GETTING STARTED

The Road to Modern SD-WAN Management

Historically in charge of IT delivery, today's CIOs now play a more strategic role, guiding the C-suite on the business implications of digital transformation and how it can help deliver innovation, speed response times, and improve experience. Instead of acquiring and configuring new technologies, organizations now "consume" IT, using new models powered by cloud computing and the Internet.

Changes brought about by digital transformation are also pressuring traditional wide area networks (WANs) because of expanded public-cloud workloads, mobile connectivity, and the security ramifications of network traffic shifting from secure corporate data centers to branch offices.

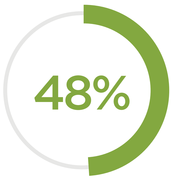
Not only do remote users require significantly more bandwidth to drive high-definition video, guest Wi-Fi, connected devices, cloud and mobile apps, and digital displays and kiosks, but they also need direct access to enterprise cloud-based applications and storage.

Altered network flows from this increased cloud traffic are forcing IT leaders to rethink their WAN strategies. Here are five questions IT leaders rethinking their WAN strategy should ask themselves:

1. Are bandwidth limitations affecting my remote users?
2. Will our organization deploy more cloud-based applications and services in the future?
3. Will the number of our branch offices and remote users continue to increase or possibly decrease?
4. IT able to provide secure direct Internet access?
5. How can IT support business initiatives such as digital transformation/ customer experience or Internet of Things (IoT)?

Technical Challenges to WAN Success

There is no question that cloud traffic and digital complexity is on the rise.



of all traffic at branch offices and remote sites can be traced to cloud applications.[1]

of enterprises will grow their overall WAN bandwidth over the next two years, mainly due to cloud adoption.[2]

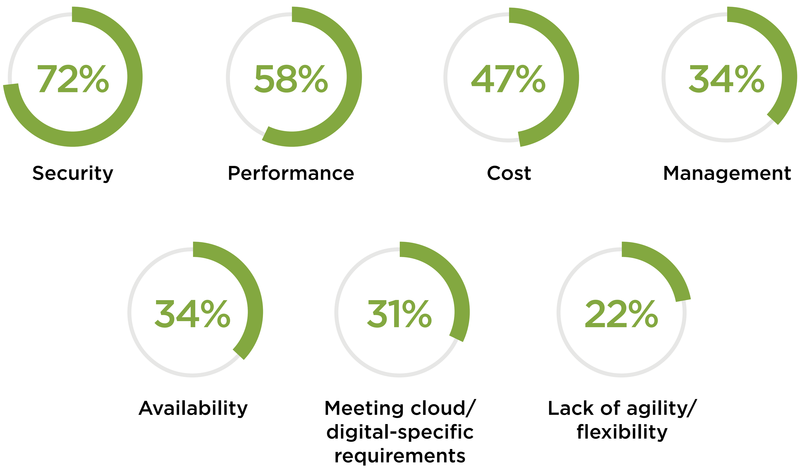
The average enterprise has 1,935 cloud applications in use.[3]

While just about everything in IT has changed significantly over the last couple of decades, enterprise WANs have stayed relatively static. They remain biased towards branch networking and wired connectivity — typically IP

virtual networks (VPNs) like Multiprotocol Label Switching (MPLS) — using hub and spoke architecture that routes all traffic through a private data center regardless of the destination.

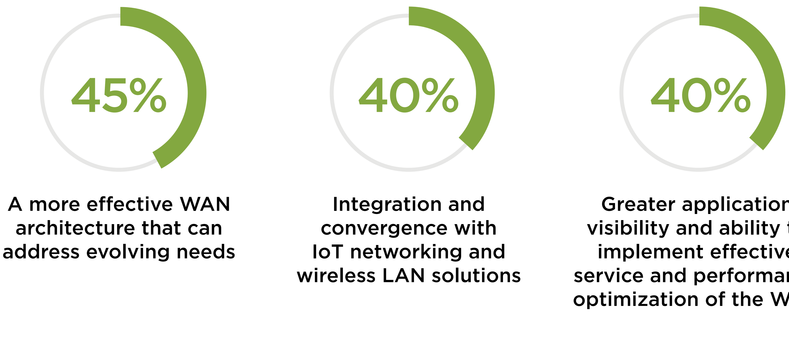
Cloud computing profoundly affects the WAN, which was designed with bandwidth that only had to accommodate loads like Internet traffic or email. This is having an increasing effect on WAN modernization efforts as IT leads other initiatives within their organizations such as hybrid cloud, connected devices or IoT.

Top concerns about current WAN:[4]



As IT leaders juggle digital innovation and WAN limitations, enterprises report struggling with network complexity associated with managing distributed infrastructures. For example, many enterprises have multiple remote sites and branch offices, each with routers, firewalls, WAN optimization controllers, local switching, Wi-Fi, and more. Network teams manage each of these elements at each site through network management software and direct command-line interface (CLI) management. This complexity is further aggravated by the fact that many remote sites lack technical onsite staff who can support tasks that require physical proximity, such as installation and certain aspects of network troubleshooting.

Top priorities for supporting cloud and digital needs:[5]



Ability to orchestrate connections and services across hybrid cloud and on-premises Further, traditional MPLS networks that transmit traffic from branch offices to a centralized data center can no longer provide low latency/high-performance access to cloud applications on their own. To achieve local area network (LAN)-like performance, organizations have typically purchased and operated private networks, such as private T1 access to an MPLS service with service-level assurances, for each different application. However, these networks are expensive and an increase in more demanding applications such as voice-over-IP (VoIP), collaboration, conferencing, and virtual desktops makes bandwidth costs prohibitive.

