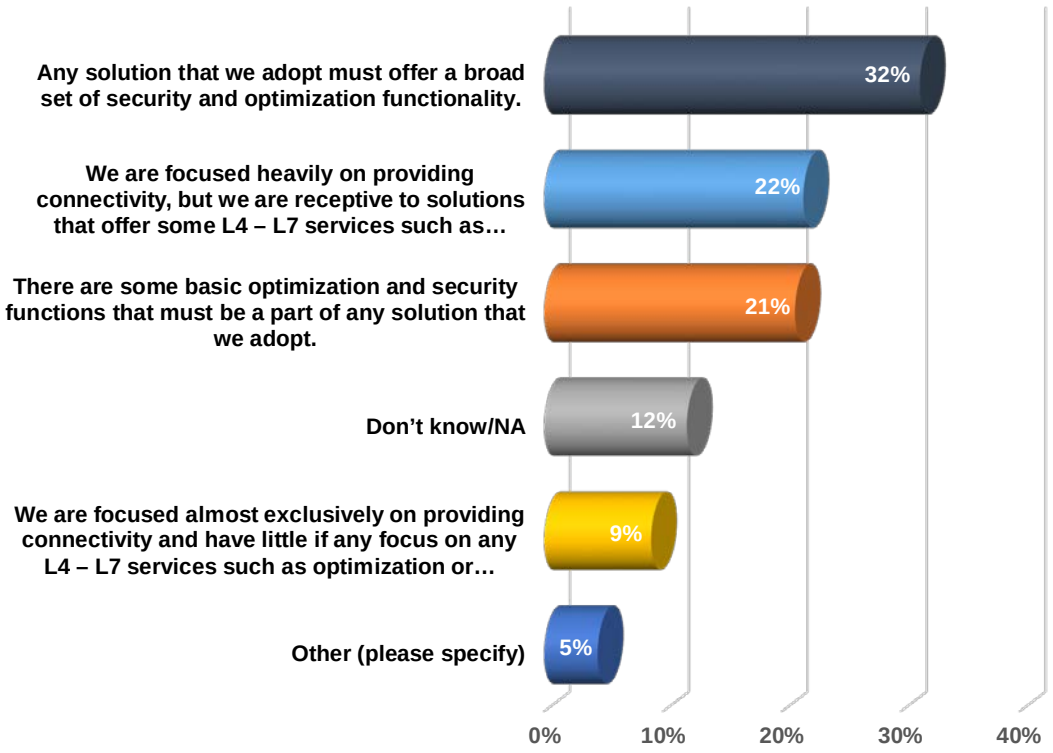
Why is this important?	The fact that so many network organizations are willing to explore alternative vendors puts pressure on the incumbent vendors and makes it unlikely that the market will converge onto a small number of providers in the short term.

Desired Functionality

Most of the initial SD-WAN solutions focused very heavily on providing low cost WAN connectivity. For many providers, that focus has expanded over time by the provider adding more functionality either on their own or through partnerships.

The Survey Respondents were asked to indicate their interest in SD-WAN solutions that offered a range of L4 – L7 functionality. As shown in **Figure 9**, in the current environment, companies are more likely than not to want the SD-WAN solution they implement to have at least some basic optimization and security functionality.

Figure 9: Interest in Highly Functional SD-WANs



The survey question focused on functionality such as optimization and security. Another alternative was raised by one of the respondents who wrote in that his/her organization was focused on solutions which provide application performance visibility and management.

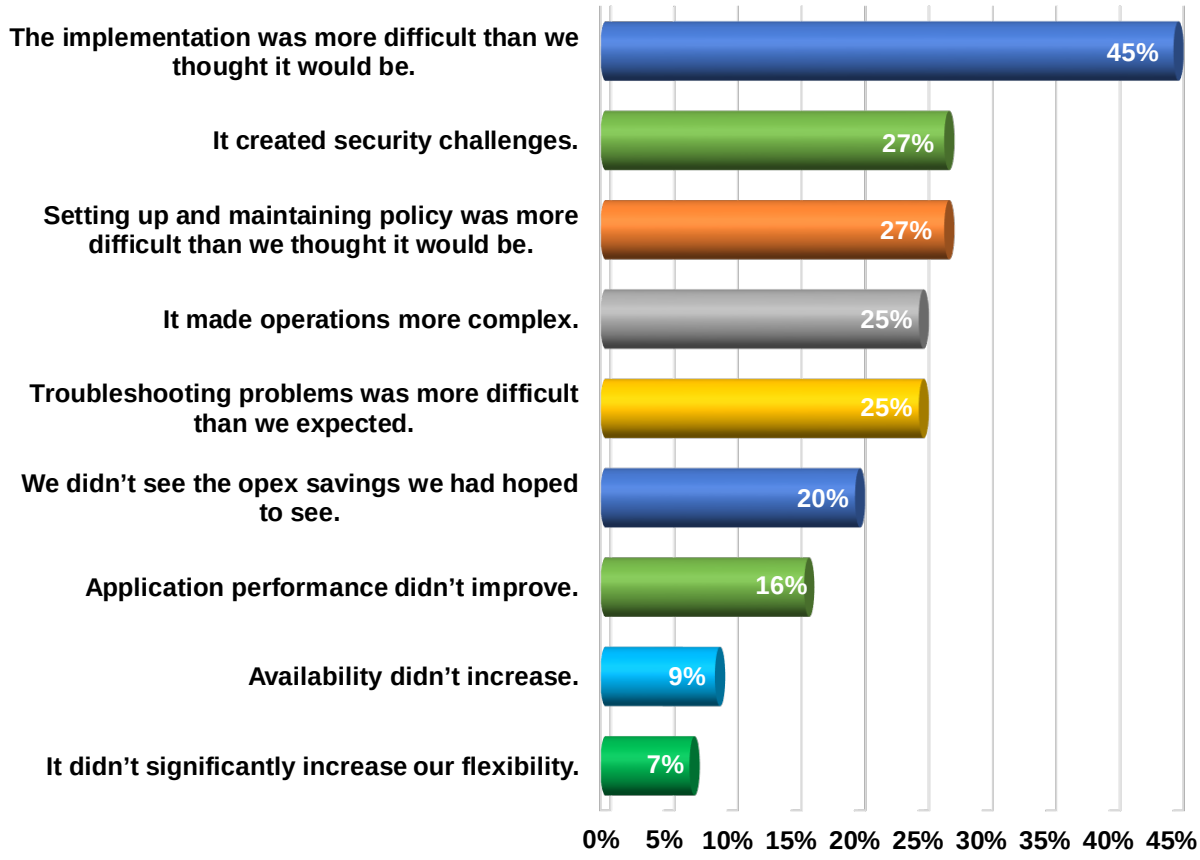
Why is this important?

Given how competitive the SD-WAN marketplace is, the strong interest that network organizations have in SD-WAN solutions that feature L4 – L7 functionality is likely to cause a virtuous cycle in which future SD-WAN solutions feature increasing amounts of higher level functionality. This raises two possibilities. One possibility is that SD-WAN solutions will become the basis of next generation branch office solutions. The other possibility is that SD-WANs will become just one feature of a next generation branch office solution.

