

WHITE PAPER

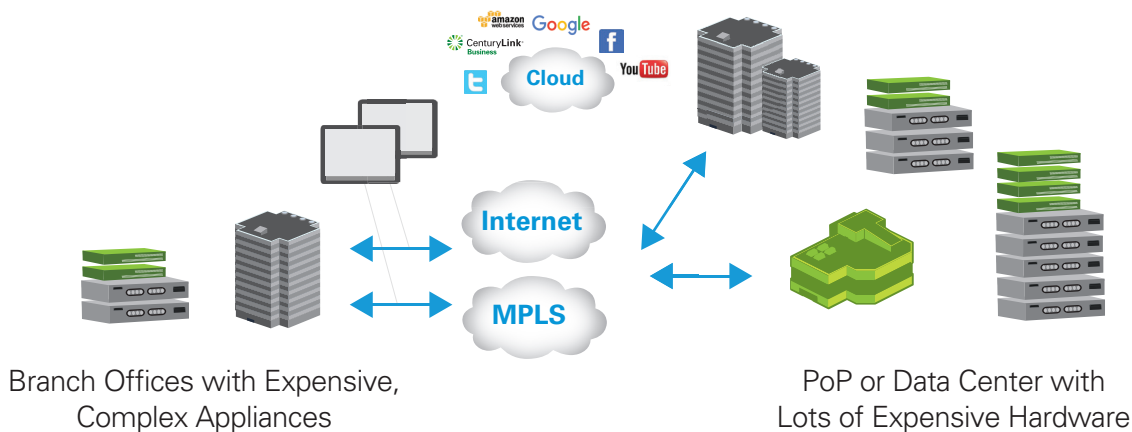
# Benefits of SD-WAN to the Distributed Enterprise



# Branch Networking Today – More Bandwidth, More Complexity

Branch or remote office network architectures, including wide-area networks (WANs), have barely changed since the 1990s. The requirements for branch connectivity have changed significantly in this time, however. The most common approach for nodes on a WAN have been to connect through a combination of MPLS circuits or broadband / IPSec. While not perfect, this has worked for businesses for many years. Today, the demands on wide area network bandwidth are seeing drastic increases as network traffic volumes are pushed by a variety of workloads including mobile, video, cloud storage/ collaboration and other high bandwidth applications. Options for dealing with this problem include adding more capacity to the existing WAN circuit or introducing an Internet connection to the branch WAN architecture.

The Internet connection approach can help mitigate the overall congestion of the WAN, but it increases the complexity, security requirements and cost of designing and managing the branch network. Internet connections require additional infrastructure, policies and management/oversight. From a bandwidth management and allocation basis, traffic engineering to ensure available bandwidth for given applications requires time consuming manual mapping of specific traffic to specific circuits. From a security perspective, adding Internet connectivity requires additional security infrastructure, policy creation and management. Finally, when Internet connectivity is added, the ability to effectively monitor and obtain an overall view of the branch WAN becomes increasingly complex, and ongoing issues are often difficult to mitigate.



## Branch Network/WAN: Enterprise Challenges

Businesses with multiple branches today either manage their networking in-house or work with a managed service provider. Either way, there are multiple (and growing) challenges that network teams must address:

### Applications Deployed Everywhere

Today, applications not only run in corporate data centers, but also exist at cloud application providers (SaaS) or are deployed in cloud infrastructure providers (IaaS). If all traffic to/from the cloud must be routed through the corporate data center for security functions, end user experience and response times will be negatively impacted. At the same time, additional security functions (e.g., firewall, access control and filtering, anti-virus/malware, DNS, etc.) are required if cloud resources are accessed directly from the branch office.

### Bandwidth Growth and Application Performance

Cloud- and SaaS-based applications, unified communication and collaboration tools continue to consume a growing amount of branch office network bandwidth. Adding direct Internet connections and broadband circuits provides needed bandwidth. At the same time, it increases operational complexity and security requirements. Additional challenges come with monitoring and troubleshooting network health across multiple circuits, communication service providers and an array of network and application performance tools.