IT Leaders Are Migrating to SD-WAN

Today's converging business and technical challenges have spurred transformation of the modern WAN through a software-defined networking (SDN) architecture that previously was seen only in the data center.

Software-defined WAN (SD-WAN) is at the leading edge of software-based networking deployments. It uses software and cloud-based technologies to simplify delivery of WAN services to branch offices. Software-based virtualization enables advanced functionality, including the following.

Business agility

Cost effectiveness

SD-WAN leverages the Internet to provide secure, reliable high-performance connections from branch offices to the cloud. Remote users can expect to see significant improvements in their experience with cloud-based applications.

Strategic vendor support

Critical network visibility

Gartner has estimated that the average cost of network downtime is $5,600 per minute, or more than $300,000 per hour.[6]

These factors have helped elevate the WAN's status from internal "network plumbing" to a strategic delivery platform for business operations. In fact, 46% of organizations surveyed have either deployed or plan to deploy SD-WAN or hybrid SD-WAN in 2019.[7]

SD-WAN offers the flexibility to migrate to hybrid WAN without penalty as organizations can seamlessly deploy SD-WAN solutions without changing their existing MPLS networks. This enables IT managers to migrate traffic growth over time towards more effective Internet bandwidth.

More Emphasis on Security and Vendor-Provided Services

When organizations migrate to SD-WAN, users can access cloud services directly from branch offices. This affects cybersecurity as the number of ingress and egress points goes from one to potentially thousands, depending on the number of branch offices.

72%

of IT leaders report that security is one of their top concerns about their current WAN.[8]

Security can no longer be considered a post-deployment activity for SD-WAN; rather, security must be integrated into SD-WAN architectures from the beginning. Organizations that are seeking secure SD-WAN solutions should look for:

- **A transport-independent design.** Traditional WANs deliver security and performance across private links that reside on a customer's data center, tying a customer to a private circuit for security and performance. Backhauled software-as-a-service applications often experience performance degradation or choke points because of the transport-specific design of WANs.

  SD-WAN solutions overcome these issues by a transport-independent design that is both secure and reliable across a combination of private-only, hybrid, dual Internet, and Internet-only sites.

- **A secure and encrypted overlay.** SD-WAN uses standard-based encryption, such as Advanced Encryption Standard (AES), to provide secure connectivity over any type of transport to form a secure cloud network.

- **A highly available architecture enhanced by distributed cloud-hosted options.** SD-WAN solutions can offer continuous availability between remote data centers by providing predictable performance, improved reliability, automated failover, performance monitoring and management, and application visibility. Cloud-enabled SD-WAN architectures that rely on providers' private backbones are guaranteed to maintain low levels of latency, packet loss, and jitter.

- **Advanced next-generation firewall capabilities.** Distributed next-generation firewalls on a security gateway protect an organization's network servers and end-user machines by filtering traffic from both the internal network and the Internet. Distributed firewalls offer several major advantages for corporate security, such as central management, logging and access-control granularity, which make it easy to deploy a corporate security policy.

Although SD-WAN security is essential, many organizations are still unwittingly leaving their SD-WANs vulnerable to attacks due to either burdensome DIY security, misguided advice, or a lack of understanding about what security features are included in their solutions.

The Modern SD-WAN: Agile, Simple, Secure

With challenges like these—an increased need for affordable, scalable bandwidth; increased network complexity; and ineffective DIY security solutions—many leaders are seeking an SD-WAN partner with a unified SD-WAN platform with fully integrated security.

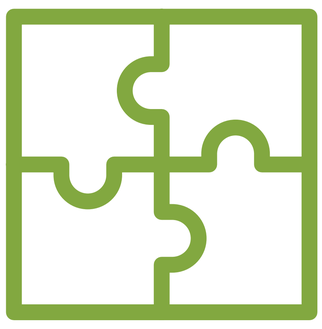
However, all SD-WAN solutions are not alike. The right SD-WAN provider can give organizations the agility to customize their platforms and maintain control. Only a truly collaborative partner can meets these standards:

A provider who partners with your team to design and operate your network, addressing your business's unique challenges and needs.

Security as a separate layer that is integrated across the unified platform.

Service-level agreements for 24/7 availability, incident resolution, and application quality.

A true single point of contact — not contractors — who responds quickly to your needs.



Best-of-breed features and technologies that simplify operations, replacing multiple third-party solutions.

A provider with a proven ability to execute and with high customer satisfaction ratings

At Open Systems, we design, build, and operate a secure, unified SD-WAN platform that provides all of the above and more to help you confidently create new growth models enabled by digital innovation. We work with your organization to create and manage the SD-WAN platform you need to simplify your operations, ensure security, and increase capabilities. With more than 6,000 deployments across 180+ countries, Open Systems has earned the trust of major enterprises worldwide.

To learn more:

Request a 30-minute assessement

Sources

[1] EMA, *Wide-Area Network Transformation: How Enterprises Succeed with Software-Defined WAN*," December 2018

[2] Ibid.

[3] McAfee, *Cloud Adoption and Risk Report*, 2019

[4] Gartner, *Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth*, November 12, 2018

[5] Ibid.

[6] Gartner, "The Cost of Downtime," July 16, 2014

[7] Gartner, *Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth*, November 12, 2018

[8] Ibid.

open systems

Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control you really want with the performance, simplicity and security you absolutely need in your network.

To learn more, visit **open-systems.com** Follow us