Primary Deployment Issues

The Survey Respondents were asked to indicate the issues their organization experienced when they either conducted a POC of an SD-WAN solution or implemented a solution in their production WAN. Their responses are shown in **Figure 10.**

Figure 10: Issues in Initial SD-WAN Deployments



Some of the respondents also wrote in issues that were not included in the survey question. The two issues that were mentioned the most were:

- Integrating an SD-WAN solution with the existing WAN during the transition is very complex.
- Implementing an SD-WAN changes how operations are performed and changing how people work is a complex task.

Why is this important?

Knowing the issues that the early adopters have experienced should help network organizations anticipate those issues and hence either eliminate or minimize their impact. Unfortunately, **Figure 10** supports the previously stated belief that at least some of the current SD-WAN solutions are highly complex to implement and manage.

State of the Branch Office

Current Deployment of Servers and Appliances

The Survey Respondents were asked to indicate how many physical servers, virtual machines, physical appliances and virtual appliances there are in one of their company's mid-sized branch offices. Their responses are shown in **Table 2**.

Table 2: Presence of Servers and Appliances in a Medium Sized Branch Office

	None	1 or 2	3 or 4	5 or 6	7 or 8	9 or more
Physical servers	23%	45%	11%	8%	3%	9%
VMs	40%	21%	10%	10%	9%	10%
Physical appliances	17%	45%	14%	10%	2%	11%
Virtual appliances	55%	20%	8%	5%	4%	8%

Table 2 indicates that the vast majority of companies have at least one server and one physical appliance in each mid-sized branch office. It also indicates that roughly one third of companies have 3 or more servers in each of their mid-sized branch offices and a slightly higher percentage has 3 or more physical appliances in each of their mid-sized branch offices. It is reasonable to expect that there are more servers and appliances in large-sized branch offices.

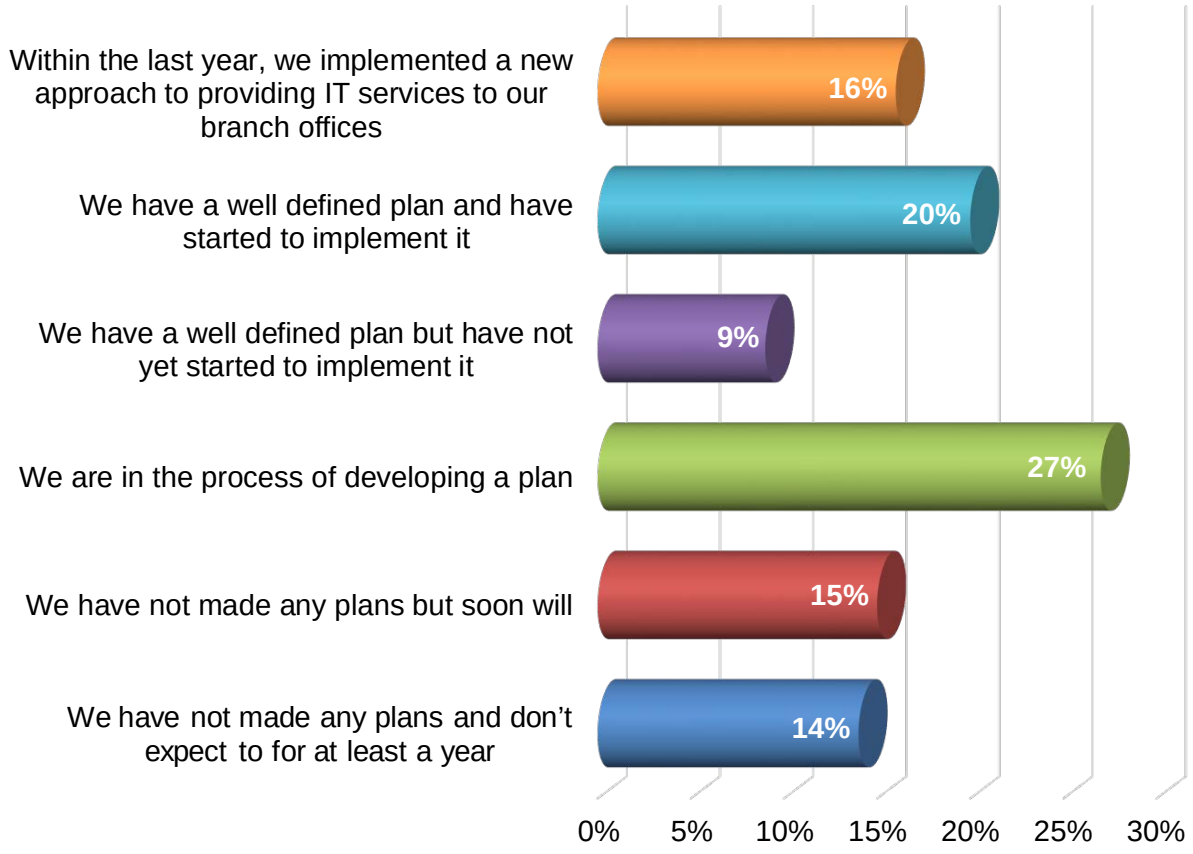
Why is this important?

The data indicates that there is a lot of distributed IT hardware that currently must be implemented and managed. The amount of distributed IT hardware is a measure of the possible operational and financial gains that could be made through the virtualization and consolidation of branch office functionality.

Planning for the Evolution of the Branch

The Survey Respondents were given a list of alternatives and were asked to indicate which alternative best described the planning that their IT organization is currently doing or has done over the last year relative to re-thinking how it provides IT services to its branch offices. Their responses are shown in **Figure 11**.

Figure 11: Branch Office IT Service Evolution



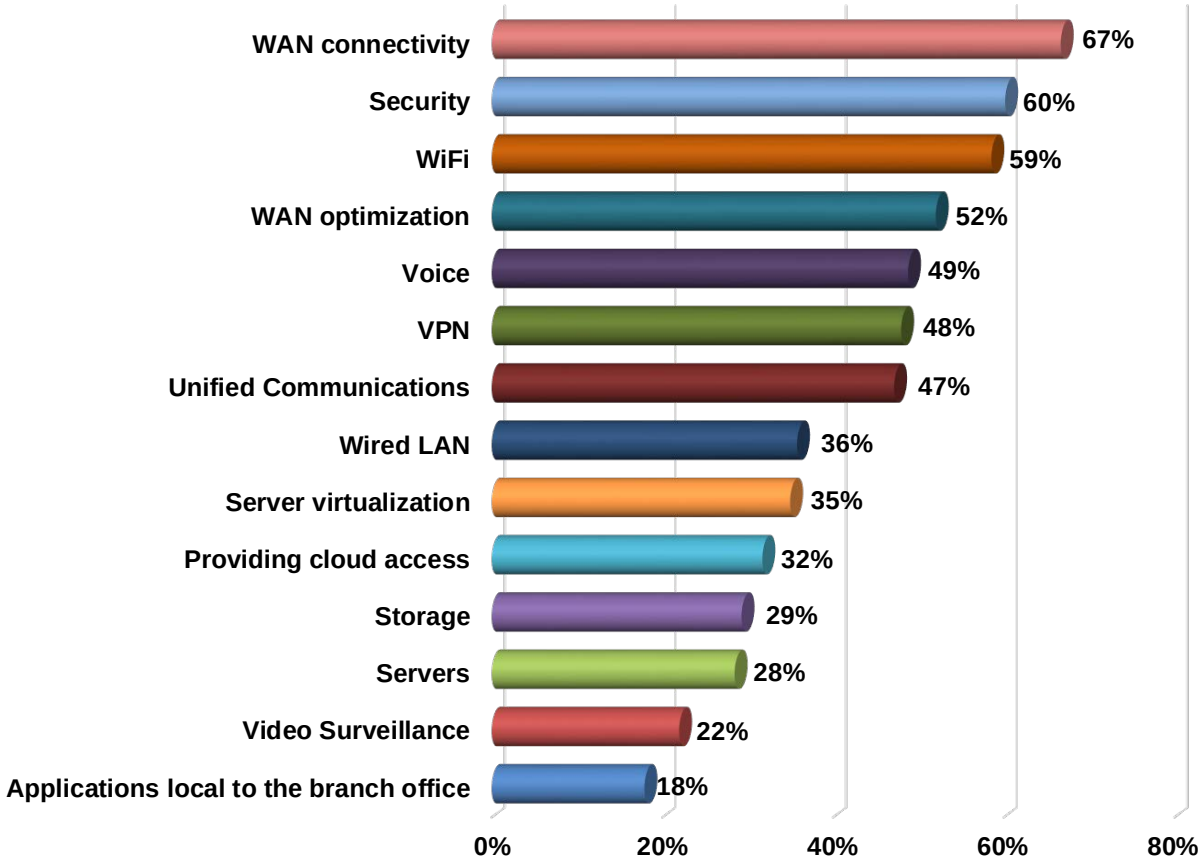
Why is this important?

