IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Dell Technologies

In a world increasingly defined by cloud and software, a flexible platform can provide compelling benefits through support for SD-WAN, virtual network functions, and edge security.

Choosing the Right Platform for SD-WAN, Virtual Network Functions, and Edge Security

November 2021

Written by: Brad Casemore, Research Vice President, Datacenter and Multicloud Networks

Introduction: The Distributed IT Landscape and Its Challenges

As organizations increasingly embrace their digital objectives, they must deal with a more distributed IT landscape. Applications are more diverse and distributed than ever before — residing in on-premises datacenters, colocation facilities, and public clouds and as SaaS applications — presenting an array of new connectivity and security challenges. The combination of hybrid IT and multicloud workload distribution and a hybrid workforce has profound implications for network architectures, infrastructure, and operations, which are all compelled to be more agile, flexible, and secure.

On the networking front, software-defined WAN (SD-WAN), virtualized network functions, and SASE have emerged to address the connectivity and security needs that have arisen as a result of hybrid IT and multicloud.

AT A GLANCE

WHAT'S IMPORTANT

Hybrid IT and multicloud have driven a need for branch platforms capable of adaptable and scalable support for SD-WAN, virtual network functions, and comprehensive security.

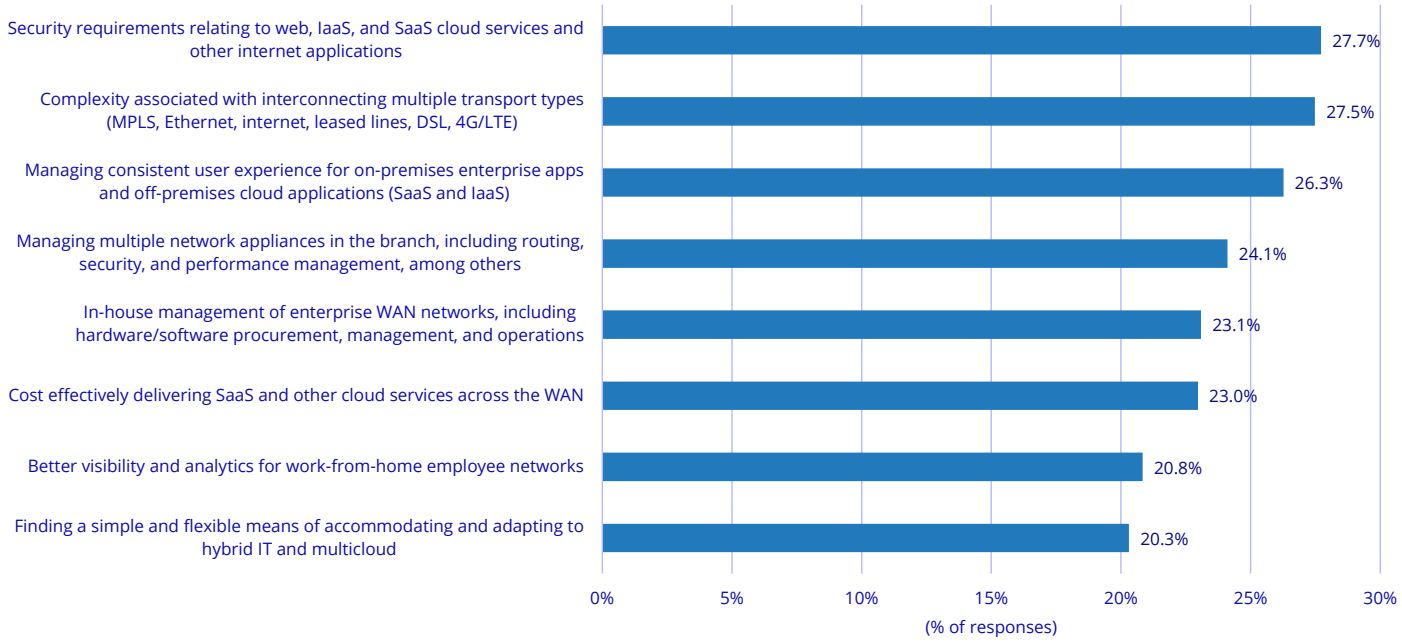
KEY TAKEAWAYS

In pursuing network modernization, organizations should ensure that the platform they deploy can reliably meet their current needs and seamlessly scale to accommodate future network and security requirements.

IDC's *SD-WAN Special Report*, based on IDC's *Software-Defined WAN (SD-WAN) Survey*, explored the degree to which enterprises worldwide are modernizing their WANs in response to the cloud era's distribution of both workloads and the workforce. As environments expand and become increasingly complex, challenges abound. Respondents to IDC's *SD-WAN Survey* indicated that their top WAN challenges are meeting the security requirements of cloud applications (SaaS and IaaS as well as other web services), dealing with the complexity associated with different underlying network transports, managing consistent user experience for cloud and on-premises applications, and managing multiple network appliances in the branch (see Figure 1).

