

SD-WAN: Providing the Network of Tomorrow for Healthcare Today



Providing healthcare today is much more than making a diagnosis or prescribing medication. The advancements in medicine, the increase in regulations to protect patients and doctors, and the digitization of the entire process require a scalable, secure, uninterrupted, and bandwidth-flexible healthcare IT network.

The burden on the network—common use cases

The networks of yesterday were not built to support the increasing demands of the modern-day healthcare organization. The following trends and evolution in care place a high burden on existing networks that must change.

Virtual desktop infrastructure

Clinicians increasingly turn to virtual desktop infrastructure (VDI) so that they can easily use technology at the point of care to access electronic medical records (EMRs). VDI supports multiple devices (smartphones and tablets) and has robust security for the Health Insurance Portability and Accountability Act (HIPAA). However, it requires high levels of bandwidth, which is often not available in most clinics or branch offices. Patient files and records have shifted to digital forms—EMRs and electronic health records (EHRs)—and organizations increasingly leverage cloud-based storage and application delivery to enable care providers with constant access.

Telehealth

Telehealth heavily utilizes video conferencing as a virtual connection point between a patient and a care provider. It also leverages cloud applications to deliver access to EMRs and the sharing of high-resolution medical images. This unified communications (UC) application requires a high level of reliable bandwidth.

Quality of service

When a patient requires over-the-phone care or physicians need to discuss patient cases for assessment and diagnosis, quality of service (QoS) is critical. Dropped calls or jitter-heavy connections are detrimental to providing high-quality care.

Remote branch offices, clinics, and pharmacies

Growth by mergers and acquisitions is a growing strategy for healthcare organizations, meaning that care often shifts to small remote or regional branch offices. Each office must adhere to the same HIPAA and care requirements as primary care offices, and a reliable and secure network connection is imperative.

BENEFITS

- Provides reliable, secure, and efficient delivery of monolithic files and information to, from, and between the cloud, data centers, and branch offices or clinics
- Ensures the ability to treat patients at all times
- Quickly turns up new sites or integrates newly acquired sites into the existing network
- Automatically complies with PCI DSS regulations at every transaction-ready location
- Simplifies deployment and eliminates human error with configurable and customizable templates and profiles
- Proactively identifies and remediates problems
- Provides continuous visibility and visualization of network performance
- Leverages low-cost and easily accessible circuits and infrastructure for remote offices
- Reduces of in-person doctor visits by residents
- Future-proofs the network for long-term projects

Pre- or post-treatment payment

Healthcare offices and clinics often require patients to render payment at the time care is provided. This requires that offices provide either a payment device or an ATM connected to the network. Not only must this highly sensitive data be segmented from regular office traffic, it must also comply with Payment Card Industry Data Security Standard (PCI DSS) regulations.

Software-defined wide area network

A software-defined wide area network (SD-WAN) enables healthcare IT to leverage existing infrastructure and any transport available to support the modern and future demands on its network. SD-WAN provides IT with the structure to deliver a seamless, simple, secure, and uninterrupted connection across the entire network, for all applications and data delivery, from the cloud to data centers to branch clinics or offices.

Application and data segmentation

Not all healthcare traffic and applications are the same and need to be treated differently. SD-WAN segments traffic from end to end to isolate various types and meet compliance requirements. With SD-WAN, IT managers have full control of traffic isolation via virtual routing and forwarding (VRF) by custom segments (voice, data, HIPAA, PCI, etc.) that can be applied by site type via established profile templates. This ensures the separation of Internet of Things (IoT) and operational technology (OT) traffic from EMR traffic, as well as corporate Internet access from guest Internet access, across all locations in the network.

Use any connection type

The VMware SD-WAN solution provides the ability to use any connection type including MPLS, LTE, WiFi and satellite, as well as broadband Internet. Any site can be quickly connected to the network and links can be added for increased bandwidth and reliability. VMware SD-WAN creates a virtual network overlay that can run over any underlying physical network with no changes required to the underlying network. The virtual overlay combines links as a logical whole and manages traffic flows over them.

Dynamic multipath optimization

Dynamic multipath optimization (DMPO) aggregates all available links, including broadband, LTE, and MPLS circuits; uses application-aware per-packet link steering and on-demand remediation; and achieves optimal performance under all conditions, including brownout or blackout scenarios. This ensures that healthcare data is accessible and transmittable at all times, including the accelerated transfer of radiological images (PACS, DICOM, etc.), and that subsecond failover maintains stable VDI sessions and real-time traffic for voice, video, and telehealth communications.

Central management and control

Cloud-delivered SD-WAN centralizes the monitoring, visibility, and cloud control to enable zero-touch branch deployment across distributed locations while delivering automatic business policy and firmware updates, configurable rules, prioritization of applications, link performance, and capacity measurements. IT personnel can manage all network traffic and applications, and remediate from a central location rather than have to roll a truck to remote sites.

Zero-touch deployment

SD-WAN edges placed in each primary and remote branch office or clinic automatically authenticate, connect, and receive configuration instructions with the centralized management portal once connected to the Internet in a zero-touch deployment. This enables healthcare organizations to quickly deploy new sites, as well as transition newly acquired locations into the overall network.

Security

A stateful and context-aware (application, user, device) integrated next-generation firewall delivers granular control of micro-applications and supports protocol-hopping applications, such as Skype and other peer-to-peer applications. The secure firewall service is user-aware and device OS-aware, with the ability to segregate voice, video, data, and compliance traffic. Additionally, SD-WAN integrates seamlessly with best-of-breed security vendors (such as Palo Alto Networks, Zscaler, Symantec, and Check Point), allowing healthcare organizations to easily implement the security profile of their choice.

A complete SD-WAN solution

VMware SD-WAN delivers a complete solution for healthcare organizations. It provides reliable, secure, and efficient connections from clinics to applications in the the cloud or in data centers, ensuring confidential access to patient information. Features like centralized management, zero touch deployment and the use of any link type means that sites can be connected quickly and devices can be easily managed. Application visibility capabilities ensure performance and ease troubleshooting for reliable operations. VMware SD-WAN enables initiatives to use digital technology and future-proofs the network.