The fact that only a small percentage of IT organizations have no interest in the short-term relative to the planning for the evolution of their branch office indicates how important this topic is to most IT organizations. That fact that 16% of IT organizations have recently implemented a new approach to providing IT services to branch offices has two important implications. One is that the movement to adopt a next generation branch office is in the early stages. The other is that the movement to adopt a next generation branch office is slightly further along the adoption curve than is SD-WANs.

Breadth of Branch Office Functionality

The Survey Respondents were asked, “If your organization has recently developed a plan, or if you are in the process of developing a plan for how to provide IT services to your company’s branch offices, which of the following functionality and/or requirements are included in that plan?” Their responses are shown in **Figure 12**.

Figure 12: Branch Office Breadth of Functionality



Why is this important?

The data shows that there is a strong linkage between planning for the evolution of branch offices and planning for the evolution of WAN connectivity. The data also shows that the plans that IT organizations are making relative to the evolution of their branch offices include a broad range of functionality.

Current and Intended Use of Virtualization

The Survey Respondents were asked to indicate the percentage of the network and security functionality that is in one of their company's typical mid-sized branch offices that is currently virtualized. They were also asked to indicate the percentage that will be virtualized by the end of 2018. Their responses are shown in **Table 3**.

Table 3: Amount of Branch Office Virtualization

	0%	1% to 25%	26% to 50%	51% to 75%	76% to 99%	100%
Now	42%	26%	18%	5%	5%	3%
End of 2018	13%	38%	14%	15%	12%	7%

Why is this important?

The data shows that by the end of 2018 that the vast majority of IT organizations will have virtualized at least some of the network and security functionality in their branch offices. The data also shows that one third of IT organizations expect that by the end of 2018 that they will have virtualized the majority of the network and security functionality in their mid-sized branch offices.

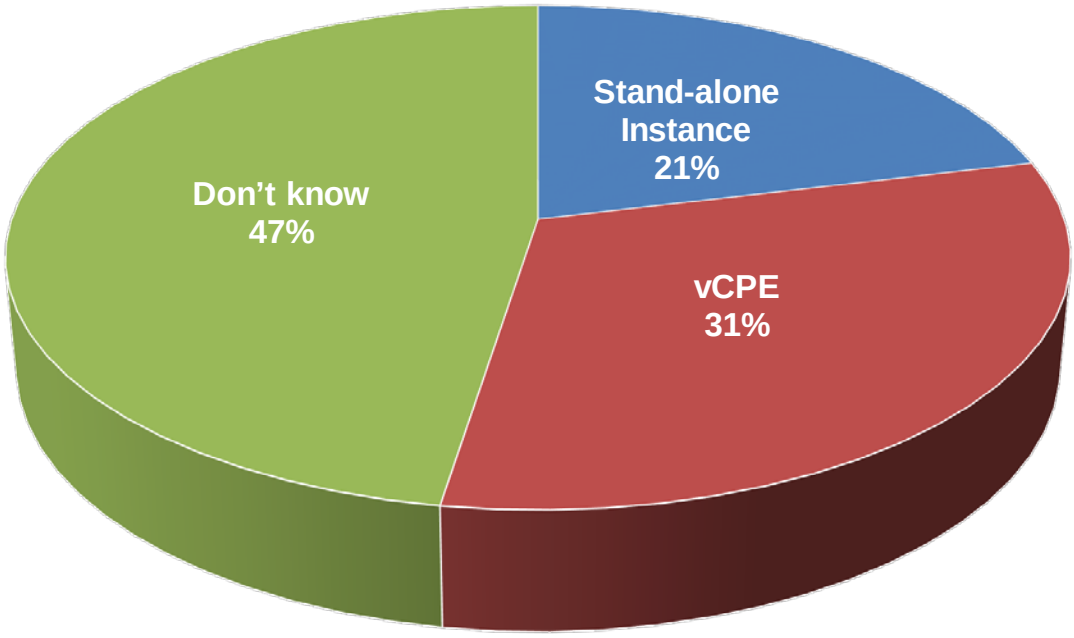
How Branch Office Virtualization will be Implemented

The Survey Respondents were asked to indicate the approach that their organization will take to virtualizing branch office functionality by the end of 2018. They were given the following two approaches as options:

- The virtualized functionality will run as a standalone instance on one or more servers that we provide
- The virtualized functionality will run as a component on a virtualized CPE (vCPE) that was designed to integrate multiple virtualized network functions (VNFs)

Their responses are shown in **Figure 13**.

Figure 13: Branch Office Virtualization Implementation Approach



Why is this important?	The data shows that there is significant interest in using virtual CPE as the basis for implementing virtualized functionality in branch offices. However, the data also indicates that there is still a lot of uncertainty about how IT organizations will implement virtualization in branch offices.

Key Considerations when Choosing new WAN and Branch Office Solutions

It is universally accepted that reducing cost is a key consideration when evaluating alternative WAN and branch office solutions. However, cost isn't the only consideration and choosing the solution with the lowest cost isn't always the best decision. Because of that, this publication will identify and discuss several considerations other than cost, that should be included in the evaluation of alternative WAN and/or branch office solutions.

The majority of considerations discussed in this publication fall into two categories. One category is the business challenges that network organizations may be facing now, or will likely face in the near term; e.g., supporting the Internet of Things (IoT). Network organizations will not be successful if they implement solutions that respond only to today's challenges. To be successful they must implement solutions that also respond to the challenges that their organization will face in the near term. This puts pressure on network organizations to correctly identify those challenges.

The other primary category of considerations is the emerging set of IT technologies and techniques. It is highly unlikely that the optimum solution to emerging business challenges will be constructed entirely of legacy technologies and techniques. This puts pressure on network organizations to correctly determine which of the emerging technologies and techniques will both meet their needs and be successful in the market.