### Complexity and Cost of Ownership

Adding bandwidth and Internet connections requires purchasing, deploying and managing point devices for different circuits and network functions (e.g., routing, WAN optimization, firewalls, etc.) at locations where there is generally little if any IT or security expertise locally. The result is a significant capital expense (CapEx) investment and increases in ongoing operating expense (OpEx). Networking and security infrastructure is expensive and labor intensive to manage. Multi-site organizations need to maintain WAN services in a cost-effective way. They want low equipment costs and operational expenses. Network and security functions are increasingly specialized as well. Whether technical support is in-house or outsourced, it can be hard finding the right people to do the work.

### Slow Response to Changing Business Needs

Responsiveness is the essence of agility. When facing unexpected events or new line-of-business requirements at the branch level, an agile company can react quickly and gain competitive advantage. Unfortunately, the process of deploying new or upgraded branch network services typically leads to long deployment times due to provisioning of new hardware devices. It also takes time to schedule consultants or integrators to install, configure, integrate and test equipment. This occurs both at initial deployments, and also when capacity upgrades are required (e.g., if a new or larger WAN circuit is provisioned, then a higher capacity router and/or firewall is required). Making a change to the branch WAN can take weeks and even months.

## Leveraging Software-Defined WAN (SD-WAN) and Network Virtualization

Recent technology advances can offset many of these challenges. Notably, a software-defined approach to networking can significantly improve the deployment and operation of managed network services. This growing trend virtualizes the network, using software to abstract the underlying hardware in the delivery of network services. The traditionally hardware-centric network and security technologies thus evolve into software-based solutions running on commodity off-the-shelf (COTS) hardware and white-box appliances.

A core element of the software-defined network is the virtualized network function (VNF), a virtualized version of a specific function like routing, CGNAT or next-generation firewall. Much more than just converting from point hardware or appliances to virtualized software instances, VNFs are centrally managed and policy orchestrated. They are “zero-touch” provisioned and service-chained to address many of the operational challenges noted earlier.

In essence, applying VNFs to enterprise WANs and managed WAN services results in the ability to “software-define” the WAN, not just in form-factor, but also in deployment and provisioning, initial configuration, ongoing management and operations. SD-WAN decouples functions from proprietary hardware, enabling the use of network and security functions in software running on commodity x86 servers and white box appliances. It also de-couples the underlying WAN transport, enabling the use of any WAN circuit type including MPLS, leased line, broadband Internet and wireless 4G and LTE connections.

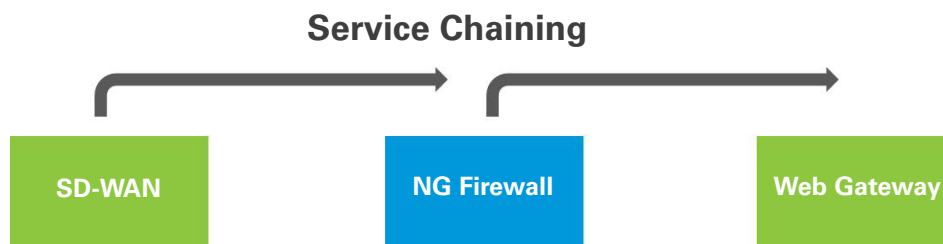
### Applying SD-WAN to Branch Offices

To understand the comparative efficiency of SD-WAN, imagine an enterprise with 400 branch offices that wants to utilize inexpensive, high-throughput broadband connections as an element of its overall WAN architecture. Instead of purchasing legacy routers and firewall appliances and shipping them to branch sites, the enterprise or service provider can ship commodity white box appliances and zero-touch provision the equipment and underlying services at the branch.

