VMware SD-WAN: The Network of Tomorrow for Healthcare Today

vmware

SD-WAN™

Benefits of VMware SD-WAN for healthcare

- Provide **reliable, secure, and efficient delivery of healthcare data** such as EHR and imaging to, from, and between the cloud, data centers, pop-up clinics, hospitals, or home offices. Deliver exceptional patient experiences through fast, stable connectivity.
- **Facilitate HIPAA compliance** with customizable settings to align with healthcare organization's outcomes and technology goals. Automatically comply with PCI-DSS regulations at every transaction-ready location.
- **Turn up new sites quickly** or integrate newly acquired sites into the existing network. Simplify deployment and greatly reduce human error with configurable and customizable templates and profiles.
- **Future-proof the network** for long-term projects. Leverage low-cost and easily accessible circuits and infrastructure for remote offices.

Over the last two years, there has been an acceleration in the use of technology to improve patient care. Patients discovered a preference for virtual care, and remote work is no longer just a trend. To meet rising patient expectations with a distributed workforce, modern-day health care organizations need a scalable, secure, uninterrupted, and bandwidth-flexible IT network infrastructure.

Common use cases that increase the network burden

Many existing networks are not built to support the increasing demands of the modern-day healthcare organization. The following trends and evolution in healthcare place a high burden on existing networks.

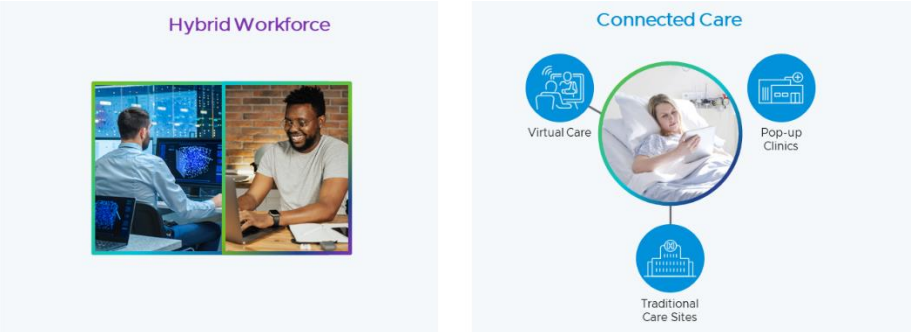

Figure 1. Digital-first healthcare is now a business imperative.

Telehealth and virtual care

Telehealth has become a must-have option to deliver care. It relies on video conferencing as a virtual connection point between a patient and a care provider. It also uses cloud applications to deliver access to electronic medical records (EMRs) and the sharing of high-resolution medical images.

Video conferencing applications require a high level of reliable bandwidth. When a patient requires virtual 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.

Distributed workforce

The healthcare workforce is becoming distributed with the rise in remote workers. Clinicians use virtual desktop infrastructure (VDI) so that they can easily use technology at the point of care to access EMRs. Organizations turn to cloud-based storage and application delivery to enable clinicians with constant access to EMRs, resulting in a need for creating and securing network connections across multi-cloud environments.

In addition, non-clinical staff working remotely use cloud-based desktops and VDI to get work done. VDI supports multiple devices, including smartphones and tablets, and has robust security to comply with regulations including the Health Insurance Portability and Accountability Act (HIPAA). However, successful VDI deployments need reliable, optimized connectivity, which is often not available in most clinics or branch offices. Remote workers using home broadband face unstable internet and VPN connections due to network issues. In addition, it can be very slow to access cloud-based applications if traffic is backhauled through a data center.

Remote branch offices and pop-up clinics

Over the last two years, many healthcare providers had to quickly set up home offices and build pop-up clinics, increasing the number of locations that rely on the network. Mergers and acquisitions are a growth strategy for healthcare organizations, meaning that care often shifts to small remote or regional branch offices. Each location must adhere to the same HIPAA and care requirements as primary care offices, and a reliable and secure network connection is imperative.

Pre- or post-treatment payment

Healthcare offices and clinics often require patients to pay at the time care is provided. This means that offices must provide either a payment device or an ATM connected to the network. This highly sensitive data must be segmented from regular office traffic and must comply with Payment Card Industry Data Security Standard (PCI DSS) regulations.

VMware SD-WAN is fundamental to digital healthcare

A software-defined wide area network (SD-WAN) enables healthcare IT to leverage existing infrastructure and any available transport to support the modern and future demands on its network. VMware 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 traditional care sites, remote offices, pop-up clinics, ambulances, or home offices.

Figure 2. VMware SASE addresses connectivity and security needs for digital-first healthcare.

VMware SD-WAN, a service of VMware SASE™, is quick and easy to set up in any location, whether it is a large care facility or pop-up site. VMware SASE is a cloud-native platform that consolidates networking and security to deliver secure, optimized, and reliable access for today's distributed model of healthcare to deliver exceptional patient experiences, anywhere.

Application and data segmentation

Not all healthcare traffic and applications are the same and need to be treated differently. VMware 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.). These 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

VMware SD-WAN provides the ability to use any connection type including 5G, MPLS, LTE, Wi-Fi, 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.

Performance and reliability

VMware SD-WAN Dynamic Multipath Optimization™ (DMPO) aggregates all available links, including broadband, cellular, and MPLS circuits; uses application-aware per-packet link steering and on-demand remediation; and achieves optimal performance, including in reduced-connectivity scenarios. This ensures that healthcare data is always accessible and transmittable, including the accelerated transfer of radiological images (PACS, DICOM, etc.). Sub-second failover can maintain stable VDI sessions and real-time traffic for voice, video, and telehealth communications.

Learn more

- VMware SASE for healthcare: *sase.vmware.com/solutions/healthcare*
- VMware SD-WAN: *sase.vmware.com/sd-wan*
- VMware SASE: *sase.vmware.com*

Cloud-ready network

VMware SASE gateways, or points of presence (PoPs) have a global footprint and serves the world's major metropolitan areas. SASE PoPs provide a quick, secure, and high-quality on-ramp to SaaS and cloud services from any location or device. This cloud-ready network eliminates data center backhaul penalties and provides an optimized direct path to public and private enterprise clouds.

Central management and control

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

Zero-touch deployment

VMware SD-WAN Edges placed in each primary and remote office or clinic—or home office—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

The VMware SD-WAN Edge provides an ICSA-compliant enterprise firewall with the ability to define security rules for incoming and outgoing data. SASE combines industry-leading SD-WAN capabilities with cloud-delivered security, including secure web gateway, zero trust network access, and firewalling for protecting sensitive healthcare data against malicious attacks. In addition, VMware SD-WAN integrates seamlessly with best-of-breed security vendors (including 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 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.