How network organizations incorporate the considerations discussed in this publication into their evaluation of alternative WAN and branch office solutions will vary based on the nature of each of the considerations. Two of the considerations that exemplify that concept are:

- Complexity
- Software defined

Nobody would argue against reducing complexity. However, complexity is hard to measure and as a result it is difficult to quantify how much complexity a given solution will reduce. It is even harder to quantify the business impact of reducing complexity. That said, some network organizations, particularly small and mid-sized organizations, place a lot of value on reducing complexity and hence tend to favor solutions that achieve that objective.

Being *software defined* is an example of the opportunities and challenges that are associated with adopting a solution based on emerging technologies and techniques. Whether or not a solution qualifies as being software defined is an important consideration because a broad set of vendors are making huge investments relative to developing and applying software defined techniques to myriad technological domains. Typically, the greatest gains in functionality and cost effectiveness occur in areas where there is a high level of investment and so it makes sense for network organizations to look closely at solutions that are software defined. However, the initial application of software defined techniques to data center networks was far less successful than was predicted. As a result, while network organizations need to pay attention to software defined solutions they must also realize that just because a solution is software defined doesn't mean that the solution will be successful in the market.

Key Considerations

Software Defined

The first modern instance of there being a broad discussion of IT functionality being *software defined* was the discussion of Software Defined Networks (SDNs) that started in earnest about five years ago. At that time, the acronym SDN referred exclusively to data center networks.

As previously mentioned, the initial SDN architecture and related protocols have not been widely adopted by enterprise organizations. However, many of the key concepts of SDN, such as a focus on software vs. hardware, the abstraction of the logical from the physical and a focus on an end-to-end approach to management and security have become an integral part of how new classes of software defined solutions are brought to market. Those new classes include: SD-WAN, SD-Branch, Software Defined Storage, Software Defined Data Centers and a Software Defined Perimeter (SDP).

Bottom Line: Because they potentially will benefit from the massive investments being made in the enabling techniques, network organizations should examine solutions that qualify as being software defined. In many instances, a given solution contains multiple components that are each software defined; e.g., a combination of SD-WAN and SDP functionality as part of a single solution.

Location of Key Functionality

In a traditional WAN or branch office, all relevant functionality is provided onsite. That's still a viable option. However, there are several other viable options. Examples include:

- On site at a customer's remote location;
- On site at a customer's regional or central location;
- In a CSP's central office;
- In a co-location facility;
- In a public site dedicated to providing functionality such as optimization;
- In an IaaS provider's facility;
- In a SaaS provider's facility.

Bottom line: The traditional approach to hosting WAN and branch office functionality onsite still has value. However, there are numerous alternatives that enterprise organizations should consider. In many instances network organizations will find that the best solution is to locate functionality in multiple types of sites.

Application Delivery

There is no doubt that a company's WAN is critical to its business success. However, in the vast majority of instances a company's business unit managers don't appreciate the value of the WAN or any other component of IT other than the applications they use to run their business unit. As such, the value of a WAN to a company's business unit managers is primarily determined by the role that the WAN plays in application delivery.

To ensure successful application delivery, and hence enable the network organization to show value to a company's business unit managers, a company's WAN must:

- Ensure acceptable levels of application performance and availability;
- Provide monitoring and management functionality that enables the organization to perform rapid root cause analysis and remediation;
- Provide appropriate security.

Bottom Line: When evaluating alternative WAN and branch office solutions, network organizations must evaluate the solutions in large part based on the ability of those solutions to ensure successful application delivery.

Edge Computing

Over the last decade, the adoption of cloud computing has been a strong factor driving the centralization of resources into a relatively small number of public and private data centers. Recently a new form of computing has started to emerge and it is driving the decentralization of at least some resources. This new form of computing, edge computing, is intended in large part to address the challenge of massive data build-up by performing data processing at the edge of the network, near the source of the data. The goals of edge computing include both minimizing cost and latency as well as controlling network bandwidth.

There are several compelling use cases for edge computing. In one of the key use cases, network functions that an enterprise might otherwise run on site are run at an edge locations that are close to the users. This includes network functions such as WAN optimization, load balancing and security.

Another key use case is exemplified by the CORD (Central Office Re-architected as a Datacenter) initiative and the transformation taking place in Radio Access Networks. Both of these activities are intended to enable service providers to fully realize the promise of NFV. The Radio Access Networks transformation was initiated in late 2014 when ETSI announced the creation of an Industry Specification Group (ISG) for Mobile-Edge Computing. Per that announcement "Mobile-Edge Computing provides IT and cloud-computing capabilities within the Radio Access Network (RAN) in close proximity to mobile subscribers. Located at the base station or at the Radio Network Controller, it also provides access to real-time radio and network information such as subscriber location or cell load that can be exploited by applications and services to offer context-related services. For application developers and content providers, the RAN edge offers a service environment characterized by proximity, ultra-low latency, high-bandwidth, as well as real-time access to radio network information and location awareness. Mobile-Edge Computing allows content, services and applications to be accelerated, maintaining a customer's experience across different radio and network conditions."

Bottom line: As discussed in the preceding chapter of The Guide, network organizations have a strong interest in running L4 – L7 functionality in the cloud. Running this functionality at edge locations provides the same benefits as running it in the cloud. In addition, this approach eliminates some of the issues, such as latency, that are associated with the cloud.
As discussed below, distributed NFV enables organizations to implement a wide range of functionality wherever they see fit. For example, a given organization may choose to implement VNFs at the edge; in a highly centralized fashion; or in a hybrid fashion with some VNFs being deployed at the edge and others in central sites.

Complexity

There are many factors driving the increasing complexity of IT, including the rapid adoption of cloud computing, virtualization, big data, IoT, mobility and new application architectures. Adding to the complexity inherent in the adoption of new technologies is that fact that when IT organizations adopt new technologies they seldom eliminate the existing technologies, at least not in the short term. As a result, IT organizations must combat the complexity that is associated with the legacy environment, the emerging environment, and the intersection of the two environments.

Part of the reason why complexity is a key concern relative to the WAN is because a highly complex environment makes it difficult for a network organization to achieve the application delivery goals previously discussed. High levels of complexity also tend to increase cost, reduce availability, create new attack vectors and increase the time it takes to add new sites or to implement new functionality. In addition, a highly complex environment is difficult to automate.

Bottom Line: The implementation of any new solution always adds complexity, at least initially. On a going forward basis, IT organizations should only adopt solutions that once in production will reduce notably more complexity than is added during the adoption process.

Mobility

Over the last two years most of the conversation about the WAN has focused on providing connectivity to an organization's branch offices. While providing that connectivity is clearly important, there are other WAN edge points that also need effective and efficient connectivity. The various devices used by an organization's mobile workers constitute an important class of WAN edge points. The size and hence importance of the mobile work force was documented in an analyst report that stated that the global mobile workforce is set to increase from 1.32 billion in 2014, accounting for 37.4% of the global workforce, to 1.75 billion in 2020, accounting for 42.0% of the global workforce.

Bottom Line: It may well be that in the short term that the best option that a network organization has is to implement a WAN solution that just supports branch offices. However, before implementing a WAN solution with a narrow scope, network organizations should develop a WAN strategy that includes how they will effectively and efficiently support mobile workers.

IoT

As noted above, branch offices are not the only class of WAN edge point. In a large and growing number of instances, the enterprise WAN must also support the IoT. The importance of the IoT was highlighted in a report published in early 2017. According to that report, 8.4 billion connected things will be in use worldwide by the end of 2017, up 31 percent from 2016, and that there will be 20.4 billion connected things by 2020. As discussed in a recent blog, the IoT impacts every industry with business-critical use cases being developed in many verticals including retail, healthcare, agriculture and transportation.