If the enterprise used the legacy appliance-based approach, they might have been able to deploy them at the rate of about 20 per month. This is an aggressive schedule, at one installation per business day. At this pace, it would take over 1.6 years to complete the project. In contrast, leveraging CenturyLink SD-WAN, an enterprise can ship commodity white box appliances to 100 branches per month, and simultaneously activate and test

25 devices per week remotely. The whole project would take four months, a time reduction of nearly 80%, coupled with a significantly lower cost of deployment (as no on-site specialists are required).

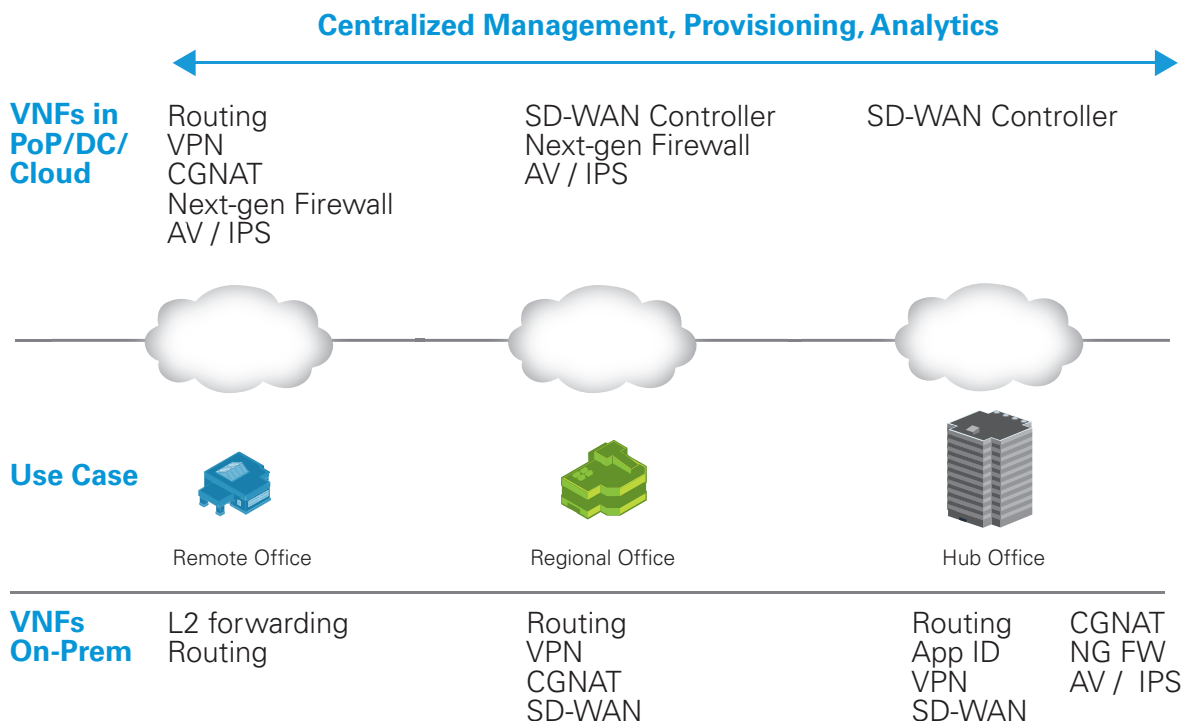
Additionally, SD-WAN enables enterprises to service chain security functions to achieve on-premises security that meets compliance and data protection requirements. CenturyLink is able to manage the service chaining process if the client desires. For example, specialized security functions like a secure web gateway can be service-chained to the SD-WAN to enable secure direct Internet access from the branch. Service creation, service definition and service-chain rules utilize templates and provide programmable, API-driven delivery of the service via centralized orchestration and management tools. This automated approach enables each branch office SD-WAN to be deployed in hours, instead of days or months.