FIGURE 1: ***Challenges of WAN***

Q *Please select the three most significant WAN challenges (from the following) that best relate to your company.*



n = 1,229

Multiple responses were allowed.

Source: IDC's Software-Defined WAN (SD-WAN) Survey, June 2021

The proliferation of cloud applications is a major factor behind these challenges, and the data from IDC's *SD-WAN Survey* explains why. When asked to describe their application distribution, about 44% of enterprise respondents said they are using SaaS, while about one-third have IaaS applications. Similarly, respondents indicated that SaaS, IaaS, and hybrid/multicloud are becoming more important to WAN technology choices.

Across this landscape of increasingly distributed applications and users, security is a paramount concern. That fact has been reflected in IDC's *SD-WAN Survey* and *Enterprise Networking: Emergence of the New Normal Survey*. In the latter survey, which was conducted in December 2020, respondents were asked to identify enhanced tools that would help them support remote workers. The top priority, cited by more than 35% of respondents, was tooling that would extend consistent application and security policies to remote workers. In a similar vein, when asked to name the most important changes to their network operations in response to COVID that will become permanent fixtures in their organizations, almost one-third identified "more integrated network and security management."

The convergence of networking and security at the branch in the enterprise edge is more important than ever, with support for SD-WAN often combined with firewalling and zone-based firewalling, as well as with other network and security functions and services in many scenarios.

Beyond SD-WAN and comprehensive security, many organizations are considering additional virtualization of network functions at the branch, mitigating the complexity and cost associated with procurement and discrete management of various fixed-function network appliances. Respondents to IDC's *SD-WAN Survey* indicated that 40% of their branch networking functions would be virtualized or hosted within the next two years.

These requirements drive a need for a flexible platform, capable of accommodating SD-WAN, virtualized network functions, and security options across a wide range of customer preferences and use cases, both today and well into the future. Ideally, a branch platform should deliver the following capabilities:

- Flexible support for key virtualized network and security functions, such as SD-WAN, firewall, and WAN optimization from a variety of third-party vendors of virtualized network and security functions, including popular options for SD-WAN and firewall
- Standardized technology that can scale to support new virtualized functions without requiring hardware upgrades
- A wide range of hardware options, from compact systems to datacenter-scale models, capable of accommodating the increased security requirements and greater bandwidth associated with broadband internet breakout at the branch
- Comprehensive platform support and services extending throughout the ownership life cycle
- Supply chain integrity and reliability
- Support for on-premises applications as well as SaaS applications and IaaS workloads

Benefits

During the past few years, SD-WAN infrastructure has been critical to the realization of enterprise digital transformation strategies worldwide. As a result, the market for SD-WAN infrastructure continues to grow robustly, with IDC estimating that it will expand at a compound annual growth rate (CAGR) of 18% to reach nearly $7.1 billion in 2025.

Adoption of SD-WAN is driven by the technology's capacity to deliver compelling benefits, such as faster (automated) provisioning and turnup of branch and remote sites; cost-effective and optimized delivery of traditional and cloud applications (IaaS and SaaS) over broadband internet, without performance or security compromises; increased operational efficiency through network automation; simplified WAN operations and management; and improved application experience for users. Consequently, the network and its operators go from being a cost center to becoming an integral enabler of digital business outcomes and digital resilience.

In conjunction with investments in SD-WAN, enterprises often bolster security at the branch. These organizations want the reduced costs and application performance benefits of SD-WAN's direct internet access (DIA) at the branch, but they want to ensure that security remains robust. Secure connectivity to cloud applications at the branch offers a viable approach, with strong protection combined with better application experience and lower latency as well as the significant cost savings that accrue from reduced dependence on expensive private WAN transports such as MPLS. With a platform capable of running a full security stack, including firewalling and IPS, enterprises can effectively integrate security and networking functionality to ensure and protect the integrity of the applications on which digital business increasingly depends.

A branch platform's flexibility gives enterprises and service providers the assurance that the platform will be able to accommodate a variety of solutions and use cases, today and in the future, as requirements evolve.

For many organizations, SD-WAN remains a critical requirement at the branch.

In addition, a standardized, scalable platform provides investment protection through its ability to scale seamlessly in lockstep with traffic volumes and evolving network or security requirements, irrespective of whether the platform includes SD-WAN, virtualized network functions, or security, or all of those capabilities in what IDC calls a software-defined branch (SD-Branch). Similarly, an edge platform's capacity to cost effectively accommodate a wide range of network and security functions gives the platform the flexibility to meet an extensive array of use cases as well as the adaptability to satisfy changing requirements as business-critical applications evolve and proliferate across a hybrid landscape. The ability to support a wide range of network and security functions means that almost any edge use case can be addressed.

An edge platform's capacity to cost effectively accommodate a wide range of network and security functions gives the platform the flexibility to meet an extensive array of use cases.