Bottom Line: It may well be that in the short term that the best option that a network organization has is to implement a WAN solution that just supports branch offices. However, before implementing a WAN solution with a narrow scope, network organizations should develop a

WAN strategy that includes how they will effectively and efficiently support the IoT. As described below, a major component of supporting the IoT is providing effective security.

The Role of Cellular

Cellular services have long been used as a back-up to wireline WAN services. In the current environment, cellular services are increasingly being used as either the primary WAN link or are used in conjunction with a wireline service in an active-active configuration. In the latter case, traffic is typically load-balanced over the cellular and wirelines services based on policy. Some of the other key use cases for cellular services in an enterprise WAN include:

- Temporary networks
  The time that it takes to get a wireline service such as MPLS installed is typically a month or longer. In the vast majority of cases that means that wireline services are not a feasible solution for the types of temporary networks that are needed to support locations such as construction trailers or pop-up stores.

- In-vehicle networks
  While it may or may not be desirable to use an MPLS or DSL-based Internet service to provide connectivity to a fixed site such as a branch office, it isn't possible to use these services to provide connectivity to vehicles such as cars, trucks and school buses.

- Internet of Things (IoT)
  The acronym *IoT* refers to the internetworking of a wide range of physical devices, buildings and other things that are embedded with electronics and/or sensors. For example, *a thing* may be a sensor inside of a traffic light. In many such instances, cellular services are the only feasible WAN option for supporting the IoT.

Another important use case for cellular services is in tertiary markets where MPLS is either not available or is prohibitively expensive. A variation of this use case involves an organization that has a large number of sites in tertiary markets. For the sake of example, assume that an organization has a few hundred sites in tertiary markets. Even if MPLS is available and somewhat affordable, the organization would be stuck with the administrative burden of having to manage contracts with a few hundred small CSPs. An alternative solution for such an organization is to deploy a router at each site that supports multiple cellular services. Based on a number of factors, including the terms of the contracts that the organization negotiated with its cellular providers, the organization may choose to implement the cellular services in an active-active configuration or in an active-passive configuration.

Bottom line: As the use of cellular evolves from being a backup service to where it is a primary service, network organizations need to include in their analysis of WAN and branch office solutions a focus on high-performing, effective cellular services. The requisite analysis involves developing an in-depth understanding of the technologies that underlie the solutions being considered. For example, the way that most SD-WAN solutions implement packet mode steering requires the solution to assemble and disassemble each packet at both ends of the WAN. While this approach is acceptable in a wired environment, in a wireless environment the associated signaling overhead can consume an unacceptable amount of the cellular capacity.

5G

Supporting the IoT is one of the drivers of a new generation of cellular services referred to as 5G. Network organizations should not look at 5G as just being a minor step in the evolution of cellular technology. For example, one analyst report discussed their belief that 5G will be as revolutionary at electricity.

Some of the characteristics of a standards based 5G service that enable it to potentially be as revolutionary as electricity include:

- Data rates of tens of megabits per second for tens of thousands of users;
- Data rates of 100 megabits per second for metropolitan areas;
- 1 Gb per second simultaneously to many workers on the same office floor;
- Several hundreds of thousands of simultaneous connections for wireless sensors;
- Coverage improved compared to 4G;
- Signaling efficiency enhanced;
- Latency reduced significantly compared to LTE.

Over time 5G will encompass many wireless technologies, including 5G New Radio, Gigabit LTE for super-fast speeds; LTE IoT for low power, long battery life, and long-range coverage; Digital TV, C-V2X, or vehicle to anything; and ultra-low latency. 5G will build on the architecture of voice (2G); voice, video, and data (3G); and massive mobile data (4G)—and add massive bandwidth and density, as well as ultra-low latency. 5G also will integrate aspects of WiFi and long-range/low-power networks.

The initial trials and deployments of 5G services are based on a non-standard architecture that is designed to be easily upgraded to a standards-based architecture when appropriate. This is likely to occur in 2018. Recognizing the importance of 5G, at least one service provider has already announced their intention to offer nationwide 5G service.

Bottom line: Within the next two years, 5G has the potential to fundamentally change networking. Network organizations evaluating new WAN and branch office solutions need to ensure that those solutions will aggressively and effectively support 5G.

Cloud Computing

When the WAN architecture that was introduced at the turn of the century was first developed, enterprises made very little use of the Internet and so effectively and efficiently supporting Internet traffic wasn't central to that architecture. As a result, even though it both added to the cost of the WAN and it made applications run slower, the vast majority of organizations opted for backhauling Internet traffic.

A recent article in Forbes quantified how the use of cloud computing has grown over the last several years and how it is expected to grow over the next few years. According to that article, "Cloud computing spending has grown at 4.5 times the rate of IT spending since 2009 and is expected to grow at better than 6 times the rate of IT spending from 2015 through 2020." The article added that "Worldwide spending on public cloud computing will increase from $67B in 2015 to $162B in 2020 attaining a 19% CAGR."

Bottom Line: Given the size and growth of cloud computing and the resultant size and growth of Internet traffic, backhauling Internet traffic is no longer acceptable from either a financial or an application performance perspective. This has given rise for the need to deploy Direct Internet Access (DIA) at the branch, which fundamentally alters the prevailing security paradigm. This is one of the several factors driving the need to implement NFV somewhere at the edge of the WAN.

Security

Large scale security breaches have become common place. One measure of the impact of security breaches comes from an IBM report which stated that by 2019 cybercrime will become a 2.1 trillion-dollar problem. Another measure is that because of the impact that a cyberattack can have on a company's profitability, brand and stock price, in many instances cyber security is both a CEO and a board level issue.

Many of the newer WAN solutions support DIA from branch offices. This approach provides a lot of value but it also creates a new attack surface. Branch offices, however, are not the only WAN end point that presents a security risk. A recent article stated that "29 percent of organizations have already experienced either a data loss or breach as a direct result of mobile working." The article went on to say that "As many as 44 percent expect that mobile workers will expose their organization to the risk of a data breach." The title of another recent article highlights the fact that the adoption of the IoT comes with significant security challenges. The title of that article is *Five nightmarish attacks that show the risks of IoT security.* One of the attacks that the article discussed was the Mirai botnet, which was used to flood DNS provider Dyn with a DDoS attack. The Mirai botnet took down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites.

Bottom line: Since branch offices are not the only class of WAN edge points, network organizations also need to ensure that their WAN architecture provides effective security to all the relevant WAN edge points, including mobile workers and the IoT.

Software Defined Perimeter

The legacy security model of the WinTel era is based on the concept of a well-defined perimeter. The security tools of this era, including VPNs and firewalls, are labor-intensive to implement and manage and in addition, these tools don't leverage user context to make access decisions.

In addition to the limitations of the security tools of the WinTel era, driven in part by the adoption of the IoT, the concept of a well-defined perimeter no longer makes sense. These factors lead to the development of a Software Defined Perimeter (SDP) which is a contemporary security framework that is designed to provide on-demand, dynamically provisioned network segmentation. The SDP framework dynamically creates one-to-one network connections between the user and the resources that they access. The framework also ensures that all the endpoints attempting to access a given infrastructure are authenticated and authorized prior to being able to access any resources on the network. According to the Software Defined Perimeter working group, the SDP security model has been shown to stop all forms of network attacks including DDoS, Man-in-the-Middle, Server Query (OWASP10) as well as Advanced Persistent Threat (APT).

