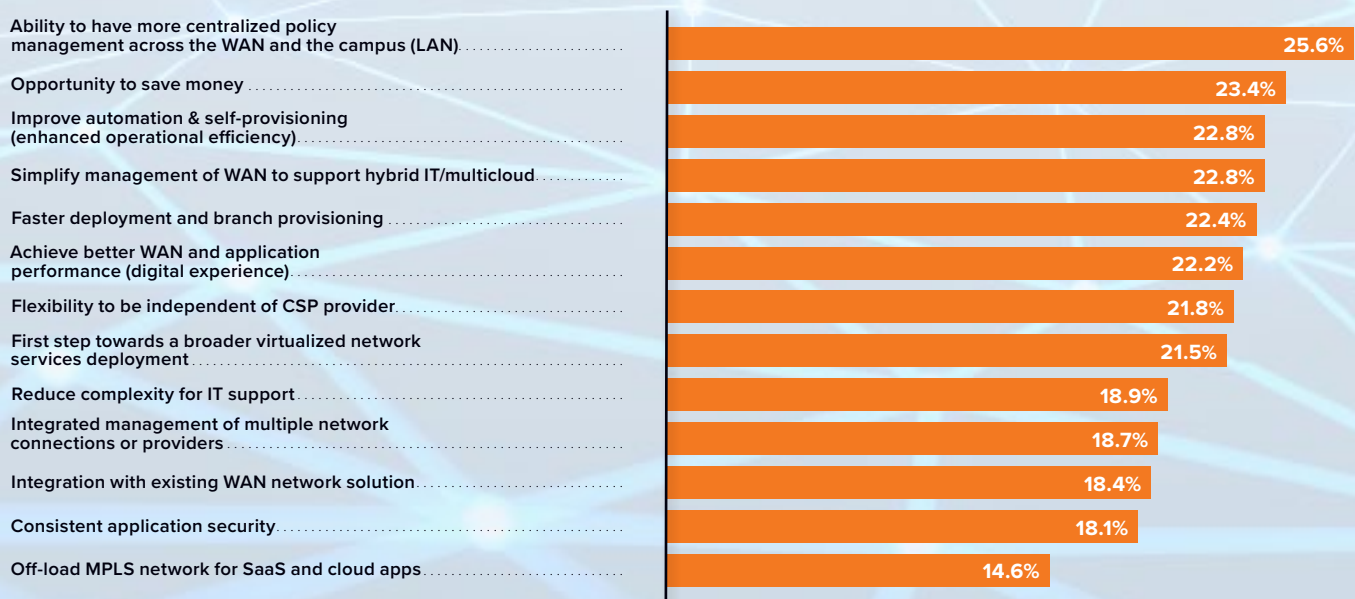




Key Considerations in SD-WAN Adoption

Top SD-WAN Motivations: Centralized WAN & LAN management; operational efficiencies; simplified WAN for multicloud

Q: Which of the following are the top 3 motivations for considering an SD-WAN deployment? (select up to three responses)



n=375. Base=Respondents currently using SD-WAN, Source: IDC's *Software-Defined WAN(SD-WAN) Survey*, 2021

When selecting an SD-WAN platform, enterprises should ensure that the platform can support application requirements today and into the foreseeable future. Indeed, respondents to IDC's most recent *SD-WAN Survey* indicated that their applications were more distributed than ever, with 44% provided as SaaS, about 33% in IaaS clouds, about 14% in an on-premises private cloud, and 9% in a hosted, managed private cloud. As result of this distribution, respondents to the survey said that SaaS, IaaS, and hybrid/multicloud were becoming increasingly important factors in their WAN technology choices.

Accordingly, organizations should ask the following questions: Where are applications today? What do applications need from the WAN to optimize connectivity and security to enable engaging digital experiences for users, including employees and customers? How will the application landscape change, and what are the WAN implications?

Respondents to IDC's *SD-WAN Survey* indicated that their most significant WAN challenges involve security requirements, mitigating network complexity, and ensuring consistent user experiences for on-premises applications and SaaS and IaaS apps. When asked to cite the most important aspects they consider when purchasing WAN infrastructure or services, a third of survey respondents said integrated security was critical, placing that consideration above all others.

Similarly, when respondents were asked to cite the most important components in an SD-WAN solution, the top selection, at more than 31%, was application and network security, just ahead of direct connections to IaaS or SaaS clouds.

In relation to security, organizations should ask: To what degree will SD-WAN investment mitigate security threats? For many organizations, mitigation will require a comprehensive approach. The SD-WAN should scale to address edge-security requirements such as zone-based firewall and secure web gateway (SWG), as well as other security functions, including SASE-related requirements such as zero trust network access (ZTNA), cloud access security broker (CASB), next-generation firewall as a service (NGFWaaS), artificial intelligence for IT operations (AIOps), data loss prevention (DLP), remote browser isolation (RBI), and user and identity behavior analytics (UEBA).

Integrated and comprehensive security is a primary consideration but having a flexible for technological innovation is also important, as is achieving greater operational efficiency. Investments in an SD-WAN platform should deliver the flexibility needed as an organization adapts to the evolving requirements of digital transformation. Simplified operations deliver cost savings and enable agility to keep pace with the speed of digital business. Platform openness provides both the flexibility to address shifts in strategy and the capacity to assimilate technology assets derived from M&As.

The network has become the digital nervous system on which modern applications, data, users, and businesses depend. SD-WAN connecting sites and users to distributed cloud applications, is an integral part of the network, providing the necessary network modernization for the WAN to serve as truly digital infrastructure. As organizations assess their SD-WAN requirements, they should do the following:

- ▶ Ensure that you understand how your organization's application roadmap will evolve. The WAN's primary aim is to facilitate and support delivery of applications to sites and users, so it's essential to know where your applications will reside and what the network will need to provide to support them. How many will be on-premises, how many on an IaaS cloud or clouds, and how many will be SaaS? If possible, understand how the picture will evolve in the next few years.
- ▶ Consider your SD-WAN and SASE security requirements. What security functions do you need today and how will security requirements evolve?
- ▶ Make sure your SD-WAN investment supports the agility, flexibility, elastic scalability, and operational efficiencies that are imperatives of digital transformation and digital infrastructure. The modern WAN must provide security and control, but not at the expense of slowing down or impeding the success of digital business.



Simplified operations deliver cost savings and enable agility to keep pace with the speed of digital business.

Message from the Sponsor

Dell Virtual Edge Platform (VEP)

VEP, powered by Intel processors, is a virtual network infrastructure solution designed to address the need for agility, flexibility, scalability, and security at the enterprise edge. Running SD-WAN solutions, it offers fast, secure, cloud-friendly connectivity across branch offices with a distributed workforce, providing operational efficiencies, cost savings, and Dell's global supply chain advantage.

[Learn more](#)

© 2022 IDC Research, Inc.

IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

[Privacy Policy](#) | [CCPA](#)