The breadth and depth of models in a platform portfolio, spanning a spectrum of performance requirements, provides for nearly all use case scenarios, both today and in the future. An organization could start with SD-WAN yet have the assurance that the platform would be able to accommodate security functions as well as any virtualized network functions that might also be required. As a result, the platform delivers a high degree of adaptability through the ability to support virtualized network functions as network requirements are redefined by future cloud applications.

Ultimately, the most salient business benefit comes in the form of cost and time savings, resulting from the platform's ability to support intelligently automated network and security functions at the edge. Such savings accrue to WAN capex, with enterprises and service providers able to consolidate functionality where desired while facilitating operational savings from the efficiency of having a single, reliable platform that is easier to provision, monitor, and manage.

Vendor Profile: How Dell EMC Addresses the Need for Platform Flexibility

The Dell EMC Virtual Edge Platform (VEP) is designed to address the need for agility, flexibility, scalability, and security at the enterprise edge. It allows organizations to replace fixed-function routers, which can carry higher costs and greater operational complexity, with a flexible platform capable of supporting SD-WAN routing, firewalling, and other network and security functions at the enterprise edge.

Based on industry standards, the platform has been tested and prevalidated to run VMware ESXi and ADVA network virtualization hypervisors and SD-WAN solutions from VMware (VeloCloud) and Versa Networks. In addition, the platform also supports a broader ecosystem of virtual network functions, including SD-WAN offerings from Aruba (Silver Peak), Cisco (Viptela), Palo Alto Networks (CloudGenix), and Nuage Networks as well as firewalls from Palo Alto Networks, Check Point, Fortinet, Juniper Networks, and Trend Micro. Support for other third-party WAN acceleration, SaaS acceleration, and service assurance offerings — for enterprises and managed service providers — is also available, as is support for a wide array of tooling and cloud applications.

Incorporating an x86 architecture and Intel processors aligned to meet the needs of virtual networking workloads, VEP models arrive at customer sites preloaded with a network virtualization hypervisor or with Versa networks, helping accelerate deployments and time to value while reducing cost and risk. Models range from the compact Intel Atom–based VEP1405 series to the datacenter-scale Xeon-D class 4600 model.

Predicated on Dell's Open Networking principles, the VEP is designed and purpose built to deliver flexibility and choice for organizations seeking to modernize their WAN and branch architectures with full-featured network and security services. The VEP platform enables organizations to deliver reliable and secure access to the growing number of SaaS, IaaS, and other cloud applications that are increasingly critical to the success of digital business. At the same time, the platform also supports the legacy applications that many organizations continue to depend on to run their businesses.

The platform's inherent multivendor support for SD-WAN and other network and security solutions provides customers with choice and readily available access to dozens of third-party network and functions extending across a range of well-understood technologies and use cases. As such, customers benefit from flexibility, retain options, and avoid vendor lock-in.

In addition, Dell EMC provides its widely recognized service and support, and customers benefit from Dell's global supply chain.

Challenges

Organizations evaluating and adopting SD-WAN, network and security virtualization, and SASE offerings tend to focus — understandably — on the software functionality first and only later concern themselves with the underlying platform or delivery vehicle. Vendors of SD-WAN overlays and virtualized functions, including security capabilities, sometimes specify a preferred hardware platform or other means of delivery, and customers can be inclined to accept vendor recommendations.

Conclusion

Although many organizations pursuing modernization of branch network and security place an understandable emphasis on the automation and programmability conferred by software, they should give careful consideration to the underlying platform that will support SD-WAN, network virtualization, and edge security. The Dell EMC Virtual Edge Platform offers the adaptability, flexibility, and openness to provide performance, reliability, and scalability for SD-WAN, network virtualization, and security functions now and in the future.

About the Analyst

Brad Casemore, *Research Vice President, Datacenter and Multicloud Networks*

Brad Casemore is Research Vice President of Datacenter and Multicloud Networks at IDC. He covers datacenter network hardware, software, IaaS cloud-delivered network services, and related technologies, including hybrid and multicloud networking software, services, and transit networks. Mr. Casemore also works closely with IDC's Enterprise Networking, Server, Storage, Cloud, and Security research analysts to assess the impact of emerging IT and converged and hyperconverged infrastructure.

MESSAGE FROM THE SPONSOR

Dell Technologies Believes the Future of IT Will Be More Open, Agile and Cloud-based

Dell Technologies has one of the broadest open networking portfolios in the industry – spanning both hardware and software. Dell's unique approach involves combining its own developed technologies with those from a broad ecosystem of technology partners, including VMware. The industry has recognized us for leadership in opening up the network through disaggregation of networking hardware and software, providing customers choice based on their unique needs.

We believe that our Open Networking approach and solutions stimulate rapid innovation by helping customers achieve unprecedented levels of flexibility and efficiency. These solutions help minimize the time and effort required to design, provision and manage networks; enable IT managers to leverage open-source tools; and provide expertise to help reduce costly overhead at the edge, in the core and into the cloud.

https://www.delltechnologies.com/VEP

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com