Bottom Line: The legacy security model of the WinTel era is rapidly becoming obsolete. As part of their adoption of new solutions to connect WAN edge points, IT organizations need to fundamentally rethink their approach to security in part to ensure that it is not based on obsolete concepts such as the existence of a well-defined perimeter. For most IT organizations this will involve adopting at least some of the key concepts of an SDP.

WAN Optimization

One of the promises of an SD-WAN is that it enables network organizations to add large volumes of relatively inexpensive Internet bandwidth. Because adding bandwidth often either eliminates or significantly reduces application performance problems, it's possible to conclude that implementing an SD-WAN negates the need for WAN optimization functionality.

There are, however, multiple use cases in which WAN optimization adds value. One of those use cases is disaster recovery (DR). DR requires large files be transmitted between a primary and a secondary data center that are usually far apart. Due to the well documented impact of the TCP window size on WAN throughput, the DR application may not be able to fully utilize the WAN bandwidth and hence may not be able to transmit all the data needed to support the company's DR plan.

While traditional WAN optimization solutions were focused on the connections between a company's branch offices and their internal data centers, increasingly WAN optimization functionality is being focused on the connections between a company's branch offices and myriad cloud providers. If a branch office is connected to an IaaS provider's facility, it is possible to have a WAN optimization functionality on both ends of the connection. Another option is that many service providers offer private cloud connect services that securely connect their managed VPN customers to some of the IaaS and SaaS providers using the service provider's MPLS infrastructure. This direct connect approach provides improved performance and security, but adopting this approach means that network organizations will not experience the cost savings that comes with substituting Internet connectivity for MPLS connectivity.

Bottom line: There is no doubt that in many instances adding WAN bandwidth eliminates application performance problems. However, there is also no doubt that in many other instances just adding bandwidth doesn't eliminate application performance problems and that WAN optimization functionality of some type is required.

Network Functions Virtualization (NFV)

While the European Telecommunications Standards Institute (ETSI) champions the interest that CSPs have with NFV, the Open Networking User Group (ONUG) has emerged to champion the corresponding interest that enterprises have. In a white paper entitled *Open Networking Challenges and Opportunities*, ONUG discussed the cost and complexity of managing a large number of Layer 4 - 7 network appliances from different vendors with different management tools. The appliances they mentioned included WAN optimization controllers and a variety of security appliances. When initially conceptualized, NFV was a centralized architecture. However, in order to support the large and growing range of WAN edge points, NFV has evolved to be a highly distributed architecture.

Bottom Line: The transition that the IT industry is undergoing is a lot broader than just improving the functionality found in the WAN or in the branch office. At its core, the transition is about

focusing broadly on supporting a wide and enlarging set of people, places and things. Distributed NFV is a key enabler of this transition.

As previously discussed, as part of the ongoing industry transition, there now is a large set of locations where functionality can be housed. Determining where functionality should be housed requires careful analysis. For example, just because functionality such as a next generation firewall can be virtualized doesn't mean that it makes sense financially or operationally to put a virtualized next generation firewall in every WAN endpoint.

*CPE

A major part of the transition that is happening in the IT industry is the movement away from solutions in which each service is comprised of hardware and software that is both tightly integrated and proprietary. The goal of this transition is to move to a more modular architecture in which a general hardware and software platform can support a wide range of services. The two primary forms of CPE which have evolved to enable this transition are uCPE and vCPE.

uCPE
Universal Consumer Premise Equipment (uCPE) is a term coined by AT&T. It denotes CPE that is not reliant on a centralized cloud for additional network functions and orchestration, but is entirely self-contained. Due to being self-contained, the hardware employed for uCPE needs to be more powerful than does the hardware used for Cloud vCPE solutions.

vCPE
This is what is most commonly thought of as being a software-defined CPE. In this type of CPE, the network functions that are provided are entirely supported by commodity hardware and virtualized network functions instead of by proprietary ASIC's. The phrase *Cloud vCPE* refers to a subset of vCPEs that include remote carrier-grade management, deployment and orchestration functionality.

Bottom line: Solutions based on either uCPE or vCPE can provide value in large part because they host multiple network functions. However, one of the limitations of branch office solutions that are based on either uCPE or vCPE is that it can be very challenging for these solutions to provide sufficient WiFi support or to tightly integrate with branch office functionality such as Ethernet switching with PoE.

WAN Management

An analyst report described the challenging state of WAN management. According to that report, only 13% of network organizations have all the functionality that they need to troubleshoot problems related to network and/or application performance degradation. In addition, 20% of network organizations reported that the troubleshooting functionality that they have is barely adequate. Unfortunately, in part because it introduces new functionality such as dynamic path selection, the adoption of an SD-WAN is likely to make WAN management even more demanding. Other factors that are further complicating the challenge of WAN management include the rapidly growing use both of DIA and cellular services as well as the exploding adoption of mobility and the IoT.

Bottom Line: As companies continually increase their reliance on the WAN to support virtually all of their business processes, the inability of the network organization to effectively

troubleshoot the WAN will increasingly have a negative impact on those business processes. A critical challenge facing network organizations is that due to the fundamental shifts in the industry, WAN management is becoming increasingly difficult. The deployment of new WAN solutions is an opportunity for network organizations to improve their ability to troubleshoot the WAN and hence improve their ability to support the company's critical business processes. As a result, network organizations need to make effective management a central component of the analysis they do of new WAN solutions.

Machine Learning

Machine Learning is a subset of Artificial intelligence (AI) that focuses on the practice of using algorithms to parse data, learn from it, and then make either a determination or prediction about something. In contrast to a static algorithm such as Dijkstra's, a critical aspect of machine learning is that the machine is *trained* using large amounts of data and algorithms that give the machine the ability to continually learn how to perform a given task.

Machine learning has the potential to enable a huge step forward in terms of automation. One use case for machine learning is the automated detection and analysis of anomalous behavior. Potentially in the not very distant future, well-trained, machine learning based systems will be able to identify security risks and intrusions and will also be able to troubleshoot performance problems before they impact users. Another key use case that could possibly be mainstream relatively soon focuses on the path selection functionality contained in SD-WAN solutions. One example is that a properly trained SD-WAN solution may soon be able to anticipate congestion on a given WAN link and automatically divert traffic to an alternative link.

Bottom line: Machine learning has the potential to fundamentally impact how IT functionality is operated and managed. As such, as they work with vendors to explore new WAN and branch office solutions, network organizations should spend time to understand the vendors' strategies relative to machine learning. However, network organizations also need to balance the enthusiasm that the industry currently has for machine learning with the realization that while AI has been around for decades, achieving the promised benefits of AI has proven to be extremely difficult.

Ongoing Role of MPLS

In many instances when a network organization implements an SD-WAN solution it makes the assumption that it needs to include in its implementation predictable transport services such as MPLS to carry latency-sensitive traffic. Part of the reason for that approach is because the Internet is usually regarded as being too unpredictable to deliver enterprise-grade, latency-sensitive applications on a predictable basis particularly between Internet regions. Network organizations that adopt that approach will not realize all the savings that they could if they were more aggressive at eliminating their use of expensive WAN services such as MPLS, potentially through the use of NaaS-based solutions as described below.