### Using an SD-WAN managed service enables:

- **Application Intelligence** – CenturyLink SD-WAN has the ability to identify over 2,800 specific applications and use that knowledge to apply a range of network and security policies to the traffic carrying them. This includes mapping applications to particular WAN connections (e.g., core business applications to MPLS and consumer web traffic to broadband), application prioritization, per application security policy and enforcement (e.g., blocking certain types of web content) and so forth.
- **Multiple Deployment Options** – CenturyLink SD-WAN is a software-based solution with a broad set of deployment options. It can be deployed directly on bare metal x86 servers, white-box appliances, virtual machines (VMware ESXi, KVM) and containers. It works across a variety of access methods such as broadband, wireless or even MPLS. It is agnostic of network provider, which significantly improves how efficiently the network is administered. Virtual Network Functions allow users to select features to complement SD-WAN environments without being constrained by vendor proprietary hardware options, resulting in significantly lower CapEx and design flexibility.
- **Flexible and Distributed Service Architecture** – With the advent of SD-WAN, enterprises have the capability (and flexibility) to decide where to deploy and run each layer of network or security function — either on-premises in the branch office or centrally in the data center, or possibly at a provider's point-of-presence (PoP). For example, compute-intensive services such as anti-virus and IPS can run centrally, while services that are key in the branch, like application identification, SD-WAN, routing and firewall can be run locally. In addition, CenturyLink SD-WAN can integrate critical network services using service chain definitions that include both local and remote functions, depending on the business need.
- **Centralized, Automated Operations** – A software-defined approach to the WAN also provides a way to provision SD-WAN equipment and deliver network and security services from a single point of control, avoiding the need for skilled personnel available on-site to deploy and configure the solution. Instead, SD-WAN services can be deployed, bandwidth and service capacity increased or enhanced with additional functions automatically, all without requiring any on-site IT presence, hardware refreshes or manual interaction. Also, if a particular branch site(s) requires a unique set of network or security functions, the branch can be serviced individually and automatically from a single management portal, including role-based administration for flexible configuration and ongoing policy management.



Enterprises looking to deploy a successful SD-WAN require a new approach to service delivery based on software-defined and virtualized network principles. These include next-generation network and security functions that make the WAN not only network-aware, but application-aware. These new SD-WAN capabilities must seamlessly integrate into a customer's routed network, and also have the ability to utilize any underlying WAN transport including MPLS, broadband and wireless connections. Internet security and control from the branch is a must-have to support the expanded use of Internet connectivity (e.g., direct Internet access) for business needs and ensuring a positive end-user experience.

Adopting the network virtualization approach to SD-WAN gives enterprises the added flexibility to easily integrate and scale the right security functions alongside advanced networking capabilities, maximizing the benefits provided by SD-WAN – agility, reduced TCO, better service levels and cloud application performance. Additionally, SD-WAN greatly improves the operational efficiency and profitability of provider-delivered managed services through the use of multi-tenant software running on commodity hardware.

## About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit [www.centurylink.com/enterprise](http://www.centurylink.com/enterprise).

## About Versa Networks

Versa Networks was founded by network industry veterans Kumar and Apurva Mehta, who built the multi-billion dollar MX Series routers at Juniper Networks. Versa is an early innovator in the rapidly growing network function virtualization (NFV) market, which is forecast to grow to \$11.6B in 2019 (Infonetics/IHS). The company has more than 35 patents in process around its unique system-level approach for creating virtualized network functions (VNF), a core NFV building block. Versa solutions enable service providers and large enterprises to transform the WAN and branch networks to achieve unprecedented business advantages. Versa's VNF software provides unmatched agility, cost savings and flexibility vs. traditional network hardware.

**Global Headquarters**  
Monroe, LA  
(800) 784-2105

**EMEA Headquarters**  
United Kingdom  
+44 (0)118 322 6000

**Asia Pacific Headquarters**  
Singapore  
+65 6768 8098

**Canada Headquarters**  
Toronto, ON  
1-877-387-3764