Bottom line: While they are exploring alternative solutions, network organizations should make sure that they analyze solutions that enable them to aggressively reduce WAN transport costs.

Alternatives to a DIY Solution

As customers adopt SD-WAN and SD-Branch, one of the deployment choices they face is whether or not to implement an SD-WAN or SD-Branch on a Do-it-Yourself (DIY) basis. Using WAN as an example, in a DIY solution the customer is responsible for the entire lifecycle of their WAN. This means that the customer is responsible for the planning, designing, implementing and managing of all components of the WAN.

As discussed in the preceding chapter of The Guide, most network organizations prefer a WAN solution other than a DIY based solution. One alternative to a DIY solution is a managed service provided by a variety of types of Managed Service Providers (MSPs), including CSPs and Systems Integrators (SIs). MSPs typically acquire and implement the same SD-WAN functionality as an enterprise network organization would and MSPs leverage that functionality to provide their customers with a turnkey solution that includes active management. In the vast majority of cases, however, the MSP also provides a portal that enables the customer to at least monitor their network and, in many cases, to make changes.

Another alternative to a DIY solution is a Network-as-a-Service (NaaS) based solution. A NaaS based solution replaces the network itself by connecting business entities such as HQ facilities, branch offices, mobile workers, and cloud facilities to a cloud-based network. When compared to a DIY based solution, a NaaS based solution results in fewer entities for a network organization to own, deploy, upgrade and troubleshoot.

Bottom Line: When evaluating SD-WAN and SD-Branch solutions, network organizations need to ask themselves if they have the expertise to implement these solutions on a DIY basis and if they do, if that is the best use of their highly skilled resources. If that is not the case, then the organizations should evaluate NaaS and managed service offerings.

The SD-WAN and the SD-Branch Office Ecosystem

This chapter of The Guide identifies the primary sub-segments of the three major components of the SD-WAN and/or the SD-Branch ecosystem. Those three components are:

- Do-It-Yourself (DIY) solutions;
- 3rd party solutions;
- The enabling hardware.

The first two components of the ecosystem that are listed above focus on the differing organizational ways that the SD-WAN and/or the SD-Branch solutions are implemented and managed. In the first case, DIY, the network organization that consumes the solution is also the organization that is responsible for the lifecycle management of the solution. In the second case, 3rd party solutions, an organization other than the network organization that consumes the solution is responsible for the lifecycle management of the solution. The third component of the ecosystem that is listed above, the enabling hardware, focuses on the varying ways that hardware, both commercial off-the-shelf and proprietary, is utilized in both DIY and 3rd party solutions.

Throughout this chapter phrases such as *branch office functionality* refer strictly to functionality that is provided to users who reside in a branch office. The use of such phrases does not necessarily mean that the functionality itself resides in the branch office.

Due to the complexity and volatile nature of the marketplace, the ecosystem described in this section is imperfect. As a result, some of the sponsors don't fit neatly into any of the sub-segments of the ecosystem. It is also important to realize that in some instances the sub-segments are overlapping; that a given SD-WAN or SD-Branch office solution may fit into multiple sub-segments; and that a given vendor may offer multiple solutions.

DIY Solutions

Traditional Routers

In addition to supporting routing, routers typically support functionality such as stateful firewalls, QoS, protocol and application optimization, encryption, content filtering and split tunnels. Some router vendors have added SD-WAN functionality to their routers to create an SD-WAN solution.

Special Purpose Appliances

Many organizations implement best of breed, single function devices in their branch offices. These single function devices include firewalls, WAN Optimization Controllers (WOCs) and WAN Path Controllers (WPCs). Some providers of this class of appliance have added SD-WAN functionality to their products to create an SD-WAN solution.

Pure Play SD-WAN Software Routers

This class of solution is a designed-from-the-ground-up to be a SD-WAN software-based router that can be deployed either on a dedicated appliance or on a vCPE, a uCPE or on ODM hardware.

Converged SD-WAN Appliances
This class of solution integrates LAN/WAN functions into a single hardware platform. In addition to being an SD-WAN software-based router, these solutions provide functionality such as wired and LTE WANs, Ethernet switching, WiFi, PoE and various security services.

Cloud-Deployable Solutions
These WAN and branch office solutions are designed-from-the-ground-up to be deployed, at least in part, in the cloud. That does not mean, however, that they necessarily must be deployed in the cloud.

3Rd Party Solutions

Network-as-a-Service (NaaS)
A NaaS offering is typically built using a core network that interconnects a distributed set of Points of Presence (POPs). In addition to basic transport, a NaaS offering typically provides functionality such as security and optimization. In virtually all instances, the provider of the NaaS offering facilitates the acquisition and management of the appropriate first and last mile services. In some instances, the functionality provided by the NaaS offering is complimented by functionality provided by a device which is located on the customer's premise. The NaaS provider may offer additional services such as consulting.

Managed Solutions
Managed Service Providers (MSPs), such as CSPs and Systems Integrators (SIs), typically acquire and implement the same functionality that an enterprise network organization would in order for the MPSs to offer a managed SD-WAN or a managed SD-Branch Office. In a managed solution, the MSP is responsible for the entire lifecycle of the solution. The MSP may offer additional services such as consulting.

Enabling Hardware

Black Boxes
A black box is a piece of purpose-built, proprietary hardware in which all the functionality provided by the CPE is implemented in physical hardware. As a result of how it is designed, the functions provided by a black box are often referred to as being PNFs (physical network functions).

White Boxes
The phrase *White-box* refers to situations in which the network and/or branch office functions are fully virtualized in software that is hosted on common off-the-shelf hardware, usually an X-86 appliance. In contrast to both black and gray boxes, a white box does not make use of proprietary ASICs.

Gray Boxes
A Gray Box is a middle ground between a black box and a white box. A gray box uses ASICs to cost-effectively accelerate the performance of certain compute-intensive functions.

DELL EMC

Where do you fit in the SD-WAN and/or the SD-WAN Branch Office ecosystem of vendors?

Dell EMC provides turn-key hardware and software solutions designed to simplify and accelerate production-ready SD-WAN deployments and services with a choice of SD-WAN software from Versa Networks, Silver Peak, and VeloCloud.

What is your value add?

Dell EMC provides a family of Ready Node offerings, designed for Service Providers and Enterprises alike that are intended to simplify and accelerate SD-WAN adoption. At the heart of the Ready Nodes are validated, pre-tested solutions comprised of Dell EMC compute platforms and industry leading SD-WAN software offerings from Silver Peak, Versa Networks, and VeloCloud.

What are the proof points?

Included in the Ready Node offerings are reference architectures, design guides, Bill of Materials (BOM), partner software SKUs for the appropriate use-cases, pre-installed drivers and firmware settings.

SD-WAN Solutions

We're Ready When You Are

Dell EMC is ready to provide turn-key hardware and software solutions designed to simplify and accelerate production-ready SD-WAN deployments and services, with a choice of SD-WAN software from Versa Networks, Silver Peak, or VeloCloud.

Introducing Dell EMC SD-WAN Ready Nodes

At Dell EMC, we view SD-WAN as a critical and necessary component for Digital Transformation. For Service Providers, SD-WAN represents an opportunity for creating new services, accelerating time-to-revenue and increasing service agility. For enterprises large and small, SD-WAN represents an opportunity to lower cloud connectivity costs, while also optimizing WAN traffic patterns and usage. Dell EMC has double down on strategy of open and verified solution choices, to build SD-WAN for production, by offering validated product options for SD-WAN services, that is built upon the industry's foremost virtualization infrastructure, and hardware platforms.

We're meeting this need with a family of Ready Node offerings, designed for Service Providers and Enterprises alike intended to simplify and accelerate SD-WAN adoption. At the heart of our Ready Nodes are validated, pre-tested solutions comprising of Dell EMC compute platforms and industry leading SD-WAN software offerings from Silver Peak, Versa Networks, and VeloCloud. Included in the Ready Node offerings are Bill of Materials (BOM), partner software SKUs for the appropriate use-cases, pre-installed drivers and firmware settings.

The choice of multiple ready node hardware platforms provides maximum deployment flexibility for large, medium or small environments. Moreover, multiple SD-WAN partners furthers that flexibility by supporting many use cases.

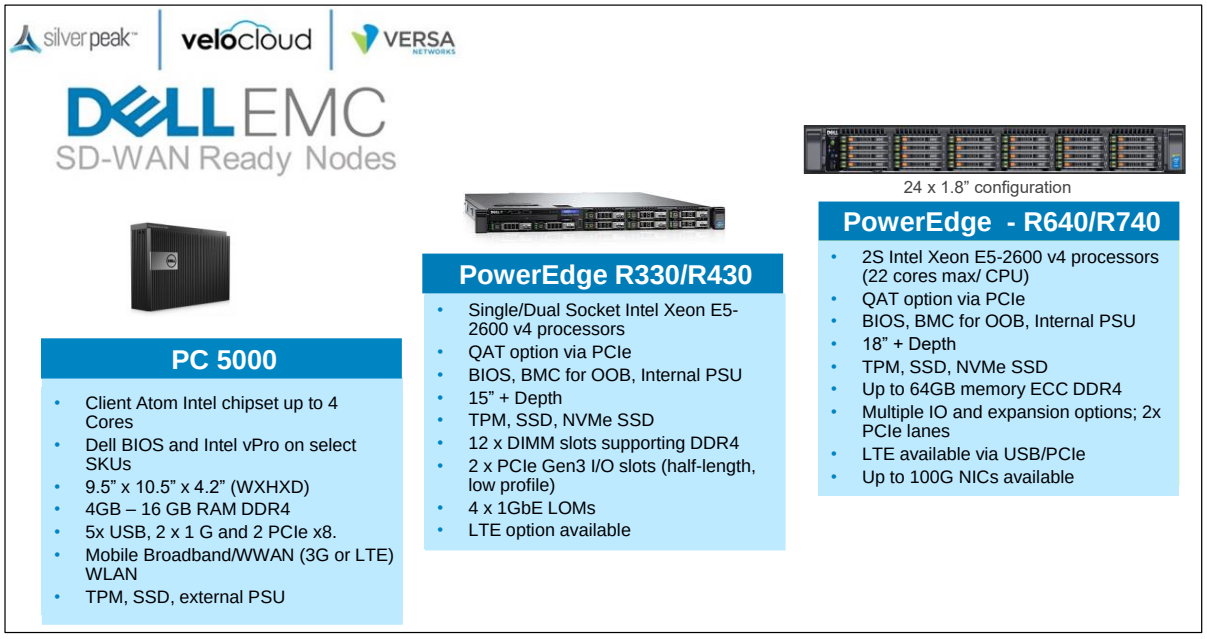


Figure 1. Dell EMC SD-WAN Ready Nodes

SD-WAN Ready Node use-cases

Service Providers can add new profitable managed services (e.g., cloud-managed SD-WAN or SD-Security service), and reduce their time-to-revenue for these new services. Communications Service Providers, for example, can improve their competitive advantage by offering a hybrid WAN allowing current customers to add managed internet bandwidth to their branches, particularly for less critical traffic flows. Managed Service Providers can generate new revenue streams by adding Managed SD-WAN services; and can further benefit in productivity improvements with features such as zero touch provisioning.

Enterprises can choose to deploy a do-it-youself on-premise SD-WAN, using the Dell EMC SD-WAN Ready Nodes. Enterprises can benefit with lower capital and operating costs, by leveraging lower-cost broadband connections and improving application performance, through intelligent route selection.

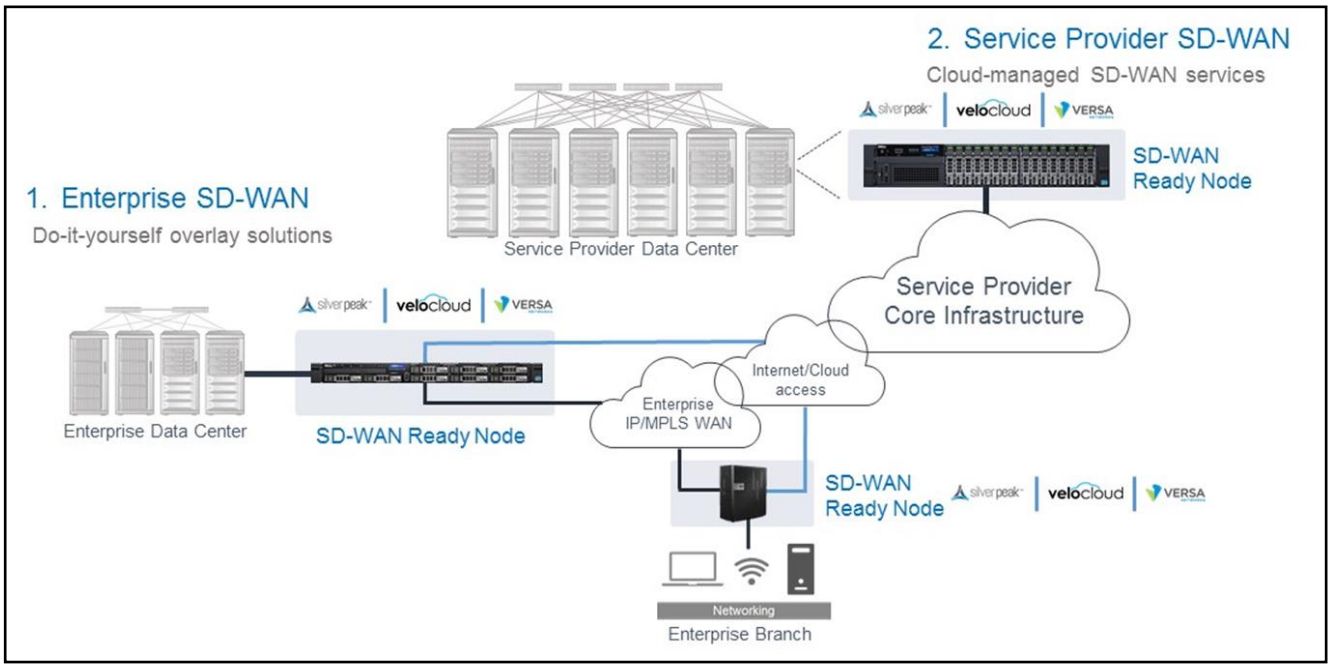


Figure 2. Dell EMC SD-WAN Ready Node use-cases

Take the next step

Contact your Dell EMC, Silver Peak, VeloCloud or Versa Networks representative to learn more about SD-WAN Read Nodes from Dell EMC.

Learn more about Dell EMC SD-WAN Solutions

Contact a Dell EMC Expert

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.